передбачити пріоритетність захисту критичної інфраструктури, оперативний обмін розвідувальною інформацією та чіткі механізми протидії дезінформації. По-друге, у повоєнний період варто закріпити набуті зусилля через довгострокові програми модернізації систем кібербезпеки, підвищення кваліфікації державних службовців і фахівців ІТ-галузі та формування в суспільстві критичного сприйняття джерел інформації. Лише синергія жорстких норм, інноваційних технологій і просвітницьких ініціатив може створити стійку систему інформаційної безпеки, здатну захистити державу й громадян як під час загрози, так і на етапі відновлення.

**Список використаних джерел**


1. Про правовий режим воєнного стану : Закон України від 12.05.2015 р. № 389-VIII. URL:https://zakon.rada.gov.ua/laws/show/389-19#Text\.
2. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. URL:https://zakon.rada.gov.ua/laws/show/2469-19#Text.
3. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 14.02.2017 р. № 47/2017 URL:https://zakon.rada.gov.ua/laws/show/47/2017#Text
4. Центр протидії дезінформації при РНБО України – Офіційний сайт, URL:https://cpd.gov.ua/
5. Ситник І.І. Інформаційна безпека в умовах гібридної війни: національний і міжнародний виміри. *Вісник НАДУ при Президентові України*. 2022. № 1. С. 52–58.
6. Костюченко О.В. Інформаційна політика держави в умовах воєнного стану. *Національна безпека і оборона*. 2023. № 2(158). С. 18–24.
7. StopFake.org. Платформа протидії дезінформації: URL:https://www.stopfake.org/.



**Майсук Романа Романівна,**
*студент навчально-наукового інституту права та психології Національної академії внутрішніх справ*


## ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В УМОВАХ ВОЄННОГО СТАНУ: ПРАВОВІ ВИКЛИКИ ТА ПРАВОЗАСТОСУВАННЯ

В наш час, в умовах воєнного стану, ще більш актуального значення набуває безпека, особливо коли відбувається не лише фізична, але й інформаційна агресія. Забезпечення інформаційної безпеки набуває критичної важливості та запобігає спробам посіяти паніку серед населення. Широке використання цифрових технологій зумовлює появу нових форм загроз, таких як кібератаки, дезінформація та маніпулювання інформацією. Однією з основних правових проблем є необхідність розробки нормативно-правових актів, які б ефективно регулювали захист від кібератак, забезпечували прозорість у використанні

інформаційних технологій державними органами, а також захищали права громадян в умовах надзвичайних ситуацій. Такі заходи допомагають не лише у протидії зовнішнім загрозам, але й у захисті від внутрішніх дестабілізуючих чинників, таких як фальсифікація інформації у медіапросторі [1, с. 289].

Науковці звертають увагу на багатовекторність цієї загрози. Так, Лизанчук В.В. у своїй праці зазначає, що ключовим елементом має стати не лише репресивна, а й превентивна стратегія: навчання населення медіаграмотності, розвиток критичного мислення та створення національних платформ перевірки фактів. Водночас Кудінов В.А., підкреслює, що варто врегулювати відповідальність за поширення фальшивої інформації, забезпечити можливість оперативного спростування фейків, а також надати правоохоронним органам необхідні інструменти для протидії інформаційним диверсіям.

Одним із ключових правових викликів у період воєнного стану є гарантування цифрової безпеки – як на рівні держави, так і на рівні кожного громадянина. Особливої уваги потребує кіберзахист об’єктів критичної інфраструктури: енергетичних, комунікаційних, банківських систем. Для цього важливо вдосконалити національне законодавство щодо кібербезпеки, розробити ефективні механізми моніторингу інформаційних потоків та забезпечити міжнародну взаємодію для протидії кіберзагрозам. Скоординована співпраця з іншими країнами допоможе своєчасно реагувати на атаки та поширювати успішні практики цифрового захисту [2, с. 88].

У часи воєнних конфліктів зростає значення боротьби з дезінформацією, яка може посилювати паніку, підривати моральний дух громадян і загалом ставити під загрозу національну безпеку. Протидія інформаційній агресії включає розробку правових норм для боротьби з маніпуляціями в ЗМІ та соціальних мережах. Це включає встановлення законодавчих обмежень щодо поширення фальшивих новин, інструкцій для правоохоронних органів щодо протидії інформаційним операціям супротивника, а також механізми швидкої перевірки і спростування фейкових повідомлень. Водночас важливо забезпечити баланс між безпекою і свободою вираження думок, що є одним із найбільших правових викликів у цьому напрямку.

Варто зазначити, що порушення інформаційної безпеки у часи війни можуть мати особливо тяжкі наслідки. Тому правова система має передбачати посилену відповідальність за дії, які підривають інформаційну стабільність держави. Це стосується не лише кібератак, а й поширення пропаганди, інформаційного шпигунства чи технічного саботажу. Також необхідно впровадити ефективний контроль за діяльністю цифрових платформ, через які може поширюватися шкідливий контент. Посилення покарань, чітке визначення диспозиції кримінального правопорушення у сфері інформаційної безпеки та правозастосування у реальному часі – критично важливі для захисту держави [3].

В умовах воєнного стану, зокрема під час цифрової війни, постає проблема захисту основних прав людини, таких як право на приватність і право на свободу вираження думок. Законодавство повинно чітко регулювати, як збирається, обробляється та використовується інформація про громадян, особливо в умовах надзвичайних ситуацій. Законодавство має чітко окреслювати межі допустимого

збору та використання інформації, а контроль з боку незалежних інституцій допоможе запобігти зловживанням. Таким чином, дотримання прав людини в умовах цифрової війни має залишатись невід'ємною частиною правової стратегії держави.

**Список використаних джерел**

1. Лизанчук В.В. Інформаційна безпека України: теорія і практика: підручник. Львів: ЛНУ ім. Івана Франка, 2017. 725 с.

2. Кудінов В.А., Яровий К.В. Інформаційне забезпечення правоохоронної діяльності: навч.-практ. посіб. Київ: Нац. акад. внутр. справ, 2024. 120 с.

3. Крайнов В.О., Маланчук М.Ф., Грозовський Р.І. Методика оцінки ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління. К.: НУОУ, *Сучасні інформаційні технології у сфері безпеки та оборони,* 2020р. №1(37). С. 103-106.

**Марченко Карина Олександрівна,**
*курсант навчально-наукового інституту поліцейської діяльності Національної академії внутрішніх справ*

## ПРАВОВІ АСПЕКТИ ОБМЕЖЕННЯ ДОСТУПУ ДО ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

У зв'язку з новими викликами, що постали в умовах воєнного стану є необхідним перманентно враховувати та переглядати інформацію, розповсюдження якої може бути причиною смертельної небезпеки для життя та здоров'я людей, а також становити загрозу територіальній цілісності держави. Відкритість функціонування органів влади підвищує їх ефективність, а систематичний громадський нагляд є гарантією справедливого розподілу ресурсів. Фактично, держава оперує величезним обсягом критично важливої інформації, тому потрібні чіткі норми, що визначатимуть її обіг як у мирний час, так і особливо в умовах воєнних дій, що і зумовлює актуальність теми дослідження.

Внаслідок збройної агресії росії проти України, нашій державі довелося вдатися до обмежень у доступі до певних документів та інформації. