УДК 004.056:34(477)
DOI https://doi.org/10.37687/2413-6433.2025-2.20

Нашинець-Наумова А. Ю.,
доктор юридичних наук, професор, академік Академії АПН,
заступник декана з науково-методичної та навчальної роботи
факультету права та міжнародних відносин
Київського столичного університету імені Бориса Грінченка
ORCID: 0000-0002-5811-7733

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

LEGAL ENSURANCE OF INFORMATION SECURITY IN THE CONDITIONS OF THE RUSSIAN-UKRAINIAN WAR

«Ми усвідомлюємо, що те, що відбувається
сьогодні в інформаційному просторі, – це війна»
Олексій Данілов, Секретар РНБО України (2019-2024 рр.)

У статті здійснено комплексний правовий аналіз нормативно-правового забезпечення інформаційної безпеки України в умовах повномасштабної збройної агресії російської федерації. Окреслено основні інформаційні загрози – дезінформація, кібератаки, витік персональних та службових даних, маніпуляції інформаційним простором. Проаналізовано діючу нормативно-правову базу, зокрема Закон України «Про правовий режим воєнного стану» [1], наукові дослідження українських фахівців та практику органів влади на інформаційні загрози. Визначено ключові прогалини та запропоновано комплекс змін у законодавстві, організаційних механізмах, процесуальних процедурах та кримінально-правових інструментах протидії інформаційним ризикам. Обґрунтовано необхідність забезпечення балансу між інтересами оборони та гарантіями свободи слова та права на інформацію.

В умовах воєнного стану особливої актуальності набуває проблема забезпечення належного балансу між необхідністю захисту національної безпеки, з одного боку, та дотриманням конституційних прав і свобод людини, з іншого. Свобода слова, право на інформацію, право на приватність та захист персональних даних, свобода вираження поглядів – усі ці фундаментальні права зазнають суттєвого впливу з боку обмежень, зумовлених військовою необхідністю. Держава змушена вдаватися до спеціальних правових режимів, обмежувати окремі інформаційні процеси, встановлювати контроль за поширенням відомостей, які можуть завдати шкоди обороноздатності та безпеці. Водночас надмірні або необґрунтовані обмеження можуть призводити до порушень прав людини, зловживань владою, звуження демократичних свобод.

Саме тому питання правового забезпечення інформаційної безпеки в умовах війни набуває особливого теоретичного та практичного значення. Воно охоплює як проблеми нормативно-правового регулювання діяльності суб'єктів інформаційних відносин, так і питання реалізації та захисту інформаційних прав громадян, функціонування медіа, відповідальності за інформаційні правопорушення, боротьби з дезінформацією та інформаційними диверсіями. Особливої уваги потребує також узгодження національного законодавства з міжнародними стандартами у сфері прав людини та інформаційної безпеки, зокрема положеннями Європейської конвенції з прав людини, практикою Європейського суду з прав людини, а також рекомендаціями міжнародних організацій.

Ключові слова: *інформаційна безпека, воєнний стан, національна безпека, дезінформація, кібербезпека, персональні дані, правове регулювання.*

The article provides a comprehensive legal analysis of the regulatory and legal support for Ukraine's information security in the context of full-scale armed aggression by the Russian Federation. The main information threats are outlined - disinformation, cyberattacks, leakage of personal and official data, manipulation of the information space. The current regulatory and legal framework is analyzed, in particular the Law of Ukraine "On the Legal Regime of Martial Law" [1], scientific research by Ukrainian specialists and the practice of government bodies on information threats. Key gaps are identified and a set of changes in legislation, organizational mechanisms, procedural procedures and criminal law instruments for countering information risks is proposed. The need to ensure a balance between defense interests and guarantees of freedom of speech and the right to information is substantiated. In conditions of martial law, the problem of ensuring an appropriate balance between the need to protect national security, on the one hand, and compliance with constitutional rights and freedoms of a person, on the other, becomes particularly relevant. Freedom of speech, the right to information, the right to privacy and protection of personal data, freedom of expression – all these fundamental

