УДК 004.056-027.543:328.16
DOI https://doi.org/10.32782/2312-1815/2025-21-23

Ярослав Лелет
ORCID: 0009-0005-8602-8446

МЕХАНІЗМИ ТА ФОРМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ КРИЗИ

У статті з'ясовано суть поняття «інформаційна безпека». Узагальнено погляди науковців на суть даного поняття та особливості соціальної безпеки на державному та регіональному рівнях. Розглянуто важливість належного забезпечення захисту інформаційного простору в умовах кризи та війни.

Розглянуто питання механізмів та форм забезпечення інформаційної безпеки в умовах кризи. Проблема інформаційної безпеки є надзвичайно важливою та потребує першочергової уваги.

Метою статті є визначення та характеристика механізмів і форм забезпечення інформаційної безпеки в умовах воєнно-політичного конфлікту.

Ключові слова: *інформаційна безпека, національна безпека, криза, війна.*

Вступ. Інформація є невід'ємною частиною життя людини. Як зауважують українські дослідники С. Обрембальський та Л. Чистоклетов, людина є своєрідною сукупністю інформації. Інформація супроводжує людину всюди: на роботі, вдома, у ресторані. Завдяки інформації ми отримуємо важливі повідомлення, навчаємося і вчимося жити. Утім, інформація у різних руках може по-різному використовуватися. Вона може нести як користь, так і завдати шкоди.

Найактивніше інформація використовується на рівні держав, адже для встановлення міжнародних відносин, дипломатичних стосунків, а також висловлення своєї позиції завжди використовується інформація.

Будь-які кризи, конфлікти та війни важко уявити без інформаційного складника. Сучасні війни вже давно перейшли у фазу гібридних, де володіння інформацією у власних цілях відіграє чималу роль. Тому щоб перемогти у війні, необхідна не лише військова перевага, а й володіння інформаційними впливами та ресурсами.

В умовах війни держави використовують інформацію на свій розсуд, і часто буває так, що її спотворення може призвести до вкрай негативних наслідків. Не дарма британський банкір Натан Ротшильд свого часу говорив: «Хто володіє інформацією, той володіє світом». Пізніше ця фраза стала крилатою після цитування прем'єр-міністром Великобританії Вінстоном Черчиллем.

Під час кризи чи війни інформація стає не лише інструментом сповіщення населення про стан справ, а й переростає у зброю, засіб виживання та впливу.

Оперативне сповіщення може зіграти ключову роль у стійкості та єдності суспільства, коли дезінформація та фейки, навпаки, дестабілізують ситуацію в країні та покликані сіяти розбрат усередині держави.

З огляду на це, кожна країна повинна дбати про інформаційну безпеку на всіх щаблях влади – від найнижчого до найвищого, адже це взаємопов'язані структури.

В умовах війни контроль, критичність, достовірність та оперативність набувають найвизначнішого значення.

Проблему інформаційної безпеки в умовах воєнно-політичного конфлікту розглядають Л. Браілко, О. Воланюк, Р. Драпушко, К. Захаренко, Л. Коваленко, В. Кротюк, Л. Мазуренко, Є. Міненко, Д. Смотрич.

Слід звернути увагу на те що К. Захаренко, Є. Міненко, О. Воланюк та Р. Драпушко розглядали інформаційну безпеку крізь призму суспільно-політичної стабільності, що є невід'ємним складником інформаційної системи держави.

Питанню інформаційної безпеки держави свої наукові статті присвятили І. Ломка, О. Липчук, Ю. Кобець, а також С. Обрембальський та Л. Чистоклетов.

Проблематика зарубіжного досвіду забезпечення інформаційної безпеки держави стала об'єктом наукового розгляду О. Пугачова. У своїй статті він розглянув досвід , Німеччини, Польщі та Угорщини та їхню політику інформаційної безпеки.

