УДК 343.1
DOI https://doi.org/10.32689/2522-4603.2023.3.3

Іван СЕРВЕЦЬКИЙ
доктор юридичних наук, доцент, заступник завідувача кафедри правоохоронної на антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом,, вул. Фрометівська, 2, м. Київ, Україна, 03039, siv2055@gmail.com
ORCID: 0000-0002-5713-8911

Олег ДЕМ'ЯНЕНКО
аспірант кафедри правоохоронної та антикорупційної діяльності Навчально-наукового інституту права імені князя Володимира Великого, Міжрегіональна Академія управління персоналом, вул. Фрометівська, 2, м. Київ, Україна, 03039
ORCID: 0009-0007-8318-5854

Ivan SERVETSKYI
Doctor of Law, Associate Professor, Deputy Head of the Law Enforcement and Anti-Corruption Department of the Educational and Scientific Institute of Law named after Prince Vladimir the Great, Interregional Academy of Personnel Management, 2, Frometivska str., Kyiv, Ukraine, 03039, siv2055@gmail.com
ORCID: 0000-0002-5713-8911

Oleg DEMYANENKO
Postgraduate student of the Law Enforcement and Anti-Corruption Department of the Educational and Scientific Institute of Law named after Prince Vladimir the Great, Interregional Academy of Personnel Management, 2, Frometivska str., Kyiv, Ukraine, 03039
ORCID: 0009-0007-8318-5854

ДЕЯКІ ПРОБЛЕМИ ПРОТИДІЇ КІБЕРШПИГУНСТВУ

SOME PROBLEMS OF COUNTERING CYBER ESPIONAGE

Стаття присвячена викриттю шпигунів «кібершпигунів», державних зрадників, виявленню колаборантів, встановленню осіб, які виправдовують, заперечують або визнають правомірною збройну агресію, глорифікації її учасників та притягненню до кримінальної відповідальності.

Статистичні дані свідчать про те, що за 2023 рік зареєстровано 57.093 злочинів проти національної безпеки, серед них – 37 за шпигунство, 712 державну зраду, 2.364 – колаборацію, 1007 за виправдовування військової агресію РФ проти України. З одного боку, це свідчить про успішну діяльність правоохоронних органів та спеціальних служб України, а з іншого це свідчить про те, що існує агентурна мережа, яка сприяє шпигунській діяльності, особливо у. кіберпросторі. України.

Тому, відносно таких осіб спецслужби здійснюють контррозвідувальні та оперативно-розшукові заходи, спрямовані, в першу чергу, на боротьбу з «кібершпигунством», негласно протидіє «кіберзлочинності», попереджає «кібератаки» щодо державних електронних інформаційних ресурсів, інформаційної інфраструктури; забезпечує реагування на всі інциденти у сфері державної безпеки.

На думку Манжая О. В. «…кіберпростір – це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами».

Отже, спецслужби повинні забезпечити гласний і негласний захист громадян, здійснювати контррозвідувальні заходи у кіберпросторі застосовуючи форми і методи протидії кібершпигунству у кіберпросторі.

Саме визначення ролі та місця контррозвідувальної діяльності у кіберпросторі і є предметом нашого дослідження.

Діордіца І. В зазначає, що «…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 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».

Термін «кіберпростір» став синонімом поняття «комп'ютерна віртуальна реальність». Якщо розглядати «кіберпростір» як скорочення словосполучення «кібернетичний простір», то кіберпростір – це простір

(територія), який створений, працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки секретної інформації).

Проблемами дослідження "кібершпигунства", "кібернетична безпека", "кіберпростір", "кіберсфера", "кіберзлочинність", "кібервійна",. "кібероборона", займаються такі науковці як І.В. Арістова, І. В. Діордіца В.А., Ліпкана, О.В. Манжай, Д.С. Мінін, І.В. Сопілко, М.М. Чеховська, В.С. Цимбалюк, В.М. Шлапаченко .

Метою статті є здійснення етимологічного аналізу поняття «кібершпигунство».

На підставі цього запропоновані конкретні шляхи удосконалення протидії «кібершпигунству» з використанням сучасних форм і методів контррозвідувальної діяльності Службою безпеки України.

Ключові слова: *шпигунство, «кібершпигунство», «кібербезпека», «кіберпростір», контррозвідувальні заходи.*

The article is dedicated to exposing "cyberspies" spies, state traitors, identifying collaborators, establishing persons who justify, deny or recognize the legitimate armed aggression, glorify its participants and bring them to criminal responsibility.

Statistics show that in 2023, 57,093 crimes against national security were registered, including 37 for espionage, 712 for treason, 2,364 for collaboration, and 1,007 for justifying the military aggression of the Russian Federation against Ukraine. On the one hand, this indicates the successful activity of law enforcement agencies and special services of Ukraine, and on the other hand, it indicates that there is an agent network that facilitates espionage activities, especially in cyberspace of Ukraine.

Therefore, in relation to such persons, the special services carry out counter-intelligence and operative investigative measures aimed, first of all, at combating "cyber-espionage", covertly countering "cyber-crime", warning of "cyber-attacks" against state electronic information resources, information infrastructure; provides response to all incidents in the sphere of state security.