rights are significantly affected by restrictions due to military necessity. The state is forced to resort to special legal regimes, limit certain information processes, establish control over the dissemination of information that may harm defense capability and security. At the same time, excessive or unjustified restrictions can lead to violations of human rights, abuse of power, and narrowing of democratic freedoms. That is why the issue of legal support for information security in wartime acquires special theoretical and practical significance. It covers both the problems of regulatory and legal regulation of the activities of subjects of information relations, and the issues of implementing and protecting citizens' information rights, the functioning of the media, liability for information offenses, and the fight against disinformation and information sabotage. Special attention also needs to be paid to harmonizing national legislation with international standards in the field of human rights and information security, in particular the provisions of the European Convention on Human Rights, the practice of the European Court of Human Rights, as well as the recommendations of international organizations.

Key words: *information security, martial law, national security, disinformation, cybersecurity, personal data, legal regulation.*

Повномасштабна війна російської федерації проти України, що триває з лютого 2022 року, стала не лише збройним протистоянням на полі бою, а й масштабною війною в інформаційному просторі. Інформація перетворилася на стратегічний ресурс, а контроль над інформаційними потоками – на один із ключових чинників національної безпеки. Сучасна війна характеризується активним застосуванням гібридних методів впливу, серед яких інформаційно-психологічні операції, масоване поширення дезінформації, маніпуляція суспільною свідомістю, кібератаки на державні ресурси та критичну інфраструктуру займають провідне місце. У таких умовах інформаційна безпека перестає бути суто технічною або комунікаційною проблемою і набуває виразного правового, політичного та суспільного виміру.

Інформаційний простір сьогодні фактично є повноцінним театром воєнних дій. Через засоби масової інформації, соціальні мережі, месенджери, інтернет-платформи здійснюється цілеспрямований вплив на масову свідомість, формується викривлена картина подій, поширюються фейкові новини, здійснюються спроби деморалізації населення, підриву довіри до органів державної влади та військового керівництва. Окремим напрямом ворожої діяльності стало втручання в роботу державних інформаційних систем, каналів військових комунікацій, а також атакування об’єктів критичної інформаційної інфраструктури. Усе це створює безпрецедентні виклики для держави, суспільства та правової системи.

Українські науковці та практики (Смотрич Д. В. [2], Котерлін І. Б. [3], Руснак Ю. І. [4], Беспалов І. О. [5] та ін.) у своїх працях наголошують на необхідності переосмислення ролі правових механізмів у забезпеченні інформаційної безпеки в період збройного конфлікту. Дослідники звертають увагу на зростання значення інформаційного суверенітету держави, посилення вимог до захисту інформаційних ресурсів, удосконалення правового статусу засобів масової інформації в умовах воєнного стану, а також на визначення меж допустимих обмежень інформаційних прав. Водночас у наукових дискусіях залишаються відкритими питання співвідношення свободи слова та державної безпеки, відповідальності за поширення дезінформації, правомірності блокування інформаційних ресурсів, застосування санкцій до медіаструктур та окремих осіб.

Актуальність дослідження зумовлюється також тим, що воєнний стан в Україні став безпрецедентним за тривалістю та масштабами впливу на всі сфери суспільного життя. Правове регулювання інформаційної сфери зазнало істотних змін: були прийняті нові нормативно-правові акти, внесені зміни до чинного законодавства, сформовано нові підходи до діяльності засобів масової інформації, телекомунікаційних операторів, інтернет-провайдерів, платформ соціальних мереж. Разом з тим практика їх застосування виявила низку проблем, колізій та прогалин, які потребують ґрунтовного наукового осмислення та вироблення пропозицій щодо вдосконалення правового регулювання.

Особливу складність становить питання протидії дезінформації в умовах війни. Ворожі інформаційні кампанії спрямовані не лише на дискредитацію української влади та Збройних Сил України, а й на послаблення міжнародної підтримки, розпалювання панічних настроїв у суспільстві, поширення недовіри між різними соціальними групами. У таких умовах держава змушена застосовувати жорсткіші механізми інформаційного контролю, що нерідко викликає гострі суспільні дискусії щодо меж допустимого втручання у свободу слова.

Не менш важливим є й аспект кібербезпеки, який тісно пов’язаний з інформаційною безпекою. Кіберпростір використовується як інструмент для проведення атак на енергетичні системи, банківську сферу, транспортну інфраструктуру, органи державної влади та оборони. Юридичне забезпечення захисту кіберпростору потребує комплексного підходу, що поєднує норми інформаційного, адміністративного, кримінального та міжнародного права.

Усе вищезазначене свідчить про необхідність системного дослідження правових засад забезпечення інформаційної безпеки України в умовах

воєнного стану. Вивчення цієї проблематики має не лише теоретичне, а й значне практичне значення, оскільки результати таких досліджень можуть бути використані для вдосконалення законодавства, підвищення ефективності державної інформаційної політики, посилення захисту національних інтересів у інформаційній сфері, а також для забезпечення належного рівня захисту прав і свобод людини.

Метою даної роботи є комплексний аналіз правових механізмів забезпечення інформаційної безпеки України в умовах повномасштабної війни, визначення основних проблем і тенденцій розвитку законодавства у цій сфері, а також обґрунтування шляхів його подальшого вдосконалення. Для досягнення поставленої мети у роботі передбачається вирішення таких завдань: дослідити сутність та зміст поняття інформаційної безпеки в умовах збройного конфлікту; проаналізувати чинну нормативно-правову базу у сфері інформаційної безпеки; визначити особливості обмеження інформаційних прав під час воєнного стану; окреслити проблеми правозастосовної практики та сформулювати пропозиції щодо її вдосконалення.

Об'єктом дослідження є суспільні відносини, що виникають у сфері забезпечення інформаційної безпеки України в умовах воєнного стану. Предметом дослідження є норми національного та міжнародного права, які регулюють інформаційні відносини, а також практика їх застосування під час повномасштабної війни.

Таким чином, дослідження проблем правового забезпечення інформаційної безпеки в умовах війни є надзвичайно актуальним і необхідним для сучасної України, оскільки від ефективності правового регулювання в цій сфері значною мірою залежить не лише захист державних інтересів, а й збереження демократичних цінностей, прав і свобод людини навіть в умовах найскладніших викликів воєнного часу.

Інформаційна безпека за умов воєнного стану має стратегічну вагу, адже інформаційний простір перетворюється на один із провідних фронтів воєнного протистояння. Російсько-українська війна засвідчила, що поряд із класичними видами збройного протистояння активно застосовуються інформаційні, кібернетичні та психологічні впливи. Саме тому правове регулювання інформаційної сфери в період війни повинно не лише гарантувати захист державних інтересів, а й забезпечувати дотримання основоположних прав і свобод людини.

Нормативно-правова база інформаційної безпеки України під час воєнного стану складається з комплексу актів різної юридичної сили: Конституції України, спеціального законодавства у сфері воєнного стану, інформаційного, кримінального, адміністративного, кібербезпекового законодавства, а також підзаконних нормативних актів органів виконавчої влади. Разом вони формують правове поле, у межах якого держава здійснює регулювання інформаційних процесів і протидіє інформаційним загрозам.

Ключовим нормативним актом, який визначає загальні засади функціонування держави в умовах війни, є Закон України «Про правовий режим воєнного стану» [1]. Саме цей закон встановлює підстави введення воєнного стану, його зміст, строки дії та правові наслідки для органів державної влади, місцевого самоврядування, підприємств, установ, організацій і громадян. Особливе місце в цьому законі посідають положення, що стосуються обмеження інформаційних прав і свобод.

Закон наділяє органи державної влади широким колом повноважень у сфері інформаційної політики. Зокрема, під час воєнного стану допускається регулювання діяльності засобів масової інформації, включно з можливістю запровадження військової цензури, встановлення обмежень щодо поширення окремих видів інформації, контролю за передаванням даних електронними комунікаційними мережами. Окрім того, держава отримує право встановлювати спеціальні правила роботи інтернет-провайдерів, обмежувати доступ до певних інформаційних ресурсів, а також здійснювати централізоване інформування населення.

Такі повноваження мають об'єктивне обґрунтування, адже в умовах війни неконтрольоване поширення інформації може становити безпосередню загрозу обороноздатності держави, життю військовослужбовців і цивільного населення. Водночас науковці звертають увагу на проблему надмірної загальності окремих формулювань Закону. Зокрема, Котерлін І. Б. [3] зазначає, що низка норм містить оціночні категорії, які допускають неоднозначне тлумачення і створюють ризики зловживання владними повноваженнями.

Важливо також підкреслити, що Закон декларує обов'язок держави забезпечувати баланс між інтересами національної безпеки та необхідністю дотримання прав людини. Обмеження прав і свобод допускаються лише в межах, визначених Конституцією України, та повинні відповідати принципам законності, необхідності й пропорційності. Проте на практиці саме реалізація цих принципів викликає найбільше дискусій, особливо в частині доступу громадян до суспільно значущої інформації.

Окрім базового Закону про воєнний стан, важливу роль у формуванні правового механізму інформаційної безпеки відіграють норми суміжних галузей законодавства. Передусім це Закон України «Про інформацію» [6], який визначає загальні принципи інформаційних відносин, гарантії права на інформацію, підстави та порядок її обмеження. У контексті воєнного стану

цей закон залишається фундаментальним, хоча потребує адаптації до нових безпекових реалій.

Значну роль відіграє також Закон України «Про захист персональних даних» [7], що регулює порядок обробки, зберігання, передачі та захисту персональної інформації. В умовах війни питання захисту персональних даних набуває особливої гостроти, оскільки витік інформації про військовослужбовців, працівників критичної інфраструктури чи посадових осіб може мати катастрофічні наслідки для національної безпеки. Проте чинна редакція закону значною мірою орієнтована на мирні умови та не враховує специфіки інформаційних загроз воєнного часу.

Суттєве значення для інформаційної безпеки мають норми Кримінального кодексу України [8], які передбачають відповідальність за несанкціоноване втручання в роботу інформаційних систем, державну зраду, шпигунство, колабораційну діяльність, поширення відомостей військового характеру. Саме кримінально-правові засоби є крайнім, але необхідним інструментом протидії найбільш небезпечним інформаційним правопорушенням.

Окрему групу нормативних актів становлять документи у сфері кібербезпеки, ухвалені Національним банком України, Державною службою спеціального зв'язку та захисту інформації, Міністерством цифрової трансформації України. Вони регулюють питання захисту інформаційних ресурсів, критичної інфраструктури, електронних реєстрів, платіжних систем та державних інформаційних систем.

Разом з тим слід зазначити, що значна частина цих нормативних актів була розроблена до 2022 року, тобто до початку повномасштабної збройної агресії російської федерації. Це зумовлює їхню обмежену ефективність у сучасних умовах, коли масштаб та інтенсивність кібер- і інформаційних загроз зросли в рази. Таким чином, існує об'єктивна потреба в оновленні та систематизації законодавства про інформаційну безпеку з урахуванням воєнного досвіду.

Повномасштабна війна виявила цілий комплекс загроз інформаційній безпеці України, які мають як зовнішній, так і внутрішній характер. Інформаційний простір став полем постійної боротьби, де вирішується питання не лише формування громадської думки, а й забезпечення стійкості державних інститутів, морально-психологічного стану суспільства та боєздатності Збройних Сил України.

Однією з найнебезпечніших загроз є дезінформація та цілеспрямовані інформаційно-психологічні операції, які системно здійснює російська федерація. Їхня мета полягає у підриві довіри громадян до органів державної влади, деморалізації населення, створенні панічних настроїв, розпалюванні внутрішніх конфліктів і дискредитації України на міжнародній арені.

До основних інструментів таких операцій належать створення та поширення фейкових повідомлень, маніпуляції інформацією, використання соціальних мереж для масового впливу на свідомість громадян, застосування мереж ботів і тролів. Особливу небезпеку становить поширення неправдивої інформації про хід бойових дій, втрати серед військових і цивільних, діяльність органів влади та міжнародну підтримку України.

Науковці, зокрема Смотрич Д. В. [2] та Турченко О. Г. [9], наголошують, що ефективна протидія дезінформації неможлива без чіткої нормативної бази, яка б визначала юридичну відповідальність за поширення воєнно значимої неправдивої інформації. Водночас законодавець має діяти надзвичайно обережно, щоб боротьба з дезінформацією не перетворилася на інструмент необґрунтованого обмеження свободи слова.

