Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий центр заочно-дистанційного навчання
Кафедра національної безпеки та політології

Кваліфікаційна робота

на здобуття освітнього ступеня магістра на тему:

«Незаконне розголошення інформації про військові операції в умовах воєнного стану: кримінально-правовий захист національної безпеки»

Виконав студент ІІ курсу, групи ЗМНб-21,
спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
Чучман Назарій Володимирович

Керівник – кандидат юридичних наук, доцент
Герасимчук Олег Павлович
Рецензент – кандидат юридичних наук, доцент
Туз Назарій Дмитрович

Острог, 2026

ЗМІСТ

ВСТУП

Постановка проблеми. Після початку повномасштабного вторгнення проти України, 24 березня 2022 року Верховною Радою України ухвалено Закон України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України (далі скорочення автора – ЗСУ) чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану». Результатом ухвалення даного законодавчого акту стало доповнення Основної частини Кримінального кодексу України (далі – КК України) ст. 114-2 «Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану».

Актуальність криміналізації цього діяння зумовлена тим, що країна-агресор активно здійснює моніторинг соціальних мереж і телеграм-каналів, а також вербує інформаторів на підконтрольних Україні територіях. Росія залучає до співпраці не лише дорослих, а й неповнолітніх. Крім того, непоодинокими є випадки засудження діючих військовослужбовців Збройних Сил України. Саме це обумовлює криміналізацію досліджуваного діяння та підвищення ефективності захисту військової інформації, що забезпечить національну безпеку держави в умовах воєнного стану.

Ступінь розробки проблеми. Незважаючи на відносну новизну запроваджених змін, у вітчизняній науковій літературі вже представлено достатньо велику кількість досліджень даного питання. Зокрема, у працях В. Батиргареєвої, Д. Євтєєвої, А. Лапкіна, К. Новікової, Ю. Пономаренка, Л. Тімофєєвої, М. Дубняка, В. Киричка, Р. Мовчана, А. Політової, О. Самчинської

та М. Хавронюка представлено окремі проблемні питання, що виникають у процесі кваліфікації протиправного діяння за ст. 114-2 КК України, а також заходи щодо її удосконалення. У роботах З. Загиней-Заболотенко, О. Кваші, В. Кузнєцова, М. Рубащенка та С. Сороки проаналізовано специфіку предмета, об'єктивної сторони та кваліфікуючих ознак складу злочину, передбаченого ст. 114-2 КК України. У свою чергу, П. Бурдою досліджувалося питання соціальної обумовленості криміналізації несанкціонованого поширення військово значущої інформації (ст. 114-2 Кримінального кодексу України), а також специфіки об'єкта вказаного кримінального правопорушення.

Попри наявність значної кількості досліджень окремих аспектів незаконного розголошення інформації про військові операції в умовах воєнного стану, ґрунтовне наукове опрацювання цієї проблеми досі відсутнє, що й зумовлює вибір теми роботи: «Незаконне розголошення інформації про військові операції в умовах воєнного стану: кримінально-правовий захист національної безпеки».

Теоретична основа дослідження. У процесі проведення дослідження нами використовувалися праці вітчизняних та зарубіжних науковців, присвячених питанням забезпечення військово значимої інформації в умовах воєнного стану, особливостями складу кримінального правопорушення, що полягає у несанкціонованому розголошенні військової інформації, специфіки кваліфікації, виявлення, розслідування та притягнення винних осіб до кримінальної відповідальності за вказані злочини, а також перспективи удосконалення зазначеного інституту.

Нами досліджено положення вітчизняного кримінального та кримінального процесуального законодавства, а також законодавчі акти у сфері захисту інформації від несанкціонованого доступу і розголошення. Додатково проаналізовано судову практику у справах про притягнення до кримінальної відповідальності осіб за вчинення злочину, передбаченого ст. 114-2 КК України.

Предметом дослідження є незаконне розголошення інформації про військові операції в умовах воєнного стану: кримінально-правовий захист національної безпеки.

Метою дослідження є визначення особливостей незаконного розголошення інформації про військові операції в умовах воєнного стану як умова ефективного кримінально-правового захисту національної безпеки.

Мета зумовлює потребу формування наступних ***завдань*** нашого дослідження:

1. Розкрити поняття та значення інформації про військові операції для гарантування національної безпеки.
2. Встановити особливості нормативно-правового регулювання захисту інформації в оборонній сфері.
3. Проаналізувати міжнародні стандарти щодо запобігання розголошенню інформації у сфері оборони.
4. Надати кримінально-правову характеристику складу злочину, передбаченого ст. 114-2 КК України, шляхом аналізу його об’єктивних та суб’єктивних ознак
5. Дослідити судову практику розгляду справ, пов’язаних із незаконним розголошенням військової інформації.
6. Визначити основні проблеми виявлення, кваліфікації та притягнення до відповідальності осіб, винних у несанкціонованому поширенні військової інформації в умовах воєнного стану.
7. Вивчити можливості імплементації позитивного зарубіжного досвіду у сфері запобігання несанкціонованому поширенню військової інформації та протидії цьому явищу.

Обґрунтування методу збору та інтерпретації даних. У процесі проведення дослідження нами використано різноманітні загальнонаукові та спеціальні методи наукового пізнання. В основу нашого дослідження покладено використання діалектичного методу наукового пізнання, за допомогою якого визначено суперечності та взаємозв’язки між необхідністю захисту національної

безпеки держави та кримінально-правовими аспектами регулювання незаконного розголошення інформації про військові операції в умовах воєнного стану. За допомогою методів аналізу та синтезу нами здійснено розкриття внутрішнього змісту досліджуваних об'єктів та їх окремих складових частин, а також узагальнення отриманих результатів. Шляхом використання методу абстрагування існує можливість для виділення окремих складових елементів досліджуваного об'єкта, його ознак та взаємозв'язків, що сприяє більш детальному розкриттю його характеристик.

Використання методів індукції та дедукції дозволило розкрити сутність об'єкту складу кримінального правопорушення, а саме несанкціонованого поширення інформації, що сприяло визначенню спільності ознак і загроз для національної безпеки у цілому. За допомогою методу порівняння нами досліджено особливості зарубіжного та міжнародного досвіду щодо притягнення до відповідальності осіб за неправомірне поширення інформації в умовах воєнного стану. Шляхом використання методу узагальнення нами визначено ключові проблеми і загрози для національної безпеки України через призму кримінального правопорушення, передбаченого ст. 114-2 КК України.

За допомогою структурного і системного методів нами здійснено аналіз складу кримінального правопорушення, передбаченого ст. 114-2 КК України, як цілісної структурно-упорядкованої єдності та множини взаємопов'язаних між собою елементів, що є загрозою для національної безпеки держави. Використання інституціонального методу визначено основні характеристики кваліфікації та притягнення винних осіб до відповідальності за вчинення злочину, передбаченого ст. 114-2 КК України.

Гіпотеза дослідження полягає у наявності припущення щодо існування потреби у забезпеченні балансу між правом на свободу слова та захистом національної безпеки в умовах воєнного стану. Вважаємо, що існує потреба у забезпеченні рівноваги між правом на свободу вираження поглядів та інтересами національної безпеки, з метою обґрунтованого обмеження яких воно обмежуючи, аргументуючи це належним чином при ухваленні обвинувального

чи виправдувального вироків. До того ж, судами майже не обґрунтовуються належним чином судові вироки, що суперечить положенням Конвенції з прав людини та основоположних свобод, у зв'язку із чим існують ризики для України у зловживанні державним примусом та недоведеності обґрунтованості суворості запроваджених заходів.

На підтвердження зазначеної гіпотези свідчать судові рішення, ухвалені за результатами розгляду за обвинуваченням у вчиненні кримінальних правопорушень, передбачених ст. 114-2 КК України. До того ж, внесені у 2022 році доповнення до КК України було зроблено досить швидко, внаслідок чого можуть виникати проблеми при трактуванні тих чи інших понять, які є ключовими для факту визначення наявності чи відсутності складу кримінального правопорушення, передбаченого ст. 114-2 КК України.

Практичне значення дослідження. Результати магістерської роботи може бути використано у процесі практичної діяльності правоохоронних органів та органів державної влади у напрямку підвищення ефективності протидії незаконному розголошенню інформації про військові операції в умовах воєнного стану. Матеріали дослідження доцільно використовувати у навчальному процесі у рамках викладання курсів «Кримінальне право», «Кримінальний процес», «Національна безпека», а також у процесі складання окремих лекцій та розділів підручників із перелічених дисциплін. Отримані результати можливо використовувати в якості основи для подальших досліджень у сфері кримінально-правового захисту воєнної та інформаційної безпеки держави.

Структура роботи. Структура кваліфікаційної роботи магістра складається зі вступу, 3 розділів, висновків до розділів, загальних висновків, списку використаних джерел із 64 найменувань і додатка на 1 сторінці. Загальний обсяг основного тексту – 81 сторінка. Робота містить 4 таблиці і 3 рисунка.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЗАХИСТУ ВІЙСЬКОВОЇ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

1.1. Поняття та роль інформації про військові операції для захисту національної безпеки

Стан безпеки завжди розглядався у якості ключової та основоположної потреби як окремих індивідів, так і суспільства у цілому, оскільки безпосередньо пов'язаний із необхідністю протидії численним зовнішнім та внутрішнім загрозам. Забезпечення стану безпеки виступає в ролі найважливішого елемента функціонування та розвитку держави, що вимагає врахування економічних, соціальних, політичних, правових, екологічних, геополітичних та техногенних аспектів. При цьому, вагому роль у цьому відіграє інформаційний аспект забезпечення національної безпеки.

Інформаційна безпека виступає в якості одного зі складових елементів національної безпеки, сутність якої полягає у формуванні стану захищеності життєво необхідних інтересів людини, суспільства та держави, коли забезпечується ефективне запобігання спричинення шкоди через наступні ризики:

неповнота, несвоєчасність та невідповідність використовуваної інформації;

здійснення негативного інформаційного впливу;

спричинення негативних наслідків використання інформаційних технологій;

несанкціоноване поширення, використання та пошкодження збереженості, конфіденційності та доступності інформації[1].

[1] Панченко О. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України, 2019. Вип. 3. С. 3.

У свою чергу, стосовно визначення категорії «інформаційна безпека», запропонованих у науковій літературі, то під даним поняттям прийнято розуміти систему нормативного забезпечення, у відповідності до якої гарантується закріплення даних, що сприяють прийняттю стратегічних рішень та захисту інформаційних ресурсів юридичних осіб, суспільства та держави у цілому[2]. Інші автори пропонують розглядати безпеку інформації в якості сукупності правових, організаційних, інженерних та технічних заходів, спрямованих на формування чи використання інформаційних технологій, інфраструктурних об'єктів та спеціального ресурсного забезпечення, захист значимої інформації та прав окремих суб'єктів, які є безпосередніми учасниками інформаційних відносин[3].

Досліджуючи питання безпеки інформації та її сутність, Т.А. Чернявська виділяє окремі складові елементи даної категорії, якими є: 1) захист інформації; 2) захист і контроль за інформаційним простором; 3) встановлення належного рівня інформаційної забезпеченості. Отже, науковцем запропоновано розглядати безпеку інформації в якості єдиного процесу, для якого є притаманними окремі функціональні характеристики та чітка визначеність об'єкта і предмета направленості[4].

Додатково науковиця звертає увагу на позицію М. Галамби, який розглядає безпеку інформації через призму можливих загроз. Так, відповідно до позиції науковця, під досліджуваною категорією слід розуміти специфічний стан захищеності інформації, за наявності якого велика кількість інформаційних операцій, окремі акти зовнішньої інформаційної агресії, випадки несанкціонованого заволодіння інформацією, зокрема, акти інформаційного тероризму чи окремих злочинів, не можуть завдати значної шкоди інтересам індивідів, суспільства та держави у цілому[5].

---

[2] Нижник Н.Р., Ситнік Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник. Ірпінь, 2000. С. 42.

[3] Щербіна О.С. Інформаційні війни та безпека інформації. Інформаційні та прикладні технології. № 4. 2021. С. 312.

[4] Чернявська Т.А. Поняття і сутність інформаційної безпеки та її місце в системі забезпечення транспортної безпеки України. Таврійський науковий вісник. № 80. 2012. С. 368.

[5] Чернявська Т.А. Поняття і сутність інформаційної безпеки та її місце в системі забезпечення транспортної безпеки України. Таврійський науковий вісник. № 80. 2012. С. 368-369.

Відповідно до наукової позиції Б.А. Кормича, безпекою інформації визнається стан захищеності законодавчо врегульованих правил і процедур, які визначають особливості провадження інформаційних процесів, сприяють реалізації державних гарантій розвитку індивіда, суспільства і держави у цілому. При цьому, зазначене визначення викликає певні дискусії у науковій літературі, оскільки враховує виключно правові аспекти безпеки інформації, повністю ігноруючи інформаційну складову впливу на окремі сфери суспільного життя[6].

У контексті досліджуваного питання доцільно зауважити, що безпека інформації полягає не лише у розкритті виключно технічних аспектів, але й особливостей соціального впливу. Тобто, до складу безпеки інформації можливо віднести окремі специфічні технічні засоби, що забезпечують безпосередній захист інформації, зокрема, міжмережеві екрани, системи контролю доступу користувачів, використання антивірусних програм, програмного і технічного забезпечення тощо. При цьому, одним із ключових складових елементів захисту інформації виступає захист інтересів та потреб окремих індивідів, суспільства та держави у цілому.

Так, категорію «безпека інформації» можливо розглядати у вузькому та широкому розумінні. Відповідно до першого підходу, під досліджуваним поняттям слід розуміти сукупність апаратно-програмного забезпечення, що сприяють збереженню, доступу та конфіденційності інформації у комп'ютерній мережі, у тому числі й під час доступу до мережі Інтернет[7]. Враховуючи погляди науковців, що дотримуються саме вузького підходу до трактування інформаційної безпеки, таким явищем є захист інформації, обробка якої здійснюється у інформаційно-обчислювальній системі.

У контексті даного питання не доцільно залишати поза увагою питання інформації та даних, що безпосередньо підлягають захисту. Згідно з ч. 2 ст. 32 Конституції України встановлено заборону на збирання, зберігання,

[6] Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навчальний посібник. Київ: Кондор, 2004. С. 117.

[7] Там само. С. 92.

використання та поширення конфіденційної інформації про особу за відсутності згоди останньої, окрім випадків, встановлених законодавством та виключно з метою забезпечення національної безпеки, економічного добробуту та прав людини[8].

Згідно зі ст. 1 Закону України «Про інформацію», інформацією виступають будь-які відомості та дані, які можливо зберегти на матеріальних носіях або відобразити в електронному вигляді. Положеннями ст. 20 зазначеного законодавчого акту, інформація, в залежності від порядку доступу до неї, може поділятися на відкриту та відомості з обмеженим доступом, одним із різновидів якої є й конфіденційна інформація[9]. Досліджуючи дане питання П.Д. Гуйван зазначає, що існує концептуальна помилка законодавця, яка полягає у віднесенні конфіденційної інформації до відомостей з обмеженим доступом, оскільки її варто було б віднести до «всеохоплюючого правового режиму обороту відомостей з обмеженим доступом»[10].

У Стратегії національної безпеки (далі – Стратегія), серед найважливіших завдань забезпечення національної безпеки сформульована задача зміцнення безпеки в оборонній та інформаційній сферах. Саме таким чином держава визначає життєву значимість заходів, спрямованих на безпеку інформаційних ресурсів держави[11]. Широке впровадження сучасних інформаційних технологій в усіх сферах життя призводить до зростання значення захисту національної безпеки України в інформаційній сфері інформаційної безпеки (Рис. 1.1) є самостійною складової національної безпеки і впливає на захищеність інтересів України в інших сферах життя суспільства.

Національна безпека України істотно залежить від забезпечення інформаційної безпеки. Розвиток технічного прогресу цивілізації призведе до

[8] Конституція України: Закон України № 254к/96-ВР від 28.06.1996 року. ВВР, 1996, № 30, ст. 141.

[9] Про інформацію: Закон України № 2657-XII від 02.10.1992 року. ВВР, 1992, № 48, ст. 650.

[10] Гуйван П.Д. Щодо співвідношення категорій персональних даних про особу і конфіденційної інформації. Науковий вісник публічного та приватного права. № 3. 2018. С. 35.

[11] Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України № 392/2020 від 14.09.2020 року. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text. (дата звернення: 05.06.2025).

подальшого зростання цієї залежності. Зокрема, маємо все більш широке поширення думки, що інформаційне століття стане століттям інформаційної зброї і «безконтактних» воєн.

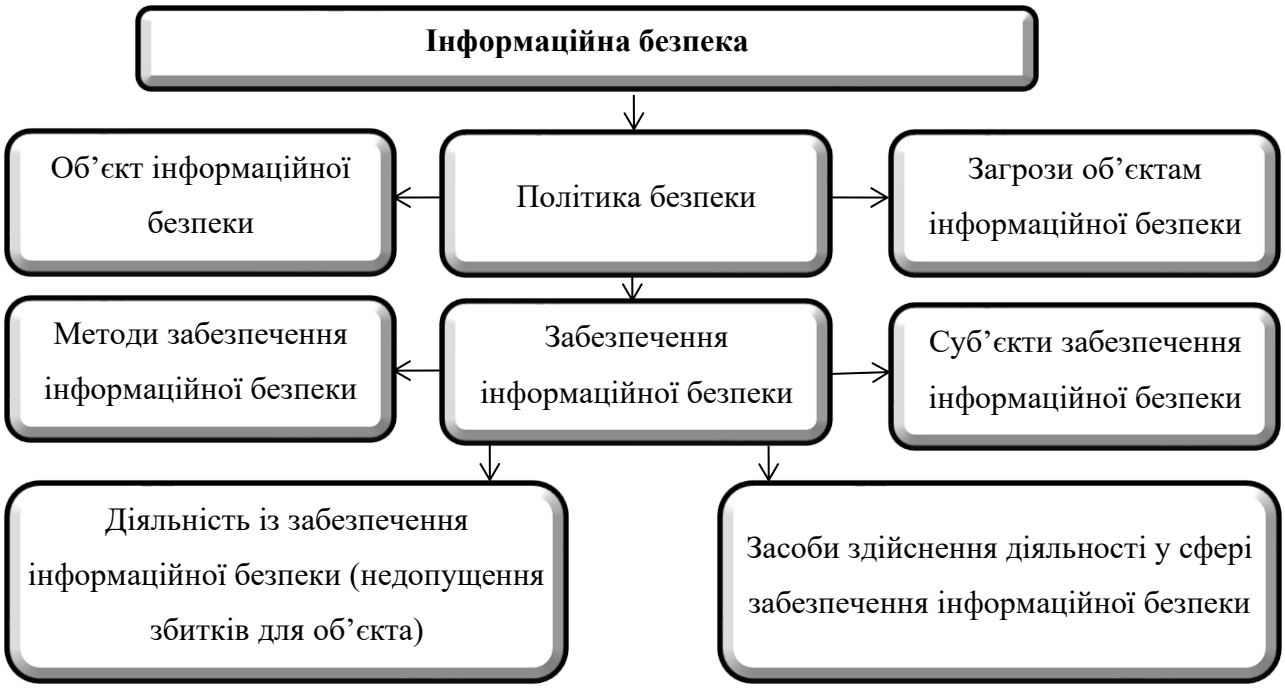

Рис. 1.1. Структура поняття «інформаційна безпека»

Джерело: складено автором на основі[12]

Стратегія національної безпеки являє собою офіційно прийняту систему поглядів на проблему забезпечення захисту інформаційного середовища, стверджує, що інформаційна безпека відіграє ключову роль у забезпеченні життєво важливих інтересів нашої держави, оскільки саме через зазначене середовище здійснюються загрози національній безпеці в різних сферах діяльності держави. Вирішення проблем інформаційної безпеки є актуальним завданням для сучасного суспільства в контексті забезпечення національної безпеки держави[13].

