УДК 351.746:316.77-049.5](477)"364"
DOI https://doi.org/10.32782/2311-8040/2025-2-7

Ніцевич Олеся Володимирівна,
доктор філософії 081 «Право»,
доцент кафедри адміністративно-правових дисциплін
Навчально-наукового інституту права та психології
Національної академії внутрішніх справ;
старший науковий співробітник
відділу організації наукової діяльності
Львівського державного університету внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: https://orcid.org/0009-0004-2346-6812

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

Анотація. *Інформаційна безпека, яка в умовах воєнного стану набуває особливого значення, розглядається як один із пріоритетних напрямів державної політики України, що зосереджена на забезпеченні захисту національних інтересів, збереженні державного суверенітету, територіальної цілісності та гарантуванні безпеки громадян, особливо в умовах масштабної цифровізації суспільства та зростання кіберзагроз.*

З огляду на воєнний стан та зростаючі кіберзагрози масштабна цифровізація та використання інформаційних технологій у поєднанні з великими масивами цифрових даних призвели до критичної ескалації злочинності в інформаційній сфері.

Значне розширення джерел доступу до інформації в умовах стрімкого розвитку цифрових технологій та водночас недостатнього рівня медіаграмотності (медіакультури) супроводжується зменшенням критичності сприйняття інформації, створює підґрунтя для можливих маніпуляцій громадською думкою, що сприяє зростанню впливу дезінформації та деструктивної пропаганди. Некритичне сприйняття інформації створює загрози політичній та економічній стабільності демократичних держав.

Під час повномасштабного вторгнення російської федерації кібератаки є усталеним типом військових операцій і синхронізуються із застосуванням військової сили. Саме це поєднання військової агресії та кібератак має глибокий вплив на цивільне населення, зачіпаючи критичну інфраструктуру.

Державна політика у сфері кібербезпеки має бути націлена на формування безпечного національного кіберпростору, унеможливлення втручання іноземних держав та їхніх атак на об'єкти інфраструктури, зміцнення кібернетичної обороноздатності країни та зменшення вразливості об'єктів кіберзахисту.

Серед ключових стратегічних напрямів правового регулювання інформаційної безпеки в умовах воєнного стану виокремлюється необхідність міжнародної співпраці в рамках євроінтеграції та членства в НАТО з метою підвищення оперативності реагування на актуальні кіберзагрози. Стратегічним пріоритетом правового регулювання інформаційної безпеки в умовах воєнного стану має стати приведення нормативно-правової бази у відповідність до сучасних викликів та налагодження ефективнішої міжвідомчої координації.

Ключові слова: *інформаційна безпека, стратегія інформаційної безпеки, кібербезпека, кіберзагрози, воєнний стан.*

Nitsevych Olesia. Information security of Ukraine under martial law

Abstract. *Information security is a priority area of Ukraine's state policy under martial law, aimed at safeguarding national interests, sovereignty, and the security of its citizens.*

Given the state of war and the growing cyber threats, large-scale digitalization and the use of information technologies in conjunction with vast volumes of digital data have led to a critical escalation of crime in the information sphere.

The significant expansion of sources of access to information amid the rapid development of digital technologies, along with a low level of media literacy (media culture), is accompanied by a decline in the critical perception of information. This creates a basis for possible manipulation of public opinion and contributes to the increasing influence of disinformation and destructive propaganda. The uncritical perception of information poses a threat to the political and economic stability of democratic states.

 ISSN 2311-8040

During the full-scale invasion by the Russian Federation, cyberattacks have become a routine type of military operation, synchronized with the use of military force. This combination of military aggression and cyberattacks has a profound impact on the civilian population, affecting critical infrastructure.

State policy in the field of cybersecurity must be aimed at forming a secure national cyberspace, preventing interference by foreign states and their attacks on infrastructure facilities, strengthening the country's cyber defense capabilities, and reducing the vulnerability of cybersecurity targets.

Among the key strategic areas of legal regulation of information security under martial law is the necessity of international cooperation within the framework of European integration and NATO membership to enhance the responsiveness to current cyber threats. A strategic priority in the legal regulation of information security under martial law should be the alignment of the regulatory framework with modern challenges and the establishment of more effective interagency coordination.