Ще однією масштабною загрозою інформаційній безпеці є кібератаки. За даними аналітичних центрів, упродовж 2022–2024 років кількість і складність кібернападів на українські інформаційні ресурси істотно зросла [10]. Основними цілями атак стали енергетичні підприємства, об'єкти військової логістики, банківська система, органи державної влади та системи управління місцевих адміністрацій.

Кібератаки спрямовані не лише на виведення з ладу інформаційних систем, а й на викрадення даних, порушення цілісності електронних реєстрів, дестабілізацію фінансової системи та створення умов для соціального хаосу. Особливо небезпечними є атаки на об'єкти критичної інфраструктури, які можуть призвести до аварій, знеструмлень, перебоїв у водо- та теплопостачанні. Проблемою залишається недостатня координація між суб'єктами кіберзахисту. Попри наявність кількох уповноважених органів, між ними не завжди існує ефективний обмін інформацією, що знижує оперативність реагування на загрози. Не менш серйозною загрозою є витік персональних і службових даних. Окремі інциденти, пов'язані з оприлюдненням баз даних державних органів, свідчать про вразливість інформаційних ресурсів України. Компрометація персональних даних військовослужбовців, співробітників спецслужб, посадових осіб органів влади може призвести до шантажу, фізичного знищення, вербування або психологічного тиску.

Чинний Закон України «Про захист персональних даних» [7] не містить спеціальних норм, адаптованих до умов війни. Відсутні чіткі правила щодо обов'язкового рівня шифрування, режиму зберігання інформації в зоні бойових дій, порядку передачі даних між органами державної влади в екстрених умовах.

Під час війни обмеження доступу до певних видів інформації є об'єктивно виправданим інструментом захисту національної безпеки.

Йдеться, зокрема, про заборону поширення відомостей про розташування військових підрозділів, пересування техніки, результати ракетних ударів, роботу систем протиповітряної оборони.

Водночас такі обмеження повинні відповідати конституційним гарантіям, принципу пропорційності та міжнародним стандартам у сфері прав людини. Дослідження Турченко О. Г. [9] вказує на те, що низка обмежень, запроваджених після 2022 року, не має достатнього нормативного обґрунтування або не супроводжується чіткими процедурами контролю за їх дотриманням.

Попри наявність значної кількості нормативно-правових актів, правове забезпечення інформаційної безпеки України в умовах воєнного стану залишається фрагментарним і потребує подальшого вдосконалення. Однією з ключових проблем є відсутність чітких законодавчих критеріїв щодо обсягу обмежень інформаційних прав, строків їх дії та процедур оскарження. Це створює правову невизначеність і ускладнює захист прав громадян у разі їх порушення.

У сфері інформаційної безпеки задіяні різні органи: Служба безпеки України, Держспецзв'язку, Міністерство цифрової трансформації, Національна поліція, Збройні Сили України. Однак між ними досі відсутній єдиний оперативний протокол реагування на інформаційні та кіберінциденти, що знижує ефективність державної політики. Відсутність спеціальних норм щодо передачі даних між органами, обов'язкового шифрування, особливого режиму зберігання інформації під час бойових дій суттєво підвищує ризик витоків і несанкціонованого доступу.

Чинне кримінальне законодавство не повною мірою охоплює такі суспільно небезпечні діяння, як поширення воєнно значимої дезінформації, оприлюднення даних про пересування військ, діяльність бот-мереж та координованих інформаційних кампаній. Це створює прогалини у притягненні винних осіб до відповідальності.

Загалом, сучасні виклики інформаційної війни потребують докорінного перегляду підходів до правового регулювання інформаційної безпеки України, системного оновлення законодавства та формування цілісної державної політики у цій сфері.

