УДК 004.056:355.45(100)
DOI 10.69550/3041-1467.6.326252

Любов ШЕПТИЦЬКА
кандидатка історичних наук, доцентка, завідувачка кафедри права та суспільних дисциплін, Національний лісотехнічний університет України, вул. ген. Чупринки, 103, м. Львів, Україна, індекс 79057 (sheptytska@nltu.edu.ua)

ORCID: 0000-0003-3070-0131

Олеся РЕМЕНЯК
кандидатка юридичних наук, доцентка кафедри права та суспільних дисциплін, Національний лісотехнічний університет України, вул. ген. Чупринки, 103, м. Львів, Україна, індекс 79057 (remenyak@nltu.edu.ua)

ORCID: 0000-0002-5175-1280

Наталія ЗАХАРЧИН
кандидатка історичних наук, доцентка кафедри права та суспільних дисциплін, Національний лісотехнічний університет України, вул. ген. Чупринки, 103, м. Львів, Україна, індекс 79057 (zakharchyn@nltu.edu.ua)

ORCID: 0000-0003-3000-2595

Lubov SHEPTYTSKA
PhD (History), Associate Professor of the Department of Law and Social Sciences, National Forestry University of Ukraine, 103 Gen. Chuprynky Str., Lviv, Ukraine, postal code 79057 (sheptytska@nltu.edu.ua)

Olesya REMENYAK
PhD (Legal), Associate Professor of the Department of Law and Social Sciences,, National Forestry University of Ukraine, 103 Gen. Chuprynky Str., Lviv, Ukraine, postal code 79057 (remenyak@nltu.edu.ua)

Nataliia ZAKHARCHYN
PhD (History), Associate Professor of the Department of Law and Social Sciences, National Forestry University of Ukraine, 103 Gen. Chuprynky Str., Lviv, Ukraine, postal code 79057 (zakharchyn@nltu.edu.ua)

Бібліографічний опис статті: Шептицька, Л., Ременяк, О., Захарчин, Н. (2025). Кібератака як новітній конфлікт та важлива форма глобального протистояння. *Axis Europae, 6,* 214–223. doi: 10.69550/3041-1467.6.326252

Bibliographic Description of the Article: Sheptytska, L., Remenyak, O., & Zakharchyn, N. (2025). Kiberataka yak novitnii konflikt ta vazhlyva forma hlobalnoho protystoiannia [Cyberattack as a new conflict and an important form of global confrontation]. *Axis Europae, 6,* 214–223. doi: 10.69550/3041-1467.6.326252 [in Ukrainian].

КІБЕРАТАКА ЯК НОВІТНІЙ КОНФЛІКТ ТА ВАЖЛИВА ФОРМА ГЛОБАЛЬНОГО ПРОТИСТОЯННЯ

***Анотація. Мета дослідження**: на основі опрацювання і вивчення низки наукових досліджень та праць, які стосуються питань кібератак, проаналізувати виникнення та чинні класифікації сучасних кібератак у глобальному контексті. **Методологія дослідження** ґрунтується на поєднанні принципів науковості, об'єктивності та історизму, загальнонаукових (аналіз, синтез, індукція, дедукція) та спеціально-історичних (історико-гентичний, історико-типологічний, історико-системний, історико-порівняльний) методів. **Наукова новизна** полягає у тому, що у статті розкрито сутність дефініції «кібератака» та її суть як форми глобального протистояння, проведено історичний екскурс, виокремлено основні різновиди поняття. З'ясовано, що кібератаки є багатоплановим і загрозливим феноменом, який впливає на розвиток сучасних держав та ведеться у різних вимірах. **Висновки.** Кібератаки становлять серйозну загрозу для безпеки сучасних держав. Світові актори та ринки по всьому світу витрачають значні ресурси для захисту своїх даних. Вони застосовують різні методи і стратегії, щоб забезпечити стабільність політичних та економічних систем на противагу злочинцям, які поширюють шкідливе програмне забезпечення. Щодня ситуація ускладнюється через появу нових форм кібератак. Тому для попередження негативних наслідків таких дій, необхідний глибший міждисциплінарний аналіз проблеми та наукові напрацювання у цій сфері. Здобутки науковців зможуть сприяти зміцненню національної політики держави у сфері кібербезпеки, створити сприятливі умови для запобігання поширення кібератак, аналізу засобів їх застосування і передусім створення потужної системи захисту інформаційного простору. Досконала система кіберзахисту – це не тільки гарантійне право громадян на отримання якісної й об'єктивної інформації, але і запорука національної безпеки держави.*

