УДК 342.9
DOI https://doi.org/10.24144/2788-6018.2024.06.98

ОСНОВНІ КІБЕРЗАГРОЗИ В УМОВАХ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ

Мазур Я.П.,
аспірант кафедри конституційного,
адміністративного та фінансового права
Хмельницького університету управління та права
імені Леоніда Юзькова

Мазур Я.П. Основні кіберзагрози в умовах ведення інформаційної війни.

У статті розглянуті основні кіберзагрози в умовах ведення інформаційної війни, як наявні та потенційно можливі явища і чинники, що створюють небезпеку важливим національним інтересам держави. Основними видами кіберзагроз є кіберзлочинність, кібертероризм, кібершпигунство, кібервійна. Інформаційна війна має три основні цілі: контроль інформаційного простору та забезпечення захисту власної інформації від дій противника, використання контролю над інформаційним простором для здійснення інформаційних атак на противника, підвищення загальної ефективності інформаційних функцій. Представлено основні проблеми в інформаційному просторі, які потребують вирішення в сучасних умовах. Інформаційна війна стала одним із найнебезпечніших видів зброї, існують такі види інформаційної війни, як командна, розвідувальна, психологічна, економічна, електронна, знищення документів, кібервійна. Психологічний вплив, дезінформація, піар-компанії та спеціальні інформаційні операції є найважливішими для інформаційної війни.

Запропоновано авторське розуміння кібершпигунства: це злочинна діяльність, яка здійснюється шляхом таємного виявлення, пошуку, збору, викрадення та передачі інформації, що становить державну таємницю, іноземній державі, організації або їх представникам, якщо це так, вчинена іноземцем або особою без громадянства в кіберпросторі. Встановлено, що предметом кібершпигунства є зовнішня безпека України, її суверенітет, територіальна цілісність і недоторканність, обороноздатність, державна, економічна чи інформаційна безпека та кіберпростір в цілому. З об'єктивної сторони шпигунство виражається в передачі або збиранні відомостей, що становлять державну таємницю, з метою передачі їх іноземній державі, іноземній організації або їх представникам. Предметом цього злочину є відомості, що містять державну таємницю. Суб'єктивно кібершпигунство характеризується прямим умислом. Кібервійна це комп'ютерне протистояння у просторі Інтернету. Інтернет давно перетворився на поле бою кібервійн. У статті досліджено сучасні ознаки поняття «кібервійна».

Ключові слова: інформаційна війна, інформаційні відносини, захист інформації, кіберполіція, кіберзлочинність, кібертероризм, кібершпигунство, кібервійна, інформаційна безпека.

Mazur Ya.P. The main cyber threats in the conditions of information warfare.

The article examines the main cyber threats in the conditions of conducting information warfare, as existing and potentially possible phenomena and factors that pose a danger to important national interests of the state. The main types of cyber threats are cyber crime, cyber terrorism, cyber espionage, and cyber war. Information warfare has three main goals: control of the information space and protection of one's own information from the actions of the enemy, use of control over the information space to carry out information attacks on the enemy, and increase the overall efficiency of information functions. The main problems in the information space that need to be solved in modern conditions are presented. Information war has become one of the most dangerous types of weapons, there are such types of information war as command, intelligence, psychological, economic, electronic, document destruction, cyber war. Psychological influence, disinformation, PR companies and special information operations are the most important for information warfare.

The author's understanding of cyberespionage is proposed: it is a criminal activity carried out by covertly identifying, searching, collecting, stealing and transmitting information that constitutes a state secret to a foreign state, organization or their representatives, if so, committed by a foreigner or a stateless person in cyberspace. It has been established that the subject of cyberespionage is the external security of Ukraine, its sovereignty, territorial integrity and inviolability, defense capability, state, economic or informational security and cyberspace as a whole. On the

objective side, espionage is expressed in the transfer or collection of information constituting a state secret, with the aim of transferring it to a foreign state, a foreign organization or their representatives. The subject of this crime is information containing state secrets. Subjectively, cyberespionage is characterized by direct intent. Cyberwar is a computer confrontation in the space of the Internet. The Internet has long been transformed into a battlefield of cyberwars. The article examines modern features of the concept of "cyberwar".