У сучасних умовах воєнного конфлікту питання інформаційної безпеки та правового регулювання набувають особливої актуальності. Аналіз практики застосування законодавства свідчить, що недостатньо чіткі або застарілі норми можуть стати серйозною перешкодою для оперативного реагування на інформаційні загрози та ефективного захисту національної безпеки. У зв'язку з цим пропонується комплекс заходів щодо вдосконалення законодавства, спрямованих на забезпечення правової визначеності, оперативності державних органів та посилення захисту інформаційного простору країни. Законодавство про воєнний стан має забезпечувати баланс між необхідністю захисту національної безпеки та гарантуванням прав і свобод громадян. На практиці часто виникають труднощі, пов'язані з нечіткістю процедур введення обмежень на інформацію, відсутністю критеріїв пропорційності та обмеженими механізмами швидкого оскарження рішень [11].

Пропонується:

1. Встановлення чітких процедур запровадження інформаційних обмежень.

Визначення обставин, за яких можуть вводитися обмеження, конкретизація органу, який приймає рішення, строки дії обмежень, порядок інформування громадськості та завершення дії заходів. Це дозволить уникнути хаотичного чи свавільного застосування обмежень.

2. Визначення критеріїв пропорційності. Обмеження мають бути виправданими, необхідними та не перевищувати обсяг, який відповідає цілям захисту національної безпеки. Критерії пропорційності дозволять зменшити ризик надмірного обмеження свободи слова, доступу до інформації та інших прав громадян.

3. Механізм швидкого судового оскарження. Забезпечення права громадян і організацій на оперативне звернення до суду для оскарження рішень влади, що обмежують їхні права, сприятиме ефективному контролю та підвищить довіру до державних органів.

4. Контроль парламентських комітетів. Введення механізму регулярного парламентського нагляду за застосуванням обмежень дозволить оцінювати ефективність заходів, своєчасно виявляти надмірні обмеження та пропонувати їх корекцію. Ефективний захист інформаційного простору в умовах воєнного конфлікту вимагає скоординованих дій усіх державних органів.

5. Пропонується створення єдиного координаційного центру, який забезпечить: Швидкий обмін інформацією. Центр об'єднає дані про кібератаки, дезінформаційні кампанії та інші загрози, що надходять від різних структур, для аналізу ситуації в режимі реального часу. Узгоджене реагування на атаки.

Завдяки централізації координації забезпечується комплексне реагування на загрози: блокування шкідливих ресурсів, повідомлення громадськості та усунення вразливостей критичної інфраструктури. Оперативне притягнення винних до відповідальності. Центр сприятиме більш ефективному збору доказів для кримінального чи адміністративного переслідування осіб, що порушують правила інформаційної безпеки.

Воєнні умови значно підвищують ризики витоку та неправомірного використання персональних даних. Традиційні норми часто не забезпечують достатнього захисту.

Пропонується:

1. Ухвалення спеціального закону про обробку даних у воєнний час.

Закон має регламентувати особливі умови збору, обробки та передачі даних, визначати відповідальних суб'єктів та встановлювати механізми контролю.

2. Запровадження обов'язкового шифрування та резервного копіювання. Це дозволить захистити дані від несанкціонованого доступу та забезпечить можливість відновлення інформації у разі кібератак або технічних збоїв.

3. Визначення санкцій за воєнний витік даних. Законодавче врегулювання відповідальності за порушення безпеки персональних даних підвищить дисципліну серед державних та приватних структур і зменшить ризики інформаційних атак.

4. Актуалізація кримінально-правових норм необхідна для ефективного протидії інформаційним загрозам.

Захист інформаційного простору неможливий без активної участі громадян, які повинні вміти критично оцінювати інформацію та розпізнавати дезінформацію.

Пропонується:

1. Медіаграмотність населення. Включення курсів з критичного мислення, перевірки фактів та виявлення дезінформації у шкільні та університетські програми.

2. Підвищення кваліфікації державних службовців. Навчальні програми для державних службовців повинні включати методи захисту інформації, реагування на загрози та алгоритми дій у кризових ситуаціях.

3. Інформаційна гігієна. Пропагування правил безпечного користування цифровими ресурсами, захисту персональних даних та запобігання поширенню неперевіреної інформації серед населення.

Висновки. Проведений аналіз дозволяє дійти висновку, що ефективний захист інформаційного простору в умовах воєнного стану потребує комплексного нормативно-правового та інституційного підходу, який поєднує заходи державного регулювання, судового контролю, міжвідомчої координації та підвищення рівня інформаційної культури суспільства.