Key words: *information security, information security strategy, cybersecurity, cyber threats, martial law.*

Вступ. Значення безпеки у сучасному суспільстві важко переоцінити. Поняття «безпека» є багатогранним і може розглядатися з різних точок зору, але у загальному сенсі воно означає стан захищеності від будь-яких загроз, небезпек або ризиків, які можуть завдати шкоди, збитків або негативно вплинути на існування, функціонування або розвиток об'єкта безпеки.

Війна кардинально змінює пріоритети та значення багатьох аспектів життя, і безпека стає одним із найважливіших, якщо не найважливішим фактором для виживання, збереження та майбутнього як окремих людей, так і цілої нації.

Використання новітніх технологій, телекомунікаційних систем роблять загальну систему безпеки вразливою щодо посягань на неї. Створюються передумови витоку інформації, можливості технічного впливу на неї з метою формування потрібної суспільної думки та створення можливості фіксувати і передавати стратегічну інформацію ворогу незначними з технічної точки зору зусиллями.

Як зазначають науковці, інформація дозволяє вигравати у війні, не зробивши жодного пострілу, шляхом формування і розпалювання внутрішніх протиріч. Така тактика є характерною для війн нового формату – гібридних, де безпосередньо військовий фактор є лише одним зі складників цілого [1, с. 145]. Гібридні загрози, що комбінують звичайні військові дії з невійськовими інструментами впливу, породжують нові, складні завдання для захисту національної безпеки та незалежності держави.

Відповідно до Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 р. № 685/2021, деструктивна пропаганда, поширення дезінформації як ззовні, так і всередині України застосовуються державою-агресором з метою підриву стійкості суспільства та інформаційної дестабілізації держави. Водночас ефективна система реагування на такі виклики в Україні досі не створена, не забезпечено функціонування розвиненої національної інформаційної інфраструктури, що обмежує можливість належним чином протидіяти інформаційній агресії з метою захисту національної безпеки та реалізації національних інтересів України [2].

Інформаційна безпека є питанням виживання людини, суспільства та держави. Адже забезпечення інформаційної безпеки визначається не тільки інтересами держави, а й інтересами особи в контексті забезпечення її прав і свобод. Основою сучасної інформаційної безпеки є цілісність даних, доступність інформації, конфіденційність і надійність її збереження [3, с. 122].

Матеріали та методи. Матеріалами для проведення дослідження слугували нормативно-правові акти України у сфері національної безпеки, інформаційної безпеки та кібербезпеки, а також наукові публікації українських і зарубіжних дослідників, присвячені проблемам протидії кіберзагрозам в умовах гібридної війни. Основу теоретичного аналізу становлять праці таких науковців, як В.Б. Авер'янов, О.М. Бандурка, В.М. Бесчастний, С.А. Вавренюк, Ю.О. Виноскуров, В.Д. Гавловський, В.М. Горовий, В.О. Голубєв, Р.А. Калюжний, А.Т. Комзюк,

М.І. Корнієнко, Н.В. Лесько, В.Я. Малиновський, О.С. Онищенко, В.В. Остроухов, Р.М. Пилипів, Є.Д. Скулиш, О.С. Проневич, В.С. Цимбалюк, О.Н. Ярмиш, та інших, які здійснювали дослідження у сфері інформаційної безпеки в умовах збройного конфлікту.

У межах дослідження використовувалися як загальнонаукові, так і спеціально-юридичні методи. Зокрема, застосовано метод системного аналізу для дослідження комплексної природи інформаційної безпеки як складової частини національної безпеки, а також для встановлення взаємозв'язку між законодавчими нормами, інституційними механізмами та реальними загрозами в інформаційному просторі.

Формально-юридичний метод був застосований для аналізу чинних нормативно-правових актів, що регулюють сферу інформаційної та кібербезпеки, з метою з'ясування їх змісту, структури та правозастосовної практики. Метод порівняльно-правового аналізу дав змогу зіставити українське законодавство із відповідними міжнародними стандартами, зокрема положеннями Будапештської конвенції та Конвенції ООН проти кіберзлочинності.