***Ключові слова:** кібератака, інформаційна війна, кібербезпека, інформаційні технології, держава.*

CYBERATTACK AS A NEW CONFLICT AND AN IMPORTANT FORM OF GLOBAL CONFLICT

***Abstract. The purpose of the study**: based on the processing and study of a number of scientific studies and works related to cyberattacks, to analyze the emergence and existing classifications of modern cyberattacks in a global context. **The research methodology** is based on a combination of the principles of scientificity, objectivity and historicism, general scientific (analysis, synthesis, induction, deduction) and special-historical (historical-genetic, historical-typological, historical-systemic, historical-comparative) methods. **The scientific novelty** lies in the fact that the article reveals the essence of the definition of «cyberattack» and its essence as a form of global confrontation, conducts a historical excursion, and identifies the main types of the concept. It is found that cyberattacks are a multifaceted and threatening phenomenon that affects the development of modern states and is carried out in different dimensions. **Conclusions**. Cyberattacks pose a serious threat to the security of modern states. Global actors and markets around the world spend significant resources to protect their data. They use various methods and strategies to ensure the stability of political and economic systems in contrast to criminals who spread malicious software. The situation is becoming*

more complicated every day due to the emergence of new forms of cyberattacks. Therefore, to prevent the negative consequences of such actions, a deeper interdisciplinary analysis of the problem and scientific developments in this area are necessary. The achievements of scientists will be able to contribute to strengthening the national policy of the state in the field of cybersecurity, create favorable conditions for preventing the spread of cyberattacks, analyzing the means of their application and, above all, creating a powerful system for protecting the information space. A perfect cyberdefense system is not only a guarantee of citizens' right to receive high-quality and objective information, but also a guarantee of the national security of the state.

Keywords: *cyberattack, information warfare, cybersecurity, information technology, state.*

Постановка проблеми. Сьогодні Україна переживає найважчі часи своєї історії – стан повномасштабної війни. Війна яка розпочалася із нападу Росії на Україну ведеться не тільки на полі бою, але і через комп'ютерні програми із використанням кібератак. Правила ведення війни суттєво змінилися, оскільки кібератаки стають значно ефективнішими за військові протистояння.

Розвиток суспільства в епоху інформаційних технологій, процеси глобалізації мають не тільки позитивний характер, їх використання для ведення інформаційних війн ведуть до послаблення суверенітету національних держав і мають руйнівний характер для людської цивілізації.

Основним засобом для ведення інформаційних війн сьогодні є саме кібератаки. В останні роки словосполучення «кібератака» стало одним із найчастіше вживаних у науковому та журналістському дискурсі. Кількість публікацій, що досліджують природу кібератак, зростає в геометричній прогресії, але при цьому не досягається узагальнення цього поняття, немає концептуальної теорії кібератак. Навпаки, розмивається сам термін, виникають численні трактування і концепції і з часом ця проблема стає більш значущою.

У сучасній науці існує необхідність обґрунтування та правомірного використання самого терміна «кібератака», дослідження саме російської кібервійни в Україні, з'ясування пливу російських кібератак на європейську безпеку та пошук спільного меседжу у міжнародному співробітництві щодо встановлення кібербезпеки.

Аналіз останніх досліджень і публікацій. При написанні статті було опрацьовано дослідження науковців з питань кібератак. Серед таких робіт можна виділити праці Ю. Завгородньої (Завгородня, 2023), В. Кононенка, С. Здоровко та А. Корольова (Кононенко, Здоровко, Корольова, 2023) та інших, які досліджують проблему кібератак із різних ракурсів. С. Федонюк вивчає аспекти міжнародної безпеки кіберпростору (Федонюк, 2022). М. Тєтєвін ділиться досвідом України в галузі міжнародного співробітництва та кібербезпеки (Тєтєвін, 2024).