[12] Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України № 392/2020 від 14.09.2020 року. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text. (дата звернення: 05.06.2025).

[13] Там само.

Національна безпека, або державна безпека, є захищеність інтересів особистості, суспільства і держави від різних загроз у всіх сферах життєдіяльності. Можна погодитись з думкою П.Д. Гуйвана про те, що забезпечення національної безпеки є одним із пріоритетних завдань, що ставиться перед державою. Система забезпечення національної безпеки сьогоднішнього дня – це складна багаторівнева функціональна система, що включає в себе органи, сили, кошти для вирішення завдань щодо забезпечення національної безпеки. У даній системі основними суб'єктами безпеки є держава, органи законодавчої, судової та виконавчої влади, які визначають критерії забезпечення її національної безпеки, тобто кордону техногенних, політичних, соціальних, природних явищ, порушення яких може завдати можливий збиток нації. На практиці національна безпека по конкретних сферах життєдіяльності підрозділяється на п'ять видів безпеки: економічну, соціальну, військову, інформаційну та екологічну[14].

У відповідності до положень Стратегії інформаційної безпеки, під категорією інформаційної безпеки України варто розуміти одну зі складових частин національної безпеки України, стану захищеності територіальної цілісності, державного суверенітету, демократичного конституційного ладу, а також інших життєво важливих інтересів індивіда, суспільства та держави, що сприяє належному забезпеченню конституційних прав та свобод людини і громадянина на збирання, зберігання, використання і поширення інформації, доступу до об'єктивної та достовірної інформації, створення ефективної системи захисту та протидії спричиненню збитків шляхом поширення негативного інформаційного впливу, у тому числі скоординованого поширення недостовірної інформації, деструктивних форм пропаганди, різноманітних інформаційних операцій, несанкціонованого розповсюдження, використання та порушення цілісності інформації з обмеженим доступом[15].

[14] Гуйван П.Д. Щодо співвідношення категорій персональних даних про особу і конфіденційної інформації. Науковий вісник публічного та приватного права. № 3. 2018. С. 34.

[15] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України № 685/2021 від 28.12.2021 року. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7. (дата звернення: 05.06.2025).

Перші спроби людини зберегти таємність будь-якої інформації поклали початок формуванню теоретичних основ інформаційної безпеки. З розвитком технологій і обсягів передачі даних змінювалися методи захисту інформації. Як показало дослідження, на сучасному етапі розвитку суспільства ефективне забезпечення інформаційної безпеки дозволяє вирішувати ключові питання практично всіх видів національної безпеки.

Інформаційна безпека є важливою складовою системи національної безпеки, і від успішного вирішення питань даної області залежить забезпечення глобальної загальносвітової безпеки. Оскільки досліджуваний процес наділений перманентним, комплексним і попереджувальним характером виникає нагальна потреба в уважному вивченні заходів забезпечення інформаційної безпеки, що дозволяють завчасно нейтралізувати небезпеки і загрози в інформаційній сфері, тим самим створюючи безперервну підтримку умов безпеки[16].

В умовах воєнного стану особливої актуальності набуває питання виявлення та реагування на інформаційні загрози, що тягне за собою обмеження прав людини, оскільки цього вимагають інтереси держави. Так, у відповідності до положень Стратегії інформаційної безпеки України, інформаційна загроза виступає в якості потенційного чи реального негативного явища, чинників чи тенденції впливу на особу, суспільство і державу, що здійснюються в інформаційній площині з метою ускладнення або перешкоджання реалізації національних інтересів держави, утвердження національних цінностей та може спричинити безпосередню або опосередковану шкоду державним інтересам, національній безпеці й обороні[17].

Отже, в умовах воєнного стану основну увагу акцентовано на виявленні та реагуванні на реальні та потенційні загрози, а також простежується тенденція до необхідності здійснення впливу на потенційні та реальні загрози, що потребують обмеження прав людини. Зокрема, в умовах введення правового режиму

[16] Основи інформаційної безпеки. Навчальний посібник для вузів / Є. Б. Бєлов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Київ: Телеком, 2006. 544с.

[17] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України № 685/2021 від 28.12.2021 року. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7. (дата звернення: 05.06.2025).

воєнного стану запроваджено тимчасові обмеження прав та законних інтересів фізичних та юридичних осіб в обсязі, що є необхідним, достатнім та обґрунтованим для повноцінної реалізації заходів, затверджених положеннями ст. 8 Закону України «Про правовий режим воєнного стану». Так, національні інтереси держави в інформаційній сфері включає три основні компоненти, якими є:

інтереси людини, тобто гарантії підтримки правового статусу людини і громадянина в інформаційній сфері;

суспільні інтереси, тобто використання інформації та інформаційної інфраструктури з метою розвитку різних сфер життя суспільства;

державні інтереси, тобто використання інформації та інформаційної інфраструктури з метою належної реалізації заходів державної політики, управління суспільними справами, захисту моральних цінностей, а також стійкого функціонування інформаційної інфраструктури[18].

Враховуючи реалії сьогодення, є зрозумілим, що інформація використовується в якості інструменту масового впливу, що потребує повноцінного забезпечення національної інформаційної безпеки та дотримання прав людини, а також створення ефективних механізмів уникнення та протидії негативним наслідкам порушення в інформаційній площині. У цьому зв’язку система захисту інформації в умовах воєнного стану базується на трьох ключових елементах, якими є:

технічний, тобто розробка та запровадження в дію необхідних технічних складових компонентів інформаційних систем;

політичний, тобто визначення ключових напрямів реалізації державної інформаційної політики та заходів безпеки інформації;

правовий, тобто нормативне закріплення ключових елементів інформаційної безпеки в умовах воєнного стану[19].

---

[18] Борисова Л.В., Логвиненко М.Ф. Правові засади захисту інформації: навчальний посібник. Харків: ХНУВС, 2013. С. 116.

[19] Русакевич А.І. Інформаційна безпека в умовах воєнного стану у аспектів забезпечення інформаційних прав громадян. Держава та регіони. № 2 (80). 2023. С. 179.

У зв'язку із вищевикладеним можливо зробити висновок, що стан безпеки, як фундаментальна суспільна потреба, охоплює широкий спектр аспектів життєдіяльності держави та її громадян. У цьому контексті інформаційна безпека постає як критично важлива складова національної безпеки, оскільки інформаційний простір є не лише джерелом ресурсів, але й полем потенційної агресії. Як показує аналіз наукових підходів, інформаційна безпека охоплює не тільки технічні та правові, але й соціальні й політичні аспекти, які забезпечують захист життєво важливих інтересів особи, суспільства та держави.

Різні науковці пропонують розглядати інформаційну безпеку як системну категорію, що поєднує в собі заходи контролю, захисту, профілактики інформаційних загроз та створення безпечного інформаційного середовища. Таким чином, забезпечення інформаційної безпеки є багатогранним процесом, що вимагає комплексного підходу, який охоплює технічні, правові, політичні й організаційні заходи. Зміцнення цієї складової системи національної безпеки стає вирішальним фактором стабільного функціонування держави, збереження її суверенітету та забезпечення прав і свобод громадян в умовах постійно зростаючих викликів сучасного інформаційного середовища.

1.2. Нормативно-правове регулювання захисту інформації у сфері оборони

Ключовим аспектом забезпечення захисту інформації у галузі оборони виступає належне нормативно-правове регулювання досліджуваної сфери. В Україні ухвалено цілу низку законних і підзаконних нормативних документів, положеннями яких врегульовано питання захисту інформації, протидії загрозам інформаційній безпеці держави, суспільства та населення, захисту прав і свобод у сфері захисту інформації, виявлення джерел загроз для інформаційної безпеки тощо. До того ж, сформована нормативно-правова база забезпечує належну та ефективну реалізацію положень Стратегії інформаційної безпеки України.

Забезпечення захисту інформації у сфері оборони потребує розробки і дотримання великої кількості норм, що виступають в якості правової основи досліджуваного питання. Особливу роль у системі правового регулювання захисту інформації у сфері оборони відіграють положення адміністративного права, оскільки охоплюють ключові аспекти інформаційної безпеки, у тому числі з питань формування та визначення організаційної структури системи інформаційної безпеки; взаємодії між органами та структурами, до компетенції яких віднесено захист інформації у сфері оборони; адміністративної відповідальності суб'єктів у сфері захисту інформації у сфері оборони тощо.

Разом із нормами адміністративного права, вагому роль відіграють положення кримінального права, якими врегульовано питання притягнення до кримінальної відповідальності за вчинення кримінальних правопорушень, пов'язаних із захистом інформації у сфері оборони. Зазначеними нормами визначається компетенція державних органів, які формують своєрідну систему забезпечення інформаційної безпеки, а також інших органів, які пов'язані зі сферою оборони.

Важливу роль також відіграють норми цивільного права, якими врегульовано майнові та особисті немайнові відносини у сфері захисту інформації, а також визначено обсяг прав та обов'язків учасників з приводу власності та використання даних, відшкодування завданих збитків у разі порушення інформаційної безпеки. У цілому нормативно-правова основа забезпечення захисту інформації передбачає використання норм різних галузей права, які у своїй сукупності сприяють формуванню комплексного підходу до регулювання та забезпечення захисту інформації у сфері оборони[20].

Одним із ключових документів у системі нормативно-правових актів, які формують основу правового регулювання забезпечення захисту інформації, у тому числі й у сфері оборони є Конституція України, яка має статус найвищого законодавчого акту держави. Положеннями Основного закону визначено

[20] Крупнова А.О. Правове регулювання сфери забезпечення інформаційної безпеки в Україні. Електронне наукове видання «Аналітично-порівняльне правознавство». № 11. 2023. С. 349-350.

конституційні аспекти реалізації права на інформацію, джерела інформації, доступ до яких гарантовано державою, а також інші важливі норми, які виступають в якості основи у сфері захисту інформації у галузі оборони. Варто зауважити, що законодавцем інформаційна безпека розглядається в якості одного з невід'ємних елементів державності, на рівні із суверенітетом та територіальною цілісністю. Так, у відповідності до ст. 17 Конституції України, захист суверенітету, територіальної цілісності держави, забезпечення її економічної та інформаційної безпеки визнається найважливішими функціями держави та справою усього Українського народу[21]. Отже, забезпечення захисту інформації, у тому числі й у сфері оборони, є одним із основних елементів суверенних прав держави та національної ідентичності.

У контексті досліджуваного питання, враховуючи дію на території України правового режиму воєнного стану, на увагу заслуговують положення КК України, Розділ І Особливої частини якого доповнено новою статтею на підставі Закону України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану»[22]. Так, у відповідності до ст. 114-2 КК України передбачено настання кримінальної відповідальності за несанкціоноване поширення інформації про направлення і переміщення зброї, боєприпасів, озброєння, ЗСУ та інших військових формувань, утворених згідно із законодавством, вчинених в умовах правового режиму воєнного чи надзвичайного стану[23].

---

[21] Конституція України: Закон України № 254к/96-ВР від 28.06.1996 року. ВВР, 1996, № 30, ст. 141.

[22] Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України № 2160-IX від 04.03.2022 року. Офіційний вісник України, 2022, № 33, стор. 90, ст. 145, код акта 110988/2022.

[23] Кримінальний кодекс України: Закон України № 2341-III від 05.04.2001 року. ВВР, 2001, № 25-26, ст. 131.

Подальший розвиток нормативно-правового регулювання у цій сфері відбувся з ухваленням Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інфраструктури» від 27 березня 2025 року № 4336-IX, яким посилено вимоги до кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури, що безпосередньо стосується й оборонного сектору. Цей закон став відповіддю на зростання кібератак проти України та спрямований на підвищення стійкості інформаційних систем державних органів, у тому числі у сфері оборони. Окрім того, у 2025 році Кабінетом Міністрів України затверджено план заходів на 2025 рік з реалізації Стратегії кібербезпеки України, який передбачає приведення захисту інформаційних систем оборони до стандартів НАТО.

Зміст правового режиму воєнного стану, процедурні аспекти його запровадження та скасування, нормативні аспекти діяльності органів державної влади, військових адміністрацій, міського самоврядування, військового командування, юридичних осіб, дотримання гарантій прав та свобод людини і громадянина, врегульовано положеннями Закону України «Про правовий режим воєнного стану». Згідно п. 12 ч. 1 ст. 8 зазначеного законодавчого акту, під час дії правового режиму воєнного стану передбачено вилучення у підприємств, установ та організацій, а також громадян електронного комунікаційного обладнання, телевізійної, аудіо- та відеоапаратури, комп’ютерів та інших засобів зв’язку[24].

Положення Конституції України знайшли своє відображення у нормах цілої низки некодифікованих законодавчих актів, у тому числі у Законах України «Про інформацію»[25], «Про захист інформації в інформаційно-комунікаційних

[24] Про правовий режим воєнного стану: Закон України № 389-VIII від 12.05.2015 року. ВВР, 2015, № 28, ст. 250.

[25] Про інформацію: Закон України № 2657-XII від 02.10.1992 року. ВВР, 1992, № 48, ст. 650.

системах»[26], «Про захист персональних даних»[27], «Про державну таємницю»[28], «Про національну безпеку України»[29], «Про основні засади забезпечення кібербезпеки України»[30], «Про електронні комунікації»[31] та інших. Так, положення Закону України «Про інформацію» забезпечують належне врегулювання відносин у сфері створення, збирання, отримання, зберігання, використання, поширення, охорони і захисту інформації. Саме нормами даного законодавчого акту визначено ключові принципи інформаційних відносин, встановлено перелік суб'єктів та об'єктів інформаційних відносин, особливості реалізації права на інформації, визначено види інформацію, а також окреслено загальні аспекти настання юридичної відповідальності за порушення законодавства у сфері інформації[32].

Наступний рівень нормативно-правового регулювання захисту інформації у сфері оборони складають підзаконні акти, ключовим завданням яких виступає запровадження необхідних механізмів інформаційної безпеки, що стосуються різноманітних аспектів досліджуваної галузі, у тому числі: захисту державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших основоположних інтересів особистості, суспільства та держави, що спрямовано на належне забезпечення конституційних прав і свобод індивіда на збирання, зберігання, використання та поширення інформації, забезпечення доступу до об’єктивної та достовірної інформації. До того ж, саме положеннями підзаконних нормативних документів врегульовуються питання ефективного функціонування протидії та захисту від негативного інформаційного впливу, у тому числі координованого поширення недостовірних відомостей, деструктивного пропагандистського впливу, інших інформаційних операцій,

[26] Про захист інформації в інформаційно-комунікаційних системах: Закон України № 80/94-ВР від 05.07.1994 року. ВВР, 1994, № 31, ст. 286.

[27] Про захист персональних даних: Закон України № 2297-VI від 01.06.2010 року. ВВР, 2010, № 34, ст. 481.

[28] Про державну таємницю: Закон України № 3855-XII від 21.01.1994 року. ВВР, 1994, 3 16, ст. 93.

[29] Про національну безпеку України: Закон України № 2469-VIII від 21.06.2018 року. ВВР, 2018, № 31, ст. 241.

[30] Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 року. ВВР, 2017, № 45, ст. 403.

[31] Про електронні комунікації: Закон України № 1089-IX від 16.12.2020 року. ВВР, Офіційний вісник України, 2021 р., № 6, стор. 10, стаття 306, код акта 102665/2021.

[32] Про інформацію: Закон України № 2657-XII від 02.10.1992 року. ВВР, 1992, № 48, ст. 650.

несанкціоноване поширення, використання та порушення цілісності інформації, доступ до якої обмежений. Саме зазначені нормативні акти відіграють вагому роль у процесі безперебійного функціонування механізмів, а також ефективного використання інструментів захисту інформації, зокрема у сфері оборони.

Основним завданням підзаконних нормативних актів виступає деталізація окремих положень Основного закону, а також законодавчих актів. Вони характеризуються предметністю спрямування та забезпечують належну регламентацію конкретної сфери суспільних відносин чи напрямів діяльності органів державного управління. Зокрема, до компетенції Президента України віднесено видання указів та розпоряджень: перші мають загальний характер, а другі – більш індивідуалізовані[33].

Особливу роль для захисту інформації у сфері оборони відіграє Стратегія інформаційної безпеки України, положеннями якої визначено ключові виклики та загрози для національної безпеки в інформаційній сфері, основні завдання та стратегічні цілі, що спрямовані на протидію таким загрозам, захист права на інформацію та персональних даних, а також недопущення поширення чутливої інформації з обмеженим доступом, до яких можливо віднести й військову інформацію[34]. Незважаючи на концептуальний характер, Стратегія інформаційної безпеки України була ухвалена у 2021 році, тобто до початку повномасштабного вторгнення, а отже потребує внесення змін та доповнень, враховуючи численні ризики, пов'язані з незаконним поширенням військової інформації. Цей стратегічний документ було ухвалено на певному етапі розвитку держави у тому виді, в якому сьогодні не достатньо відповідає сучасним викликам і загрозам у сфері захисту інформації у галузі оборони. При цьому, цей підзаконний акт має виступати як ключовий документ, у якому закріплено стратегічні напрямки удосконалення інформаційної безпеки держави. Так, саме Стратегія інформаційної безпеки має виступати в якості найвищого

---

33 Крупнова А.О. Правове регулювання сфери забезпечення інформаційної безпеки в Україні. Електронне наукове видання «Аналітично-порівняльне правознавство». № 11. 2023. С. 351.

34 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України № 685/2021 від 28.12.2021 року. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7. (дата звернення: 05.06.2025).

нормативного акту, окреслюючи різні напрями забезпечення захисту інформації у сфері оборони.

Важливе місце серед підзаконних нормативних актів у сфері захисту інформації у галузі оборони також займає й ціла низка інших указів Президента України. Серед них можливо виділити наступні: укази Президента України «Про Положення про технічний захист інформації в Україні»[35], «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо удосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»»[36], «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»»[37], «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»»[38], «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»»[39] та інші.

Суб'єктом нормотворчості у сфері захисту інформації у галузі оборони виступає Кабінет Міністрів України. У цьому зв'язку важливими документами, прийнятими урядом, є наступні: постанови Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»[40], «Деякі питання ліцензування господарської діяльності з надання послуг у галузі

---

[35] Про Положення про технічний захист інформації в Україні: Указ Президента України № 1229/99 від 27.09.1999 року. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text. (дата звернення: 06.06.2025).

[36] Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо удосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»: Указ Президента України № 449/2014 від 01.05.2014 року. URL: https://zakon.rada.gov.ua/laws/show/449/2014#n2. (дата звернення: 06.06.2025).