Key words: information warfare, information relations, information protection, cyber police, cyber crime, cyber terrorism, cyber espionage, cyber war, information security.

Постановка проблеми. Інформаційні війни супроводжують всю історію людства. Перш за все, вони мали релігійно-ідеологічний характер, а в боротьбі з захисниками чужорідних поглядів використовувалися всі форми репресій. У далекому минулому інквізиція або репресивний апарат тоталітарних держав XX століття вів активну боротьбу з носіями чужих ідей. Кожен з нас асоціюється з терміном «інформаційна війна», тому що сьогодні, як ніколи, ми надто прив'язані до неї, у світі домінує інформація. Сьогодні інформаційна війна стала одним із найнебезпечніших видів зброї. Використання секретної інформації, поширення бруду, поширення неправдивої інформації та спроби ввести в оману з використанням інформації стали основою існування багатьох тоталітарних систем.

Після розвитку новітніх технологій вплив інформації на прогрес людства зріс у тисячі разів. Інформація має вплив на маси. Інформація, що є власністю держави, або інформація з обмеженим доступом має оброблятися в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах із застосуванням комплексної системи захисту інформації [8].

Завдяки поширенню інформації влада чи особа, відповідальна за процес, формує в суспільстві чи групі людей необхідну точку зору, громадську думку, хід взаємодоповнюючих логічних думок, вичерпну систему поглядів на ті чи інші питання.

Мета дослідження. Метою дослідження є визначення основних кіберзагроз в умовах ведення інформаційної війни.

Актуальність проблеми кіберзагрози в умовах ведення інформаційної війни зумовлена тим, що потенційно можливі явища і чинники, які створюють небезпеку важливим національним інтересам державі, зловмисна дія чинників спрямована на пошкодження, викрадення або таємне змінення даних. Необхідна комплексна система захисту інформації.

Комплексна система захисту інформації складається з захисту від несанкціонованих дій з інформацією, окремі положення правового регулювання відносин у сфері інформації відображено в указах та розпорядженнях Президента України, Постановах та розпорядженнях Кабінету Міністрів України, нормативних актах міністерств і відомств.

Стан опрацювання проблематики. Деякі аспекти проблемки кібернетичної безпеки та кібернетичних загроз у той чи інший спосіб досліджувались у наукових працях таких вітчизняних учених, як наукова школа В.А. Ліпкана І.В. Арістова, В.С. Цимбалюк та інші, проте питання правового регулювання кібербезпеки, зокрема формування ефективного механізму правового регулювання протидії загрозам у кібернетичній сфері, на сучасному етапі є абсолютно новим, що зумовлює потребу в його ґрунтовному дослідженні.

Інформаційна війна це комплексна цілісна стратегія, спрямована на надання належної важливості та цінності інформації в питаннях командування, контролю та управління.

Інформаційна війна це цілеспрямоване використання інформації та засобів масової комунікації для впливу на громадську думку, політику та поведінку груп та окремих осіб.

Логінова Н.І. вважає, що інформаційна війна – це протиборство між сторонами за допомогою поширення спеціально підготовлених даних і протидія однотипним зовнішнім впливам на себе.

Манжай О.В пише, що інформаційну війну найчастіше ведуть групи людей, які намагаються вплинути на міжнародну спільноту та змінити ситуацію на свою користь. З іншого боку, жертви упереджених звинувачень повинні прагнути довести протилежне. Тому інформаційні війни завжди призводять до фінансових втрат, зриву бізнес-процесів та інших негативних наслідків. Необхідно, щоб населення та підприємці усвідомлювали можливі загрози та розуміли, які заходи захисту необхідно вживати в тих чи інших випадках.

Норми інформаційного права, поступово зростають, мають диспозитивний характер, згідно з яким суб'єкт інформаційного права отримує право обирати свою поведінку в його межах або ситуації.