Використано деякі нормативно-правові акти, які регулюють питання кібербезпеки (Закон України «Про основні засади забезпечення кібербезпеки України», 2017), (Указ Президента України «Про Стратегію кібербезпеки України», 2021).

Опрацьовано низку інтернет-ресурсних джерел, які висвітлюють питання кібератак (Основні типи кібератак, 2024), (Garnet.team, 2024) (Атака «людина посередині», 2024), (Секрети чистої пошти, 2024), (Інформаційна система ІТС, 2023) тощо.

Мета статті – представити результати дослідження кібератак як частини інформаційної війни та складової зовнішньополітичного курсу сучасних агентів впливу у глобальному масштабі.

Виклад основного матеріалу. Усі сфери життєдіяльності суспільства сучасності перебувають у безперервному процесі інтенсивної інформатизації як запоруки соціально-економічного, інтелектуального та духовного розвитку людства. Водночас спостерігається розвиток нових суспільних відносин, названих інформаційними війнами. Особливої актуальності інформаційна складова набула після повномасштабного вторгнення ворога на територію нашої держави як ключовий елемент гібридної війни проти України. Інформаційна безпека стає пріоритетним напрямом державної політики, зокрема як суттєва складова протидії інформаційним загрозам.

Основною загрозою об'єктам інформаційної інфраструктури – інформаційно-телекомунікаційним системам є кібератаки. Закон України «Про основні засади забезпечення кібербезпеки» трактує кібератаку як «спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту» (Закон України «Про основні засади забезпечення кібербезпеки України», 2017).

Винайдення комп'ютера та історія комп'ютеризації сягає у минуле століття (1943). Безумовно, що питання кібератак у цей час взагалі не виникали в силу обмеженого доступу суспільства до електронних машин та відсутності інтернет-мережі, що унеможливлювало виникнення реальних загроз. Проте прогнозування можливості зловживань у сфері комп'ютерних технологій мали місце. Так, американський вчений Джон фон Нейман уперше у 1949 р. оприлюднив теорію щодо комп'ютерних вірусів.

Можна вважати, що лише з 1970-х рр. розпочалася ера кібербезпеки. В цей період фіксується поява інтернет-вірусів, що вимагало певного реагування державних структур через створення спеціальних систем запобігання та захисту. Першим таким заходом стала мережа агентств передових дослідницьких проєктів (ARPANET). У 1980-х р. почастішали атаки, зокрема напади на National CSS, AT&T і Національну лабораторію Лос-Аламоса. Терміни «троянський кінь» і «комп'ютерний вірус» стали відомі також у 80-ті рр. Хробак Морріса 1988 р. став тривожним сигналом, продемонструвавши потенційні масштаби кібератак.

У 1990-х рр. відбувається швидкий розвиток як цивілізаційного становлення інформаційних потоків, так і небезпек, які набувають політичної цінності, оскільки коли небезпека глобалізується, а система захисту не ефективна, приходить розуміння потреби політичного впливу у формі міждержавних політичних рішень (Завгородня, 2023, с. 43).

Усе частіше науковці почали звертати увагу на дефініцію «кібервійна», яку сьогодні визначають як «продовження політики діями, що здійснюються

в кіберпросторі державними суб'єктами (або недержавними суб'єктами зі значною державною підтримкою), які становлять серйозну загрозу безпеці іншої держави, або діями такого ж характеру, що здійснюються у відповідь на серйозну загрозу безпеці держави (реальну або уявну)» (Shakarian, Shakarian, & Ruef, 2013, p. 7).

2020 р. був рекордним за кількістю кібератак. Це пояснюється застосуванням нових технологій, таких як машинне навчання й штучний інтелект, а також посиленням корупційної співпраці між хакерськими групами й представниками державних органів влади. Дуже стрімко зростає активність груп, що фінансуються державами й організованою злочинністю (Федонюк, 2022, с. 11).

З кожним роком збитки від кіберзлочинності зростають у геометричній прогресії і вимірюються десятками трлн доларів. За прогнозами експертів – кількість кібератак однозначно буде збільшуватися і перетвориться на глобальну проблему людства.