[37] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України № 447/2021 від 26.08.2021 року. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text. (дата звернення: 06.06.2025).

[38] Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України № 37/2022 від 01.02.2022 року. URL: https://zakon.rada.gov.ua/laws/show/37/2022#n5. (дата звернення: 06.06.2025).

[39] Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»: Указ Президента України № 56/2022 від 16.02.2022 року. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text. (дата звернення: 06.06.2025).

[40] Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: Постанова Кабінету Міністрів України № 373 від 29.03.2006 року. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text. (дата звернення: 06.06.2025).

криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України»[41], «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану»[42]; розпорядження Кабінету Міністрів України «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»[43], «Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року»[44], «Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки»[45] та інші.

На рівні центральних органів виконавчої влади ухвалюються накази, розпорядження та інструкції, що спрямовані на деталізацію та конкретизацію законодавчо закріплених норм. Такі нормативні акти забезпечують детальне врегулювання та уточнення організаційних і технічних аспектів захисту інформації у сфері оборони. До того ж, центральними органами виконавчої влади приймаються стандарти, правила та інструкції у сфері захисту інформації, які є обов'язковими для усіх юридичних та фізичних осіб. Зазначеною категорію підзаконних актів врегульовуються переважно наступні питання: процедури автентифікацію, стандарти шифрування, вимоги до захисту інформації, механізми обробки інформації, заходи щодо протидії кібератакам тощо. Вони сприяють забезпеченню більш ефективного дотримання норм щодо захисту

[41] Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України: Постанова Кабінету Міністрів України № 821 від 16.11.2016 року. URL: https://zakon.rada.gov.ua/laws/show/821-2016-%D0%BF#Text. (дата звернення: 06.06.2025).

[42] Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України № 263 від 12.03.2022 року. URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text. (дата звернення: 06.06.2025).

[43] Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України № 299 від 04.04.2023 року. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text. (дата звернення: 06.06.2025).

[44] Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України № 272-р від 30.03.2023 року. URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text. (дата звернення: 06.06.2025).

[45] Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки: Розпорядження Кабінету Міністрів України № 328-р від 18.04.2023 року. URL: https://zakon.rada.gov.ua/laws/show/328-2023-%D1%80#Text. (дата звернення: 06.06.2025).

інформації, у тому числі й у галузі оборони, а також більш ефективному управлінню уповноваженими суб'єктами.

Також нормативно-технічну основу захисту інформації в Україні відіграють численні галузеві стандарти, які розробляються і затверджуються державними органами чи спеціально уповноваженими організаціями, положеннями яких визначаються обов'язкові вимоги до захисту інформації у різноманітних сферах, зокрема у галузі оборони. Стандарти відіграють достатньо важливу роль у процесі захисту інформації, оскільки забезпечують дотримання принципів єдиного підходу до реалізації інформаційної безпеки, стандартизують процедури захисту інформації, механізми забезпечення цілісності, доступності та конфіденційності даних, а також заходів щодо реагування і запобігання на інформаційні загрози[46].

В Україні розроблено на прийнято цілу низку державних стандартів та нормативних документів у сфері забезпечення інформаційної безпеки. Так, серед основних державних стандартів та нормативних документів у досліджуваній сфері можливо виділити наступні: Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1-002-99)[47]; Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 2.5-004-99)[48]; Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 (НД ТЗІ 2.5-008-02)[49]; Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження,

[46] Крупнова А.О. Правове регулювання сфери забезпечення інформаційної безпеки в Україні. Електронне наукове видання «Аналітично-порівняльне правознавство». № 11. 2023. С. 352.

[47] Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1-002-99): Нормативний документ від 01.07.1999 року. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tzi.com.ua/downloads/1.1-002-99.pdf. (дата звернення: 06.06.2025).

[48] Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 2.5-004-99): Нормативний документ від 01.07.1999 року. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tzi.com.ua/downloads/2.5-004-99.pdf. (дата звернення: 06.06.2025).

[49] Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 (НД ТЗІ 2.5-008-02): Нормативний документ від 20.12.2002 року. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tzi.com.ua/downloads/2.5-008-2002.pdf. (дата звернення: 06.06.2025).

супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу[50]; Захист інформації. Технічний захист інформації. Порядок проведення робіт (ДСТУ 3396.1-96)[51] та інші.

Одним із ключових напрямів розвитку національної правової бази щодо захисту інформації виступає забезпечення їх відповідності міжнародним стандартам. Так, 04 червня 2020 року було ухвалено Закон України «Про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації». Основною метою ухвалення зазначеного законодавчого акту стало забезпечення повноцінної інтеграції європейських вимог і критеріїв оцінки захисту інформації від кіберзагроз, а також української законодавчої системи захисту інформації. Положеннями закону визначено потребу у забезпеченні відповідності між національними стандартами та європейськими стандартами у сфері управління захистом інформації щодо окремої категорії даних[52].

Додатково Державною службою спеціального зв'язку та захисту інформації було розроблено та запроваджено низку стандартів, що враховують європейські вимоги та критерії оцінки захисту інформації від кіберзагроз. Серед таких стандартів можливо виділити наступні: Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці (НД ТЗІ 1.6-005-2013)[53]; Порядок здійснення моніторингу систем захисту інформації в

---

[50]Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу: Нормативний документ від 25.12.2000 року. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tzi.com.ua/downloads/3.6-001-2000.pdf. (дата звернення: 06.06.2025.

[51] Захист інформації. Технічний захист інформації. Порядок проведення робіт (ДСТУ 3396.1-96): Державний стандарт України від 01.07.1997 року. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf. (дата звернення: 06.06.2025).

[52] Про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації: Закон України № 681-IX від 04.06.2020 року. ВВР, 2020, № 42, ст. 349.

[53] Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці (НД ТЗІ 1.6-005-2013): Нормативний документ від 15.04.2013 року. URL: https://zakon.rada.gov.ua/rada/show/v0215519-13?utm_source=chatgpt.com#Text. (дата звернення: 06.06.2025).

інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням базових та цільових профілів безпеки інформації[54]; Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (НД ТЗІ 3.6-007-21)[55]; Рекомендації з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації[56]; Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці (НД ТЗІ 3.6-004-21)[57] та інші.

У зв'язку із вищевикладеним можливо зробити висновок, що належне нормативно-правове регулювання є основоположним чинником забезпечення ефективного захисту інформації у сфері оборони України. Діюча правова база охоплює широкий спектр законодавчих і підзаконних актів, що забезпечують комплексний підхід до протидії інформаційним загрозам, охорони національної безпеки, захисту прав суб'єктів інформаційних відносин та реалізації державної інформаційної політики. Особливу роль у регулюванні цієї сфери відіграють Конституція України, норми адміністративного, кримінального та цивільного

[54] Порядок здійснення моніторингу систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використаням базових та цільових профілів безпеки інформації: Нормативний документ від 10.03.2025 року. URL: https://zakon.rada.gov.ua/laws/show/z0448-25#Text. (дата звернення: 06.06.2025).

[55] Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (НД ТЗІ 3.6-007-21): Нормативний документ від 01.07.2021 року. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66075. (дата звернення: 06.06.2025).

[56] Про затвердження Рекомендацій з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 354 від 10.07.2024 року. URL: https://zakon.rada.gov.ua/rada/show/v0354519-24#Text. (дата звернення: 06.06.2025).

[57] Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці (НД ТЗІ 3.6-004-21): Нормативний документ від 01.07.2021 року. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66072. (дата звернення: 06.06.2025).

права, спеціальні закони, укази Президента, постанови Кабінету Міністрів та нормативно-технічні акти.

Правовий режим воєнного стану, а також специфічні нормативні положення, що виникли у відповідь на актуальні виклики воєнного часу, додатково підвищили потребу у формуванні правових механізмів протидії незаконному розголошенню чутливої військової інформації. Окрім цього, вектор на гармонізацію національного законодавства із міжнародними стандартами посилює здатність держави ефективно реагувати на сучасні кіберзагрози та інші форми інформаційного впливу.

1.3. Міжнародні стандарти запобігання розголошенню інформації у сфері оборони

Нормативно-правове забезпечення запобіганню розголошенню інформації у сфері оборони на міжнародному рівні виступає в якості однієї з основною умови світового миру і порядку. Так, обмеження доступу до воєнної інформації та захист даних у сфері оборони врегульовано положеннями цілої низки законодавчих актів. Зокрема, у відповідності до ч. 2 ст. 3 Конвенції Ради Європи про доступ до офіційних документів, у доступі до інформації може бути відмовлено у випадках, коли її розголошення може спричинити загрозу національній безпеці, обороні, міжнародним відносинам та громадській безпеці за умови, що відсутній переважаючий суспільний інтерес щодо оприлюднення таких даних[58].

Більш детальне тлумачення підстав для обмеження поширення інформації у сфері оборони представлено у так званих Йоганнесбурзьких принципах «Національна безпека, свобода висловлювання і доступ до інформації». Серед ключових засад встановлення обмежень визначено наступні: визначеність на законодавчому рівні; забезпечення національної безпеки та узгодженість із

[58] Конвенція Ради Європи про доступ до офіційних документів: Міжнародний документ від 18.06.2009 року. URL: https://zakon.rada.gov.ua/laws/show/994_001-09#Text. (дата звернення: 09.06.2025).

демократичними засадами функціонування суспільства. При цьому, будь-яке обмеження щодо доступу та поширення інформації має бути закріплено у положеннях законодавчого акту, який є чітким, загальнодоступним та конкретним, що надає можливість для визначення наявності або відсутності протиправності певної дії. Законодавством має бути встановлено адекватні гарантії щодо недопущення порушення таких вимог, у тому числі повного, оперативного та ефективного юридичного розгляду обґрунтованості встановлених обмежень судовими органами. Зазначеними принципами встановлено заборону на категоричну відмову в доступі до будь-якої інформації у сфері безпеки та оборони, проте законодавством має бути конкретизовано ті різновиди інформації, які підлягають обмеженому доступу з метою повноцінного забезпечення національної безпеки та оборони[59].

У випадках, коли запроваджені обмеження не мають на меті забезпечення реального захисту національної безпеки чи територіальної цілісності держави від застосування чи потенційної загрози застосування військової сили, воно визнається нелегітимним. У разі запровадження правових режимів надзвичайного стану, що зумовлено загрозами для існування держави, можуть бути встановлено обмеження на доступ і поширення інформації, проте виключно в обсязі, достатньому для забезпечення національної безпеки, а також за умови, що це не суперечить міжнародним зобов'язанням уряду[60].

У контексті досліджуваного питання варто звернути на принцип 15 «Загальне правило оприлюднення таємної інформації», у відповідності до якого жодну особу не може бути піддано покаранню, обґрунтовуючи це потребами забезпеченням національної безпеки, за поширення таємної інформації у наступних випадках:

внаслідок такого оприлюднення не спричинено та об'єктивно не може бути спричинено шкоду національній безпеці та обороні;

---

[59] The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. URL: https://www.refworld.org/legal/resolution/art19/1995/en/41603. (дата звернення: 09.06.2025).

[60] Прокопчук Т. Міжнародні стандарти кримінально-правової охорони інформації з обмеженим доступом. Підприємництво, господарство і право. № 3, 2021. С. 234.

шкода від оприлюднення таємної інформації є меншою, аніж суспільний інтерес.

Окрім цього, жодну особу не може бути піддано переслідуванню, обґрунтовуючи це інтересами національної безпеки, за поширення інформації, яку було отримано у процесі проходження державної служби. При цьому, суспільний інтерес має значно перевищувати шкоду від поширення такої інформації[61].

У випадках, коли інформацію вже було оприлюднено, навіть незаконним шляхом, будь-яке обґрунтування щодо припинення її поширення є нікчемним на фоні права суспільства на дотримання важливої інформації. Отже, юридично значимим є виключно той факт розголошення, що має відношення до конкретної інформації вперше. У разі, коли інформація вже стала загальнодоступною, повторне її поширення не може кваліфікуватися як неправомірне. До того ж, будь-які обмеження, санкції та міра юридичної відповідальності мають встановлюватися із дотриманням принципу співмірності із тяжкістю вчиненого діяння[62].

Ще одним міжнародно-правовим актом, яким врегульовано окремі аспекти захисту інформації у сфері оборони, є Конвенція про кіберзлочинність. у відповідності до зазначеного документа на держав-підписантів покладено обов'язок щодо вжиття таких законодавчих та інших заходів, що є необхідними для встановлення кримінального покарання за скоєння навмисного перешкоджання функціонуванню комп'ютерних систем (несанкціонованого введення, передача, знищення, пошкодження, заміна, погіршення чи приховування комп'ютерних баз даних) на національному рівні[63].

Новітнім етапом розвитку міжнародно-правового регулювання у цій сфері стало ухвалення Генеральною Асамблеєю ООН у грудні 2024 року Конвенції

---

[61] The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. URL: https://www.refworld.org/legal/resolution/art19/1995/en/41603. (дата звернення: 09.06.2025).

[62] Там само.

[63] Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text. (дата звернення: 09.06.2025).

ООН проти кіберзлочинності, яка була відкрита для підписання державами у Ханої (В'єтнам) у 2025 році. Це перший універсальний договір ООН, спрямований на боротьбу з цифровими злочинами, що встановлює юридично обов'язкові інструменти для зміцнення колективного захисту від кіберзлочинності. Конвенція передбачає криміналізацію широкого спектра діянь, пов'язаних із несанкціонованим доступом, перехопленням та втручанням у комп'ютерні дані, а також закріплює механізми міжнародного співробітництва для збирання електронних доказів, що є критично важливим для розслідування витоків оборонної інформації. 25 жовтня 2025 року цей документ підписали 65 держав, і він набуде чинності через 90 днів після його ратифікації 40 країнами. Підписання та подальша ратифікація цієї Конвенції Україною сприятиме гармонізації національного законодавства з новітніми міжнародними стандартами у сфері захисту інформації та посилить здатність держави ефективно протидіяти інформаційним загрозам, зокрема у сфері оборони в умовах воєнного стану.

Також важливим нормативно-правовим документом у сфері захисту інформації є Директива Європейського парламенту і ради ЄС № 2022/2555 про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу. Так, згідно положень зазначеного міжнародного документа передбачено встановлення інструментів, які сприяють забезпеченню високого рівня безпеки інформаційних та мережевих систем, а також покращення внутрішнього ринку. Нормами досліджуваного міжнародного документа на держави-члени ЄС покладено наступні обов'язки:

ухвалення на національному рівні стратегій безпеки інформаційних і мережевих систем;

створення Групи співпраці для сприяння та підтримки стратегічній взаємодії та обміну інформацією між державами-членами, а також підвищення довіри між ними;

створення мережі груп реагування на ризики і загрози, пов'язані з безпекою комп'ютерних систем (мережа CSIRT), що має на меті забезпечення ефективній співпраці та оперативній взаємодії між державами;

встановлення вимог щодо безпеки та повідомлень для операторів мережевих і комп'ютерних послуг;

призначення на національному рівні уповноважених осіб чи створення спеціалізованих структур, єдиних комунікаційних пунктів CSIRT, на яких покладено виконання функцій щодо забезпечення безпеки інформаційних і мережевих систем[64].

При цьому, положеннями вказаної вище Директиви не обмежуються дії та заходи держав, які запроваджуються з метою захисту національної безпеки, зокрема щодо захисту інформації, розкриття якої можуть суперечити основоположним принципам безпеки держави, підтримці правопорядку, чи зашкодити розслідуванню, розкриттю або кримінальному переслідуванню осіб, винних у скоєнні кримінального правопорушення. Зазначений документ є одним із ключових інструментів внутрішнього ринку, що сприяє підвищенню здатності ЄС до протистояння загрозам в інформаційному просторі. До того ж, вказаним міжнародним документом передбачено запровадження конкретних заходів підвищення кібербезпеки та зниження впливу зростаючих загроз для інформаційних та мережевих систем, що використовуються в основних державних секторах, у тому числі й у галузі оборони[65].

Поряд із цим, у грудні 2025 року завершилася імплементація державами-членами ЄС Директиви NIS 2 (2022/2555), яка поширює підвищені вимоги кібербезпеки на оборонно-промисловий комплекс. Крім того, набув чинності Кібер-Акт стійкості (Cyber Resilience Act), котрий зобов'язує виробників продуктів із цифровими компонентами, у тому числі військового призначення,

[64] Директива Європейського парламенту і ради ЄС про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Міжнародний документ № 2022/2555 від 14.12.2022 року. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text. (дата звернення: 09.06.2025).

[65] Директива Європейського парламенту і ради ЄС про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Міжнародний документ № 2022/2555 від 14.12.2022 року. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text. (дата звернення: 09.06.2025).

повідомляти про інциденти безпеки протягом 24 годин. Ці інструменти формують додаткові зобов'язання для України в контексті євроінтеграції, стимулюючи уніфікацію національних підходів до захисту оборонної інформації з європейськими.

Після початку повномасштабного вторгнення проти України особливо актуалізується проблема пропаганди війни, що спричиняє шкоду чи несе реальну загрозу її спричинення для безпеки інформаційного простору, що зумовлено спотворенням фактів, маніпулюванням суспільством та поширенням дезінформації. Пропаганда війни здатна сформувати роз'єднуюче та вороже інформаційне середовище, негативно вплинути на міжнародні відносини, підвищити ворожість та недовіру між державами, призвести до порушень міжнародного гуманітарного права шляхом підбурювання до вчинення злочинів геноциду, воєнних злочинів та злочинів проти людяності, а також виступати в якості інструмента применшення, приховування чи викривлення наслідків таких злочинів.

Пропаганда є специфічною формою соціальних відносин між окремими суб’єктами глобалізації, які дотримуються певних стандартів і моделей світу. Залежно від характеру, спрямованості та особливостей агресивних інформаційних впливів виокремлюють різні види технологій їх реалізації. Особлива активізація пропаганди спостерігається в умовах воєнного конфлікту. Незважаючи на те, що військова пропаганда існує протягом тривалого часу, нині відбувається зміна її форм та методів[66].

У цьому зв'язку варто звернути увагу на положення IV Конвенції про закони і звичаї війни на суходолі. Незважаючи на те, що у них чітко не встановлено заборону на пропаганду війни, проте саме у цих міжнародних документах закладено основу для врегулювання поведінки держав у випадку воєнного конфлікту. Зокрема, ст. 29 зазначеного міжнародного документа врегульовано питання шпигунства як одного із правомірних способів ведення

[66] Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки: монографія / за заг. ред.. В.І. Борисова, М.В. Карчевського, М.В. Шепітька. Харків: Право, 2023. С. 44.

війни. Як зазначено у ч. 1 вказаної норми, шпигуном визнається виключно особа, яка діє таємно чи під фальшивим приводом, а також реалізовує заходи щодо збирання інформації у зоні бойових дій в інтересах однієї з воюючих держав, що має на меті її подальшу передачу супротивнику. При цьому, ст. 31 встановлено, що шпигун, який повернувся до своєї армії, проте у подальшому потрапив у полон, не несе відповідальності за попередні акти шпигунства та визнається військовополоненим[67].