According to Manzhai O. V. "...cyberspace is an information environment (space) that arises (exists) with the help of technical (computer) systems during the interaction of people with each other, the interaction of technical (computer) systems and the management of these people technical (computer) systems".

Therefore, the special services must provide public and private protection of citizens, carry out counterintelligence measures in cyberspace using forms and methods of countering cyberespionage in cyberspace.

Defining the role and place of counterintelligence activities in cyberspace is the subject of our research.

Diorditsa I. V notes that "... the development and improvement of measures of criminal law protection of state secrets (secret information) involves a thorough study and improvement of the disposition of the relevant norms of the Criminal Code of Ukraine, in particular espionage, and the introduction of such a new legal category into it as " cyberespionage". At the same time, important aspects are the consideration of modern social and political changes in the legislative regulation of the circulation of secret information, the maximum specification and unification of the conceptual and categorical apparatus used in the disposition of the norm, as well as the observance of established principles of legislative technique and the use of existing foreign practice, norms and doctrines ".

The term "cyberspace" has become synonymous with the concept of "computer virtual reality." If we consider "cyberspace" as an abbreviation of the phrase "cybernetic space", then cyberspace is a space (territory) that is created and works on the basis of the principles and methods of cybernetics (the science of the general laws of receiving, storing, transmitting and processing secret information).

Research problems of "cyberespionage", "cybernetic security", "cyberspace", "cybersphere", "cybercrime", "cyberwar". "cyber defense", such scientists as I.V. Aristova, I.V. Diorditsa V.A., Lipkana, Manzhai O.V., D.S. Minin, I.V. Sopilko, M.M. Chekhovska, V.S. Tsymbalyuk, V.M. Shlapachenko.

The purpose of the article is to carry out an etymological analysis of the concept of "cyber espionage".

On the basis of this, specific ways of improving counteraction to "cyber espionage" using modern forms and methods of counterintelligence activities by the Security Service of Ukraine are proposed.

Key words: *espionage, "cyber espionage", "cyber security", "cyber space", counterintelligence measures.*

Постановка проблеми. Проведення розвідувальних операцій спецслужбами російської федерації проти України під час військових дій тісно пов'язані з використанням шпигунів та державних зрадників. За таких обставин головними завданнями правоохоронних органів та спеціальних служб є активна протидія військовій агресії російської федерації з викриття державних зрадників, шпигунів, виявлення колаборантів, встановлення осіб, які виправдовують, заперечують або визнають правомірною збройну агресію, глорифікація її учасників та притягнення до кримінальної відповідальності [1].

Станом на 1 січня 2024 року правоохоронними органами та спеціальними службами за 2023 рік зареєстровано 57.093 злочинів проти національної безпеки, серед них – 37 за шпигунство, 712 державну зраду, 2.364 – колаборацію, 1007 за виправдовування військової агресію РФ проти України [2].

Ці статистичні дані, з одного боку, свідчать про успішну діяльність правоохоронних органів та спеціальних служб України з викриття осіб, які вчиняють злочини проти основ національної безпеки, а з іншої, це свідчить про те, що серед громадян України створена агентурна мережа за допомогою якої спецслужби російської федерації намагаються підірвати основи нашої незалежності.

Для цього вони активно проводять шпигунські операції у кіберпросторі, застосовуючи при цьому новітні технології та найвищі досягнення людства у космічній галузях науки та техніки.

Тому, СБУ повинна здійснювати активні контррозвідувальні заходи із запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі [3].

Здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібершпигунством, негласно протидіє кіберзлочинності, розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформаційної інфраструктури; забезпечує реагування на всі інциденти у сфері державної безпеки [4].

Саме «кібершпигунство» передбачає використання в процесі шпигунської діяльності віртуального простору – кіберпростору.

На думку Манжай О.В. «…кіберпростір – це інформаційне середовище (простір), яке виникає (існує) за допомогою технічних (комп'ютерних) систем при взаємодії людей між собою, взаємодії технічних (комп'ютерних) систем та управлінні людьми цими технічними (комп'ютерними) системами» [5 , с. 216]. Тобто – це простір де громадяни України використовують комп'ютерні технології та для задоволення власних та державних потреб.

Відповідно спецслужби повинні забезпечити гласний і негласний захист громадян, здійснювати контррозвідувальні заходи у кіберпросторі застосовуючи форми і методи протидії кібершпигунству у кіберпросторі. Саме визначення ролі та місця контррозвідувальної діяльності у кіберпросторі і є предметом нашого дослідження.

Вперше термін «кіберпростір» було використано у вжиток письменником В. Гібсоном у 1982 р. у новелі «Спалення Хром» («Burning Chrome»). У 1984 р. це поняття було більш детально розкрито у творі «Нейромант» («Neuromancer»). На думку В. Гібсона, кіберпростір (cyberspace) – це створена галюцинація, під дією якої щодня перебувають мільярди звичайних операторів у всьому світі. Це логічне представлення відомостей, збережених у пам'яті та на магнітних носіях комп'ютерів усього людства, потоки даних у просторі розуму; скупчення та сузір'я інформації [6, с. 32].

На думку І.В. Діордіца «…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» [7].