Лідерами у сфері поширення кібератак у XXI ст. стала Росія. Особливо велика кількість російських кібератак припадала на кінець 2021 р., і це були передвісники початку повномасштабного вторгнення в Україну. Дослідниця Ю. Завгородня, аналізуючи війну в Україні наголошує, що зараз відбувається перша світова кібервійна (Завгородня, 2022, с. 104).

Інститут AV-TEST щодня реєструє понад 350 000 нових шкідливих програм та потенційно небажаних програм (PUA – potentially unwanted application). Кількість нових штамів вірусів перевищує 140 млн щороку.

Класифікація кібератак за певними ознаками є досить широкою та динамічною. Науковці у сфері кібербезпеки подають доволі багато класифікацій кібератак. Більшість дослідників переконані, що усі кібератаки в основному здійснюються за допомогою: технічних засобів (шпигунське устаткування (кейлогери (keylogger), аналізатори бездротових пакетів), апаратні закладки, генератори та боєприпаси електромагнітного імпульсу тощо); програмних засобів (бот-мережі, трояни, віруси, хробаки, експлойти, руткіти, бекдори, програми підбору паролів, шпигунські програми, сніфери).

Єдиної думки щодо класифікації кібератак не існує. За різними критеріями кібератаки поділяються на різні види. Розглянемо деякі з них.

За характером їх поділяють на:

- пасивні;
- умовно-пасивні;
- активні.

Пасивна дія кібератаки може лише порушити політику безпеки Інформаційно-технологічного супроводу (ІТС – найповніший інформаційний ресурс для людей, які працюють з програмами для автоматизації бізнесу) (Garnet.team, 2024).

Активна кібератака має за мету нанести прямі збитки ІТС, порушує конфіденційність, цілісність і доступність інформації, а також виводять із ладу комп'ютерні комунікації і здійснюють психологічні впливи на користувачів ІТС.

Умовно-пасивні кібератаки спрямовані на ведення комп'ютерної розвідки і подолання системи захисту ІТС.

Найчастіше фахівці використовують класифікацію кібератак за метою здійснення інформаційно-технічного впливу, яка має чітку мету:

- виведення з ладу об'єктів інформаційної інфраструктури; блокування доступу до інформаційних ресурсів;
- прослуховування інформаційних каналів;
- несанкціонований доступ до інформаційних ресурсів;

• контроль інформаційного простору.

Атаки на відмову в обслуговуванні (denial of service) (Gridinsoft, 2024) ставлять метою змусити сервер не відповідати на запити. Такий вид атаки не передбачає отримання деякої секретної інформації, але іноді буває підмогою в ініціалізації інших атак.

Аналізатори протоколів (sniffers) – досить поширений вид атаки, заснований на роботі мережної карти в режимі promiscuous mode, а також monitor mode для мереж Wi-Fi. У такому режимі всі пакети, отримані мережною картою, пересилаються на обробку спеціальному додатку, званому сніффером (Слободяник, 2023). У результаті зловмисник може отримати значну кількість службової інформації: хто, звідки і куди передавав пакети, через які адреси ці вони проходили. Найбільшою небезпекою такої атаки є отримання самої інформації, до прикладу, логінів і паролів співробітників, які можна використовувати для незаконного проникнення у систему під виглядом звичайного співробітника компанії.

Mailbombing (спам e-mail) вважається найстарішим методом атак, хоча суть його проста і примітивна: значна кількість поштових повідомлень роблять неможливими роботу з поштовими скриньками, а іноді і з цілими поштовими серверами (Секрети чистої пошти, 2024). Для цієї мети було розроблено безліч програм, і навіть недосвідчений користувач міг зробити атаку, вказавши лише e-mail жертви, текст і кількість необхідних повідомлень. Такі програми дозволяють ховати реальний IP-адрес відправника, використовуючи для розсилки анонімний поштовий сервер. Такій атаці складно запобігти, тому що навіть поштові фільтри провайдерів не можуть визначити реального відправника спаму.

Man-in-the-Middle («людина посередині») – вид атаки, коли зловмисник перехоплює канал зв'язку між двома системами, і отримує доступ до всієї інформації, що передається. При отриманні доступу на такому рівні зловмисник може модифікувати інформацію у потрібний йому спосіб, щоб досягти своєї мети. Мета такої атаки – незаконне отримання, крадіжка або фальсифікування переданої інформації, або ж отримання доступу до ресурсів мережі (Атака «людина посередині», 2024). Такі атаки вкрай складно відстежити, оскільки зазвичай зловмисник перебуває всередині організації.