Також положеннями Статуту Нюрнберзького трибуналу було встановлено, що особа, винна у вчиненні злочинів проти миру, людяності та воєнних злочинів, у тому числі у ролі керівників, організаторів, підбурювачів та пособників, яка приймала участь у складанні чи реалізації спільного плану чи змови, спрямованих на скоєння будь-якого із перелічених міжнародних злочинів, несе індивідуальну відповідальність, зокрема за діяння інших осіб, якими безпосередньо реалізовані заходи, спрямовані на досягнення злочинної мети. Саме зазначені положення у подальшому виступили в якості правової основи у процесі притягнення до міжнародної кримінальної відповідальності головних пропагандистів фашистської Німеччини: головного редактора пропагандистського друкованого видання «Der Stürmer» Ю. Штрайхера та очільника преси третього рейху О. Дітріха, якими було допущено «зараження свідомості німецького народу вірусом антисемізму» та підбурили німців до здійснення активного переслідування[68].

Питання пропаганди як однієї із загроз для національної безпеки розкрито й у положеннях Заключого акту наради з питань безпеки та співробітництва в Європі 1975 року. Одним із ключових принципів зазначеного документа було визнано обов'язок кожної держави щодо сприяння у створенні атмосфери поваги та довіри на міжнародному рівні, у тому числі шляхом утримання від пропаганди

---

[67] IV Конвенція про закони і звичаї війни на суходолі та додаток до неї: Положення про закони і звичаї війни на суходолі: Міжнародний документ від 18.0.1907 року. URL: https://zakon.rada.gov.ua/laws/show/995_222#Text. (дата звернення: 09.06.2025).

[68] Gordon G. S. The Propaganda Prosecutions at Nuremberg: The Origin of Atrocity Speech Law and the Touchstone for Normative Evolution. Loyola of Los Angeles International and Comparative Law Review. 2017. Vol. 39, № 1. P. 219.

ведення агресивної війни, застосування сили чи погрози силою, оскільки це порушує ключові засади міждержавної співпраці[69].

Додатковим важелем захисту оборонної інформації на рівні ЄС став Регламент (ЄС) 2025/2643 Європейського Парламенту та Ради від 16 грудня 2025 року, яким затверджено Європейську програму оборонної промисловості (EDIP). Цей нормативний акт встановлює обов'язок держав-членів, Європейської комісії, Європейської служби зовнішніх справ та Європейського оборонного агентства забезпечувати захист секретної інформації, а також комерційної таємниці й іншої чутливої інформації, отриманої або створеної в процесі реалізації програми. Таким чином, на рівні ЄС створюється єдиний режим охорони оборонних даних, що поширюється на всі етапи – від створення до обміну та зберігання інформації.

Заборона пропаганди війни перебуває у тісному взаємозв'язку із дезінформаційним впливом. У сучасних економічних конфліктах дезінформація стала суттєвим оперативним, тактичним і стратегічним елементом приховування своїх намірів. Вона поширюється з метою певного впливу на опонента (конкурента) та зниження його управлінської спроможності, а також контролю поточної ринкової ситуації. В умовах війни дезінформація призводить до поширення фейкових наративів, негативних стереотипів, дискримінації та мови ворожнечі, зростання суспільної поляризації, а також виступає в якості одного з ключових інструментів ведення гібридної війни у міжнародних конфліктах[70].

У контексті досліджуваного питання на увагу заслуговують положення Спільної декларації щодо свободи вираження поглядів і «фейкових новин», дезінформації та пропаганди 2017 року. Положеннями зазначеного міжнародного документа встановлено заборону на поширення інформації, в основу якої покладено нечіткі або двозначні ідеї, у тому числі й неправдивих новинних повідомлень чи необ'єктивної інформації, що суперечить цілій низці міжнародних стандартів. До того ж, норми національного кримінального

[69] Helsinki Final Act. Organization for Security and Cooperation in Europe . 1 August 1975. URL: https://www.osce.org/helsinki-final-act. (дата звернення: 09.06.2025).

[70] Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки: монографія / за заг. ред.. В.І. Борисова, М.В. Карчевського, М.В. Шепітька. Харків: Право, 2023. С. 44.

законодавства щодо здійснення наклепу є надмірно суворими та підлягають скасуванню. При цьому, положення національного цивільного законодавства щодо притягнення до юридичної відповідальності за наклеп визнаються законними виключно у випадку, коли інша сторона має можливість для реального доведення правдивості тверджень та використовувати інші засоби захисту[71].

У зв'язку із вищевикладеним можливо зробити висновок, що нормативно-правове забезпечення у сфері запобігання розголошенню інформації у сфері оборони на міжнародному рівні ґрунтується на комплексі актів, що покликані збалансувати захист національної безпеки з повагою до прав людини та принципів демократії. Основу становлять міжнародні договори, такі як Конвенція Ради Європи про доступ до офіційних документів, Йоганнесбурзькі принципи, Конвенція про кіберзлочинність, Директива ЄС № 2022/2555, а також акти міжнародного гуманітарного та кримінального права. Ці документи визначають чіткі правові межі для обмеження доступу до інформації, вимагаючи законодавчої визначеності, пропорційності, судового контролю та пріоритету суспільного інтересу. Окрема увага приділяється недопущенню зловживань поняттям «національна безпека» для придушення свободи вираження. Забороняється кримінальне переслідування за розголошення даних, яке не несе реальної загрози обороні або коли суспільна цінність такої інформації переважає можливу шкоду.

Поряд із цим, у контексті сучасних воєнних конфліктів, акцент робиться на боротьбі з пропагандою війни, дезінформацією та фейками як елементами гібридної агресії. Міжнародне право засуджує пропаганду агресії як загрозу миру, вимагаючи від держав утримуватися від таких дій та створювати атмосферу міжнародної довіри. Отже, міжнародна правова система у сфері захисту інформації в оборонній галузі визнає критичну важливість інформаційної безпеки, встановлюючи високі стандарти захисту оборонної

[71] Joint Declaration on freedom of expression and «fake news», disinformation and PROPAGANDA № FOM.GAL/3/17 on 3 March 2017. URL: https://www.osce.org/files/f/ documents/6/8/302796.pdf. (дата звернення: 09.06.2025).

інформації, зберігаючи водночас баланс між безпекою, прозорістю та свободою вираження поглядів.

Висновки до розділу 1

Стан безпеки виступає в якості фундаментальної потреби держави і суспільства, одним зі складових елементів якого є інформаційна безпека, відіграючи вагому роль для захисту важливих інтересів, оскільки інформаційний простір одночасно є ресурсом та полем потенційної агресії. Інформаційна безпека включає правові, технічні, соціальні та політичні аспекти, що спрямовані на запобігання загрозам, захист інформаційних ресурсів та гарантуванні прав людини і громадянина. Особливої значимості інформаційна безпека набуває в умовах воєнного стану, оскільки саме вона спрямована на забезпечення стійкості національної безпеки, стабільного розвитку держави та збереження суверенітету.

Нормативно-правове регулювання виступає в якості основи захисту інформації у галузі оборони України, та включає Конституцію України, норми адміністративного, цивільного та кримінального права, а також сукупність спеціальних законодавчих і підзаконних актів. В умовах воєнного стану особливо важливим є вдосконалення механізмів протидії незаконному поширенню чутливої військової інформації та узгодження національного законодавства з міжнародними стандартами, що гарантує стійкість оборонної системи й захист національних інтересів.

Міжнародне нормативно-правове забезпечення захисту оборонної інформації поєднує захист національної безпеки з дотриманням прав людини та демократичних принципів. Ключові акти, як-от Конвенція Ради Європи, Йоганнесбурзькі принципи, Конвенція про кіберзлочинність та Директива ЄС № 2022/2555, визначають межі обмеження доступу до інформації, забезпечують пропорційність, законодавчу визначеність і судовий контроль. Особлива увага приділяється протидії пропаганді, дезінформації та фейкам, що загрожують міжнародній безпеці, забезпечуючи баланс між оборонною безпекою та свободою вираження.

РОЗДІЛ 2
КРИМІНАЛЬНО-ПРАВОВИЙ АНАЛІЗ НЕЗАКОННОГО РОЗГОЛОШЕННЯ ІНФОРМАЦІЇ ПРО ВІЙСЬКОВІ ОПЕРАЦІЇ

2.1. Загальна характеристика складу злочину, передбаченого ст. 114-2 КК України

Після початку повномасштабного вторгнення проти України особливої значимості набувають кримінально-правові норми, спрямовані на захист національної безпеки та обороноздатності держави в цілому. Однією з таких кримінально-правових норм виступає ст. 114-2 КК України, якою встановлено кримінальну відповідальність за несанкціоноване поширення інформації щодо переміщення, розміщення та направлення ЗСУ чи інших військових формувань, створених та існуючих у відповідності до законодавства України[72].

Стаття 114-2 КК України виступає в якості відносно новельної кримінально-правової норми, на доповнення якою положення кримінального закону напряму впливає існування нагальної потреби у підвищенні рівня захисту системи національної безпеки держави в умовах збройної агресії. Доповнення кримінального закону вказаною нормою стало своєрідною формою реагування законодавця на новітні виклики, які виникають через поширення використання інформаційно-комунікаційних технологій, цифрових засобів передачі інформації та соціальних мереж, внаслідок чого значно спрощено процес поширення інформації військового значення. При цьому, в умовах воєнного стану та активного ведення бойових дій навіть незначні чи неповні відомості щодо переміщення або розташування військових підрозділів може використовуватися ворогом для досягнення власних цілей, що значно підвищує ступінь суспільної небезпечності вказаних діянь.

Диспозицією статті 114-2 КК України передбачено настання кримінальної відповідальності за несанкціоноване поширення інформації про направлення,

[72] Кримінальний кодекс України: Закон України № 2341-III від 05.04.2001 року. ВВР, 2001, № 25-26, ст. 131.

переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану. У той же час, законодавцем не встановлено вичерпного переліку інформації, яка визнається забороненою для поширення, що свідчить про бланкетний характер вказаної кримінально-правової норми. Отже, з метою розуміння її змісту та меж застосування існує потреба у зверненні до інших нормативно-правових актів, якими регламентовано питання оборони, національної та інформаційної безпеки, дотримання режиму секретності та правового режиму воєнного стану в цілому.

Подальший розвиток нормативно-правового регулювання у цій сфері відбувся з ухваленням Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інфраструктури» від 27 березня 2025 року № 4336-IX, яким посилено вимоги до кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури, що безпосередньо стосується й оборонного сектору[73]. Цей закон став відповіддю на зростання кібератак проти України та спрямований на підвищення стійкості інформаційних систем державних органів, у тому числі у сфері оборони. Окрім того, у 2025 році Кабінетом Міністрів України затверджено план заходів на 2025 рік з реалізації Стратегії кібербезпеки України, який передбачає приведення захисту інформаційних систем оборони до стандартів НАТО.

Юридичний зміст кримінально-правової заборони, закріпленої у ст. 114-2 КК України, надає можливість стверджувати про її належність до категорії злочинів проти основ національної безпеки України, незважаючи на притаманність спеціалізованого характеру. Порівняно з класичними формами посягань на національну безпеку, зокрема шпигунством чи державною зрадою,

[73] Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України № 2160-IX від 04.03.2022 року. Офіційний вісник України, 2022, № 33, стор. 90, ст. 145, код акта 110988/2022.

законодавцем ухвалено рішення щодо криміналізації самого факту несанкціонованого поширення інформації, незалежно на спричинення конкретних суспільно-небезпечних наслідків. Отже, склад кримінального правопорушення, передбаченого ст. 114-2 КК України, є формальним, а кримінально-протиправне діяння вважається закінченим з моменту поширення відповідної інформації хоча б одному сторонньому суб'єкту.

Специфіка практичного застосування даної кримінально-правової норми полягає у тому, що притягнення до кримінальної відповідальності винних осіб може бути здійснено виключно у випадку, коли таке поширення інформації було здійснено у період дії правового режиму воєнного стану. Саме запровадження і дія правового режиму воєнного стану відіграє роль своєрідної передумови криміналізації поведінки суб'єкта кримінального правопорушення. Отже, у випадку вчинення відповідних дій після завершення чи скасування дії правового режиму воєнного стану не може йти мова про наявність складу злочину, передбаченого ст. 114-2 КК України, проте можуть виступати в якості самостійного складу кримінального правопорушення, передбаченого іншою статтею кримінального закону. Наявність такої законодавчої конструкції свідчить про існування тісного взаємозв'язку між досліджуваною нормою та конкретною суспільно-політичною обстановкою, тобто для неї є притаманним адаптивний характер.

Одним із ключових елементів об'єктивної сторони кримінального правопорушення, передбаченого ст. 114-2 КК України, виступає категорія «несанкціоноване поширення інформації», що відрізняється оціночним характером, оскільки відсутнє чітке визначення даної категорії на законодавчому рівні. У науковій літературі під досліджуваною категорією прийнято розуміти доведення інформації до інших осіб будь-яким способом за умови відсутності відповідного дозволу уповноважених органів державної влади. Окрему увагу варто звернути на те, що не має значення форма такого поширення: воно може здійснюватися у форматі публікації у відкритих джерелах, передача інформації у приватному спілкуванні, у тому числі із використанням месенджерів, засобів

електронного поштового зв'язку чи в усній формі. Отже, навіть у випадку передачі охоронюваної кримінальним законом інформації одній особі за відсутності відповідного дозволу мова йде про існування самостійного складу кримінального правопорушення.

Основною метою криміналізації вказаного діяння виступає забезпечення високого рівня інформаційної безпеки, яка є важливим елементом національної безпеки будь-якої держави. Ключовим завданням законодавця при криміналізації досліджуваного діяння виступає запобігання витоку інформації, що може використовуватися агресором для планування і проведення військових операцій, коригування вогню чи реалізації диверсійних заходів. Особливої значимості це набуває в умовах ведення сучасної війни, коли інформація відіграє ключову роль та має вагоме значення, на рівні з матеріальними ресурсами і військовою технікою. Отже, існування кримінально-правової заборони, закріпленої у ст. 114-2 КК України, має яскраво виражений превентивний характер, оскільки спрямована переважно на попередження виникнення потенційно негативних наслідків.

У контексті досліджуваного питання варто звернути увагу на те, що у мирний час такі діяння могли кваліфікуватися як форма порушення режиму інформаційної безпеки чи трудової дисципліни. Проте, в умовах воєнного стану вони здійснюють безпосередній вплив на результативність та ефективність проведення військових операцій. Несанкціоноване поширення інформації щодо місцезнаходження військових підрозділів, маршрути переміщення військової техніки та озброєння, місця розташування об'єктів військової інфраструктури тощо, може призвести до нанесення агресором точкових ударів, коригування артилерійських обстрілів чи організації і проведення диверсійних заходів. Отже, навіть у випадку відсутності безпосередньої комунікації з ворогом особа, якою вчинено несанкціоноване поширення відповідної військової інформації, здійснює об'єктивне сприяння підриву обороноздатності держави[74].

[74] Гурін, О. М., Леках, А. А., Старцев, В. В., Мусієнко, О. П., & Гурін, І. О. (2023). Аналіз підходів сучасності щодо створювання системи моніторингу та трекінгу переміщення військових вантажів. Системи озброєння і військова техніка, (2 (74)), 42-51.

Вагомим фактором, який обумовлює криміналізацію несанкціонованого поширення військової інформації, виступає активізація розвитку інформаційних і цифрових технологій, месенджерів та соціальних мереж. Більшість сучасних засобів комунікації дозволяють миттєво поширювати інформацію серед необмеженого кола суб'єктів, що лише ускладнює контроль за її обігом. Окрім цього, специфіка цифрового середовища полягає у можливості легкого переадресування приватних повідомлень чи їх оприлюднення, внаслідок чого формується ефект «лавиноподібного» поширення інформації. У зазначених умовах традиційні механізми притягнення до адміністративної чи дисциплінарної відповідальності залишаються неефективними, у зв'язку з чим існує потреба у застосуванні кримінально-правових засобів реагування.

У той же час, на практиці застосування вказаної норми зумовлює виникнення цілої низки проблемних питань. Зокрема, це пов'язано з невизначеністю предмета кримінального правопорушення, оскільки відсутнє законодавче закріплення переліку інформації, що підлягає захисту. Окрім цього, такі категорії як «переміщення», «направлення», «розміщення» тощо мають переважно оціночний характер, що призводить до розбіжностей при їх тлумаченні у процесі правозастосування.

Також вагомою проблемою виступає необхідність розмежування кримінального правопорушення, передбаченого ст. 114-2 КК України, від суміжних складів злочинів проти національної безпеки, зокрема від державної зради чи шпигунства, внаслідок чого виникає своєрідна конкуренція між кримінально-правовими нормами. В окремих випадках це може призводити до підвищення ризиків надмірної криміналізації, коли до кримінальної відповідальності притягаються особи, які не усвідомлювали у повній мірі рівень суспільної небезпечності вчиненого діяння.

У великій кількості випадків вчинення поширення військової інформації зазначене діяння не має прямого умислу на спричинення шкоди державі, а здійснюються переважно з необережності, недооцінювання потенційних наслідків чи необізнаності. При цьому, в умовах воєнного стану такі діяння

можуть призводити до катастрофічних наслідків, що зумовлює потребу у встановленні кримінальної відповідальності незалежно від наявності спеціальної мети – сприяння агресору. У даному випадку законодавець виходить з того, що існує досить високий рівень об'єктивної небезпеки таких діянь, що потребує жорстких превентивних заходів реагування[75].

Ще одним вагомим аргументом на підтримку криміналізації поширення військової інформації в умовах воєнного стану виступає існування потреби у формуванні в суспільстві високого рівня правосвідомості та усвідомлення громадянами відповідальності за користування інформацією. Окрім каральної функції, кримінально-правові заборони виконують виховну та превентивну, що свідчить про особливу значимість військової інформації. Завдяки цьому забезпечується формування в громадськості усвідомлення того, що навіть вчинення таких незначних на перший погляд дій як опублікування фотознімків чи відео, може призвести до настання потенційних чи реальних загроз для національної безпеки держави в цілому.

Окрім цього, криміналізація досліджуваного діяння виступає в якості своєрідної форми реагування на нові форми та способи ведення гібридної війни, в яких активізується використання інформаційно-психологічних операцій. Агресор прагне здійснювати цілеспрямоване стимулювання громадян до поширення певної інформації чи використання відкритих джерел для отримання розвідувальної інформації. У такому випадку навіть несвідоме поширення інформації надає можливість для фактичного інтегрування у систему розвідувальної діяльності супротивника.

У той же час, доцільність криміналізації поширення військової інформації варто оцінювати через призму критеріїв пропорційності кримінально-правового впливу. Надмірно широке тлумачення встановлених заборон може призводити до необґрунтованого обмеження свободи слова та вираження поглядів, а також інших конституційних прав. У цьому зв'язку важливим елементом виступає

[75] Дубняк, М. В. (2022). Конституційне право на свободу слова та кримінальна відповідальність за несанкціоноване поширення інформації. *Правові засоби протидії злочинам проти основ національної безпеки в умовах військової агресії*, 68-72.

забезпечення балансу між інтересами національної безпеки і правами людини. Проте, в умовах правового режиму воєнного стану перевага надається безпеці держави, що у повній мірі узгоджується як із нормами національного законодавства, так і міжнародними стандартами.