Термін «кіберпростір» став синонімом поняття «комп'ютерна віртуальна реальність». Для того щоб з'ясувати значення слова «кіберпростір» у сучасному його контексті, необхідно дослідити його етимологію. Як бачимо, термін «кіберпростір» є сполученням двох слів – «кібер» та «простір». Слово «кібер» походить від грецького κυβερ та означає *над*. Згідно з одним із визначень великого тлумачного словника сучасної української мови [8, с. 1170] під простором розуміють вільний великий обшир; просторінь; територію.

Таким чином, якщо розглядати кіберпростір як скорочення словосполучення «кібернетичний простір», то кіберпростір – це простір (територія), який створений, працює на основі принципів, методів кібернетики (науки про загальні закони одержання, зберігання, передачі та обробки секретної інформації) [8, с. 539].

Аналіз останніх досліджень та публікацій. Проблемами дослідження «кібершпигунства», «кібернетична безпека», «кіберпростір», «кіберсфера», «кіберзлочинність», «кібервійна», «кібероборона», займаються такі науковці як І.В. Аріστова [20–21], І.В. Діордіца, В.А., Ліпкана [1–5], О. В. Манжай, Д.С. Мінін [6], І.В. Сопілко [26], М.М. Чеховська [7], В.С. Цимбалюк [22–25], В.М. Шлапаченко [8].

Мета статті (постановка завдань) – здійснити етимологічний аналіз понять «кібершпигунство». його основні складові, які становлять основу категорійного ряду дослідження, а саме: «кібернетична безпека», «кіберпростір», інформаційний, загроза, кібернетичний і безпека, яке здійснюється з використанням обходу (злому) систем комп'ютерної безпеки, із застосуванням програмного забезпечення, включно з шпигунськими програмами, а потім шляхом їх поєднання визначити його небезпеку під час воєнних дій.

Основні завдання дослідження направлені на з'ясування науково-теоретичних проблем, а саме:

1) дослідити поняття «кібершпигунства», а також точки зору вчених щодо його суспільної небезпеки в сучасних умовах військової агресії проти України.

2) визначити кіберпростір, в якому здійснюються шпигунська діяльність та проаналізувати юрисдикційну складову «кібершпигунства» та підставі кримінальної юрисдикції.

3) надати авторські пропозиції у підвищенні ефективної діяльності СБУ у здійсненні контрозвідувальних заходів з протидії «кібершпигунству».

Виклад основного матеріалу дослідження. Сьогодні в Україні особливої гостроти набуває проблема протидія «кібершпигунству» як необхідної складової забезпечення національної безпеки, територіальної цілісності та існування незалежності держави.

За останні десятиліття інформаційні технології міцно увійшли у повсякденне життя кожної людини. При цьому слід зазначити, що активний розвиток інформаційних технологій пов'язаний не з розробкою новітніх технологій, зі створенням найбільш удосконаленого, універсального програмного забезпечення. Ці технології успішно використовують шпигуни у своїй протиправній шпигунській діяльності [9].

Досліджуючи поняття та зміст кібершпигунства, перш за все зазначу, що до цієї категорії входять два окремі поняття: шпіон «шпигун», шпіонаж, шпіонство, шпіонити; – р. болг. шпибн, бр. шпіен, п. (рідк.) szpion, ч. (розм.) spion, слц. spion, вл. spion, м. иіпион, схв. шпщун, слн. spijon; – запозичення з німецької мови; н. Spion п «шпіон, шпигун за посередництвом французької «і та іспанської (фр. espion. icп. spionе «тс.») запозичене з італійської; іт. spionе «шпигун» утворене від spїaге «шпіонити, вистежу вати, підстерігати», джерелом якого є германські мови (пор. пгер. speph-де «уважно, гостро дивитися» і генетично, пов'язані з ним двн. spehoп, spiohопте.«стежити, вистежувати [10, с. 404] та терміни – «кібер» («кібернетичне») [11, с. 168], утворюючи сучасне слово «кібершпигунство»

Отже, для здійснення ґрунтовного дослідження вищезазначеної категорії, проаналізуємо окремо. В словнику української мови *«шпигунство»* – це злочинна діяльність, яка полягає в таємному збиранні відомостей або викраданні матеріалів, вистежування, розшук матеріалів, що становлять державну таємницю з метою передачі їх іншій державі [8, с. 1404]. Відповідно «кібернетичний» стосується кібернетики; який створено, працює на основі принципів, методів кібернетики [11, с. 168].

«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.

Отже, під кібершпигунством Діордіца І.В. слід розуміти злочинну діяльність, яка здійснюється шляхом таємного вистежування, розшуку, збирання, викрадання та передачі інформації, що становить державну таємницю, інформації, якщо ці дії вчинені іноземцем або особою без громадянства із використанням кібернетичного простору [13].

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) [1]. *Безпосереднім об'єктом шпигунства* (кібершпигунства – *Д. І.*) є к*ібернетична загроза* зовнішній безпеці України, її суверенітет, територіальна цілісність і недоторканність, обороноздатність, державна, економічна чи інформаційна безпека.