Також використовувалися методи дедукції, індукції, логіко-семантичного аналізу для формулювання теоретичних висновків і обґрунтування пропозицій щодо вдосконалення державної політики у сфері інформаційної безпеки. На основі узагальнення наукових підходів сформульовано авторське бачення ключових напрямів правового регулювання у цій сфері в умовах воєнного стану.

Результати. Національна безпека визначається як багатокомпонентне явище, що відображає стан захищеності життєво важливих інтересів особи, суспільства та держави від реальних та потенційних загроз [4]. Її складовою частиною є інформаційна безпека.

Прийняття законів України «Про інформацію» (1992 р.), «Про захист інформації в інформаційно-телекомунікаційних системах» (1994 р.), «Про кібербезпеку України» (2017 р.), «Про національну безпеку України» (2018 р.), та стратегічних документів, включаючи Стратегію національної безпеки України (2020 р.), Стратегію інформаційної безпеки (2021 р.), Стратегію кібербезпеки (2021 р.), Стратегію забезпечення державної безпеки (2022 р.), створило фундамент для розгалуженої системи інформаційної безпеки України, під якою розуміють стан захищеності життєво важливих інтересів особи, суспільства та держави, за якого досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний тощо). При цьому сторонні інформаційні впливи не завдають їм суттєвої шкоди [5, с. 11].

Інформаційна безпека є станом захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, наявна ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [2].

Значне розширення джерел доступу до інформації в умовах стрімкого розвитку цифрових технологій та водночас недостатнього рівня медіаграмотності (медіакультури) супроводжується зменшенням критичності сприйняття інформації, створює підґрунтя для можливих маніпуляцій громадською думкою, що сприяє зростанню впливу дезінформації та деструктивної пропаганди. Некритичне сприйняття інформації створює загрози політичній та економічній стабільності демократичних держав.

Зростаючі обсяги інформаційних ресурсів, що знаходяться в доступі, у сучасних інформаційних обмінах використовуються потенційним противником для посилення стресових ситуацій, паніки та дезорганізації серед громадян країни – об'єкта інформаційної агресії [6, с. 9].

ISSN 2311-8040

З огляду на воєнний стан та зростаючі кіберзагрози масштабна цифровізація та використання інформаційних технологій у поєднанні з великими масивами цифрових даних призвели до критичної ескалації злочинності в інформаційній сфері. В умовах кіберпротистояння та активних воєнних дій ця зростаюча загроза інформаційних атак спричинила значне збільшення суспільно небезпечних діянь та породила нові, вкрай серйозні вразливості важливих об'єктів, від стабільного функціонування яких залежить обороноздатність та життєдіяльність країни.

Відповідно до Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 р. № 447/2021, забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету здійснюється шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури [7].

Під час повномасштабного вторгнення російської федерації кібератаки є усталеним типом військових операцій і синхронізуються із застосуванням військової сили. Саме це поєднання військової агресії та кібератак має глибокий вплив на цивільне населення, зачіпаючи критичну інфраструктуру [8, с. 6].

Кібератаки під час війни були розгорнуті з метою знищення баз даних і систем, порушення роботи критично важливої інфраструктури, контролю інформаційного простору, вилучення значних обсягів персональних даних, проведення розвідки та шпигунства, а також здійснення операцій впливу (включаючи дезінформаційні кампанії з метою підриву довіри до публічної влади та дискредитації України). Це:

1) деструктивні атаки – кібератаки, спрямовані на безповоротне видалення даних або пошкодження систем, що робить їх невідновлюваними. Ці атаки можуть мати довготривалі наслідки для організацій, якщо вони не можуть відновити резервні копії. Прикладами є шкідливе програмне забезпечення для стирання даних, спрямоване на державні установи та інші сектори;

2) руйнівні DDoS кібератаки – атаки, які мають на меті не просто тимчасово вивести з ладу вебсайт або сервіс, а завдати значної та довготривалої шкоди. Вони характеризуються надзвичайно великим об'ємом шкідливого трафіку, який генерується з величезної кількості скомпрометованих пристроїв (ботнетів). Цей трафік спрямовується на ціль, перевантажуючи її сервери та мережеву інфраструктуру до повного виснаження ресурсів;

DDoS-атаки становлять 87,5% усіх кібератак, зареєстрованих Інститутом кібермиру (CyberPeace Institute) [8, с. 8]. Найбільше атак було спрямовано на фінансовий, державний та сектор інформаційно-комунікаційних технологій.