Отже, доповнення КК України статтею 114-2 виступає в якості важливого інструмента забезпечення інформаційної безпеки як важливого складового елемента національної безпеки в умовах воєнного стану. Її специфіка полягає у формальному складі кримінального правопорушення, а також наявності динамічного і розширеного предмета кримінально-правового регулювання, що залежить від контексту правозастосування. У той же час, низка проблемних питань, що виникають у процесі тлумачення та практичного застосування даної кримінально-правової норми, свідчать про існування нагальної потреби в її подальшому науковому осмисленні та вдосконаленні.

2.2. Об'єктивні ознаки незаконного розголошення інформації про військові операції

Об’єктивні ознаки злочину, передбаченого статтею 114-2 Кримінального кодексу України, є ключовим елементом його кримінально-правової характеристики, оскільки саме через їх дослідження розкривається зовнішній прояв суспільно небезпечного посягання, визначаються межі кримінальної відповідальності та забезпечується правильна кваліфікація відповідних діянь. У сучасних умовах ведення збройної боротьби, що характеризується тісною інтеграцією військових, інформаційних та технологічних компонентів, об’єктивна сторона злочинів, пов’язаних із поширенням інформації про військові операції, набуває особливої складності та багатовимірності. Це обумовлює необхідність її комплексного аналізу з урахуванням як традиційних кримінально-правових підходів, так і новітніх викликів, пов’язаних із розвитком цифрового середовища.

Передусім слід зазначити, що центральною ознакою об’єктивної сторони є суспільно небезпечне діяння у формі несанкціонованого поширення інформації. У теорії кримінального права діяння розглядається як усвідомлена поведінка особи, яка має зовнішній прояв у вигляді дії або бездіяльності. У випадку злочину, передбаченого статтею 114-2 КК України, мова йде саме про активну форму поведінки, що виражається у доведенні певних відомостей до відома інших осіб. Водночас особливістю цього діяння є те, що воно не обмежується класичним розумінням передачі інформації, а охоплює будь-які форми її доведення до інших суб’єктів, включаючи опосередковані способи комунікації.

Поняття «поширення інформації» у контексті досліджуваної норми має максимально широкий зміст і підлягає розширювальному тлумаченню. Воно охоплює як публічні форми комунікації, так і приватні канали передачі даних. При цьому принципово важливим є те, що кількість осіб, яким стала відома інформація, не має вирішального значення для кваліфікації діяння. Навіть передача відомостей одній особі утворює склад злочину, оскільки створює потенційну можливість їх подальшого неконтрольованого поширення. У цьому проявляється специфіка інформаційних відносин у сучасному суспільстві, де будь-яке повідомлення може бути миттєво репліковане та поширене серед необмеженого кола осіб.

Особливої уваги заслуговує характеристика несанкціонованості як обов’язкової ознаки об’єктивної сторони. Несанкціонованість означає відсутність передбаченого законом або відповідними нормативними актами дозволу на поширення інформації. Вона може проявлятися у різних формах, зокрема як повне ігнорування встановлених обмежень, так і як порушення визначеного порядку обігу інформації. Важливо підкреслити, що наявність доступу до інформації не означає автоматичного права на її поширення. Особа може легально отримати відповідні відомості, однак їх подальше розголошення без належного погодження буде визнаватися протиправним.

Предметом злочину виступає інформація про військові операції, яка характеризується особливим змістом і значенням для забезпечення

обороноздатності держави. У сучасному науковому розумінні така інформація не обмежується лише безпосередніми відомостями про бойові дії, але включає широкий спектр даних, що можуть бути використані для аналізу військової обстановки. Це можуть бути відомості про місцезнаходження військових підрозділів, маршрути їх переміщення, обсяги та характер озброєння, логістичні маршрути, результати бойових операцій, а також інші дані, які дозволяють зробити висновки про стан і діяльність військових формувань [76].

Суттєвою особливістю предмета є його багаторівневий характер. Інформація може мати як прямий, так і опосередкований зв'язок із військовими операціями. Наприклад, прямими є дані про координати військових об'єктів або час їх переміщення, тоді як опосередкованими можуть бути зображення місцевості, звуки бойових дій або навіть коментарі, що дозволяють ідентифікувати певні обставини. У сучасних умовах особливого значення набувають так звані метадані, зокрема інформація про час, місце та технічні параметри створення цифрових файлів. Такі дані можуть бути непомітними для пересічного користувача, однак становлять значну цінність для спеціалізованих служб противника.

Окремо слід акцентувати увагу на феномені кумулятивного ефекту інформації, який полягає у тому, що окремі фрагменти даних, які самі по собі не мають вирішального значення, у сукупності можуть утворювати повну та достовірну картину військової обстановки. У цьому контексті навіть незначні повідомлення можуть відігравати роль елементів більшої інформаційної мозаїки, яка використовується для розвідувальних цілей. Саме ця обставина обумовлює необхідність криміналізації навіть таких форм поведінки, які на перший погляд здаються малозначними.

Формальний характер складу злочину є ще однією визначальною рисою об'єктивної сторони. Це означає, що для визнання діяння закінченим достатньо встановити сам факт поширення інформації без необхідності доведення настання

[76] Карпенко, М. І., & Попченкова, І. М. (2016). Причини, наслідки та профілактика військових злочинів, зокрема за ст. 422 КК України. *Юридична наука*, (1), 93-109.

конкретних шкідливих наслідків. Такий підхід пояснюється високим рівнем латентності та складністю фіксації наслідків у сфері інформаційної безпеки. У багатьох випадках використання поширеної інформації противником залишається непомітним або не піддається точному встановленню. Водночас потенційна небезпека таких дій є настільки значною, що законодавець визнає за необхідне реагувати на них вже на стадії створення загрози.

Разом із тим у науковій літературі звертається увага на те, що формальний склад не виключає врахування наслідків як додаткового критерію оцінки суспільної небезпечності діяння. Якщо буде встановлено, що поширена інформація спричинила конкретні негативні наслідки, це може свідчити про підвищений ступінь тяжкості злочину та впливати на призначення покарання. Таким чином, наслідки, хоча і не є обов'язковою ознакою складу, відіграють важливу роль у правозастосовній практиці.

Обстановка вчинення злочину, яка полягає у наявності воєнного або надзвичайного стану, є обов'язковою конструктивною ознакою об'єктивної сторони. Саме ця обставина надає відповідним діям підвищеної суспільної небезпечності та обумовлює їх криміналізацію. У мирний час аналогічні дії могли б розглядатися як адміністративні правопорушення або дисциплінарні проступки, однак в умовах війни вони набувають якісно нового значення. Воєнний стан створює специфічні умови, за яких інформація стає одним із ключових факторів успішності військових операцій, а її витік може мати безпосередній вплив на їх результати.

Не менш важливим є аналіз способів вчинення злочину, які відображають конкретні механізми поширення інформації. У сучасних умовах домінуючими є цифрові способи, що включають використання соціальних мереж, месенджерів, форумів, блогів та інших інтернет-платформ. Ці засоби забезпечують миттєве поширення інформації та створюють ефект її лавиноподібного розповсюдження. Водночас не можна виключати і традиційні способи передачі інформації, які, хоча і мають менший масштаб, можуть бути не менш небезпечними у конкретних ситуаціях.

Особливістю сучасного інформаційного середовища є також те, що поширення інформації часто має багатоступеневий характер. Первинне повідомлення може бути підхоплене іншими особами, модифіковане, доповнене або переосмислене, після чого знову поширене. У зв'язку з цим об'єктивна сторона злочину повинна охоплювати не лише первинні дії, але й похідні форми поширення інформації. Це включає репости, пересилання, копіювання та інші форми відтворення контенту. Такий підхід дозволяє забезпечити повноту кримінально-правової охорони та запобігти обходу заборони шляхом формального уникнення первинного розголошення.

Важливим аспектом є також оцінка об'єктивної сторони у випадках трансформації інформації. У сучасному цифровому середовищі інформація може бути змінена, скорочена, доповнена або подана у новому контексті. У таких випадках необхідно встановити, чи зберігає вона свій військово значущий характер і чи може бути використана для завдання шкоди. Це вимагає глибокого аналізу змісту інформації та її потенційного впливу.

Крім того, об'єктивна сторона включає просторові та часові характеристики діяння. Час поширення інформації має вирішальне значення, оскільки відомості, оприлюднені у момент проведення військової операції, є значно більш небезпечними, ніж ті, що стали відомі після її завершення. Просторовий аспект втрачає традиційне значення у зв'язку з глобалізацією інформаційного простору, однак залишається важливим для визначення юрисдикції та встановлення обставин вчинення злочину.

Отже, об'єктивні ознаки незаконного розголошення інформації про військові операції згідно зі статтею 114-2 КК України характеризуються надзвичайною складністю, багаторівневістю та динамічністю. Вони охоплюють широкий спектр дій, пов'язаних із поширенням інформації, передбачають формальний склад злочину, обов'язкову наявність спеціальної обстановки та різноманітність способів його вчинення. У сучасних умовах інформаційної війни ці ознаки набувають особливого значення, оскільки саме через них

забезпечується ефективний кримінально-правовий захист національної безпеки держави [77].

2.3. Суб'єктивні ознаки складу злочину, передбаченого ст. 114-2 КК України

Суб’єктивні ознаки складу злочину, передбаченого статтею 114-2 Кримінального кодексу України, є невід’ємним елементом його кримінально-правової характеристики, що відображає внутрішній психічний зміст протиправної поведінки особи. Вони охоплюють форму вини, зміст умислу, мотиви та цілі вчинення діяння, а також особливості інтелектуального та вольового ставлення особи до власних дій і їх можливих наслідків. У контексті досліджуваного злочину аналіз суб’єктивної сторони набуває особливої складності, що зумовлено як специфікою предмета посягання, так і різноманітністю життєвих ситуацій, у яких може відбуватися поширення військово значущої інформації.

Передусім слід зазначити, що вина у складі злочину, передбаченого статтею 114-2 КК України, може проявлятися у формі умислу, який у більшості випадків має прямий характер. Особа усвідомлює, що поширює інформацію про переміщення, розміщення або діяльність Збройних Сил України чи інших військових формувань, передбачає можливість або неминучість створення загрози для національної безпеки та бажає або свідомо допускає настання таких наслідків. Інтелектуальний момент умислу полягає у розумінні фактичних обставин діяння, зокрема характеру інформації, її потенційної значущості для противника та відсутності дозволу на її поширення. Вольовий момент проявляється у спрямованості поведінки на доведення цієї інформації до інших осіб.

Водночас не виключається можливість вчинення цього злочину з непрямим умислом, коли особа не прагне настання шкідливих наслідків, однак

[77] Альошин, Д. П., & Рудик, М. В. (2006). Міжнародний досвід протидії незаконному збуту та розповсюдженню конфіденційної інформації. *Актуальні проблеми держави і права*, (27), 222-228.

усвідомлює можливість їх виникнення і свідомо допускає таку можливість. Така форма вини може мати місце у випадках, коли особа, наприклад, публікує фото або відео з місця розташування військових об'єктів, розуміючи, що це може бути використано противником, але не надає цьому вирішального значення. У таких ситуаціях вирішальним є встановлення того, чи усвідомлювала особа потенційну небезпечність своїх дій та чи могла вона передбачити їх наслідки з урахуванням конкретних обставин.

Особливу складність становить питання можливості вчинення злочину з необережності. У теорії кримінального права переважає підхід, відповідно до якого склад злочину, передбаченого статтею 114-2 КК України, передбачає саме умисну форму вини. Це пояснюється тим, що поширення інформації є активною дією, яка, як правило, здійснюється свідомо. Водночас у практиці можуть виникати ситуації, коли особа не усвідомлює повною мірою характеру інформації або її значення для національної безпеки. Наприклад, це може стосуватися випадків публікації матеріалів у соціальних мережах без розуміння їх потенційної небезпеки. У таких випадках виникає питання про межі кримінальної відповідальності та можливість кваліфікації діяння як необережного, що залишається дискусійним у науці[78].

Інтелектуальний момент вини у складі цього злочину має багатокомпонентний характер. Особа повинна усвідомлювати не лише сам факт поширення інформації, але й її зміст, а також те, що вона стосується військових операцій або діяльності військових формувань. Крім того, важливим є усвідомлення відсутності дозволу на поширення таких відомостей. У сучасних умовах це питання ускладнюється тим, що межі дозволеної інформації не завжди є чітко визначеними, а значна частина даних перебуває у відкритому доступі. Це створює ситуації, коли особа може помилково вважати свої дії правомірними, що потребує ретельного аналізу її психічного ставлення до вчиненого.

[78] Карпенко, М. І. (2013). Причини і запобігання необережним військовим злочинам легковажної мотивації. *Юридична наука*, (4), 113-120.

Вольовий момент суб'єктивної сторони проявляється у спрямованості поведінки особи на поширення інформації. Він характеризується свідомим вибором певної лінії поведінки, яка призводить до доведення відомостей до інших осіб. У цьому контексті важливим є встановлення того, чи діяла особа активно, чи її поведінка мала пасивний характер. Наприклад, якщо особа лише зберігала інформацію без наміру її поширення, склад злочину може бути відсутнім. Натомість будь-які дії, спрямовані на передачу або оприлюднення інформації, свідчать про наявність вольового елементу.

Мотиви вчинення злочину можуть бути різноманітними і не завжди мають визначальне значення для кваліфікації, однак вони відіграють важливу роль у розумінні характеру поведінки особи та індивідуалізації кримінальної відповідальності. Серед найбільш поширених мотивів можна виділити необережність, бажання привернути увагу, прагнення отримати популярність у соціальних мережах, а також корисливі або ідеологічні мотиви. В окремих випадках діяння можуть бути вчинені з метою сприяння противнику, що наближає їх до складу державної зради та може впливати на кваліфікацію.

Особливе значення має мета вчинення злочину, яка, хоча і не є обов'язковою ознакою базового складу, може виступати кваліфікуючим фактором. Якщо буде встановлено, що особа діяла з метою передачі інформації представникам держави-агресора або іншим ворожим структурам, це свідчить про підвищений рівень суспільної небезпечності та може впливати на правову оцінку діяння. У таких випадках виникає необхідність розмежування цього злочину з іншими кримінальними правопорушеннями проти національної безпеки.

Важливим аспектом суб'єктивної сторони є також питання усвідомлення особою обстановки вчинення злочину, зокрема факту дії воєнного або надзвичайного стану. Оскільки ця обставина є обов'язковою ознакою складу злочину, особа повинна розуміти, що її дії відбуваються у відповідних умовах. У сучасних умовах, коли інформація про введення воєнного стану є загальновідомою, таке усвідомлення, як правило, презюмується. Водночас у

окремих випадках може виникати необхідність доведення того, що особа дійсно знала або повинна була знати про існування відповідного правового режиму.

Окрему увагу слід приділити проблемі помилки у суб'єктивній стороні злочину. Помилка може стосуватися як фактичних обставин, так і правової оцінки діяння. Наприклад, особа може помилково вважати, що поширювана нею інформація не має військового значення або вже є загальнодоступною. У таких випадках необхідно встановити, чи була така помилка виправданою і чи виключає вона вину особи. Це питання є особливо актуальним у контексті стрімкого розвитку інформаційного простору, де межі між відкритою та обмеженою інформацією є розмитими [79].

Слід також враховувати, що суб'єктивна сторона цього злочину тісно пов'язана з рівнем правової свідомості населення. У багатьох випадках поширення інформації про військові операції здійснюється особами, які не мають злочинного наміру, але не усвідомлюють повною мірою небезпечності своїх дій. Це обумовлює необхідність не лише кримінально-правового реагування, але й проведення інформаційно-роз'яснювальної роботи, спрямованої на підвищення обізнаності громадян.

Таким чином можливо зробити висновок, що суб'єктивні ознаки складу злочину, передбаченого статтею 114-2 КК України, характеризуються складністю та багатогранністю. Вони охоплюють різні форми умислу, включають інтелектуальний та вольовий елементи, а також враховують мотиви та цілі поведінки особи. Їх правильне встановлення має вирішальне значення для кваліфікації діяння, відмежування його від суміжних складів злочинів та забезпечення справедливого застосування кримінального закону. У сучасних умовах інформаційної війни саме аналіз суб'єктивної сторони дозволяє найбільш точно оцінити характер і ступінь суспільної небезпечності незаконного поширення військово значущої інформації.

[79] Тімофєєва, Л. Ю. (2023). Пропорційність обмежень поширення інформації в умовах воєнного режиму. *Вісник асоціації кримінального права України*, *1*(19), 53-69.

2.4. Аналіз судової практики щодо розгляду справ, пов'язаних із незаконним розголошенням військової інформації

У частині першій статті 114-2 Кримінального кодексу України встановлено базовий склад кримінального правопорушення, який полягає у поширенні відомостей щодо направлення, транспортування та переміщення зброї, озброєння і бойових припасів на територію України, у тому числі їх пересування в межах держави, за умови, що відповідна інформація не була попередньо оприлюднена у відкритому доступі Генеральним штабом Збройних Сил України, Міністерством оборони України, Службою безпеки України або офіційними джерелами держав-партнерів. Обов’язковою умовою притягнення до кримінальної відповідальності є вчинення таких дій в умовах правового режиму воєнного або надзвичайного стану. Вказане кримінальне правопорушення законодавцем віднесене до категорії нетяжких злочинів.

У частині другій статті 114-2 КК України закріплено інший основний склад злочину, який відрізняється як предметом посягання, так і ступенем суспільної небезпечності. Йдеться про незаконне поширення інформації щодо переміщення, руху або місцезнаходження Збройних Сил України чи інших військових формувань, створених відповідно до законодавства України, за наявності можливості їх ідентифікації на місцевості. Як і в попередньому випадку, обов’язковою умовою є те, що така інформація не була попередньо оприлюднена уповноваженими державними органами. Вчинення зазначених дій у період дії воєнного або надзвичайного стану зумовлює кваліфікацію цього діяння як тяжкого злочину.

Частина третя статті 114-2 КК України містить кваліфікуючі ознаки, що істотно підвищують рівень суспільної небезпечності відповідних діянь. До таких обставин належить вчинення злочину за попередньою змовою групою осіб, наявність корисливого мотиву, а також спеціальна мета передача відповідної інформації державі, яка здійснює збройну агресію проти України, її представникам або іншим незаконним збройним формуванням. Окремо

виділяються випадки, коли такі дії спричинили тяжкі наслідки. За наявності перелічених обставин відповідне кримінальне правопорушення кваліфікується як особливо тяжке.

Предметом злочину, передбаченого статтею 114-2 КК України, виступає інформація, що стосується зброї, озброєння, бойових припасів, а також розташування, переміщення чи функціонування Збройних Сил України або інших військових формувань, утворених відповідно до законів України. При цьому обов'язковою конструктивною ознакою об'єктивної сторони є наявність спеціальної обстановки вчинення злочину, а саме умов воєнного або надзвичайного стану, які істотно впливають на кримінально-правову оцінку відповідних діянь.

Проведений аналіз обвинувальних вироків, ухвалених судами України за статтею 114-2 КК України, на підставі даних Єдиного державного реєстру судових рішень, дозволив встановити низку характерних особливостей, що стосуються як предмета злочину та ознак його об'єктивної сторони, так і суб'єктивних характеристик та окремих рис особи правопорушника.