Кібернетична загроза (кіберзагроза) – наявні й потенційно можливі явища та чинники, що створюють небезпеку інтересам людини, суспільства й держави через порушення доступності, повноти, цілісності, достовірності, автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури [4].

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, та які визнані в порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [13].

Ці відомості мають гриф секретності і входять до компетенції у сфері забезпечення охорони державної таємниці є Служба безпеки України [3].

Для того, щоб з'ясувати питання компетенції в кіберпросторі, перш за все, необхідно визначити зміст поняття «юрисдикція». Юрисдикція (лат. jurisdictio – судочинство, від jus (juris) – право і dicere – говорити, проголошувати) – це повноваження давати правову оцінку фактам, розв'язувати правові питання [14, с. 1644]. У юридичній енциклопедії

зазначено, що юрисдикція (в тому значенні, що нас цікавить) поділяється на *юрисдикцію держави* та *юридикцію міжнародну*.

Юрисдикція держави поділяється на *територіальну* та *особисту* (національну). Юрисдикція територіальна зумовлюється суверенністю влади держави в межах її території, де вона має абсолютну юрисдикцію, за винятком випадків, коли відповідними міжнародними угодами не передбачається інше. Особиста (національна) юрисдикція держави поширюється на своїх громадян, які перебува- ють за межами її території (наприклад, у відкритому морі, океані, в космічному просторі). В окремих випадках, передбачених національним законодавством, юрисдикція держави поширюється на громадян цієї держави, які перебувають на території іншої держави, однак здійснюватися така юрисдикція може лише на території своєї держави, якщо інше не передбачено міжнародними угодами. Юрисдикція міжнародна – це підсудність певної категорії справ міжнародним органам. Даний вид юрисдикції, на відміну від юрисдикції держави, є певним обмеженням державного суверенітету. Цей фактор зумовлює те, що для визнання юрисдикції будь-якого міжнародного органу необхідна явно виражена згода відповідної держави [14, с. 490]. Одним з основних завдань для визначення юрисдикції у сфері кіберпростору є встановлення факту поширення внутрішньодержавних правових норм на відносини в цьому середовищі.

У ст. 2 Конституції України [15] вказується, що суверенітет України поширюється на всю її територію. Згідно зі ст. 8 Конституції України вона має найвищу юридичну силу. Таким чином, законодавчо стверджується влада України над своєю територією.

На цей момент під територією держави розуміють не лише певну ділянку землі область (сухопутна територія), але й води (внутрішні та територіальні води), повітряний простір, розташований над сушею і водами (тропосфера, стратосфера, іоносфера, а також значна частина простору). Надра, що знаходяться під сухопутною і водною територією, є приналежністю даної держави до технічно доступної глибини [16, с. 509]. Свого часу Г. Кельзен указував на те, що територія – не річ, зокрема, не земля або її частина. Це образний вираз, що позначає певне якісне право, територіальну сферу, національного юридичного порядку [17, с. 226]. Виходячи з наведених тверджень та самого визначення терміна «кіберпростір», його можна умовно розглядати як специфічний вид території, що не має геологічної основи, з усіма відповідними правовими наслідками.

Отже, на думку Монжая О.В. кіберпростір у широкому сенсі можна співвіднести з поняттям «територія», тож необхідно з'ясувати її вид: міжнародна, державна або зі змішаним статусом. Крім того необхідно проаналізувати правові концепції, що можуть застосовуватися до кіберпростору. Слід зазначити, що досить часто кіберпростір асоціюють зі поняттям «Інтернет». Однак це велике узагальнення, яке не враховує окремі випадки [5, с. 226].

Так, Манжая О.В. кіберпростір характеризує за трьома основними ознаками

– це інформаційний простір;

– комунікативним середовищем;

– він утворюється за допомогою технічних систем [5, с. 216].

У першому та другому випадках на кіберпростір безумовно має поширюватися відповідна територіальна юрисдикція. Щодо третього випадку, то багато юристів схиляється до думки про необхідність оголошення кіберпростору, який має транскордонні масштаби (Інтернет), міжнародною територією на кшталт Антарктиди або космічного простору.

Найбільш обґрунтовану позицію щодо цього питання було викладено в роботі Д. Менте «Юрисдикція в кіберпросторі: теорія міжнародних просторів» [18] у якій він зазначає, що суттєвий поштовх у розвитку інформаційних технологій дала популяризація та активне використання у різних процесах глобальної інформаційно-телекомунікаційної мережі Інтернет. У ній Д. Менте пропонує вважати Інтернет територією, на яку не поширюється суверенітет окремої держави. Як аналогію автор наводить відносини в Антарктиді, космосі та нейтральних водах. У той же час у деяких державах спостерігалися спроби встановити власну компетенцію над частиною Інтернету або поширити особисту юрисдикцію на окремі сфери діяльності в цьому середовищі**.**

Отже Манжай В.О. пропонує три шляхи вирішення питання щодо правового режиму Інтернету і відповідно визначення компетенції держави в цій сфері:

1) Інтернет є міжнародним простором, і його правовий режим має визначатися нормами міжнародного права;

2) Інтернет є територією зі змішаним правовим режимом на кшталт континентального шельфу прибережних держав;

3) в окремих випадках інтернет можна віднести до державної території [5].