3) перетворення інформації на зброю – це кібератаки, що призводять до крадіжки та вилучення даних (копіювання та переміщення даних на контрольовані зловмисниками сервери), шпигунство (отримання несанкціонованого доступу до інформації для збору розвідувальних даних про діяльність), моніторинг дій користувачів та збір інформації про інфраструктуру, системи безпеки для майбутніх атак;

4) дезінформація – це інформаційні операції, спрямовані на поширення неправдивої, спотвореної або маніпулятивної інформації з метою введення в оману, впливу на громадську думку, підриву довіри до певних інституцій або осіб, а також для досягнення політичних, економічних чи соціальних цілей. Це створення фейкових вебсайтів новин; масове розсилання електронних листів з неправди-

вою інформацією або фішинговими посиланнями, що ведуть на дезінформаційні ресурси; поширення діпфейків, які створюються або змінюються за допомогою штучного інтелекту. Як зазначає В.М. Горовий, розробляються спеціальні технології, що підвищують ефективність інформаційних каналів, посилюють маніпулятивні впливи на аудиторію користувачів. Також формується чітка диференціація об'єктів впливу та охоплення масштабних аудиторій, зменшується здатність об'єктів впливу блокувати інформацію, організовувати протидію небажаній інформації в мережі [9, с. 108].

Стратегія кібербезпеки України окреслює такі загрози кібербезпеці України:

1) гібридна агресія російської федерації проти України у кіберпросторі. Держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки російської федерації спрямовані насамперед на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності;

2) кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо;

3) організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності. Особливостями таких кібератак є їх тривалість, складність та прихований характер, що ускладнює їх попередження, виявлення та нейтралізацію;

4) використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності [7].

Сучасні загрози інформаційній безпеці мають транскордонний характер, виходячи далеко за межі України. Їхній вплив не обмежується внутрішньою територією держави, а сягає глобальних масштабів, спричиняючи серйозні наслідки на міжнародному рівні.

Необхідність зміцнення міжнародної співпраці для ефективного реагування на еволюцію гібридних загроз обговорюється науковою спільнотою [10, с. 173]. Кіберпростір не має фізичних кордонів. Країни часто розробляють власні стратегії кібербезпеки, засновані виключно на своїх ідеалах та уявленнях про безпеку. Це призводить до існування різних підходів до забезпечення безпеки в інформаційному просторі в різних країнах. Тому в умовах постійних кібератак, спрямованих проти України, міжнародна співпраця є критично важливим фактором для забезпечення стійкості національного кіберпростору та захисту від зовнішніх загроз. Це дає можливість обмінюватися позитивним досвідом, інформацією про загрози, отримувати та координувати технічну, фінансову допомогу.

Україні необхідно враховувати міжнародний досвід під час формування державної політики та створення національної правової та організаційної бази для захисту кібербезпеки, особливо в умовах гібридної війни [11, с. 197].

ISSN 2311-8040

Міжнародно-правовим стандартом у сфері кіберзлочинності вважається Конвенція про кіберзлочинність (Будапештська конвенція), прийнята Комітетом міністрів Ради Європи 23 листопада 2001 р. [12]. Вона стала першим міжнародним договором, спрямованим на боротьбу із кримінальними правопорушеннями, вчиненими за допомогою комп'ютерних систем та мережі Інтернет.