Військовий компонент, який прямо впливає на інформаційну безпеку держави, вивчали науковці Л. Коваленко, В. Кротюк, Л. Мазуренко, С. Обрембальський, С. Присяжнюк, Л. Чистоклетов, К. Шевченко та ін.

Результати та обговорення. Інформаційна безпека є невід'ємним складником цілісної національної безпеки держави, тому передусім слід визначити термін «інформаційна безпека» і що вона собою являє, адже це дасть змогу краще та всебічно дослідити проблему механізмів та форм забезпечення інформаційної безпеки держави.

Так, українська науковиця Л. Мазуренко трактує інформаційну безпеку як певний достатній рівень інформаційної культури особистості, а також розглядає її крізь призму спроможності держави створити необхідні умови для розвитку та задоволення потреб індивідів в інформації [10, с. 51].

Її колеги Є. Міненко, К. Захаренко, Р. Драпушко, О. Воланюк, синтезуючи всю зарубіжну та вітчизняну наукову думку, дійшли висновку, що інформаційна безпека є фундаментальним елементом національної безпеки, що окрім автономних сфер є інтегральною та всеохоплюючою характеристикою, яка у цілому впливає на громадянську, соціальну та національну сфери. Науковці доводять, що ключовим аспектом інформаційної безпеки стан захищеності інформаційного простору [16, с. 43].

Слід додати, що Д. Смотрич та Л. Браілко слушно зауважують, що держави завдяки інформації нерідко виграють політичні конфлікти чи війни без єдиного пострілу. Задля таких перемог суб'єкти міжнародної політики можуть розпалювати внутрішні протиріччя, не вторгаючись на територію іншої держави [15, с. 122].

Інформаційна безпека, відповідно до позиції Л. Кочубей, розглядається як стан інформаційної озброєності держави, суспільства та зокрема особи [10, с. 51].

Представник української наукової думки В. Гурковський розглядає інформаційну безпеку України в контексті суспільних відносин, що пов'язані із захистом життєво необхідних важливих інтересів людини, громадянина та держави від потенційних інформаційних загроз у інформаційному просторі [16, с. 43].

Згідно з позицією І. Ломаки, Ю. Кобець та О. Липчук, інформаційна безпека визначається сукупністю певних методів і засобів підтримки й захисту інформації від випадкового чи навмисного впливу. Водночас в обох випадках власник інформації (це може бути як держава, так і бізнес чи фізична особа) зазнає тих чи інших збитків [11].

На нашу думку, в умовах кризи, а особливо війни, ключовими у забезпеченні інформаційної безпеки є оперативність, достовірність, координація, законодавча гнучкість, а також єдність суспільства в контексті інформації.

Л. Чистоклетов та С. Обрембальський слушно зауважують, що життя в Україні, у тому числі в інформаційному плані, здавалося відносно безпечним до лютого 2022 р. Після початку повномасштабного вторгнення Україна, на думку дослідників, була змушена переглянути

підходи до інформаційної безпеки власної держави. Ці заходи здійснювалися з огляду на військову, політичну, економічну, релігійну, культурну та інформаційну небезпеку, що несла за собою війна, розпочата російською федерацією [19, с. 4].

Досліджуючи питання забезпечення інформаційної безпеки в умовах криз, а також воєн, Л. Чистоклетов та С. Обрембальський відзначають ключові напрями, на які Україна повинна звернути увагу у сфері державної політики захисту інформації. Ці компоненти можна розглядати як методи і форми забезпечення інформаційної безпеки держави, зокрема:

– безпосередня оцінка зовнішніх та внутрішніх загроз національним інтересам та безпеці у сфері інформації;

– запровадження й удосконалення системи моніторингу інформаційного простору. Цей процес охоплює збір, обробку, збереження та аналіз усієї наявної інформації про ситуацію в інформаційній сфері держави;

– посилення міжнародних відносин у сфері інформаційних правовідносин (обмін досвідом та інформацією);

– підвищення рівня інформаційної культури населення;

– удосконалення національної нормативно-правової бази, що покликана найкраще забезпечувати інформаційну безпеку нашої держави [19, с. 7].