Становлення інформаційних технологій в Україні та удосконалення комп'ютерної техніки, використання телекомунікаційних мереж майже в усіх сферах життєдіяльності людини полегшило можливість передання інформації

в системі Інтернет створили низку проблем. У період глобалізації швидкий розвиток інформаційних технологій та комп'ютерних систем супроводжується зловживаннями цими технологіями, що призводить до вчинення злочинів з використанням комп'ютерної техніки створюючи при цьому сприятливі умови для реалізації нових схем і методів злочинної діяльності. Рівень можливостей, які отримують зловмисники, тенденція до збільшення кількості вчинення злочинів у сфері комп'ютерних інформаційних технологій, становлять загрозу не лише демократичним перетворенням і розвитку інформаційного суспільства в Україні, а й безпосередньо національній безпеці.

На думку Н.А. Чеснокова «… Інтернет охоплює всі країни світу, оскільки із застосуванням нових технологій (використання мобільних супутникових пристроїв зв'язку) можливе підключення до мережі Інтернет із будь-якої точки земної кулі. Якщо вести розмову про розгорнуту інфраструктуру, то в такому контексті Інтернет охоплює сьогодні понад 150 країн світу» [19]. пов'язаних зі створенням безпечних умов використання віртуального простору. Так, відповідно до офіційної статистики Офісу Генерального прокурора України за 2023 рік, проти «кіберзлочинів» зареєстровано – 3415, а саме: «несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», ст. 361 КК України – 1 403, «створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут», ст. 361-1 КК України – 280, «несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації», ст. 361-2 КК України – 60, «несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї», ст. 362 КК України – 1 664, «порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється», ст. 363 КК України – 3, «перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку», ст. 363-1 КК України – 5 [2].

Наведені статистичні дані кіберзлочинності свідчить, що удосконалилися й інструменти для шпигунства з використанням як спеціалізованих пристроїв, так і з використанням програмного забезпечення. На відміну від класичних методів розвідки та шпигунства нові технології внесли до них суттєві коригування. Нині часом неможливо встановити, хто саме розробив те чи інше програмне забезпечення для проведення розвідувальних чи шпигунських дій у сфері високих технологій. Розробниками такого спеціалізованого програмного забезпечення є як приватні особи, так і організації різної організаційно-правової форми з різними джерелами фінансування (у тому числі за державні кошти). Як заявила директор з розвідки компанії з кібербезпеки бізнесу Red Canary, старший науковий співробітник програми Cyber Statecraft Initiative Атлантичної ради Кеті Нікелс «кібершпигунство» – це те, що є ніби очікуваним від російських розвідувальних служб, фінансованих державою-супротивником. Вони прагнуть отримати інформацію про уряд або пов'язані з урядом об'єкти. Це потребує зовсім іншої політичної відповіді, ніж та, коли йдеться про російських кіберзлочинців, які стоять за більшістю атак вимагачів». За її словами, шпигунство здійснюють державні структури російської федерації, повністю підконтрольні уряду, тоді як оператори програм-викупів «можливо, не контролюються безпосередньо російським урядом» [20]. Крім того, урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA на виконання Закону України "Про основні засади забезпечення кібербезпеки України" [4], з'ясовано, що однією з найбільших «кіберзагроз» є UAC-0010 (Armageddon), діяльність якої здійснюється колишніми "офіцерами" ГУ СБУ в АР Крим, які у 2014 році зрадили військовій присязі і почали прислужувати ФСБ російської федерації [21]. Основним завданням цього угрупування є «кібершпигунство» у відносно сил безпеки та оборони України. При цьому, відомо, щонайменше, про один випадок здійснення деструктивної діяльності на об'єкті інформаційної інфраструктури. За наявною інформацією кількість одночасно інфікованих комп'ютерів, переважно функціонуючих в межах інформаційно-комунікаційних систем державних органів, може сягати кількох тисяч [22].

У 2022 році команда CERT-UA загалом обробила 2194 випадки ворожих атак, з яких

1148 інцидентів мали критичний або високий рівень небезпеки. Найбільш атакованим сектором з боку ворожого кібершпигунства та агресивних операцій, за даними Держспецзв'язку, залишається цивільна інфраструктура України, зокрема державні установи та об'єкти критичної інфраструктури (енергетичні та логістичні компанії, комерційні організації, Міністерство енергетики, Міністерство фінансів, Міністерство закордонних справ тощо). Мішенню також є оборонні організації – Міністерство оборони, Державна прикордонна служба тощо. Особливу небезпеку становлять повільні та "тихі" атаки, спрямовані на шпигунство. Зокрема, такі атаки здійснює угрупування InvisiMole (Служба зовнішньої розвідки російської федерації). Їхньою основною мішенню є високопосадовці, дипломати та інші фахівці, які мають доступ до найбільш чутливої інформації. Оскільки такі "тихі" атаки складніше виявити, вони можуть мати більш критичні наслідки [22]. Як зазначає А.Ю. Нашинець-Наумова, іноді особи, які розробили шкідливе програмне забезпечення або спеціальне обладнання, не є тими хто його використовує у своїй шпигунській діяльності, що часто призводить до неможливості встановити особу, яка здійснює злочину діяльність з метою її притягнення до відповідальності [23]. Крім того, Сполучені Штати та країни всього світу покладають на Китайську Народну Республіку відповідальність за підривну і дестабілізуючу поведінку в кіберпросторі, яка становить серйозну загрозу їх економічній і національній безпеці. У заяві пресслужби Білого дому, зокрема, наголошується, що Міністерство державної безпеки (МДБ) КНР сприяло створенню системи злочинних хакерів-контрактників, які здійснюють спонсоровані державою кіберзлочини. Офіційно підтверджено, що хакери МДБ Китаю використовували вразливість Microsoft Exchange Server для масштабної операції з кібершпигування, внаслідок якої були зламані тисячі комп'ютерів і мереж, ідеться в повідомленні. Як свідчить обвинувальний висновок щодо трьох співробітників МДБ і одного з їхніх хакерів-контрактників, Сполучені Штати накладатимуть санкції на кіберзлочинців КНР за їхню безвідповідальну поведінку в кіберпросторі. Державний департамент США закликав усі держави, які прагнуть стабільності в кіберпросторі, приєднатися до цих зусиль [24].