Значним кроком міжнародного співробітництва у боротьбі з кіберзлочинністю та пов'язаними з нею кримінальними правопорушеннями є прийняття резолюції Генеральної асамблеї ООН № 79/243 від 27 грудня 2024 р. «Конвенція Організації Об'єднаних Націй проти кіберзлочинності» [13]. Вона створює спільну правову основу для міжнародної співпраці, що є необхідною умовою для ефективного протистояння транснаціональним кіберзагрозам. Універсальний характер Конвенції сприятиме гармонізації національного законодавства та покращенню координації між правоохоронними органами різних країн.

Закон України «Про основні засади забезпечення кібербезпеки України» [14] визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки. Відповідно до ст. 5 зазначеного Закону координація діяльності у сфері кібербезпеки як складника національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та загальний контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку. Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних сил України, розвідувальні органи України, Національний банк України, Міністерство закордонних справ України.

Значна кількість суб'єктів національної системи кібербезпеки ускладнює ефективний обмін інформацією про загрози, правопорушення та передовий досвід. Забезпечення ефективної взаємодії та координації між цими численними органами є ключовим для створення стійкої та дієздатної національної системи кібербезпеки України, здатної ефективно протистояти сучасним та майбутнім кіберзагрозам, особливо в умовах воєнного стану.

Науковий аналіз кібербезпеки також підкреслив необхідність посилення міжвідомчої координації для ефективного реагування на еволюцію гібридних загроз [10, с. 173].

Важливе місце у національній системі кібербезпеки належить Національній поліції України, яка забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, кримінальних правопорушень проти об'єктів критичної інформаційної інфраструктури; здійснює заходи з інформування громадян про безпеку в кіберпросторі [14].

Висновки. Інформаційна безпека залишається пріоритетним напрямом державної політики України в умовах воєнного стану, спрямованим на захист національних інтересів, суверенітету та безпеки громадян. В умовах війни ефективна політика інформаційної безпеки має базуватися на гнучкості, адаптивності та проактивному підході. Це передбачає постійний моніторинг інформаційного простору, аналіз нових загроз, розробку та оперативне оновлення стратегій і технологій.

Державна політика у сфері кібербезпеки має бути націлена на формування безпечного національного кіберпростору, унеможливлення втручання іноземних держав та їхніх атак на інфраструктурні об'єкти, зміцнення

кібернетичної обороноздатності країни та зменшення вразливості об'єктів кіберзахисту.

Серед ключових стратегічних напрямів правового регулювання інформаційної безпеки в умовах воєнного стану виокремлюється необхідність міжнародної співпраці в рамках євроінтеграції та членства в НАТО з метою підвищення оперативності реагування на актуальні кіберзагрози.

Стратегічним пріоритетом правового регулювання інформаційної безпеки в умовах воєнного стану має стати приведення нормативно-правової бази у відповідність до сучасних викликів та налагодження ефективнішої міжвідомчої координації, що виключить конфліктність між військовими та цивільними підходами до національної стратегії інформаційної безпеки.

Список використаних джерел:

1. Котерлін І.Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 1. С. 145–150.

2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 грудня 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

3. Смотрич Д.В., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету*. *Серія «Право».* 2023. Випуск 77, частина 2. С. 121–127.

4. Про національну безпеку : Закон України від 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

5. Інформаційна безпека : підручник / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін. ; під ред. В.В. Остроухова. Київ : Видавництво Ліра-К, 2021. 412 с.

6. Горовий В.М. Інформаційні можливості нейтралізації стресових явищ серед українського населення в умовах особливого періоду. *Інформаційна безпека людини, суспільства, держави.* 2022. № 1–3 (34–36). С. 6–13.

7. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

8. Duguin S., Pavlova P. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. Policy Department, Directorate-General for External Policies. European Union. 2023. 47 s.

9. Горовий В.М. Інформаційні фактори розвитку постіндустріального суспільства : монографія. Київ : НАН України, Нац. б-ка України ім. В.І. Вернадського, 2024. 180 с.

10. Balan S., Balan L., Vorotynskyy V., Rybak I., Tarasiuk V. State information policy in the context of hybrid threats: Legal and political aspects. *Social & Legal Studios*. 2025. Volume 8, No. 1. Pp. 166–177.