Дослідники розглядали це питання в контексті України, але ці напрями можуть бути належним чином використані та пройдені й іншими європейськими країнами.

Водночас М. Сенченко вважає, що Україні для ефективної протидії інформаційним загрозам із боку російської федерації необхідно мати:

– ефективну концепцію інформаційної війни;

– ефективну відповідну систему ведення цієї інформаційної війни;

– стратегію ведення інформаційної війни [6, с. 41].

Держава має всі необхідні інструменти та може застосовувати методи, які мають на меті покращити інформаційну безпеку держави. Сюди входить законодавче регулювання інформаційного простору (йдеться більшою мірою про обмеження ворожих інформаційних каналів, сайтів та застосунків, які сіють пропаганду та мають на меті створити паніку та ворожнечу всередині держави).

Ще одним механізмом забезпечення інформаційної безпеки в умовах кризи є підвищення кримінальної відповідальності за поширення дезінформації та фейків. Це повинно створити відповідне розуміння у суспільстві, що слід перевіряти будь-яку інформацію, адже поширення недостовірної інформації тягне за собою відповідну кримінальну чи інший вид відповідальності.

Вітчизняний науковець С. Присяжнюк відзначає, що гуманітарна політика держави є одним із ключових та найвагоміших механізмів забезпечення інформаційної безпеки держави в умовах кризи. Він уважає, що гуманітарна політика є консолідуючим фактором суспільства у переломні моменти, зокрема у періоди криз та війн. Ця політика є стримуючим чинником гібридної агресії російської федерації. Також вона слугує механізмом збереження національної ідентичності, що дуже важливо у контексті інформаційної безпеки не лише України, а й кожної цивілізованої держави [12, с. 62; 14, с. 162–163].

С. Присяжнюк додає, що гуманітарна політика держави, зокрема України, є вагомим складником механізму забезпечення інформаційної безпеки держави в умовах криз та війн, бо вона є певним чином гуманітарною стійкістю, взаємовипливає з національної стійкості, що формується відповідною державною політикою.

Гуманітарна політика також має розглядатися як інструмент інституційної та громадянської форми забезпечення інформаційної безпеки. Адже, як стверджує С. Присяжнюк, вона є обов’язковим механізмом впливу держави на суспільну та громадянську свідомість, що є важливим фактором у питанні інформаційної безпеки держави [12, с. 64; 18].

Серед усього іншого до механізмів забезпечення інформаційної політики на держрівні належать формування та забезпечення кібербезпеки та інформаційної контрпропаганди.

Що стосується першого, то слід розуміти, що йдеться про протидію хакерським атакам на держустанови та інші сайти. На протидію кібер- та інформаційним загрозам здійснює діяльність Ситуаційний центр кібербезпеки СБ України. Його головними завданнями є:

– реагування на кіберінциденти у сфері держбезпеки;

– негласна перевірка готовності об'єктів критичної інфраструктури до кібератак та кіберінцидентів;

– протидія злочинності у кіберсфері;

– виявлення, запобігання, розкриття та протидія злочинам проти миру і людини, скоєні у кіберпросторі [7, с. 58].

До контрпропаганди можна віднести взаємодію державних відомств із громадянським суспільством, яке можна розглядати крізь призму форм забезпечення інформаційної безпеки держави в умовах криз та війн. Українські органи влади, міністерства та відомства в умовах повномасштабної війни, на думку В. Кротюк, систематично доводять актуальну інформацію до суспільства. Як стверджує науковець, це є проявом високого рівня взаємодії органів державної влади, місцевого самоврядування з громадянами держави [8, с. 55].