Аналіз міжнародного досвіду з протидії кіберзлочинності та кібершахрайству виокремлює Конвенцію про кіберзлочинність (ратифікована Україною 1 липня 2004 р.) Вона представляється первинною міжнародною угодою у сфері протидії правопорушенням, вчиненим посередництвом комп'ютера. В рамках одинадцятого і дванадцятого Конгресів організації щодо запобігання злочинності та кримінального правосуддя (UN Congress on Crime Prevention and Criminal Justice) обговорювалися проблеми інтернаціонального партнерства у війні з кіберзлочинністю. Члени Конгресів обговорювали заходи щодо інтенсифікації інтернаціонального партнерства і поліпшення державного законодавства у галузі боротьби з відмиванням коштів, торгівлі наркотиками, тероризмом та кіберзлочинністю. Тобто, ООН встановила комп'ютерні правопорушення в єдиний цикл з тероризмом, що вказує на спеціальний інтерес до даного питання зі сторони світової спільноти [25].

Висновок. Сьогодні в Україні особливої гостроти набуває проблема протидії «кібершпигунству» як необхідної складової забезпечення національної безпеки, територіальної цілісності та існування незалежності держави.

Отже, «кібершпигунство» або комп'ютерний шпіонаж – термін, який позначає несанкціоноване проникнення в інформаційні системи з метою отримання особистої, економічної, політичної чи військової переваги, здійснюваний з використанням (злому), вербування громадян України, що використовують кіберпростір та працюють з інформацією обмеженого користування, із застосуванням шпигунського програмного забезпечення.

Доведено, що сприятливим середовищем для шпигунської діяльності є кіберпростір, а це підтверджує наше дослідження, що «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.

На думку вчених у цій сфері «кібершпигунством визначає» є злочином, який здійснюється шляхом таємного вистежування, розшуку, збирання, викрадання та передачі інформації, що становить державну таємницю, іноземній державі, іноземній організації або їх представникам, якщо ці дії вчинені іноземцем або особою без громадянства і з використанням методів кібернетики, що підпадає під ознаки стаття 114 Кримінального кодексу України, а громадяни України які їм сприяють у кіберпросторі несуть кримінальну відповідальність за ст.ст. 114 ч. 2, 111 ч. 2, 436 ч. 2, як такі, що вчинені при обтяжуючих обставинах.

Таким чином, це дозволить активно протидіяти «кібершпигунству», що дало б можливість успішно попереджати та викривати та притягувати їх до кримінальної відповідальності.

Література:

1. Кримінальний кодекс України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України (ВВР).* 2001. № 25–26, ст. 131.

2. Про роботу органів прокуратури · Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Про осіб, які вчинили кримінальні правопорушення. Статистика – Офіс Генерального прокурора. 2023. new.gp.gov.ua › posts › statistika

3. Закон України Про Службу безпеки України. Відомості Верховної Ради України від 7 липня 1992, № 27, Ст.382. Закон України «Про контррозвідувальну діяльність». *Відомості Верховної Ради України*, від 3 квітня 2003, № 12, Ст. 89.

4. Закон України "Про основні засади забезпечення кібербезпеки України" Зведена інформація щодо діяльності угрупування UAC-0010 станом на липень 2023 року. URL: https://cert.gov.ua/article/5160737

5. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності / О. В. Манжай. *Право і Безпека*. 2009. № 4. С. 215–219. URL: http://nbuv.gov.ua/UJRN/Pib_2009_4_50

6. Gibson W. Neuromancer / W. Gibson. London : HarperCollins, 1994. 271 p.

7. Діордіца І. В. Поняття і зміст кіберзагроз на сучасному етапі. *Підприємство, господарство і право. Адміністративний процес.* 2017. № 4. С. 76–84.

8. Великий тлумачний словник сучасної української мови / [уклад. і голов. ред. В. Г. Бусел]. К. ; Ірпінь : ВТФ «Перун», 2003. 1440 с.

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

10. Етимологічний словник Української мови. Вид. «Наукова думка». 2012. Т. 7. С. 404.