Щодо предмета злочину встановлено, що несанкціоноване поширення інформації найчастіше стосувалося відомостей про переміщення, рух або місцезнаходження особового складу Збройних Сил України, підрозділів територіальної оборони, блокпостів, військової техніки, зокрема танків, літаків, зенітно-ракетних комплексів, бойових машин піхоти, а також залізничних платформ із гаубицями. Крім того, предметом поширення виступали дані про військові частини, військові містечка, територіальні центри комплектування, окремі військові об'єкти, включаючи, наприклад, наплавні залізничні мости, вогневі позиції, систему оборонних фортифікаційних споруд, а також інформація про боєприпаси калібру 155 мм. У ряді випадків поширювалися відомості про розташування та напрямки функціонування систем протиповітряної оборони,

результати ураження повітряних цілей, а також навіть паролі, що використовувалися для проходження блокпостів [80].

Водночас найбільш типовою категорією є поширення інформації про переміщення, рух або розташування підрозділів Збройних Сил України з можливістю їх ідентифікації на місцевості, що підтверджується даними 61 обвинувального вироку. Важливо зазначити, що у значній кількості випадків така інформація поширювалася одночасно з відомостями про направлення, переміщення зброї, озброєння та бойових припасів на територію України, що відображено у 44 вироках. Фактично це означає, що поширювалися комплексні відомості, які дозволяли встановити місця дислокації військових підрозділів разом із наявним у них озброєнням.

У семи випадках зафіксовано поширення інформації, що стосується розташування систем протиповітряної оборони та результатів ураження повітряних цілей. Такі правопорушення здебільшого вчинялися у великих містах, зокрема у Києві та Одесі. Наприклад, в одному з випадків у місті Одеса іноземний громадянин здійснив відеофіксацію роботи системи протиповітряної оборони та, здійснюючи діяльність у сфері блогінгу, оприлюднив відповідний матеріал на власному каналі, супроводивши його коментарями щодо місця, часу події, характеристик звуків, факту ураження повітряної цілі та наслідків її знищення. Його дії були кваліфіковані за частиною другою статті 114-2 КК України, і суд призначив покарання у вигляді позбавлення волі строком на 5 років із застосуванням іспитового строку тривалістю 1 рік.

Аналіз об’єктивної сторони злочину свідчить про те, що більшість осіб була засуджена саме за частиною другою статті 114-2 КК України. Зокрема, 78 осіб (34 вироки у 2022 році та 44 у 2023 році) були визнані винними у поширенні інформації про переміщення, рух або розташування військових формувань із можливістю їх ідентифікації на місцевості. За частиною третьою статті 114-2 КК

[80] Старко, О. Л. (2024). Аналіз практики застосування ст. 114-2 Кримінального кодексу України (несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення збройних сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану).

України було засуджено 26 осіб (6 у 2022 році та 20 у 2023 році). У переважній більшості випадків ці особи передавали відповідну інформацію представникам ФСБ Російської Федерації або представникам так званих «ДНР» та «ЛНР» (дані 17 вироків).

Наприклад, вироком Слов'янського міськрайонного суду Донецької області від 4 квітня 2024 р. у справі № 243/1591/24 особу засуджено за ч. 3 ст. 114-2 КК України. Як встановив суд, обвинувачена, використовуючи мобільний додаток «Telegram», за грошову винагороду систематично передавала представнику збройних сил рф GPS-координати місць розташування особового складу та військової техніки Збройних Сил України.

Також встановлено випадки, коли поширення інформації призводило до нанесення ракетних ударів, унаслідок яких гинули військовослужбовці та цивільні особи, а також зазнавала руйнувань цивільна інфраструктура (дані 3 вироків).

Прикладом є вирок Ленінського районного суду м. Миколаєва від 27 лютого 2024 р. у справі № 489/2711/22, яким особу визнано винною за ч. 3 ст. 114-2 КК України. Судом встановлено, що внаслідок передачі обвинуваченим точних координат військового об'єкта через месенджер «Telegram» було здійснено прицільний ракетний обстріл, що спричинив загибель військовослужбовців та значні руйнування.

За частиною першою статті 114-2 КК України було засуджено 8 осіб (2 у 2022 році та 6 у 2023 році). У цих випадках поширювалася інформація про військову техніку та боєприпаси без зазначення точних координат їх розташування.

У ході дослідження також було виявлено випадки вчинення злочину, передбаченого статтею 114-2 КК України, у сукупності з іншими кримінальними правопорушеннями, зокрема передбаченими статтями 436-2 (4 випадки), частиною першою статті 263 (3 випадки), частиною першою статті 161 (1 випадок), частиною першою статті 368 (1 випадок).

Аналіз способів вчинення злочину свідчить, що найпоширенішими є розміщення власноруч створених фото- та відеоматеріалів, а також картографічних схем із зазначенням координат у соціальних мережах, а також передача таких матеріалів представникам ворожих структур. Значно рідше використовуються такі способи, як передача інформації за допомогою SMS або MMS-повідомлень, телефонних розмов, особистих зустрічей або написання коментарів у загальнодоступних чатах. Окремо слід відзначити нетиповий випадок, коли заборонена інформація була оприлюднена державним службовцем через електронну систему публічних закупівель шляхом розміщення оголошення про проведення тендеру, в якому були зазначені географічні координати військового об'єкта.

Щодо засобів поширення інформації встановлено, що переважна більшість таких дій здійснюється через мережу Інтернет. Зокрема, активно використовуються соціальні мережі та месенджери: Telegram (61 вирок), TikTok (5 вироків), Instagram (3 вироки), Facebook (2 вироки), Spaces.im (2 вироки), «ВКонтакте» (1 вирок), «Однокласники» (4 вироки), YouTube (2 вироки), а також месенджери Viber та WhatsApp (по 7 вироків). В одному випадку встановлено, що інформація накопичувалася у хмарному середовищі комп'ютера, до якого мали доступ громадяни Російської Федерації. Як знаряддя вчинення злочину найчастіше використовувалися мобільні телефони, рідше стаціонарні комп'ютери та ноутбуки.

Показовим є вирок Київського районного суду м. Харкова від 7 жовтня 2022 р. у справі № 953/3948/22. Засуджена за допомогою власного мобільного телефону сфотографувала переміщення військової техніки ЗСУ вулицями міста та надіслала знімки через месенджер «Viber» знайомим, після чого інформація неконтрольовано поширилася. Дії кваліфіковано за ч. 2 ст. 114-2 КК України.

Щодо суб'єкта злочину, ним визнається фізична осудна особа, яка досягла 16-річного віку. З метою формування узагальненого портрета правопорушника було проаналізовано статистичні дані Офісу Генерального прокурора України, а також 112 обвинувальних вироків. Встановлено, що у 2022–2023 роках було

виявлено 245 осіб, які вчинили цей злочин, з яких 197 є громадянами України, а 63 жінки. Значна частина правопорушень вчиняється особами віком від 40 до 54 років (85 осіб), а також особами старшого віку. Переважають особи з базовою або повною середньою освітою (84 особи), значна частина з яких є працездатними, але не мають постійного місця роботи або навчання (87 осіб), або перебувають у статусі безробітних (27 осіб). Як правило, такі особи раніше не притягувалися до кримінальної відповідальності. Лише один випадок було вчинено за попередньою змовою групою осіб.

Додатковий аналіз судових вироків дозволив встановити дані про місце народження засуджених, їх сімейний стан та соціальні характеристики. Зокрема, найбільша кількість осіб є уродженцями Донецької області (32 особи), Харківської (13 осіб), Миколаївської (7 осіб), Дніпропетровської (6 осіб), Луганської (5 осіб), Одеської (4 особи), а також інших регіонів України. Серед засуджених є також особи, народжені за межами України, зокрема в Російській Федерації (11 осіб), а також в інших державах. За сімейним станом переважають неодружені особи (54), тоді як одружених 39. Частина засуджених має на утриманні неповнолітніх дітей.

Щодо суб'єктивної сторони злочину встановлено, що вина у більшості випадків проявляється у формі прямого умислу. Основними мотивами є ідеологічні переконання, зокрема виправдовування або заперечення збройної агресії Російської Федерації проти України, бажання сприяти противнику або завдати шкоди обороноздатності держави, негативне ставлення до України, а також ностальгія за радянським минулим (71 вирок). У 7 випадках встановлено корисливий мотив.

Водночас у 13 випадках встановлено, що поширення інформації відбувалося з необережності, імпульсивно або без належного обдумування наслідків. Наприклад, в одному з випадків суд зазначив, що особа діяла «випадково, необдумано». В іншому випадку жінка здійснила відеозапис переміщення зенітно-ракетного комплексу тривалістю 21 секунду, який переслала знайомій особі та оприлюднила у соціальній мережі Facebook, за що

була засуджена до позбавлення волі строком на 4 роки із застосуванням іспитового строку.

Також зафіксовано випадки, коли мотивом була зацікавленість діяльністю держави у сфері оборони. Наприклад, військовослужбовець строкової служби здійснював фотофіксацію розташування військової частини та боєприпасів і передавав ці матеріали знайомим особам через електронні сервіси.

Щодо практики призначення покарання встановлено, що 62 особам було призначено реальне позбавлення волі, тоді як 46 осіб були звільнені від його відбування з випробуванням. У двох випадках застосовано штраф, а також додаткові покарання у вигляді заборони обіймати певні посади. У ряді випадків застосовувалася спеціальна конфіскація технічних засобів.

Таким чином, узагальнення судової практики дозволяє сформувати типовий портрет особи, яка вчиняє злочин, передбачений статтею 114-2 КК України, а також визначити найбільш характерні об’єктивні та суб’єктивні ознаки цього складу злочину, що має важливе значення для вдосконалення правозастосовної діяльності у сфері забезпечення національної безпеки України.

Висновки до розділу 2

Склад злочину, передбаченого ст. 114-2 КК України, відображає адаптацію кримінального законодавства до умов воєнного стану та сучасних інформаційних загроз. Його особливість полягає у формальному характері, коли кримінальна відповідальність настає вже за сам факт несанкціонованого поширення відповідної інформації незалежно від настання наслідків. Норма має бланкетний та водночас динамічний зміст, що зумовлює необхідність звернення до інших нормативних актів для її правильного застосування. Загалом вона виконує превентивну функцію, спрямовану на захист інформаційної складової національної безпеки, однак потребує подальшого вдосконалення з огляду на проблеми тлумачення та правозастосування.

Об’єктивні ознаки незаконного розголошення інформації про військові операції характеризуються складністю, широким змістом і багаторівневістю. Ключовим елементом виступає несанкціоноване поширення інформації, яке може здійснюватися у будь-якій формі та охоплює як публічні, так і приватні способи комунікації. Предмет злочину має комплексний характер і включає як прямі, так і опосередковані відомості, що можуть бути використані противником. Важливими є також формальний склад, спеціальна обстановка воєнного стану та різноманітність способів вчинення, що у сукупності забезпечує кримінально-правову охорону інформаційної безпеки в умовах сучасної війни.

Суб’єктивні ознаки складу злочину, передбаченого ст. 114-2 КК України, вирізняються складністю та багатогранністю, охоплюючи різні форми умислу, а також інтелектуальні та вольові елементи поведінки особи. Вина здебільшого проявляється у формі прямого або непрямого умислу, однак у практиці виникають дискусійні питання щодо можливості необережної форми вини. Мотиви і цілі не є обов’язковими для кваліфікації, але мають значення для індивідуалізації відповідальності та відмежування від суміжних складів злочинів. Правильне встановлення суб’єктивної сторони є ключовим для

справедливого застосування кримінального закону та адекватної оцінки суспільної небезпечності діяння.

Підсумовуючи аналіз судової практики, слід зазначити, що застосування ст. 114-2 КК України характеризується наявністю усталених підходів до кваліфікації, але водночас виявляє певні проблеми та тенденції. Найбільш поширеними є випадки розповсюдження інформації через соціальні мережі та месенджери, причому значна частина правопорушень пов'язана з можливістю ідентифікації військових об'єктів. Типовий суб'єкт злочину це особа без попередньої судимості, яка часто діє з необережності або під впливом власних переконань. Узагальнення практики підтверджує високу суспільну небезпечність таких діянь та необхідність подальшого вдосконалення як законодавчого регулювання, так і правозастосовної діяльності у цій сфері.

РОЗДІЛ 3
ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ УДОСКОНАЛЕННЯ КРИМІНАЛЬНОГО ЗАХИСТУ ВІЙСЬКОВОЇ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Ключові проблеми у сфері виявлення, кваліфікації та притягнення до відповідальності осіб, винних у несанкціонованому поширенні військової інформації в умовах воєнного стану

Практична реалізація кримінально-правової заборони, закріпленої у ст. 114-2 Кримінального кодексу України, супроводжується широким спектром проблем, які виникають послідовно на всіх етапах кримінального переслідування – від моменту виявлення факту протиправного поширення інформації до постановлення остаточного судового рішення та звернення його до виконання. Зазначені труднощі зумовлені як відносною новизною складу злочину, так і специфікою цифрового середовища, в якому вчиняється переважна більшість таких діянь, а також тими особливими умовами воєнного стану, що суттєво ускладнюють роботу правоохоронних і судових органів. Вивчення цих проблем є необхідною передумовою для вироблення науково обґрунтованих пропозицій щодо вдосконалення законодавства та правозастосовної практики.

Для кращого розуміння характеру та взаємозв’язку існуючих проблем у табл. 3.1 та на рис. А.1 (додаток А) представлена їх систематизація.

Таблиця 3.1

Систематизований перелік ключових проблем

Етап	Проблема	Стислий прояв
Виявлення	1. Технічна складність моніторингу	Наскрізне шифрування в месенджерах, анонімність, автоматичне видалення повідомлень

	2. Величезний обсяг інформаційного потоку	Відсутність автоматизованих систем виявлення забороненого контенту
	3. Нечіткість меж між дозволеною та забороненою інформацією	Громадяни не завжди розуміють, які відомості вже офіційно оприлюднені
Кваліфікація	4. Оціночний характер об'єктивних ознак	Категорія «можливість ідентифікації на місцевості» потребує спеціальних знань
	5. Конкуренція з іншими складами злочинів	Відмежування від державної зради, шпигунства, ст. 114-1 КК
	6. Визначення форми вини	Ризик об'єктивного ставлення за необережного або імпульсивного поширення
	7. Доведення причинно-наслідкового зв'язку (ч. 3 ст. 114-2)	Важко встановити, чи саме це повідомлення спричинило тяжкі наслідки
Притягнення до відповідальності	8. Збирання допустимих доказів	Вилучення цифрових пристроїв, отримання даних із закордонних серверів
	9. Строки досудового розслідування	Перевантаженість органів слідства, тривале перебування під підозрою
	10. Диференціація покарань	Широке застосування іспитового строку за тяжкі злочини, недостатня індивідуалізація
	11. Низька правова обізнаність населення	Багато громадян не усвідомлюють суспільну небезпеку власних дій
	12. Латентність	Значна частина правопорушень залишається невиявленою через обмежені можливості моніторингу

*Джерело: систематизовано автором

Розглянемо детальніше кожну з виокремлених проблем, зосередившись на їхніх причинах, конкретних проявах у правозастосовній діяльності та впливі на загальну ефективність кримінально-правового захисту військової інформації.

Проблеми на етапі виявлення значною мірою обумовлені тим, що основний масив несанкціонованого поширення інформації відбувається в цифровому просторі. Як засвідчив проведений аналіз судової практики, найчастіше такі діяння вчиняються через месенджери Telegram, Viber, WhatsApp, а також соціальні мережі TikTok, Facebook, Instagram. Особливу складність становлять випадки використання Telegram-каналів, де за замовчуванням застосовується наскрізне шифрування в секретних чатах, а власники каналів можуть залишатися анонімними. Правоохоронні органи позбавлені можливості в автоматичному режимі відстежувати зміст таких комунікацій; доступ до них, як правило, потребує фізичного вилучення мобільного пристрою, що не завжди можливо зробити оперативно, особливо в районах ведення активних бойових дій. Додатково варто враховувати, що деякі платформи впровадили функцію автоматичного видалення повідомлень через заданий проміжок часу, що призводить до безповоротної втрати цифрових слідів ще до початку дослідчої перевірки. Крім того, загальний обсяг контенту, що генерується українськими користувачами щодня, є колосальним. Відсутність у розпорядженні державних органів спеціалізованих програмних комплексів, здатних у режимі реального часу сканувати відкриті публікації за ключовими словами, географічними мітками та метаданими, перетворює виявлення забороненої інформації на значною мірою випадковий процес. Частково це компенсується високою громадянською активністю – повідомленнями військовослужбовців, волонтерів, небайдужих громадян. Однак такий підхід не є системним і не гарантує виявлення значної частки правопорушень, що об’єктивно підвищує рівень латентності цієї категорії злочинів.

Нечіткість меж між дозволеною та забороненою для поширення інформацією є ще одним чинником, що ускладнює не лише кваліфікацію, а й

саме виявлення діянь. Законодавець у ст. 114-2 КК України прямо зазначив, що кримінальна відповідальність виключається, якщо інформацію раніше офіційно оприлюднили Генеральний штаб Збройних Сил України, Міністерство оборони, Служба безпеки України або офіційні джерела держав-партнерів. Проте на практиці визначити, чи була конкретна інформація офіційно поширена, часто складно навіть для фахівців, не кажучи вже про пересічних громадян. Наприклад, загальна інформація про наявність певного озброєння в регіоні може бути оприлюднена офіційно, тоді як конкретні координати його розташування – ні. Крім того, інформація з часом може застарівати або втрачати свою актуальність, однак критеріїв такої оцінки закон не містить. Це створює ситуацію правової невизначеності, за якої одні й ті самі дії можуть сприйматися як злочинні або як цілком правомірні залежно від суб'єктивного тлумачення.

Проблеми кваліфікації посідають центральне місце в системі труднощів, пов'язаних із застосуванням ст. 114-2 КК України. Перш за все, слід відзначити оціночний характер ключової ознаки об'єктивної сторони – «можливість ідентифікації на місцевості» Збройних Сил України чи інших військових формувань. Ні кримінальний закон, ні відомчі нормативні акти не визначають, який саме ступінь ідентифікації є достатнім для наявності складу злочину. Чи достатньо того, що на оприлюдненому фото видно військову техніку на фоні загальновідомої будівлі, чи потрібна точна геоприв'язка з координатами? Чи охоплюється складом злочину ситуація, коли особа повідомляє лише назву населеного пункту, в якому перебувають військові? Ці питання не мають однозначної відповіді, що призводить до різної практики в різних регіонах України. У низці випадків суди потребують проведення спеціальних експертиз – топографічних, картографічних або військово-тактичних – для встановлення наявності можливості ідентифікації, однак такі експертизи проводяться не завжди, зокрема через брак відповідних фахівців або часові обмеження.