У ході інформаційної війни «влучання» досягаються не фізично, а безперешкодно. Злочинці намагаються «закріпити» у свідомості суспільства матеріал, щоб нав'язати своє бачення ситуації. Такий спосіб досягнення мети робить напад менш надійним, але не менш небезпечним і руйнівним. Інформаційна війна – це не відкрите протистояння сторін і не протистояння у звичному розумінні. Серед загроз – руйнуван-

ня єдиного інформаційного простору держави, маніпулювання суспільством, недостатня координація діяльності органів державної влади, слабкість системи освіти та виховання, незаконне використання спеціальних засобів впливу на суспільну свідомість. Основними видами кіберзагроз є кіберзлочинність, кібертероризм, кібершпигунство та кібервійна [5].

Цій проблемі присвятили свої праці такі українські вчені: В. Бурячок, А. Войціховський, О. Грицун, І. Забара, О. Мережко, Є. Скулиш. Із закордонних учених свої праці присвятили Ч. Данлеп, Р. Кларк, Н. Ладарєв, М. Лібицький, Л. Муравець, Б. Рабоін, Т. Рід, С. Гілдрет, Г. Шинкарецька, М. Шмідт та інші.

Ліпкан В.А стверджує, що кіберзлочин – це злочинна діяльність, спрямована на отримання інформації з баз даних, перехоплення інформації, знищення інформації шляхом розповсюдження вірусних програм, фішингових програм і злому з корисливих, політичних чи особистих мотивів. Кіберзлочинці, стають все більш витонченими, а сучасні системи реалізації кіберзахисту не встигають адаптуватися до нових обставин.

Виклад основного матеріалу. Майже кожен чув про кіберзлочинність, навіть стикався з нею. До кіберзлочинності належать різні види злочинів, вчинені з використанням комп'ютера та Інтернету. Основні типи кіберзлочинів включають розповсюдження шкідливого програмного забезпечення, викрадення номерів кредитних карток і банківських рахунків, злом паролів і порушення авторських прав. До кіберзлочинів в Україні належать порушення авторського права та суміжних прав, шахрайство, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, а також обладнанням для їх виготовлення, ухилення від сплати податків, зборів (обов'язкових платежів), ввезення, виготовлення, збут і розповсюдження порнографічних виробів, незаконне збирання з метою використання або використання відомостей, що становлять комерційну чи банківську таємницю.

Закон України «Про інформацію» [1] регулює відносини щодо отримання та поширення інформації. Ст. 6 Закону України «Про інформацію» визначає зміст державної інформаційної політики, її головні напрями та способи.

Існування кіберзлочинності є досить серйозною проблемою з огляду на глобальне багатство інноваційних і технологічних ресурсів. Від цього страждають як фізичні, так і юридичні особи, а також об'єкти критичної інфраструктури та державні установи. Окрім пов'язаної прямої шкоди, кіберзлочинність є основною перешкодою для цифрової довіри та значно підриває переваги кіберпростору[11].

М.Ш. Магомедов вказує на необхідність створення відповідної міжнародної договірної бази. У більш вузькому значенні, на його думку, інформаційна війна складається з «інформаційних операцій, які здійснюються під час виникнення кризи чи конфлікту з метою досягнення або сприяння досягненню конкретних цілей проти конкретного противника» [14].

В останні роки в Україні спостерігається зростання кількості кібератак та їх негативних наслідків. Тому кількість злочинів у сфері інформаційних технологій постійно зростає. Огляд статистичних даних Генеральної прокуратури України свідчить, що станом на 31 грудня 2022 року за звітний період зареєстровано 3415 злочинів у сфері інформаційних технологій, у 2023 році кіберполіція виявила понад 3600 кіберзлочинів[8].

Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції, який входить до структури карного розшуку та відповідно до законодавства України забезпечує реалізацію державної політики у сфері протидію кіберзлочинності, організовує та проводить відповідно до законодавства оперативно-розшукову діяльність. Ухвалено Стратегію кібербезпеки України, Президент України підписав Указ від 28.01.2020 р. № 27/2020, про створення Національного координаційного центру кібербезпеки.