Слід зауважити, що 28 грудня 2021 р. було прийнято «Стратегію інформаційної безпеки України», що ґрунтується на семи стратегічних цілях, які є першочерговими для виконання в умовах військового стану:

1. Протидія інформаційним операціям та дезінформації. Проявом забезпечення інформаційної безпеки можна назвати Указ Президента № 152/2022 про введення в дію рішення РНБО «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», де визначено, що єдина інформаційна політика є пріоритетним завданням національної безпеки України. Це вже є механізмом забезпечення інформаційної політики, адже держава дбає про інформаційне поле під час війни та прагне, щоб громадяни отримували правдиву й точну інформацію і могли протидіяти російській пропаганді [1–4].

2. Усебічний розвиток української культури та утвердження громадянської ідентичності.

3. Підвищення рівня медіаграмотності та медіакультури громадянського суспільства – здійснюється державними органами влади, органами місцевого самоврядування з використанням засобів масової інформації, де проводиться відповідна роз'яснювальна робота серед населення.

4. Забезпечення інформаційних прав особи, захист прав журналістів.

5. Реінтеграція українців, що живуть на тимчасово окупованих територіях України, у контексті реалізації інформаційної політики безпеки.

6. Створення, функціонування та підтримка системи стратегічних комунікації – полягає у взаємодії органів державної влади, місцевого самоврядування у питаннях кризових ситуацій.

7. Розвиток інформаційного суспільства та культури діалогу [8, с. 52–55].

Окрім вищенаведених методів та форм забезпечення інформаційної безпеки, ніхто не відміняв індивідуальний рівень, що стосується кожної людини. На фактично найнижчому рівні процесу забезпечення необхідно критично мислити, бути медіаграмотним (це залежить від залученості у державні процеси та ступеня залученості держави у цей процес).

Усю наявну інформацію, на нашу думку, кожен повинен завжди перевіряти та находити надійні джерела інформування. В умовах війни слід не піддаватися фейкам, а головне – не поширювати відео та фото з позиціями Збройних сил України.

У контексті цього питання для забезпечення інформаційної безпеки необхідно налаштувати двофакторну автентифікацію, шифрування переписок, а також треба бути обережним у месенджерах.

Для повноцінного дослідження даної проблематики слід вивчити зарубіжний досвід забезпечення інформаційної безпеки.

До прикладу, у Польщі створено Агентство внутрішньої безпеки (ABW). Воно покликане забезпечувати кібернетичну безпеку держави. Слід сказати, що дане Агентство створило урядову команду для реагування на комп'ютерні загрози (CERT). Її завданням є забезпечення можливостей органів держуправління у питанні захисту від кіберзагроз, насамперед від атак на інфраструктуру, що складається з ІТ-систем та комп'ютерних мереж, та щодо порушення роботи чи руйнації, що може призвести до загроз життю та здоров'ю громадян Польщі або ж до значних фінансових збитків та великих збоїв у функціонуванні органів державної влади країни – сусідки України [13, с. 5].

Інший сусід нашої держави – Угорщина є однією з перших постсоціалістичних держав, де було прийнято нормативно-правовий акт про захист персональних даних. Ідеться про «Закон про захист інформації про особу та доступ до інформації, що містить суспільний інтерес». Він був прийнятий у далекому 1992 р.

Угорське законодавство зобов'язує законодавців надавати достовірну та своєчасну інформацію, а громадяни цієї країни наділені правом оформляти запити стосовно отримання доступу до інформаційних ресурсів, що викликають чималий суспільний інтерес [13, с. 6].

Ураховуючи вище сказане, для покращення забезпечення інформаційної стійкості в умовах криз та воєн Україна, на нашу суб'єктивну думку, повинна створити інтегровану у суспільство платформу, яку координуватиме Кабінет Міністрів та РНБО з метою надсилання відповідних повідомлень у народні маси.

Українське законодавство потребує посилення нормативно-правової бази щодо відповідальності за поширення фейків, дезінформації, але при цьому орієнтуватися на забезпечення свободи слова.