Другою серйозною проблемою є конкуренція кримінально-правових норм. Склад злочину, передбаченого ст. 114-2 КК України, тісно межує з державною зрадою (ст. 111 КК), шпигунством (ст. 114 КК) та перешкоджанням законній

діяльності Збройних Сил України (ст. 114-1 КК). Особливо гостро це питання постає при кваліфікації дій за ч. 3 ст. 114-2 КК, яка передбачає підвищену відповідальність за вчинення діяння «з метою передачі інформації державі, що здійснює збройну агресію проти України, або її представникам». У такому разі поведінка особи фактично охоплюється й ознаками державної зради у формі надання допомоги іноземній державі в проведенні підривної діяльності. Судова практика нині йде шляхом визнання ч. 3 ст. 114-2 КК спеціальною нормою, що підлягає застосуванню в таких випадках. Однак такий підхід викликає обґрунтовані заперечення, оскільки державна зрада передбачає більш суворе покарання (позбавлення волі на строк до п'ятнадцяти років або довічне позбавлення волі), ніж ч. 3 ст. 114-2 КК (до дванадцяти років). Виникає запитання: чи не призводить це до невиправданої лібералізації відповідальності за фактично пособницьку діяльність на користь ворога? Відсутність чітких законодавчих правил подолання такої конкуренції потребує якнайшвидшого наукового вирішення та, можливо, внесення відповідних змін до закону.

Надзвичайно дискусійним залишається питання форми вини. Хоча ст. 114-2 КК України сконструйована як формальний склад, що передбачає умисну форму вини, судова практика демонструє значну кількість випадків, коли особи поширювали заборонену інформацію через необережність, імпульсивно або внаслідок неусвідомлення значення своїх дій. Наприклад, в одному з вироків прямо зазначено, що засуджена «випадково, необдумано» сфотографувала переміщення техніки та надіслала знайомим. Утім, такі дії кваліфікуються як умисний злочин із посиланням на те, що особа усвідомлювала сам факт поширення інформації. Така практика межує з об'єктивним ставленням у вину, що є несумісним із фундаментальними принципами кримінального права. У науковому середовищі неодноразово висловлювалася пропозиція доповнити КК України складом необережного розголошення військової інформації, який би передбачав менш суворе покарання, однак ця пропозиція досі не знайшла законодавчого втілення.

Окремою складністю в межах кваліфікації за ч. 3 ст. 114-2 КК є необхідність доведення причинно-наслідкового зв'язку між поширенням інформації та настанням тяжких наслідків. Як показує вивчення вироків, у більшості випадків суди обмежуються констатацією самого факту настання шкоди (ракетний удар, загибель людей, руйнування), не проводячи глибокого аналізу механізму причинності. Довести, що саме конкретне повідомлення особи стало безпосередньою причиною вогневого ураження, вкрай складно, особливо з урахуванням того, що противник міг отримати аналогічну інформацію з інших джерел. Це створює ризики необґрунтованого засудження за кваліфікуючою ознакою, що значно обтяжує становище особи.

Проблеми притягнення до відповідальності включають як процесуальні, так і матеріально-правові аспекти. Першочерговою перешкодою є збирання допустимих доказів в умовах воєнного стану. Знаряддями вчинення злочину переважно виступають мобільні телефони, планшети, ноутбуки, які потребують негайного вилучення та експертного дослідження. Проте евакуація населення, пошкодження мереж електроживлення, тимчасова окупація окремих територій часто унеможливлюють своєчасне проведення слідчих дій. До того ж, значна частина цифрових доказів зберігається на серверах іноземних компаній (Meta, Telegram, Google), що вимагає надсилання запитів про міжнародну правову допомогу. Як свідчить практика, такі запити виконуються місяцями, що негативно позначається на загальних строках досудового розслідування. У деяких випадках це призводить до того, що провадження розслідуються з порушенням розумних строків, а це, у свою чергу, може бути підставою для закриття кримінального провадження або для визнання доказів недопустимими.

Навантаження на органи досудового розслідування є ще одним значущим чинником. Масовість учинюваних злочинів, передбачених ст. 114-2 КК України, в умовах обмежених кадрових ресурсів слідчих підрозділів призводить до того, що частина проваджень тривалий час залишається без належного руху. Це не лише порушує право особи на розгляд справи в розумний строк, а й знижує

загальний профілактичний ефект кримінальної відповідальності, оскільки невідворотність покарання в таких умовах не забезпечується.

Проблема диференціації покарань також заслуговує на окрему увагу. Проведений аналіз 112 обвинувальних вироків показав, що 46 засуджених (понад 40%) було звільнено від відбування покарання з випробуванням на підставі ст. 75 КК України. При цьому іспитовий строк застосовувався в тому числі до осіб, засуджених за ч. 2 ст. 114-2 КК, яка є тяжким злочином. Такий підхід, з одного боку, дозволяє врахувати щире каяття, позитивні характеристики особи, відсутність злочинного наміру та інші пом'якшуючі обставини. З іншого боку, надто широке застосування звільнення від покарання може сприйматися в суспільстві як безкарність, що підриває авторитет кримінального закону та знижує стримуючий вплив заборони. Водночас трапляються випадки, коли за спонтанне поширення інформації без будь-якого наміру завдати шкоди особі призначають реальне позбавлення волі на строк від 5 до 8 років, що може викликати сумніви щодо співмірності такого покарання. Відсутність чітких критеріїв, які б дозволяли судам однаково вирішувати питання про можливість застосування ст. 75 КК України в цій категорії справ, залишається відкритою проблемою.

Нарешті, не можна оминути увагою ***проблему низького рівня правової обізнаності населення***, яка є наскрізною та пронизує всі етапи – від виявлення до виконання покарання. Незважаючи на неодноразові заклики військового командування, інформаційні кампанії в засобах масової інформації, значна частина громадян продовжує за звичкою фіксувати на камеру переміщення військової техніки, розташування блокпостів, роботу систем протиповітряної оборони, після чого оприлюднювати ці матеріали в соціальних мережах, не замислюючись над потенційними наслідками. Це свідчить про те, що потенціал превентивної функції кримінального закону використовується не повною мірою. Лише поєднання кримінально-правових заборон із системною, постійною та адресною роз'яснювальною роботою серед усіх верств населення здатне

сформувати належний рівень правосвідомості та мінімізувати кількість випадків несанкціонованого поширення військової інформації.

Підсумовуючи викладене, слід визнати, що ефективність кримінально-правового захисту військової інформації в умовах воєнного стану значною мірою залежить від здатності держави комплексно вирішувати проблеми технічного, правового та соціального характеру. Це обумовлює необхідність подальшого наукового осмислення окреслених труднощів, а також розроблення конкретних пропозицій щодо вдосконалення як змісту ст. 114-2 КК України, так і механізму її застосування на практиці.

3.2. Можливість запровадження позитивного зарубіжного досвіду у сфері запобігання та протидії несанкціонованому поширенню військової інформації

Практика держав, які мають тривалий досвід протистояння гібридним та воєнним загрозам, доводить, що ефективний захист оборонної інформації не може бути зведений винятково до встановлення кримінально-правової заборони. Успішні національні моделі поєднують чітку законодавчу регламентацію, застосування сучасних технологічних рішень для моніторингу та блокування небезпечного контенту, розгалужену інституційну координацію, а також безперервну просвітницьку роботу, спрямовану на формування в суспільстві стійких навичок оперативної безпеки.

Саме комплексний характер таких систем становить найбільшу цінність для України, яка в умовах воєнного стану потребує невідкладного вдосконалення механізмів захисту військово значущої інформації [81].

Вивчення досвіду Ізраїлю, Сполучених Штатів Америки, Великої Британії, Німеччини та країн Балтії дозволяє виокремити чотири основні функціональні блоки, на яких ґрунтуються системи запобігання та протидії несанкціонованому поширенню оборонних відомостей: правовий, технічний, інституційний та освітньо-інформаційний. Їхнє співвідношення, а також конкретні інструменти, що застосовуються в різних юрисдикціях, унаочнюються в порівняльній табл. 3.2.

[81] Сторожинецький, Т. (2025). Еволюція військової інтеграції нордичних країн у контексті російських гібридних та воєнних загроз. *Український політико-правовий дискурс*, (15).

Таблиця 3.2

Порівняльний огляд зарубіжних підходів до запобігання та протидії несанкціонованому поширенню військової інформації

Країна / об’єднання	Основні акценти	Приклади інструментів і практик
Ізраїль	– Сувора військова цензура (превентивний контроль) – Висока культура оперативної безпеки серед цивільних – Швидке реагування на витік	– Угода між ЗМІ та цензурою про попередній перегляд матеріалів – Регулярні тренінги з ОБ (оперативної безпеки) в школах, університетах, на підприємствах – Миттєве видалення заборонених публікацій за вимогою військових
США	– Кримінальна відповідальність за розголошення «національної оборонної інформації» (Espionage Act) – Активна кіберпротидія та відстеження витоків – Публічні кампанії «If You See Something, Say Something»	– Законодавство про шпигунство з широким визначенням оборонної інформації – Спеціалізовані підрозділи з моніторингу соціальних мереж у ФБР та армії – Навчальні програми OPSEC (Operations Security) для військовослужбовців та їхніх родин
Велика Британія	– Офіційний закон про державну таємницю (Official Secrets Act) з окремим	– Криміналізація несанкціонованого

	регулюванням інформації про оборону – Тісна співпраця держави з інтернет-провайдерами та платформами	розкриття інформації, яка може допомогти ворогу – Центр урядового зв'язку (GCHQ) здійснює технічний моніторинг – Гаряча лінія для повідомлень про підозрілі публікації
Німеччина	– Чітка категоризація службової інформації та матеріалів із обмеженим доступом – Обов'язок недержавних суб'єктів повідомляти про кіберінциденти	– Закон про Федеральне відомство з питань інформаційної безпеки (BSI) – Галузеві стандарти безпеки для оборонної промисловості – Включення цифрової гігієни до освітніх курсів для держслужбовців
Країни Балтії (Литва, Латвія, Естонія)	– Комплексний підхід до гібридних загроз: від контрпропаганди до кримінальних санкцій – Максимальна прозорість офіційної інформації для запобігання чуткам	– Стратегічні комунікаційні центри, які швидко спростовують фейки – Обов'язкові курси медіаграмотності в школах – Законодавча заборона на поширення даних, що загрожують безпеці оборони

*Джерело: систематизовано автором

Наведений огляд свідчить, що, попри відмінності в національних правових традиціях та безпековому середовищі, спільним для всіх ефективних систем є

поєднання чотирьох базових компонентів. Узагальнену модель, придатну для адаптації в Україні, подано на рис. А.2 (додаток А).

Правовий блок є фундаментом усієї системи. Аналіз зарубіжного законодавства дозволяє дійти висновку, що ефективна нормативна база має включати не лише криміналізацію умисного поширення військових відомостей, а й диференційовану відповідальність за необережне розголошення, чіткі визначення предмета охорони та пропорційну шкалу санкцій. Більш детальне порівняння кримінально-правових підходів подано в табл. 3.3.

Таблиця 3.3

Порівняння кримінально-правових підходів до захисту оборонної інформації в окремих державах

Країна	Нормативний акт	Суб'єкт	Форма вини	Основне покарання	Диференціація
США	Espionage Act (18 U.S.C. §§ 793–798)	Загальний суб'єкт	Умисел (злочинна недбалість у окремих випадках)	До 10 років, за обтяжуючих обставин – довічне	Виділено самостійний склад за «грубу недбалість»
Велика Британія	Official Secrets Act 1989, National	Спеціальний та загальний суб'єкт	Умисел	До 14 років (за шпигунство – довічне)	Окрема відповідальність за розкриття інформації,

	Security Act 2023				що ставить під загрозу оборону
Німеччина	Кримінальний кодекс (§§ 93–101a)	Загальний суб’єкт	Умисел	Від 3 місяців до 10 років	Градація залежно від ступеня загрози безпеці ФРН
Ізраїль	Закон про безпеку держави, військові накази	Загальний суб’єкт, військовослужбовець	Умисел	До 15 років	Превентивна цензура фактично виключає кримінальне переслідування за попередньо перевірені матеріали
Україна	ст. 114-2 КК України	Загальний суб’єкт (з 16 років)	Умисел (формально)	Від 3 до 12 років	Три частини, кваліфікуючі ознаки: група, корисливий мотив, мета передачі ворогу, тяжкі наслідки

*Джерело: систематизовано автором

Дані табл. 3.3 показують, що більшість держав передбачає диференційовані санкції залежно від тяжкості наслідків, мети та суб’єкта.

Особливу увагу привертає американський підхід, де кримінальна відповідальність може наставати й у випадку «грубої недбалості», що дозволяє карати за безвідповідальне поводження з чутливою інформацією без доведення спеціального умислу. Для України запозичення подібного конструкту (спеціальний необережний склад) допомогло б усунути проблему об'єктивного ставлення у вину, яка була виявлена в попередньому підрозділі. Також корисним є досвід Ізраїлю, де попередня військова цензура знімає ризик мимовільного порушення закону журналістами та блогерами, водночас не підмінюючи собою кримінальне переслідування за свідому передачу ворогові закритих даних [82].

Технічний та інституційний блоки в зарубіжних системах тісно пов'язані між собою. Сучасні технології моніторингу відкритих джерел, що використовуються, зокрема, в США та Великій Британії, спираються на алгоритми машинного навчання, здатні виявляти підозрілі публікації за комбінацією ключових слів, геоданих та метаданих файлів. Функціонування таких систем неможливе без постійної взаємодії правоохоронних органів, військових структур та адміністрацій цифрових платформ. Наприклад, у країнах Балтії укладено спеціальні меморандуми з компаніями Meta, Twitter, Telegram, які передбачають пріоритетний розгляд запитів, пов'язаних із національною безпекою, та видалення контенту, що становить загрозу обороні.

Не менш значущим є освітньо-інформаційний компонент, практична реалізація якого в різних державах має свої особливості. Узагальнені дані про основні освітні та просвітницькі ініціативи наведено в табл. 3.4.

Таблиця 3.4

Порівняння освітніх та інформаційних кампаній з оперативної безпеки в зарубіжних країнах

[82] Малашенкова, Т. М. (2021). Окремі аспекти реалізації принципу винної відповідальності судді. Правничий часопис, 75.

Країна	Цільова аудиторія	Основна ініціатива / програма	Формат	Періодичність
Ізраїль	Усе населення	«Оперативна безпека – справа кожного»	Шкільні уроки, армійські інструктажі, соціальна реклама	Постійно
США	Військовослужбовці, їхні родини, цивільні	OPSEC Awareness, «If You See Something, Say Something»	Онлайн-курси, плакати в частинах, публічні оголошення	Щороку обов'язкове оновлення для військових
Велика Британія	Держслужбовці, підрядники оборонної сфери	«Think Before You Link» (MOD)	Тренінги з кібергігієни, тестування на фішинг	Регулярно, при допуску до секретної інформації
Естонія	Учні шкіл, державні службовці	Національна програма медіаграмотності	Обов'язковий шкільний курс, електронні модулі для чиновників	Щорічно оновлюється
Литва	Широка громадськість	Кампанії «Не стань мішенню для ворога»	Відеоролики в соцмережах, інформаційні стенди в	Хвилями, під час загострення загроз

			публічних місцях	

*Джерело: систематизовано автором

Як видно з табл. 3.4, найбільш успішними є ті програми, які мають не разовий, а системний характер, охоплюють різні вікові та соціальні групи і використовують сучасні канали комунікації. Ізраїльський досвід засвідчує, що культура оперативної безпеки, сформована з дитинства, здатна значно зменшити потребу в застосуванні кримінальної репресії. Для України, де значна частина порушень ст. 114-2 КК України вчиняється через необізнаність, імпульсивність або хибне уявлення про нешкідливість власних дій, імплементація такого підходу має стати пріоритетом. Доцільним було б запровадження обов'язкових модулів з інформаційної безпеки в закладах загальної середньої освіти, а також регулярних тренінгів для державних службовців та військовослужбовців. Окрему увагу слід приділити роботі з родинами військовослужбовців, оскільки саме через них часто відбувається витік даних про місцеперебування підрозділів.

Підсумовуючи, можна стверджувати, що зарубіжний досвід пропонує не поодинокі точкові рішення, а цілісну модель, яка об'єднує правову визначеність, технологічну оснащеність, міжвідомчу координацію та суспільну свідомість. Саме такий комплексний підхід дозволив Ізраїлю мінімізувати шкоду від інформаційних витоків, а країнам Балтії – вибудувати стійку систему стратегічних комунікацій. Для України адаптація цих напрацювань не лише підвищить ефективність застосування ст. 114-2 КК України, а й сприятиме зменшенню самої кількості таких правопорушень завдяки зміні поведінкових моделей громадян та посиленню загальнонаціональної культури інформаційної безпеки.

Висновки до розділу 3

Проведений аналіз ключових проблем, що виникають у процесі виявлення, кваліфікації та притягнення до кримінальної відповідальності за несанкціоноване поширення військової інформації, свідчить про існування системних перешкод, які знижують ефективність кримінально-правової охорони національної безпеки в умовах воєнного стану. Основні труднощі сконцентровані на трьох етапах. На етапі виявлення головною перешкодою є цифрове середовище вчинення злочинів – наскрізне шифрування месенджерів, автоматичне видалення повідомлень та колосальний обсяг інформаційного потоку, який неможливо опрацювати без автоматизованих моніторингових систем. Додаткову невизначеність створює нечітке розмежування дозволеної та забороненої для поширення інформації, що призводить до об'єктивних труднощів і для громадян, і для правоохоронних органів. На етапі кваліфікації найгострішими виявилися проблеми оціночного характеру об'єктивних ознак (насамперед «можливість ідентифікації військових формувань на місцевості»), конкуренції ст. 114-2 КК України з суміжними складами злочинів (державна зрада, шпигунство), а також визначення форми вини, коли фактично необережне діяння нерідко кваліфікується як умисне, що межує з об'єктивним ставленням у вину. На етапі притягнення до відповідальності суттєвими перешкодами залишаються труднощі збирання допустимих доказів у бойових умовах, порушення строків досудового розслідування, недостатня диференціація покарань (з одного боку, широке застосування іспитового строку за тяжкі злочини, з іншого – непропорційно суворі вироки за спонтанні дії), а також низький рівень правової обізнаності населення, що пронизує всі стадії кримінального переслідування та сприяє високій латентності цих правопорушень.

Узагальнення зарубіжного досвіду (Ізраїль, США, Велика Британія, Німеччина, країни Балтії) дозволило дійти висновку, що дієва система запобігання та протидії несанкціонованому поширенню військової інформації

має ґрунтуватися не на окремих ізольованих заходах, а на комплексній інтегрованій моделі, яка охоплює чотири взаємопов'язані блоки: правовий, технічний, інституційний та освітньо-інформаційний. Правовий блок потребує уточнення предмета злочину, чіткого визначення критеріїв «можливості ідентифікації на місцевості», встановлення диференційованої відповідальності за умисне та необережне розголошення, а також запровадження механізмів превентивної цензури на добровільних засадах. Технічний блок передбачає створення автоматизованих систем моніторингу відкритих джерел на основі алгоритмів штучного інтелекту, а також налагодження постійної взаємодії з адміністраціями цифрових платформ для оперативного блокування небезпечного контенту. Інституційний блок має забезпечити міжвідомчу координацію через єдиний центр швидкого реагування, до функцій якого належатиме акумуляція інформації, аналітика та стратегічні комунікації. Освітньо-інформаційний блок є найбільш довготривалою інвестицією в безпеку і має включати обов'язкові курси медіаграмотності в закладах освіти, системні тренінги з оперативної безпеки для військовослужбовців і держслужбовців, а також постійні загальнонаціональні просвітницькі кампанії.