Одним зі шляхів протидії кіберзлочинності є прийняття на законодавчому рівні нормативно-правових актів, які регулюють відносини в інформаційній сфері. Зокрема, нормативно-правову базу у цій сфері складають: Конституція України, Кримінальний кодекс України, Закони України: «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про основи національної безпеки», Конвенції Ради Європи про комп'ютерні злочини та інших міжнародних договорів [4].

Кібертероризм виникає у сфері кібербезпеки. Загрози національній безпеці України в інформаційній сфері – сукупність умов і факторів, що створюють загрозу важливим інтересам держави, суспільства та особи внаслідок можливості негативного інформаційного впливу на свідомість і поведінку громадян, а також як на інформаційні ресурси, так і на інформаційну інфраструктуру [11].

В.М. Фурашев стверджує, що кібертероризм є багатогранним явищем, багато в чому зумовленим неконтрольованим використанням глобальних мереж, недостатньою увагою держави, громадянського суспільства та спецслужб до цього сегменту інформаційного простору. Кібертероризм проявляється в атаках на комп'ютери, комп'ютерні програми та мережеву інформацію.

Ці напади спрямовані на створення в суспільстві атмосфери страху та безнадійності для реалізації цілей та інтересів суб'єктів терористичної діяльності. Тероризм у сфері комп'ютерних технологій має такі характеристики: анонімність, віддаленість злочинця, відносна дешевизна, відсутність необхідності використання вибухівки та терактів смертників, широке поширення інформації [3].

Аналіз наукової літератури свідчить, що більшість дослідників поділяють позицію про те, що інформаційний тероризм є видом терористичної діяльності, пов'язаної з досягненнями інформаційних технологій.

Лісовська Ю.П. стверджує, що одним із методів кібертероризму є політично мотивована атака на інформацію, що знаходиться під безпосереднім контролем суспільства, шляхом превентивного залякування. Другий спосіб кібертероризму – інформаційна атака на комп'ютерну інформацію, комп'ютерні системи, пристрої передачі даних та інші компоненти інформаційної інфраструктури, що здійснюється групами або окремими особами. Така атака дає можливість проникнути в систему, перехопити або придушити контроль над обміном інформацією в мережі та досягти інших руйнівних ефектів [4].

Рулов І.М. пише про рівні можливості кібертероризму, наприклад, про простий неструктурований кібертероризм, який має здатність здійснювати базові атаки на окремі інформаційні системи. Більш просунутий кібертероризм має здатність здійснювати більш складні атаки на численні системи або мережі, потенційно модифікуючи або створюючи основні інструменти злому, а організація має елементарну систему аналізу, управління та контролю. Існує також кібертероризм, при якому дії є складно скоординованими, які можуть призвести до масового руйнування інтегрованих неоднорідних систем захисту [11].

Кібершпигунство становить все більш серйозну загрозу для бізнесу в епоху цифрових технологій. Цей тип кіберзлочинності передбачає незаконне отримання конфіденційної або розвідувальної інформації за допомогою комп'ютерних технологій. Злочинці, які займаються кібершпигунством, можуть мати різні мотиви, зокрема економічну вигоду, політичні цілі або шантаж.

Під кібершпигунством розуміється передача або збирання з метою передачі іноземній державі, іноземній організації або їх представникам інформації з обмеженим доступом, що здійснюється в кіберпросторі [15].

Пропоную під кібершпигунством розуміти злочинну діяльність, яка здійснюється шляхом негласного виявлення, пошуку, збору, викрадення та передачі інформації, що становить державну таємницю, іноземній державі, іноземній організації або їх представникам, якщо ці дії здійснюються одним вчинені іноземцями або особою без громадянства з використанням кіберпростору.

