http://www.moderntechno.de/index.php/meit/article/view/meit31-00-050
DOI: 10.30890/2567-5273.2024-31-00-050

**УДК 343.1**

# THE GENESIS OF THE INTERPRETATION OF THE CONCEPTS OF ESPIONAGE AND "CYBER ESPIONAGE"

## ГЕНЕЗА ТЛУМАЧЕННЯ ПОНЯТЬ ШПИГУНСТВО ТА «КІБЕРШПИГУНСТВО»

**Servetskyi Ivan / Сервецький Іван Васильвич**
*ORCID : 0000-0002-5713-8911*
*Doctor of Law, Associate Professor, Deputy Head of the Law Enforcement and Anti-Corruption Department of the Educational Scientific Institute of Law*
*доктор юридичних наук, доцент, заступник завідувача кафедри правоохоронної на антикорупційної діяльності*
*Interregional Academy of Personnel Management, named after Volodymyra Velyky, 03039, Kyiv, str. Frometivska, 2.*
*Навчально-наукового інституту права Міжрегіональна академія управління персоналом, ім. Володимира Великого, 03039, м. Київ, вул. Фрометівська, 2. Україна*

***Анотації.*** *Стаття присвячена тлумаченню понять шпигунство та його співвідношення з «кібершпигунством», що дасть можливість більш активніше викривати державних зрадників, колаборантів, встановленню осіб, які виправдовують, заперечують або визнають правомірною збройну агресію, глорифікації її учасників та притягувати їх до кримінальної відповідальності.*

*З метою успішного виявлення таких осіб СБУ здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані, в першу чергу, на боротьбу з шпигунством у кіберпросторі.*

*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».*

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

*Термін «кіберпростір» став синонімом поняття «комп'ютерна віртуальна реальність». 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, Манжай О. В., Д.С. Мінін, І.В. Сопілко, М.М. Чеховська, В.С. Цимбалюк, В.М. Шлапаченко .*

*Метою статті є здійснення етимологічного аналізу поняття «кібершпигунство», як одного із сучасних способі шпигунства.*

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

## Постановка проблеми:

Протидія спецслужбам російської федерації під час військових дій, пов'язані з викриттям шпигунів та державних зрадників та притягнення їх 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 шпигуни активно проводять шпигунські операції у кіберпросторі, застосовуючи при цьому новітні технології та найвищі досягнення людства у космічній галузі, науки та техніки.

Тому 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.

Відповідно, СБУ повинна здійснювати попереджувальні заходи із запобігання, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі [3] та здійснювати активні контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібершпигунством, негласно протидіяти кіберзлочинності, розслідувати кібератаки щодо державних електронних інформаційних ресурсів, інформаційної інфраструктури; забезпечувати реагування на всі інциденти у сфері державної безпеки [4].

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

На думку О. В. Манжай «…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.

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.

Отже, кіберпростір 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. Арістова,, І. В. Діордіца, О. В Манжай., Д.С. Мінін, І.В. Сопілко, М.М. Чеховська, В.С. Цимбалюк,В.М. Шлапаченко.

**Мета статті (постановка завдань)** – здійснити етимологічний аналіз понять «кібершпигунство». його основні складові, які становлять їх основу.

**Виклад основного матеріалу дослідження**.

Сьогодні в Україні особливої гостроти набуває проблема протидії «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. 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. ісп. spioпe «тс.») запозичене з італійської; іт. spioпe «шпигун» утворене від spїare «шпіонити, вистежу вати, підстерігати», джерелом якого є германські мови (пор. пгер. speph-де «уважно, гостро дивитися» і генетично, пов'язані з ним двн.. spehoп, spiohoпte.«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, діяльність яких направлена на отримання доступу до державної таємниці [12].

Під кібершпигунством І. В. Діордіца 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 кібернетична загроза зовнішній безпеці України, її суверенітет, територіальна цілісність і недоторканність, обороноздатність, державна, економічна чи інформаційна безпека.

Предметом цієї статті 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].

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 міжнародну юрисдикцію.

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.

На думку О.В. Монжая 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].

Найбільш обґрунтовану позицію щодо цього питання було викладено в роботі Д. Менте «Юрисдикція в кіберпросторі: теорія міжнародних просторів»[15] 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 цій роботі 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**.**

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 цього питання зі сторони світової спільноти [16].

**Висновок.**

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 тезу, 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.