11 Словник іншомовних слів. 23000 слів та термінологічних словосполучень / уклад. Л. О. Пустовіт та ін. К. : Довіра, 2000, 338 с.

12. Про державну таємницю : Закон України від 21 січня 1994 року № 3855-XII зі змінами. URL: http://zakon4.rada.gov.ua/laws/show/3855- 12/print1360009387090304

13. Діордіца І. В. Поняття та зміст кібершпигунства / І. В. Діордіца. URL: https://goal-int.org/ponya

14. Юридична енциклопедія : в 6 т. Т. 6 Т–Я / [редкол. Ю. С. Шемшученко (голова редкол.) та ін.]. К. : Укр. енцикл., 2004. 768 с.

15. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. С. 141.

16. Большая советская энциклопедия : в 30 т. Т. 25. Струнино – Тихорецк / [гл. ред. А. М. Прохоров]. Изд. 3-е. М. : Советская энциклопедия, 1976. 600 с.

17. Kelsen H. Principles of International Law / Hans Kelsen. New York : Rinehart & Company Inc., 1952. 461 p.

18. Menthe D. Jurisdiction In Cyberspace: A Theory of International Spaces / D. Menthe. *Mich. Telecomm.* Tech. L. Rev. URL: http://www.mttlr.org/volfour/menthe.html

19. Чесноков Н.А. Правові основи інформаційної безпеки у сучасних умовах. *Правова ініціатива.* 2013. № 4.

20. Директор з розвідки компанії з кібербезпеки бізнесу Red Canary, старший науковий співробітник програми Cyber Statecraft Initiative Атлантичної ради Кеті Нікелс… «кібершпигунство – це те, що є ніби очікуваним від російських розвідувальних служб».

21. Зведена інформація щодо діяльності угрупування UAC-0010 станом на липень 2023 року. URL: https://cert.gov.ua/article/5160737 ; URL: https://www.ukrinform.ua/rubric-world/3285329-kiberataki-rf-peresliduut-dvi-rizni-cili-spigunstvo-ta-vimaganna-grosej-ekspert.html

22. Кібервійна проти України: Держспецзв'язку дослідила мотивацію, методи та інструменти російських хакерів. URL: https://ms.detector.media/withoutsection/post/31351/2023-03-08-kiberviyna-proty-ukrainy-derzhspetszvyazku-doslidyla-motyvatsiyu-metody-ta-instrumenty-rosiyskykh-khakeriv/

23.Нашинець-Наумова А. Ю. Кібершпіонаж – загроза сучасному інформаційному суспільству. *Кібербезпека в Україні: правові та організаційні питання* : матеріали міжнар. наук.-практ. конф., (Одеса, 22 листоп. 2019 р.). Одеса : ОУВС, 2019. С. 11–13.

24. Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace. URL: https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/

25. Міжнародний досвід протидії кіберзлочинності та кібершахрайству URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/08/74.pdf Вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/%D0%9A%

References:

1. Kryminalnyi kodeks Ukrainy vid 05.04.2001 № 2341-III [Criminal Code of Ukraine dated April 5, 2001 No. 2341-III. *Bulletin of the Verkhovna Rada of Ukraine (VVR)*], 2001, No. 25–26, Article 131. [in Ukrainian].

2. Pro robotu orhaniv prokuratury · Pro zareiestrovani kryminalni pravoporushennia ta rezultaty yikh dosudovoho rozsliduvannia · Pro osib, yaki vchynyly kryminalni pravoporushennia [About the work of prosecutor's offices. About registered criminal offenses and the results of their pre-trial investigation. About persons who have committed criminal offenses]. Statistics – Office of the Prosecutor General. (2023). new.gp.gov.ua › posts › statistics [in Ukrainian].

3. Zakon Ukrainy Pro Sluzhbu bezpeky Ukrainy. Vidomosti Verkhovnoi Rady Ukrainy vid 7 lypnia 1992, № 27, St.382. Zakon Ukrainy «Pro kontrrozviduvalnu diialnist» [Law of Ukraine On the Security Service

of Ukraine. Information of the Verkhovna Rada of Ukraine of July 7, 1992, No. 27, Article 382. The Law of Ukraine "On counter-intelligence activities"]. *Bulletin of the Verkhovna Rada of Ukraine*, dated April 3, 2003, No. 12, Art. 89. [in Ukrainian].

4. Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" Zvedena informatsiia shchodo diialnosti uhrupuvannia UAC-0010 stanom na lypen 2023 roku [Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine" Summarized information on the activities of the UAC-0010 group as of July 2023]. Retrieved from https://cert.gov.ua/article/5160737 [in Ukrainian].

5. Manzhai O.V. Vykorystannia kiberprostoru v operatyvno-rozshukovii diialnosti [Use of cyberspace in operational and investigative activities] / O. V. Manzhai. *Law and Security*. 2009. No. 4. P. 215–219. Retrieved from http://nbuv.gov.ua/UJRN/Pib_2009_4_50 [in Ukrainian].