З об'єктивної сторони шпигунство може проявлятися у двох формах – це передача відомостей, що становлять державну таємницю, іноземній державі, іноземній організації або їх представникам та збирання тієї самої інформації з метою передачі її іноземній державі, її організаціям або їх представникам. Закінченим шпигунство вважається з моменту початку збирання зазначених відомостей або з моменту їх передачі[7]. Ініціатива збору чи передачі відповідної інформації може належати як виконавцю, так і одержувачу шпигунства. Для кваліфікації злочину це не грає ролі.

Левченко О.В. визначає, що кібершпигунство характеризується прямим умислом, та якщо шпигунство вчинене шляхом незаконного втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, то необхідна додаткова кваліфікація за статтею 361 Кримінального кодексу України та шляхом викрадення, розтрати, вимагання або заволодіння нею шляхом шахрайства чи зловживання службової особи своїм службовим становищем ст. 362 ККУ[12].

Останнім часом до кібершпигунства також відноситься аналіз поведінки користувачів соціальних мереж, таких як Facebook і Twitter, через спеціальні служби з метою виявлення екстремістської, терористичної чи антиурядової діяльності. Наприклад, програма Athena дозволяє агентам ЦРУ дистанційно змінювати налаштування операційної системи, вводити віруси, а потім завантажувати файли із заражених пристроїв. Athena працює на комп'ютерах з програмним забезпеченням Windows. Програму розробило ЦРУ спільно з американською компанією Siege Technologies, яка займається питаннями кібербезпеки [9].

Захист від кібершпигунства вимагає постійного моніторингу, оновлень безпеки та поінформованості про загрози. Ретельне планування та впровадження заходів безпеки допоможе захистити від кіберзлочинності та зберегти конфіденційність інформації.

Кібервійна насамперед спрямована на дестабілізацію комп'ютерних систем та доступу до Інтернету державних установ, фінансових і бізнес-центрів, а також на створення безладу та хаосу в житті країн, які покладаються на Інтернет у повсякденному житті. Кібервійна може спрямовувати, спотворювати або порушувати потік інформації, щоб впливати на думку суспільство, державних чиновників чи військових. Міністерство оборони України працює над легальним визначенням терміну «кібервійна». Ре-

алізація цього кроку на законодавчому рівні є важливою для протидії кіберзагрозам.

Кібервійна, яку іноді називають цифровою війною, може включати атаки на: цивільну інфраструктуру, таку як електромережі або системи контролю руху; фінансові установи, такі як банки та кредитні спілки; військові об'єкти, підрядники та інші установи національної безпеки, окремі громадяни країни. Питання про застосовність до регулювання кібервійн норм чинного міжнародного права потребує окремих досліджень.

Мацюк В.Я. вважає, що існують такі види інформаційної війни, як управління командою, розвідка, психологічна, економічна, електронна війна, знищення документів та кібервійна. Для інформаційної війни найважливішими є психологічний вплив, дезінформація, піар-компанії та спеціальні інформаційні операції [7].

Інформаційні війни – це контентні війни, спрямовані на зміну свідомості мас, груп та індивідів, нав'язування ворогу своєї волі та перепрограмування його поведінки. Під час інформаційної війни відбувається боротьба за свідомість, цінності, переконання, моделі поведінки тощо. Вони виникли тисячі років тому, і Інтернет дав їм новий рівень інтенсивності, масштабу та ефективності. Об'єктами впливу інформаційних війн є різноманітні суб'єкти – від малих груп до конкретних народів і націй до населення держав. Засобами впливу є спеціально підготовлені смислові повідомлення у вигляді текстів, відео- та аудіо матеріалів. Кібервійна – це дії однієї національної держави з проникнення в комп'ютери чи мережі іншої національної держави з метою досягнення конкретної мети завдання шкоди чи руйнування. Інформаційні війни та кібервійни це два типи воєн, які ведуться переважно через комп'ютерні мережі. Сьогодні Україна стоїть на межі загроз в інформаційному просторі та має вміти адекватно реагувати, щоб захиститися від них. Глобальні інформаційні мережі, які вийшли з-під контролю, стрімко розвиваються, щодня з'являються нові електронні ресурси, зокрема ЗМІ та вебсайт, удосконалюються засоби та методи донесення інформації та пропагандистських матеріалів до аудиторії, з'являються нові засоби масової інформації [7].