Таким чином, лише комплексне поєднання зазначених чотирьох компонентів з урахуванням адаптованого зарубіжного досвіду здатне мінімізувати кількість випадків несанкціонованого поширення військово значущої інформації та водночас підвищити дієвість кримінально-правового захисту національної безпеки України в умовах воєнного стану. Реалізація такого підходу дозволить не лише посилити невідворотність і справедливість кримінальної відповідальності за ст. 114-2 КК України, а й сформувати в суспільстві стійку культуру оперативної безпеки, що є запорукою зменшення самої потреби в застосуванні кримінальної репресії.

ВИСНОВКИ

За результатами проведеного дослідження кримінально-правового захисту національної безпеки через призму незаконного розголошення інформації про військові операції в умовах воєнного стану можливо сформулювати наступні висновки.

1. Інформація про військові операції є критичним елементом системи національної безпеки, оскільки в умовах збройного конфлікту вона безпосередньо впливає на обороноздатність держави. Інформаційна безпека виступає самостійною складовою національної безпеки, що забезпечує стан захищеності життєво важливих інтересів людини, суспільства і держави. В умовах воєнного стану значення такої інформації багатократно зростає: відомості про переміщення, дислокацію військ, озброєння та результати бойових дій стають чинником, здатним або забезпечити успіх військових операцій, або, у разі витоку, спричинити тяжкі втрати. Тому захист цієї категорії даних є пріоритетним завданням державної політики.

2. Визначено особливості нормативно-правового регулювання захисту інформації у сфері оборони. Система правового регулювання охоплює Конституцію України, яка відносить інформаційну безпеку до найважливіших функцій держави, Кримінальний кодекс України (зокрема ст. 114-2), закони України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про національну безпеку України», «Про правовий режим воєнного стану», а також Стратегію інформаційної безпеки, затверджену Указом Президента України, яка визначає стратегічні пріоритети та напрями захисту інформації в умовах воєнного конфлікту, та численні підзаконні акти. У сукупності ці нормативні акти утворюють багаторівневу систему, яка, однак, потребує подальшого вдосконалення в частині конкретизації предмета злочину та процедур моніторингу забороненої інформації.

3. Проаналізовано міжнародні стандарти запобігання розголошенню інформації у сфері оборони. Міжнародне право (зокрема, Конвенція Ради Європи про доступ до офіційних документів, Йоганнесбурзькі принципи, Конвенція про кіберзлочинність, Директива ЄС № 2022/2555 та новітня Конвенція ООН проти кіберзлочинності 2024 р.) встановлює баланс між захистом національної безпеки і свободою вираження поглядів. Визначено, що будь-які обмеження доступу до інформації мають бути законними, пропорційними та необхідними в демократичному суспільстві. Водночас міжнародне право визнає правомірність криміналізації діянь, що створюють реальну загрозу обороні, засуджує пропаганду війни та дезінформацію як складові гібридної агресії. Ці стандарти ратифіковано або враховано в національному законодавстві, що легітимізує застосування ст. 114-2 КК України.

4. Охарактеризовано об'єктивні та суб'єктивні ознаки складу злочину, передбаченого ст. 114-2 КК України. Об'єктивна сторона полягає у несанкціонованому поширенні специфічної військово значущої інформації, яка не була офіційно оприлюднена уповноваженими органами, в умовах воєнного або надзвичайного стану. Склад злочину – формальний, він вважається закінченим з моменту доведення інформації хоча б до одного стороннього суб'єкта. Предметом є дані про направлення, переміщення зброї, озброєння, бойових припасів, а також про рух, переміщення або розміщення Збройних Сил України чи інших військових формувань із можливістю їх ідентифікації на місцевості. Суб'єктивна сторона передбачає переважно прямий умисел; мотиви (корисливі, ідеологічні) та мета (у тому числі передача ворогові) впливають на кваліфікацію за ч. 3 ст. 114-2. Суб'єкт – загальний (осудна фізична особа з 16 років). Встановлено, що конструкція норми, попри загальну визначеність, містить низку оціночних понять, що ускладнює її одноманітне застосування.

5. Проаналізовано судову практику щодо розгляду справ, пов'язаних із незаконним розголошенням військової інформації. Узагальнення 112 обвинувальних вироків за 2022–2024 рр. показало, що переважна більшість злочинів кваліфікується за ч. 2 ст. 114-2 КК України, де предметом виступає

інформація про переміщення або розміщення ЗСУ з можливістю ідентифікації. Основними способами є поширення фото- та відеоматеріалів через Telegram, TikTok, Facebook, Viber. Типовий портрет засудженого – громадянин України віком 40–54 років із середньою освітою, без постійного місця роботи, раніше не судимий. У значній кількості випадків (46 зі 112) суди застосовують звільнення від відбування покарання з випробуванням, що засвідчує наявність проблеми диференціації кримінальної відповідальності. Водночас виявлено випадки реального позбавлення волі за діяння, вчинені через необережність або імпульсивно, що підтверджує гіпотезу про існування дисбалансу між свободою вираження та захистом національної безпеки.

6. Визначено ключові проблеми у сфері виявлення, кваліфікації та притягнення до відповідальності осіб, винних у несанкціонованому поширенні військової інформації в умовах воєнного стану. На етапі виявлення головними перешкодами є технічна складність моніторингу зашифрованих месенджерів, величезний обсяг інформаційного потоку та нечіткість меж між дозволеною та забороненою інформацією. При кваліфікації виникають труднощі з тлумаченням оціночних ознак («можливість ідентифікації на місцевості»), розмежуванням із державною зрадою і шпигунством, а також із доведенням форми вини, що створює ризик об’єктивного ставлення у вину. На стадії притягнення до відповідальності проблеми пов’язані зі збиранням доказів у бойових умовах, отриманням даних із закордонних серверів, порушенням строків слідства та недостатньою диференціацією покарань, а також із низьким рівнем правової обізнаності населення, що обумовлює високу латентність цих злочинів.

7. Проаналізовано можливість запровадження позитивного зарубіжного досвіду у сфері запобігання та протидії несанкціонованому поширенню військової інформації. Досвід Ізраїлю, США, Великої Британії, Німеччини та країн Балтії демонструє, що ефективна система має базуватися на інтегрованій моделі, яка поєднує чотири блоки: правовий (чіткі дефініції, диференціація відповідальності за умисел і необережність, пропорційні санкції), технічний (автоматизований моніторинг відкритих джерел, співпраця з

платформами), інституційний (єдиний координаційний центр для швидкого реагування) та освітньо-інформаційний (обов'язкова медіаграмотність, системні тренінги з оперативної безпеки, загальнонаціональні просвітницькі кампанії). Адаптація цих компонентів до українських реалій дозволить зменшити кількість порушень та підвищити ефективність кримінально-правової охорони.

Таким чином, мета дослідження досягнута: визначено особливості незаконного розголошення інформації про військові операції в умовах воєнного стану та запропоновано шляхи вдосконалення кримінально-правового захисту національної безпеки. Гіпотеза про необхідність забезпечення балансу між правом на свободу слова та потребами безпеки, а також про наявність проблем у конструюванні та застосуванні ст. 114-2 КК України, знайшла своє підтвердження. Практичне значення отриманих результатів полягає в тому, що сформульовані висновки та пропозиції можуть бути використані для подальшого вдосконалення кримінального законодавства, підвищення ефективності правозастосовної діяльності, а також у освітньому процесі при підготовці фахівців-правників. Перспективи подальших наукових розвідок пов'язані з моніторингом ефективності запроваджених змін до ст. 114-2 КК України та вивченням новітніх викликів в інформаційній сфері в умовах триваючої збройної агресії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Альошин, Д. П., & Рудик, М. В. (2006). Міжнародний досвід протидії незаконному збуту та розповсюдженню конфіденційної інформації. Актуальні проблеми держави і права, (27), 222-228.

2. Борисова Л.В., Логвиненко М.Ф. Правові засади захисту інформації: навчальний посібник. Харків: ХНУВС, 2013. 212 с.

3. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 (НД ТЗІ 2.5-008-02): Нормативний документ від 20.12.2002 року. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tzi.com.ua/downloads/2.5-008-2002.pdf. (дата звернення: 06.06.2025).

4. Гуйван П.Д. Щодо співвідношення категорій персональних даних про особу і конфіденційної інформації. Науковий вісник публічного та приватного права. № 3. 2018. С. 31-37.

5. Гурін, О. М., Леках, А. А., Старцев, В. В., Мусієнко, О. П., & Гурін, І. О. (2023). Аналіз підходів сучасності щодо створювання системи моніторингу та трекінгу переміщення військових вантажів. Системи озброєння і військова техніка, (2 (74)), 42-51. https://doi.org/10.30748/soivt.2023.74.05

6. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України № 263 від 12.03.2022 року. URL: https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text. (дата звернення: 06.06.2025).

7. Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України: Постанова Кабінету Міністрів України № 821 від 16.11.2016 року. URL: https://zakon.rada.gov.ua/laws/show/821-2016-%D0%BF#Text. (дата звернення: 06.06.2025).

8. Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова Кабінету Міністрів України № 299 від 04.04.2023 року. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text. (дата звернення: 06.06.2025).

9. Директива Європейського парламенту і ради ЄС про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: Міжнародний документ № 2022/2555 від 14.12.2022 року. URL: https://zakon.rada.gov.ua/laws/show/9a3_001-22#Text. (дата звернення: 09.06.2025).

10. Дубняк, М. В. (2022). Конституційне право на свободу слова та кримінальна відповідальність за несанкціоноване поширення інформації. Правові засоби протидії злочинам проти основ національної безпеки в умовах військової агресії, 68-72. https://kigap.kpi.ua/wp-content/uploads/2022/06/Zbirka-tez_Kruglii-stil-26.05.2022___.pdf#page=68

11. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу (НД ТЗІ 1.1-002-99): Нормативний документ від 01.07.1999 року. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tzi.com.ua/downloads/1.1-002-99.pdf. (дата звернення: 06.06.2025).

12. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці (НД ТЗІ 1.6-005-2013): Нормативний документ від 15.04.2013 року. URL: https://zakon.rada.gov.ua/rada/show/v0215519-13?utm_source=chatgpt.com#Text. (дата звернення: 06.06.2025).

13. Захист інформації. Технічний захист інформації. Порядок проведення робіт (ДСТУ 3396.1-96): Державний стандарт України від 01.07.1997 року. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf. (дата звернення: 06.06.2025).

14. Карпенко, М. І., & Попченкова, І. М. (2016). Причини, наслідки та профілактика військових злочинів, зокрема за ст. 422 КК України. Юридична наука, (1), 93-109.

15. Карпенко, М. І. (2013). Причини і запобігання необережним військовим злочинам легковажної мотивації. Юридична наука, (4), 113-120.

16. Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text. (дата звернення: 09.06.2025).

17. Конвенція Ради Європи про доступ до офіційних документів: Міжнародний документ від 18.06.2009 року. URL: https://zakon.rada.gov.ua/laws/show/994_001-09#Text. (дата звернення: 09.06.2025).

18. Конституція України: Закон України № 254к/96-ВР від 28.06.1996 року. ВВР, 1996, № 30, ст. 141.

19. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навчальний посібник. Київ: Кондор, 2004. 382 с.

20. Кримінальний кодекс України: Закон України № 2341-III від 05.04.2001 року. ВВР, 2001, № 25-26, ст. 131.

21. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 2.5-004-99): Нормативний документ від 01.07.1999 року. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tzi.com.ua/downloads/2.5-004-99.pdf. (дата звернення: 06.06.2025).

22. Крупнова А.О. Правове регулювання сфери забезпечення інформаційної безпеки в Україні. Електронне наукове видання «Аналітично-порівняльне правознавство». № 11. 2023. С. 348-354.

23. Малашенкова, Т. М. (2021). Окремі аспекти реалізації принципу винної відповідальності судді. Правничий часопис, 75. https://doi.org/10.32850/sulj.2021.1.13

24. Міжнародні стандарти та національна кримінально-правова політика у сфері охорони інформаційної безпеки: монографія / за заг. ред.. В.І. Борисова, М.В. Карчевського, М.В. Шепітька. Харків: Право, 2023. 152 с.

25. Нижник Н.Р., Ситнік Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник. Ірпінь, 2000. 304 с.

26. Основи інформаційної безпеки. Навчальний посібник для вузів / Є. Б. Бєлов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. Київ: Телеком, 2006. 544с.

27. Панченко О. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України, 2019. Вип. 3. С. 1-11.

28. Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем (НД ТЗІ 3.6-007-21): Нормативний документ від 01.07.2021 року. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66075. (дата звернення: 06.06.2025).

29. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці (НД ТЗІ 3.6-004-21): Нормативний документ від 01.07.2021 року. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=66072. (дата звернення: 06.06.2025).

30. Порядок здійснення моніторингу систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використаням базових та цільових профілів безпеки інформації: Нормативний документ від 10.03.2025 року. URL: https://zakon.rada.gov.ua/laws/show/z0448-25#Text. (дата звернення: 06.06.2025).

31. Про внесення змін до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації: Закон України № 681-IX від 04.06.2020 року. ВВР, 2020, № 42, ст. 349.

32. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України № 2160-IX від 04.03.2022 року. Офіційний вісник України, 2022, № 33, стор. 90, ст. 145, код акта 110988/2022.

33. Про державну таємницю: Закон України № 3855-XII від 21.01.1994 року. ВВР, 1994, 3 16, ст. 93.

34. Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах: Постанова Кабінету Міністрів України № 373 від 29.03.2006 року. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text. (дата звернення: 06.06.2025).

35. Про електронні комунікації: Закон України № 1089-IX від 16.12.2020 року. ВВР, Офіційний вісник України, 2021 р., № 6, стор. 10, стаття 306, код акта 102665/2021.

36. Про затвердження плану заходів з реалізації Стратегії забезпечення державної безпеки: Розпорядження Кабінету Міністрів України № 328-р від 18.04.2023 року. URL: https://zakon.rada.gov.ua/laws/show/328-2023-%D1%80#Text. (дата звернення: 06.06.2025).

37. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: Розпорядження Кабінету Міністрів України № 272-р від 30.03.2023 року. URL:

https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text. (дата звернення: 06.06.2025).

38. Про затвердження Рекомендацій з оцінки достатності заходів захисту інформації комплексних систем захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, створених з використанням профілів безпеки інформації: Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 354 від 10.07.2024 року. URL: https://zakon.rada.gov.ua/rada/show/v0354519-24#Text. (дата звернення: 06.06.2025).

39. Про захист інформації в інформаційно-комунікаційних системах: Закон України № 80/94-ВР від 05.07.1994 року. ВВР, 1994, № 31, ст. 286.

40. Про захист персональних даних: Закон України № 2297-VI від 01.06.2010 року. ВВР, 2010, № 34, ст. 481.

41. Про інформацію: Закон України № 2657-XII від 02.10.1992 року. ВВР, 1992, № 48, ст. 650.

42. Прокопчук Т. Міжнародні стандарти кримінально-правової охорони інформації з обмеженим доступом. Підприємництво, господарство і право. № 3, 2021. С. 232-239.

43. Про національну безпеку України: Закон України № 2469-VIII від 21.06.2018 року. ВВР, 2018, № 31, ст. 241.

44. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII від 05.10.2017 року. ВВР, 2017, № 45, ст. 403.

45. Про Положення про технічний захист інформації в Україні: Указ Президента України № 1229/99 від 27.09.1999 року. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text. (дата звернення: 06.06.2025).

46. Про правовий режим воєнного стану: Закон України № 389-VIII від 12.05.2015 року. ВВР, 2015, № 28, ст. 250.

47. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо удосконалення формування та реалізації державної політики у сфері інформаційної безпеки України»: Указ Президента

України № 449/2014 від 01.05.2014 року. URL: https://zakon.rada.gov.ua/laws/show/449/2014#n2. (дата звернення: 06.06.2025).

48. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України № 447/2021 від 26.08.2021 року. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text. (дата звернення: 06.06.2025).

49. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України № 392/2020 від 14.09.2020 року. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text. (дата звернення: 05.06.2025).

50. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України № 685/2021 від 28.12.2021 року. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n7. (дата звернення: 05.06.2025).

51. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України»: Указ Президента України № 37/2022 від 01.02.2022 року. URL: https://zakon.rada.gov.ua/laws/show/37/2022#n5. (дата звернення: 06.06.2025).

52. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»: Указ Президента України № 56/2022 від 16.02.2022 року. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text. (дата звернення: 06.06.2025).

53. Русакевич А.І. Інформаційна безпека в умовах воєнного стану у аспектів забезпечення інформаційних прав громадян. Держава та регіони. № 2 (80). 2023. С. 177-180.

54. Старко, О. Л. (2024). Аналіз практики застосування ст. 114-2 Кримінального кодексу України (несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення збройних сил України чи інших утворених

відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану). https://dspace.uzhnu.edu.ua/jspui/handle/lib/70579

55. Сторожинецький, Т. (2025). Еволюція військової інтеграції нордичних країн у контексті російських гібридних та воєнних загроз. Український політико-правовий дискурс, (15). https://doi.org/10.5281/zenodo.17348405

56. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу: Нормативний документ від 25.12.2000 року. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://tzi.com.ua/downloads/3.6-001-2000.pdf. (дата звернення: 06.06.2025.

57. Тімофєєва, Л. Ю. (2023). Пропорційність обмежень поширення інформації в умовах воєнного режиму. Вісник асоціації кримінального права України, 1(19), 53-69. https://doi.org/10.21564/2311-9640.2023.19.281122

58. Чернявська Т.А. Поняття і сутність інформаційної безпеки та її місце в системі забезпечення транспортної безпеки України. Таврійський науковий вісник. № 80. 2012. С. 364-372.

59. Щербіна О.С. Інформаційні війни та безпека інформації. Інформаційні та прикладні технології. № 4. 2021. С. 311-313.

60. Gordon G. S. The Propaganda Prosecutions at Nuremberg: The Origin of Atrocity Speech Law and the Touchstone for Normative Evolution. Loyola of Los Angeles International and Comparative Law Review. 2017. Vol. 39, № 1. P. 209–245.

61. Joint Declaration on freedom of expression and «fake news», disinformation and PROPAGANDA № FOM.GAL/3/17 on 3 March 2017. URL: https://www.osce.org/files/f/ documents/6/8/302796.pdf..

62. Helsinki Final Act. Organization for Security and Cooperation in Europe . 1 August 1975. URL: https://www.osce.org/helsinki-final-act. (дата звернення: 09.06.2025).

63. The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. URL: https://www.refworld.org/legal/resolution/art19/1995/en/41603.

64. IV Конвенція про закони і звичаї війни на суходолі та додаток до неї: Положення про закони і звичаї війни на суходолі: Міжнародний документ від 18.0.1907 року. URL: https://zakon.rada.gov.ua/laws/show/995_222#Text. (дата звернення: 09.06.2025).

Додаток А

Рис. А.1. Взаємозв'язок проблем у процесі кримінального переслідування за ст. 114-2 КК України

Рис. А.2. Інтегрована модель запобігання та протидії несанкціонованому поширенню військової інформації (на основі зарубіжного досвіду)