Умови XXI ст. та розвиток комп'ютерних технологій змушують держави вкладати кошти у розвиток кіберрозвідки, а також OSINT-аналітику та кіберзасоби виявлення фейкових повідомлень та новин на ранніх стадіях їх появи.

Що стосується військового сектору, то досвід російсько-української війни показав, що не лише Україна, а й інші держави повинні вкладати кошти у підготовку військових безпекового сектору у питаннях інформаційної безпеки, що також тісно пов'язана з психологічною стійкістю та засобами інформаційного впливу.

Часті інформаційно-психологічні операції на різних рівнях як внутрішньої, так і зовнішньої арени особливо посилюються під час конфліктів чи воєн, тому варто звернути особливу увагу на розроблення протоколів реагування на ІПСО та масштабні інформаційні атаки. Варто лише згадати DDoS-атаки 15 січня, 15, 16 та 23 лютого 2022 р., що передували початку повномасштабної війни. Об'єктами атаки стали банківська сфера та державний сектор. Атаки тривали годинами, та попри все Україні вдалося їх відбити.

Водночас низка інформаційних ресурсів (УНІАН, РБК-Україна та ін.) стверджувала, що 15 лютого 2022 р. Україна зазнала найбільшої кібератаки на свої сайти [9; 17; 20].

До слова, у 2024 р. російські хакери атакували Monobank, але надійно сформована інформаційна система безпеки дала можливість вистояти під час ворожої інформаційно-психологічної операції [9].

Що стосується громадянського суспільства, то державам, і Україні у тому числі, необхідно розробляти національні програми медіаграмотності: інформаційна гігієна, порядок дій під час інформаційних атак, як визначити фейки та ІПСО та інші критично важливі питання в умовах кризи та війни.

Ми вважаємо, що держава має сприяти формуванню незалежних фактчекінгових платформ, які мають викликати довіру у суспільстві.

Важливо також розробляти та поглиблювати міжнародну співпрацю у сфері кібербезпеки. Зокрема, у цьому напрямі необхідно розвивати співпрацю з великими організаціями та корпораціями, як-от Google, Meta, Microsoft, які контролюють чималу частку ринку та платформ, що повинно позитивно вплинути на швидкість реагування на ворожі атаки та відповідний контент, що шкодить національним інтересам тієї чи іншої держави світу.

Висновки. Кризи та війни у світі, а особливо війна в Україні, показали критичне значення інформації, насамперед у сфері національного захисту не лише України, а й кожної цивілізованої держави.

Кібератаки, злам даних, заволодіння паролями спонукали держави розробляти більш ефективні системи протидії та захисту власного інформаційного простору.

Інформація зайняла чи не найважливіше місце у питаннях забезпечення національного суверенітету та безпеки.

Військовий досвід України від початку повномасштабного вторгнення демонструє гнучкість підходу до кібербезпеки. Водночас слід зауважити, що цей досвід вивчають міжнародні партнери, щоб ефективніше протидіяти дезінформації ворожих держав.

Утім, на нашу думку, питання інформаційного забезпечення національної безпеки потребує, насамперед, покращення міжвідомчої взаємодії, яка покликана пришвидшити обмін даними та якнайкраще їх оброблення, а отже, прийняття найкращого рішення у тій чи іншій ситуації.

В умовах сучасного розвитку технологій та поширення гібридних загроз кордони між тилом і фронтом досить часто стираються, тому інформація стає ідеологічним інструментом, а інформаційна безпека є не менш важливою за фізичну оборону.

На нашу думку, сучасні війни дуже важко виграти лише військовим шляхом (танками та ракетами), адже вкрай важливу роль відіграє здатність держави та суспільства критично мислити та оцінювати ситуацію, зберігаючи єдність та діючи в національних інтересах, що вкрай важливо в сучасному світі обману та маніпуляцій.