SQL ін'єкції – один із найпоширеніших методів атаки на комп'ютерні системи. Хакер вводить шкідливий код у систему для її дестабілізації та подальшого контролю. Коли доступ отримано, зловмисники крадуть облікові дані, паролі, паспортні дані, надалі можуть продовжувати керувати системою та заважати її роботі (Основні типи кібератак, 2024). Для захисту потрібно обирати захищені мережі, вмикати двофакторну аутентифікацію.

Спуфінг (підробка) – кібератака, яка використовує людську неуважність. Злочинці надсилають користувачам листи від служб підтримки соціальних мереж, банків, поліції та інших довірених послуг. Після відкриття листа хакери отримують доступ до даних користувачів (логін / пароль, фінансові облікові дані тощо). Суттєвим є те, що спуфінг нерозривно пов'язаний з фішингом (виманювання особистих даних, паролів, банківської інформації з метою шахрайства). Для бізнесів це небезпечно, бо через одного працівника злочинці можуть отримати доступ до корпоративної системи. Найчастіше використовуються фальшиві сторінки зі схожими доменами, щоб неуважний користувач перейшов за посиланням та «злив» свої дані (Основні типи кібератак, 2024).

Перелік видів та форм кіберзагроз та кібератак є далеко невичерпним, зазнає постійних змін та трансформацій. Україна зіткнулася зі значними викликами у сфері кібербезпеки, особливо з урахуванням її геополітичної ситуації. Наша країна стала частим об'єктом кібератак з боку країни – агресора.

Наймасштабнішими кібератаками вважаються:

- 2015: Атака на українську енергосистему, що призвела до відключення електроенергії у сотень тисяч людей. Ця атака є однією з перших відомих атак на енергетичну інфраструктуру.
- 2017: Атака NotPetya, спочатку спрямована на українські системи, швидко поширилася глобально, завдавши шкоди на мільярди доларів.
- 2022: Атака на українські урядові вебсайти та інфраструктуру напередодні повномасштабного російського вторгнення, що включала поширення шкідливого ПЗ та DDoS-атаки.
- 2023: Атака на «Київстар» спричинила зникнення зв'язку у 24 мільйонів абонентів. Її вважають найбільшою у світі хакерською атакою на телеком-інфраструктуру.
- 2024: Атаки на державні реєстри: сайти Національних інформаційних систем та Міністерства юстиції України, спричинили блокування багатьох процесів: реєстрацію бізнесів, роботу податкової, пенсійного фонду, ринку нерухомості.

Найбільшу загрозу для інформаційної безпеки становлять не тільки кібератаки, але і дезінформація в умовах воєнного стану, інформаційна політика країни-агресора, маніпулювання у соціальних мережах та, на нашу думку, особливо небезпечна і водночас актуальна загроза – недостатній рівень медійної культури, медіа- та інформаційної грамотності українців (Шептицька, Ременяк, Захарчин, 2024, с. 40).

З початком гострої фази війни, урядом України було вжито низку заходів для зміцнення своєї кібербезпекової інфраструктури, зокрема створено Національний координаційний центр кібербезпеки та налагоджено співпрацю з міжнародними партнерами для підвищення кіберстійкості.

Кабінетом Міністрів України в травні 2023 року було затверджено Порядок пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (Тєтєвін, 2024, с. 264). А Указ Президента «Про Стратегію кібербезпеки України» спрямований на створення максимально вільного, безпечного, відкритого і стабільного кіберпростору в інтересах захисту прав людини (Указ Президента України «Про Стратегію кібербезпеки України», 2021).

Міжнародною організацією, яка найактивніше працює у сфері інформаційної безпеки, є НАТО. Центр кібербезпеки НАТО, який успішно функціонує у деяких країнах, є структурним підрозділом збройних сил Північноатлантичного альянсу, отримує фінансування від держав-спонсорів та з внесків держав-членів НАТО (Кононенко, Здоровко, Корольова, 2023).