Запропоноване запровадження чітких процедур встановлення інформаційних обмежень, визначення критеріїв їх пропорційності, а також створення механізмів оперативного судового оскарження сприятиме забезпеченню балансу між потребами національної безпеки та дотриманням основоположних прав і свобод людини. Посилення парламентського контролю за застосуванням таких обмежень дозволить мінімізувати ризики їх надмірного або необґрунтованого використання.

Обґрунтовано доцільність створення єдиного координаційного центру з протидії інформаційним загрозам, діяльність якого забезпечить своєчасний обмін інформацією між уповноваженими суб'єктами, узгоджене реагування на кібератаки та дезінформаційні кампанії, а також підвищить ефективність притягнення винних осіб до юридичної відповідальності.

Окрему увагу приділено проблемі захисту персональних даних у воєнний час. Ухвалення спеціального законодавства, запровадження обов'язкових технічних заходів безпеки та визначення посиленої відповідальності за порушення режиму обробки даних є необхідними умовами зниження ризиків витоку та неправомірного використання інформації. Водночас актуалізація кримінально-правових норм розглядається як важливий інструмент протидії сучасним інформаційним загрозам.

Наголошено, що довгострокова стійкість інформаційного простору неможлива без активної участі громадян. Розвиток медіаграмотності населення, підвищення кваліфікації державних службовців та формування навичок інформаційної гігієни сприятимуть зменшенню впливу дезінформації та підвищенню загального рівня інформаційної безпеки.

Комплексна реалізація запропонованих заходів забезпечить підвищення ефективності державного реагування на інформаційні загрози, створення правової визначеності у застосуванні обмежень під час воєнного стану, посилення юридичної відповідальності за інформаційні правопорушення та формування в суспільстві навичок критичного сприйняття інформації. У підсумку це сприятиме зміцненню національної безпеки, підвищенню стійкості державних інституцій і належному захисту прав та інтересів громадян в умовах воєнного часу.

Список використаних джерел:

1. Про правовий режим воєнного стану : Закон України від 12 трав. 2015 р. № 389-VIII. Режим доступу: https://zakon.rada.gov.ua/laws/show/389-19 (дата звернення: 10.01.2026).

2. Смотрич Д. В. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 77. С. 121–127.

3. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану в аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції*. 2022. С. 150–155.

4. Руснак Ю. І. Правові аспекти забезпечення інформаційної безпеки в умовах російсько-української війни. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Історичні науки*. 2025. Т. 36 (75). № 1. С. 135–143.

5. Беспалов І. О. Правові засади інформаційної безпеки під час дії правового режиму воєнного стану. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2024. Режим доступу: https://doi.org/10.54929/2786-5746-2024-11-01-05 (дата звернення: 10.01.2026).

6. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. Режим доступу: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 12.01.2026).

7. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // База даних «Законодавство України» / Верховна Рада України. Режим доступу: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 12.01.2026).

8. Кримінальний кодекс України : Кодекс України; Закон від 05.04.2001 № 2341-III (ред. станом на 17.07.2025)//Базаданих«ЗаконодавствоУкраїни»/ВерховнаРадаУкраїни.Режимдоступу:https://zakon.rada.gov.ua/go/2341-14 (дата звернення: 12.01.2026).

9. Турченко О. Г. Обмеження права на доступ до публічної інформації в умовах воєнного стану. *Аналітично-порівняльне правознавство* : електрон. наук. вид. С. 107–113.

10. Кібербезпека України: досягнення і перспективи : аналіт. огляд / Держ. наук. установа «Інститут інформації, безпеки і права НАПрН України» ; Нац. б-ка України ім. В. І. Вернадського. Київ, 2023. № 10 (жовт.). 320 с.

11. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 7 берез. 2025 р. № 204-р. *Урядовий кур'єр*. 2025. № 54. 13 берез.

Дата першого надходження статті до видання: 17.11.2025
Дата прийняття статті до друку після рецензування: 19.12.2025
Дата публікації (оприлюднення) статті: 31.12.2025