Сьогодні Україна формує унікальний кейс інформаційного спротиву, який, без сумніву, може стати і стане орієнтиром та прикладом для інших демократичних та цивілізованих держав.

Література:

1. Указ Президента України від 28 грудня 2021 р. «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

2. Рішення Ради національної безпеки і оборони України від 15 жовтня 2021 р. «Про стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/n0080525-21#n2

3. Указ Президента України від 19 березня 2022 р. «Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану». URL: https://zakon.rada.gov.ua/laws/show/152/2022#n2

4. Рішення Ради національної безпеки і оборони України від 18 березня 2022 року «До реалізації єдиної інформаційної політики в умовах воєнного стану». URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#Text

5. Дмитренко М. Інформаційно-психологічні операції у контексті інформаційної безпеки України. *Інформація і право*. 2025. № 1(52). С. 112–122. URL: http://il.ippi.org.ua/article/download/324704/314751

6. Клочко А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. *Наукові праці Міжрегіональної академії управління персоналом.* 2022. № 3(63). С. 38–42. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/2a00dddd-3a2e-4f11-8962-9d23d72607f2/content (дата звернення: 03.09.2024).

7. Коваленко Л. Правове забезпечення інформаційної безпеки держави в умовах війни. *Інформаційне протиборство в умовах російської української війни* : матеріали наук. семінару з міжнар. участю, м. Харків, 30 листопада 2023 р. Харків, 2023. С. 56–61. URL: https://hups.mil.gov.ua/assets/doc/science/stud-conf/30-lystopada-2023.pdf#page=56

8. Кротюк В. Інформаційна безпека держави в умовах війни. *Інформаційне протиборство в умовах російської української війни* : матеріали наук. семінару з міжнар. участю, м. Харків, 30 листопада 2023 р. Харків, 2023. С. 49–56. URL: https://hups.mil.gov.ua/assets/doc/science/stud-conf/30-lystopada-2023.pdf#page=49

9. Кузьменко Ю. DDos-атака на Monobank припинилася. *Суспільне Новини*. URL: https://suspilne.media/816449-75-mlrd-zapitiv-za-tri-dobi-ddos-ataka-na-monobank-pripinilasa/

10. Мазуренко Л. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Питання політології»*. 2022. № 42. С. 50–57. URL: https://periodicals.karazin.ua/politology/article/view/22088/20387 (дата звернення: 02.09.2024).

11. Ломака І., Липчук О., Кобець Ю. Інформаційна безпека держави: теоретико-методологічні засади та особливості в умовах збройного конфлікту. *Регіональні студії*. 2022. № 31. С. 113–118. URL: http://regionalstudies.uzhnu.uz.ua/archive/31/31_2022.pdf#page=113

12. Присяжнюк С. Функціонал гуманітарної політики як чинник протидії інформаційній агресії. *Політичне життя*. 2024. № 3. С. 61–66. URL: https://jpl.donnu.edu.ua/article/view/16381

13. Пугачов О. Зарубіжний досвід забезпечення інформаційної безпеки держави. *Проблеми сучасних трансформацій. Серія «Право, публічне управління та адміністрування»*. 2024. № 13. С. 2–7. URL: https://reicst.com.ua/pmtl/article/view/2024-13-02-07

14. Сергієнко Л. Гуманітарна політика України: ідентифікація складників, об'єктів, суб'єктів та пріоритетів. *Вісник ЖДТУ. Економіка, управління та адміністрування*. 2019. Вип. 2(88). DOI: https://doi.org/10.26642/jen-2019-2(88)-162-173.

15. Смотрич Д., Браілко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2023. № 77. С. 121–127. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/22-2.pdf (дата звернення: 04.09.2024).