Висновки та перспективи подальших досліджень. Кібератаки є значною проблемою у світі Інтернет-безпеки. Сучасні засоби інформаційного суспільства дають змогу кібер-терористам легко пропагувати свої ідеї, розширювати лави своїх учасників і досягати мети, використовуючи кіберпростір. Світові уряди та бізнес в усьому світі докладають величезних зусиль для захисту своїх даних. Вони використовують різноманітні засоби і методи, щоб підтримувати сталий розвиток як політичних, так і економічних систем, на противагу зловмисникам, які намагаються порушити безпеку та надсилають шкідливе програмне забезпечення. Щодня ситуація погіршується через

появу нових типів зловмисного програмного забезпечення. Тому для того, щоб зрозуміти цілі, мету кібератак, попередити їхні негативні наслідки, необхідний подальший глибокий міждисциплінарний аналіз таких небезпек. Загроза кібератак і поширення кібер-тероризму є фактором прихованого воєнно-політичного тиску і залякування, чинником, що здатен порушити світову і регіональну стабільність і безпеку. Через це на міжнародному рівні повинен здійснюватися моніторинг поширення кібератак та існувати потужна системи кіберзахисту.

Уважаємо, що першочерговим завданням України в інформаційному протистоянні є: створення нормативно-правової бази, розробка комплексного плану безпеки, проведення регулярних аудитів, моніторингу систем захисту, навчання з питань кібергігієни, підвищення медіаграмотності населення, інформаційне волонтерство тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ

Атака «людина посередині». (2023). URL*:* https://question.com.ua/question/1081

Закон України. (2017). *Закон України «Про основні засади забезпечення кібербезпеки України».* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

Інформаційна система ITC. (2024). *URL:* https://garnet.team/support/services/information_system/

Що таке атаки типу «відмова в обслуговуванні» (DDoS)? (2024). *URL:* https://gridinsoft.ua/ddos

Завгородня, Ю. (2023). Історія становлення кібервійни як складової політичного процесу. *Актуальні проблеми політики, 72,* 42–46.

Завгородня, Ю. (2022). Теоретичне усвідомлення сутності поняття «кібервійна» у політичному просторі. *Політичні процеси сучасності: глобальний та регіональні виміри. Збірник матеріалів IV Всеукраїнської науково-практичної конференції*, 103–105.

Основні типи кібератак. (2024). URL: https://volz.ua/news/--

Секрети чистої пошти. (2024). Секрети чистої пошти. Як зупинити спам-атаку в Gmail: 3 простих способи. (2024). *RBC*. URL:https://www.rbc.ua/rus/styler/sekreti-chistoyi-poshti-k-zupiniti-spam-ataku-1727285660.html

Кононенко, В., Здоровко, С., Корольова, А. (2023). Інформаційна безпека як стан. *Науковий вісник Ужгородського Національного університету, Серія: Право, 76,* 244–248.

Слободяник, Д. (2016). *Використання програм-sniffer-ів при досліджуванні мережі*. URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2016/paper/download/859/612

Указ Президента України. (2021). *Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»*. URL: https://zakon.rada.gov.ua/laws/show/447/2021.

Федонюк, С. (2022). *Міжнародні аспекти безпеки кіберпростору: монографія.* Луцьк: Вежа-Друк.

Тєтєвін, М. (2024). Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки. *Науковий вісник Ужгородського Національного університету, Серія: Право, 82,* 263–266.

Шептицька, Л., Ременяк, О., Захарчин, Н. (2024). Досвід інформаційних війн в історії та сучасності як об'єкт досліджень сучасної науки та освіти. *Проблеми*

гуманітарних наук: збірник наукових праць Дрогобицького державного педагогічного університету імені Івана Франка. Серія: Історія. Спецвипуск, 35–43.

Shakarian, P., Shakarian, J., Ruef, A. (2013). Introduction to cyber-warfare: A multidisciplinary approach. *Newnes, 7.*

REFERENCES

Ataka «liudyna poseredyni». (2023). [Man-in-the-middle attack]. URL*:* https://question.com.ua/question/1081 [in Ukrainian].

Zakon Ukrainy. (2017). *Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy»* [The Law of Ukraine «On the Basic Principles of Ensuring Cyber Security of Ukraine»]. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

Informatsijna systema ITS. (2024). [Information system ITS]. URL: https://garnet.team/support/services/information_system/ [in Ukrainian].