Тому, «кібершпигунство» є злочином, яке 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 статей КК України, а громадяни України які їм сприяють повинні нести кримінальну відповідальність за ст.ст. 114 ч.2, 111 ч.2, 436 ч. 2, як такі, що вчинені при обтяжуючих обставинах.

**Список використаних джерел**

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. Закону України "Про основні засади забезпечення кібербезпеки України" Зведена інформація щодо діяльності угрупування UAC-0010 станом на липень 2023 року. [Електронний ресурс]. – Режим доступу: 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. - Режим доступу: 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 № 4, 2017,

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 [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/3855- 12/print1360009387090304.

13. Діордіца І. В. Поняття та зміст кібершпигунства / І. В. Діордіца [Електронний ресурс]. – Режим доступу : 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. Menthe D. Jurisdiction In Cyberspace: A Theory of International Spaces [Електронний ресурс] / D. Menthe // Mich. Telecomm. Tech. L. Rev. – Режим доступу : http://www.mttlr.org/volfour/menthe.html.

16. Міжнародний досвід протидії кіберзлочинності та кібершахрайству [Електронний ресурс]. – Режим доступу: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/08/74.pdf Вільна енциклопедія // [Електронний ресурс]. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%9A%.

**References**

1. 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.

2. 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.

3. 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.

4. 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. [Electronic resource]. – Access mode: https://cert.gov.ua/article/5160737

5. Manzhai O.V. Use of cyberspace in operational and investigative activities / O.V. Manzhai // Law and Security. - 2009. - No. 4. - P. 215-219. - Access mode: http://nbuv.gov.ua/UJRN/Pib_2009_4_50.

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

7. Diorditsa I.V. The concept and content of cyber threats at the modern stage. Enterprise, economy and law. Administrative process No. 4, 2017, p. 76-84.

8. A large explanatory dictionary of the modern Ukrainian language / [comp. and heads ed.V.G. Bussel]. – K.; Irpin: VTF "Perun", 2003. - 1440 p.

9. Shlapachenko V.M. Espionage as an information gathering activity. Information security of a person, society, state. Kyiv, 2015. No. 1 (17). P. 99–109.

10. Etymological dictionary of the Ukrainian language. Kind. Scientific thought. 2012, vol. 7.

P. 404.

11 Dictionary of foreign words. 23,000 words and terminological phrases / Compilation. L.O. Pustovit et al.. - K.: Dovira, 2000, -338 p.

12. On state secrets: Law of Ukraine dated January 21, 1994 No. 3855-XII as amended [Electronic resource]. – Access mode: http://zakon4.rada.gov.ua/laws/show/3855-12/print1360009387090304.

13. Diorditsa I. V. Concept and content of cyber espionage / I. V. Diorditsa [Electronic resource]. – Access mode: https://goal-int.org/ponya

14. Legal encyclopedia: in 6 vols. T. 6 T–Я / [ed. Yu. S. Shemshuchenko (chief editor) and others]. -K. : Ukr. encyclopedia, 2004. – 768 p.

15. Menthe D. Jurisdiction In Cyberspace: A Theory of International Spaces [Electronic resource] / D. Menthe // Mich. Telecomm. Tech. L.Rev. – Access mode: http://www.mttlr.org/volfour/menthe.html.

16. International experience of combating cybercrime and cyberfraud [Electronic resource]. – Access mode: https://visnyk-juris-uzhnu.com/wp-content/uploads/2021/08/74.pdf Free encyclopedia // [Electronic resource]. – Access mode: https://uk.wikipedia.org/wiki/%D0%9A%.

***Abstracts***. *The article is devoted to the interpretation of the concepts of espionage and its relationship with "cyber-espionage", which will make it possible to more actively expose state traitors, collaborators, establish persons who justify, deny or recognize the legitimate armed aggression, glorify its participants and bring them to criminal responsibility.*

*In order to successfully identify such persons, SBU special service carries out counter-intelligence and operational-search measures aimed, first of all, at combating espionage in cyberspace.*

*Cyberspace is an information environment (space) that arises (exists) with the help of technical (computer) systems when people interact with each other, the interaction of technical (computer) systems and the management of these technical (computer) systems by people."*

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

*The term "cyberspace" has become synonymous with the concept of "computer virtual reality." Cyberspace is a space (territory) that is created and operates on the basis of the principles and methods of cybernetics (the science of the general laws of obtaining, 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" as one of the modern methods of espionage.*

***Keywords:*** *espionage, "cyber espionage", "cyber security", "cyber space", counterintelligence measures*