16. Суспільно-політична стабільність як складник системи інформаційної безпеки: виклики в умовах воєнного стану / Є. Міненко та ін. *Міждисциплінарні дослідження складних систем*. 2023. № 23. С. 41–54. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/45598/Minenko-41-54.pdf?sequence=1&isAllowed=y (дата звернення: 04.09.2024).

17. Україна успішно відбила найбільшу DDoS-атаку у своїй історії. *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://cip.gov.ua/ua/news/ukrayina-uspishno-vidbila-naibilshu-ddos-ataku-v-svoyii-istoriyi

18. Чечель О. Поняття і зміст механізмів державного управління в гуманітарній сфері. *Публічне управління та митне адміністрування.* 2019. № 3(22). С. 137–145.

19. Чистоклетов Л., Обрембальський С. Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. *Академічні візії*. 2024. № 31. С. 1–11. URL: https://www.academy-vision.org/index.php/av/article/view/1141 (дата звернення: 25.06.2025).

20. Шварц Д., Доломанжи А. Кібератака в Україні 15 лютого була найбільшою в історії держави: в Кабміні назвали вартість. *УНІАН.* URL: https://www.unian.ua/techno/communications/kiberataka-v-ukrajini-15-lyutogo-bula-naybilshoyu-v-istoriji-derzhavi-v-kabmini-nazvali-vartist-11706571.html (дата звернення: 25.06.2025).

21. Шевченко К. Соціально-правове забезпечення інформаційної безпеки України в умовах війни. *Інформаційне протиборство в умовах російської української війни* : матеріали наук. семінару з міжнар. участю, м. Харків, 30 листопада 2023 р. Харків, 2023. С. 146–151. URL: https://hups.mil.gov.ua/assets/doc/science/stud-conf/30-lystopada-2023.pdf#page=146

References:

1. Ukaz Prezydenta Ukrainy vid 28 grudnia 2021 roky «Pro rishennia Rady Nacionalnoi Bezpeky ta Oborony vid 15 zhovtnia 2021 roky «Pro strategiyu informaciynoi bezpeky» [Decree of the President of Ukraine dated December 28, 2021 «On the Decision of the National Security and Defense Council of Ukraine dated October 15, 2021 «On the Information Security Strategy»] [in Ukrainian].

2. Rishennia Rady Nacionalnoi Bezpeky ta Oborony vid 15 zhovtnia 2021 roky «Pro strategiyu informaciynoi bezpeky» [Decision of the National Security and Defense Council of Ukraine dated October 15, 2021 "On the Information Security Strategy"] [in Ukrainian].

3. Ukaz Prezydenta Ukrainy vid 19 bereznia 2022 roky «Pro rishennia Rady Nacionalnoi Bezpeky ta Oborony vid 18 bereznia 2022 roky «Shchodo realizacii yedynoi informaciynoi polityky v umovah voyennogo stanu» [Decree of the President of Ukraine «On the Decision of the National Security and Defense Council of Ukraine dated March 18, 2022 «On the Implementation of a Unified Information Policy in Conditions of Martial Law»] [in Ukrainian].

4. Rishennia Rady Nacionalnoi Bezpeky ta Oborony vid 18 bereznia 2022 roky «Shchodo realizacii yedynoi informaciynoi polityky v umovah voyennogo stanu» [Decision of the National Security and Defense Council of Ukraine dated March 18, 2022 «On the Implementation of a Unified Information Policy in Conditions of Martial Law».] [in Ukrainian].

5. Dmytrenko, M. (2025). Informaciyno-psyhologicni operacii y konteksti informaciynoi bezpeky Ukrainy. [Information and psychological operations in the context of information security of Ukraine] [in Ukrainian].

6. Klochko, A. (2022). Zabezpechennia informaciynoi bezpeky v ymovah sychasnoho syspilstva. [Enssuring information security in the conditions of modern society] [in Ukrainian].

7. Kovalenko, L. (2023) Pravove zabezpechennia informaciynoi bezpeky derzhavy v ymovah viyny. [Legal provision of information security of the state in conditions of war] [in Ukrainian].