Scho take ataky typu «vidmova v obsluhovuvanni» (DDoS)? (2024). [What are denial of service (DDoS) attacks?]. URL: https://gridinsoft.ua/ddos [in Ukrainian].

Zavhorodnya, Yu. V. (2023). Istoriia stanovlennia kibervijny iak skladovoi politychnoho protsesu. [The history of the formation of cyber warfare as a component of the political process]. *Aktual'ni problemy polityky – Current problems of politics, 72,* 42–46. [in Ukrainian].

Zavhorodnia, Yu. (2022). Teoretychne usvidomlennia sutnosti poniattia «kibervijna» u politychnomu prostori. [Theoretical understanding of the meaning of the concept of «cyberwar» in the political space]. *Politychni protsesy suchasnosti: hlobal'nyj ta rehional'ni vymiry. Zbirnyk materialiv IV Vseukrains'koi naukovo-praktychnoi konferentsii – Political processes of our time: global and regional dimensions. Collection of materials of the IV All-Ukrainian Scientific and Practical Conference,* 103–105. [in Ukrainian].

Osnovni typy kiberatak. (2024). [The main types of cyberattacks]. *URL*: https://volz.ua/news/-- [in Ukrainian].

Sekrety chystoi poshty. (2024). *Sekrety chystoi poshty. Yak zupynyty spam-ataku v Gmail: 3 prostykh sposoby* [Secrets of clean email. How to stop a spam attack in Gmail: 3 simple ways]. URL: https://www.rbc.ua/rus/styler/sekreti-chistoyi-poshti-k-zupiniti-spam-ataku-1727285660.html [in Ukrainian].

Kononenko, V., Zdorovko, S., & Korol'ova, A. (2023). Informatsijna bezpeka iak stan [Information security as a special state]. *Naukovyj visnyk Uzhhorods'koho Natsional'noho universytetu, Seriia: Pravo – Uzhhorod National University Herald. Series: Law, 76,* 244–248. [in Ukrainian].

Slobodianyk, D. (2016). Vykorystannia prohram-sniffer-iv pry doslidzhuvanni merezhi [Using sniffer programs for network research] URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2016/paper/download/85-9/612 [in Ukrainian].

Ukaz Prezydenta Ukrainy. (2021). *Ukaz Prezydenta Ukrainy «Pro rishennia Rady natsional'noi bezpeky i oborony Ukrainy «Pro Stratehiiu kiberbezpeky Ukrainy»* [Decree of the President of Ukraine «On the Decision of the National Security and Defense Council of Ukraine "On the Cyber Security Strategy of Ukraine»]. URL: https://zakon.rada.gov.ua/laws/show/447/2021. [in Ukrainian].

Fedoniuk, S. (2022). *Mizhnarodni aspekty bezpeky kiberprostoru: monohrafiia.* [International aspects of cyberspace security: monograph]. Lutsk: Vezha-Druk [in Ukrainian].

Tietievin, M. (2024). Dosvid Ukrainy v haluzi mizhnarodnoho spivrobitnytstva v haluzi kiberbezpeky [Experience of Ukraine in the field of international cooperation in the field of Cyber Security]. *Naukovyj visnyk Uzhhorods'koho Natsional'noho universytetu, Seriia: Pravo – Uzhhorod National University Herald. Series: Law, 82,* 263–266. [in Ukrainian].

Sheptytska, L., Remeniak, O., & Zakharchyn, N. (2024). Dosvid informatsijnykh vijn v istorii ta suchasnosti iak ob'iekt doslidzhen' suchasnoi nauky ta osvity. [The experience of information wars in history and modernity as an object of research in modern science and education]. *Problemy humanitarnykh nauk. Seriia: Istoriia. Spetsvypusk – Problems of the humanities. History Series. Special Issue,* 35–43. [in Ukrainian].

Shakarian, P., Shakarian, J., & Ruef, A. (2013). Introduction to cyber-warfare: A multidisciplinary approach. *Newnes, 7.*

Стаття надійшла до редакції 29 січня 2025 р.
Стаття рекомендована до публікації 21.03.2025.