11. Semenenko O., Dobrovolskyi U., Sliusarenko M., Levchenko I., Mytchenko S. Legal aspects of the cybertechnology development and the cyberweapon use in the state defence sphere: Global and Ukrainian experience. *Social & Legal Studios*. 2023. Volume 6, No. 4. Pp. 192–199.

12. Конвенція про кіберзлочинність від 23 листопада 2001 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

13. Конвенція Організації Об'єднаних Націй проти кіберзлочинності від 27 грудня 2024 р. URL: https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf.

14. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

References:

1. Koterlin, I.B. (2022). Informatsiina bezpeka v umovakh voiennoho stanu u aspekti zabezpechennia informatsiinykh prav ta svobod [Information security under martial law in the context of ensuring information rights and freedoms]. *Aktualni problemy vitchyznianoi yurysprudentsii – Actual Problems of Domestic Jurisprudence*. № 1. S. 145–150 [in Ukrainian].

2. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 r. "Pro Stratehiiu informatsiinoi bezpeky": Ukaz Prezydenta Ukrainy [On the decision of the National Security and Defense Council of Ukraine "On the Information Security Strategy"] vid 28 hrudnia 2021 r. № 685/2021. Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021#Text [in Ukrainian].

3. Smotrych, D.V., Brailko, L. (2023). Informatsiina bezpeka v umovakh voiennoho stanu [Information security under martial law]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia "Pravo" – Scientific Bulletin of Uzhhorod National University. Law Series*. Vypusk 77: chastyna 2. S. 121–127 [in Ukrainian].

4. Pro natsionalnu bezpeku: Zakonu Ukrainy [*On National Security: Law of Ukraine*] vid 21 chervnia 2018 r. № 2469-VIII. Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian].

5. Informatsiina bezpeka: pidruchnyk [*Information security: Textbook*]. / V.V. Ostroukhov, M.M. Prysiazhniuk, O.I. Farmahei, M.M. Chekhovska ta in.; pid red. V.V. Ostroukhova. Kyiv: Vydavnytstvo Lira-K, 2021. 412 s. [in Ukrainian].

6. Horovyi, V.M. (2022). Informatsiini mozhlyvosti neitralizatsii stresovykh yavyshch sered ukrainskoho naselennia v umovakh osoblyvoho periodu [Information capabilities to neutralize stress phenomena among the Ukrainian population under special conditions]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy – Information Security of the Individual, Society, and the State*. № 1–3 (34–36). S. 6–13 [in Ukrainian].

7. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 r. «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy [*On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"*] vid 26 serpnia 2021 r. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text [in Ukrainian].

8. Duguin, S., Pavlova, P. (2023). The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. Policy Department, Directorate-General for External Policies. European Union. 47 s. [in English].

9. Horovyi, V.M. (2024). Informatsiini faktory rozvytku postindustrialnoho suspilstva: monohrafiia [*Informational factors in the development of post-industrial society: Monograph*]. Kyiv: NAN Ukrainy, Nats. b-ka Ukrainy im. V.I. Vernadskoho, 180 s. [in Ukrainian].

10. Balan, S., Balan, L., Vorotynskyy, V., Rybak, I., Tarasiuk, V. (2025). State information policy in the context of hybrid threats: Legal and political aspects. *Social & Legal Studios*. Volume 8, No. 1. Pp. 166–177 [in English].

11. Semenenko, O., Dobrovolskyi, U., Sliusarenko, M., Levchenko, I., Mytchenko, S. (2023). Legal aspects of the cybertechnology development and the cyberweapon use in the state defence sphere: Global and Ukrainian experience. *Social & Legal Studios*. Volume 6, No. 4. Pp. 192–199 [in English].

12. Konventsiia pro kiberzlochynnist [*Convention on Cybercrime*] vid 23 lystopada 2001 r. Retrieved from: https://zakon.rada.gov.ua/laws/show/994_575#Text.

13. Konventsiia Orhanizatsii Obiednanykh Natsii proty kiberzlochynnosti [*UN Convention on Cybercrime*] vid 27 hrudnia 2024 r. Retrieved from: https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf [in Ukrainian].

14. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovtnia 2017 r. № 2163-VIII. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].