8. Krotiuk, L. (2022). Informaciyna bezpeka v umovah rosiysko-ukrainskoi viyny: vyklyky ta zagrozy. [Information security in the conditions of the Russian-Ukrainian war: challenges and threats] [in Ukrainian].

9. Lomaka, I, Lypchuk, O, & Kobec' Y. Informaciyna bezpeka derzhavy: teoretyko-metodologichni zasady ta osoblyvosti v umovah zbroynogo konflikty [Information security of the state: theoretical and methodological principles and features in the conditions of armed conflict.] [in Ukrainian].

10. Prysiazhniuk, C. (2024). Funkcional gumanitarnoi polityky yak chynnyka protydii informaciynii agresii. [The functionality of humanitarian policy as a factor in countering informational aggression] [in Ukrainian].

11. Pugachov, O. (2024) Zarubizhyi dosvid zabezpechennia informaciynoi brezpeky derzhavy. [Foreign experience in ensuring state information security] [in Ukrainian].

12. Sergienko, L. (2019). Gumanitarna polityka Ukrainy: identyfikacia skladovyh, obiektiv, subiektiv ta priorytetiv. [Humanitarian policy of Ukraine: identification of components, objects, subjects and priorities] [in Ukrainian].

13. Smortych, D. & Brailko, L.B. (2023). Informaciyna bezpeka v umovah voyennogo stanu [Information security in the conditions of martial law] [in Ukrainian].

14. Minenko, Ye., Zakharenko, K., Drapushko, R., & Volaniuk, O. (2023). Suspilno-politychna stabilnist' yak skladova systemy informaciynos bezpeky: vyklyky v umovah voyennogo stanu [Socio-political stability as a component of the information security system: challenges in the conditions of martial law] [in Ukrainian].

15. CIP. (2022). Ukraina uspishno vidbyla naibilshy DDoS-ataky y svoiy istorii. [Ukraine successfully repelled the largest DDoS attack in its history] [in Ukrainian].

16. Chechel, O. (2019). Poniattia i zmist mehanizmiv derzhavnogo upravlinnia v gumanitarniy sferi. [The concept and content of state management mechanisms in the humanitarian sphere.] [in Ukrainian].

17. Chystokletov, L. & Obrembalskyi, S. (2024). Osoblyvosti zabezpechennia informaciynoi bezpeky v umovah rosiysko-ukrainskoi viyny. [Features of ensuring information security in the conditions of the Russian-Ukrainian war]

18. Shvarc, D. & Dolomandzhy, A. (2022), Kiberatakaka v Ukraini 15 lutogo byla naibilshoyu v istorii derzhavy: u Kabminu nazvaly vartist. [The cyber attack in Ukraine on February 15 was the largest in the history of the country: the Cabinet of Ministers named the cost] [in Ukrainian].

19. Shevchenko, K. (2023). Socialno-pravove zabezpechennia informaciynoi bezpeky Ukrainy v umovah viyny. [Social and legal provision of information security of Ukraine in conditions of war] [in Ukrainian].

Yaroslav Lelet. Mechanisms and forms of ensuring information security in times of crisis

The article clarifies the essence of the concept of «information security». The views of scientists on the essence of this concept and the features of social security at the state and regional levels are summarized. The importance of properly ensuring the protection of the information space in times of crisis and war is considered.

The issue of mechanisms and forms of ensuring information security in times of crisis is considered. The problem of information security is extremely important and requires priority attention.

The purpose of the article is to define and characterize the mechanisms and forms of ensuring information security in times of military-political conflict

Key words: *information security, national security, crisis, war.*

Відомості про автора:
Лелет Ярослав – аспірант кафедри політичних наук,
Карпатський національний університет імені Василя Стефаника.

Надійшла 11.08.2025
Прийнята 13.08.2025
Опублікована 30.10.2025