6. Gibson W. Neuromancer / W. Gibson. London : HarperCollins, 1994. 271 p.

7. Diorditsa I. V. Poniattia i zmist kiberzahroz na suchasnomu etapi [The concept and content of cyber threats at the modern stage]. *Enterprise, economy and law. Administrative process.* 2017. No. 4. P. 76–84. [in Ukrainian].

8. Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy [A large explanatory dictionary of the modern Ukrainian language] / [comp. and heads ed.V.G. Bussel]. K. ; Irpin : VTF "Perun", 2003. 1440 p. [in Ukrainian].

9. Shlapachenko V. M. Shpyhunstvo yak diialnist zi zdobuvannia informatsii. [Espionage as an information gathering activity]. *Information security of a person, society, state*. Kyiv, 2015. No. 1(17). P. 99–109. [in Ukrainian].

10. Etymolohichnyi slovnyk Ukrainskoi movy [Etymological dictionary of the Ukrainian language]. Kind. Scientific thought. 2012, vol. 7. P. 404. [in Ukrainian].

11 Slovnyk inshomovnykh sliv [Dictionary of foreign words]. 23,000 words and terminological phrases / Compilation. L. O. Pustovit et al. K. : Dovira. 2000. 338 p. [in Ukrainian].

12. Pro derzhavnu taiemnytsiu : Zakon Ukrainy vid 21 sichnia 1994 roku № 3855-XII zi zminamy [On state secrets: Law of Ukraine dated January 21, 1994 No. 3855-XII as amended] Retrieved from http://zakon4.rada.gov.ua/laws/show/3855-12/print1360009387090304 [in Ukrainian].

13. Diorditsa I. V. Poniattia ta zmist kibershpyhunstva [Concept and content of cyber espionage] / I. V. Diorditsa Retrieved from https://goal-int.org/ponya [in Ukrainian].

14. Yurydychna entsyklopediia [Legal encyclopedia]: in 6 vols. T. 6 T–Я / [ed. Yu. S. Shemshuchenko (head of editorial) and others]. K. : Ukr. encyclopedia, 2004. 768 p. [in Ukrainian].

15. Konstytutsiia Ukrainy. *Vidomosti Verkhovnoi Rady Ukrainy* [Constitution of Ukraine. *Bulletin of the Verkhovna Rada of Ukraine*]. (1996). No. 30. Art. 141. [in Ukrainian].

16. Bolshaya sovetskaya encyclopedia: in 30 vols. Vol. 25. Strunino – Tikhoretsk / [ch. ed. A. M. Prokhorov]. Ed. 3rd M. : Soviet encyclopedia, 1976. 600 p.

17. Kelsen H. Principles of International Law / Hans Kelsen. New York : Rinehart & Company Inc., 1952. 461 p.

18. Menthe D. Jurisdiction In Cyberspace: A Theory of International Spaces / D. Menthe // Mich. Telecomm. Tech. L. Rev. Retrieved from http://www.mttlr.org/volfour/menthe.html

19. Chesnokov N.A. Legal foundations of information security in modern conditions. *Law initiative.* 2013. No. 4.

20. Dyrektor z rozvidky kompanii z kiberbezpeky biznesu Red Canary, starshyi naukovyi spivrobitnyk prohramy Cyber Statecraft Initiative Atlantychnoi rady Keti Nikels [Director of Intelligence at business cybersecurity firm Red Canary, senior fellow at the Atlantic Council's Cyber Statecraft Initiative, Kathy Nickels]... “cyber espionage is what is expected of Russian intelligence

21. Zvedena informatsiia shchodo diialnosti uhrupuvannia UAC-0010 stanom na lypen 2023 roku [Summary information on the activities of the UAC-0010 group as of July 2023]. Retrieved from https://cert.gov.ua/article/5160737. Retrieved from https://www.ukrinform.ua/rubric-world/3285329-kiberataki-rf-peresliduut-dvi-rizni-cili-spigunstvo-ta-vimaganna-grosej-ekspert.html [in Ukrainian].

22. Kiberviina proty Ukrainy: Derzhspetszviazku doslidyla motyvatsiiu, metody ta instrumenty rosiiskykh khakeriv [Cyber war against Ukraine: The State Intelligence Service investigated the motivation, methods and tools of Russian hackers]. Retrieved from https://ms.detector.media/withoutsection/post/31351/2023-03-08-kiberviyna-proty-ukrainy-derzhspetszvyazku-doslidyla-motyvatsiyu-metody-ta-instrumenty-rosiyskykh-khakeriv/ [in Ukrainian].

23. Nashinets-Naumova A. Yu. Kibershpionazh – zahroza suchasnomu informatsiinomu suspilstvu [Cyberespionage is a threat to the modern information society]. Cybersecurity in Ukraine: legal and organizational issues: materials of the International science and practice conference, (Odesa, November 22, 2019). Odesa : OUVS, 2019. P. 11–13. [in Ukrainian].

24. Responding to the PRC's Destabilizing and Irresponsible Behavior in Cyberspace. Retrieved from https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/

25. Mizhnarodnyi dosvid protydii kiberzlochynnosti ta kibershakhraistvu [International experience of combating cybercrime and cyberfraud] Retrieved from https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/08/74.pdf Free encyclopedia // Retrieved from https://uk.wikipedia.org/wiki/%D0%9A% [in Ukrainian].