Основним засобом в кібервійні є спеціальний програмний код, який порушує роботу, скасовує робочий стан або дозволяє перехоплювати контроль над різними видами матеріальних об'єктів і мереж, обладнаних електронними системами управління [5]. Кібервійна має проблематичну та руйнівну дію в реальному світі [5].

Створити стовідсотковий захист інформації неможливо за жодних обставин, тому метою є досягнення не теоретично максимального рівня захисту, а скоріше мінімального, необхідного за даних конкретних умов і з огляду на рівень можливої загрози. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29.03.2006 № 373. Ефективна боротьба з інформаційною агресією вимагає розробки та впровадження комплексних стратегій. За відсутності цілісної політики, нормативної консолідації та чіткого уніфікованого понятєвого апарату в кіберсфері, норм міжнародного права, кібервійни продовжують де стабілізувати комп'ютерні системи, створюють хаос і сіють хаос у житті країн.

Висновки. Інформаційна війна є невіддільною (частина/ознака) частиною ідеологічної боротьби. Такі війни безпосередньо не призводять до кровопролиття і руйнувань, втрат немає, ніхто не позбавлений їжі та даху над головою. Інформаційна війна включає дві істотні частини: вплив на інформаційні системи та вплив на суспільну та індивідуальну свідомість.

Основними видами кіберзагроз є кіберзлочинність, кібертероризм, кібершпигунство та кібервійна. Необхідно розглянути питання про створення інформаційного кодексу, який об'єднував би всі норми інформаційного права. Для комплексної боротьби потрібні спільні зусилля держави, громадян та міжнародної спільноти. Поняття кібервійни закріпити в нормах міжнародного права, також кібершпигунство, як злочин має бути законодавчо закріплений на міжнародному рівні, щоб уніфікувати чинних норм та об'єднати їх в єдине ціле. Україна потребує подальшого розвитку кібербезпеки, оскільки кіберзлочинці завжди принаймні на крок попереду тих механізмів, які використовують відповідні державні органи для боротьби з цим видом злочинності. Лише завдяки належному рівню кібербезпеки відбувається нормальне функціонування мереж і систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про інформацію: Закон України. № 2658-XII (2658-12) від 02.10.92. *ВВР*, 1992, № 48, ст. 651. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.
2. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам: Закон 2137-IX. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text.
3. Левченко О.В., Охрімчук В.В. Особливості антиукраїнського інформаційного (кібер) впливу на Україну. *Захист інформації*. 2022. № 4. С. 156–163.

4. Ліпкан В.А. Національна безпека України : нормативно-правові аспекти забезпечення. Київ : Знання, 2003. 180 с.
5. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. К.: Видавничий дім «Кондор. 2019.
6. Лісовська ЮП. Кібербезпека: ризики та заходи: навч. посібник. Київ.: Видавничий дім «Кондор. 2019. 80 с.
7. Логінова Н.І. Правовий захист інформації. Одеса : Фенікс, 2015. 264 с
8. Макаренко Є.А. Міжнародні інформаційна безпека: сучасні виклики та загрози. Київ : Центр вільної преси, 2006. 916 с.
9. Манжай О.В Правові заходи захисту інформації. Харків : Панов, 2020. 162 с.
10. Мацюк В.Я. Інформаційне суспільство – новий щабель суспільної формації. *Часопис Київського університету права*. 2006. № 2. С. 102–106.
11. Рульов І.М. Співвідношення кібертероризму та кіберзлочину. *Юридичний вісник*. Одеса : Гельветика, 2021. № 3. С. 178–185.
12. Чаплінська Ю. Кіберкультура та кібербезпека в умовах війни. Національна академія педагогічних наук України, Інститут соціальної та політичної психології. Київ, 2023.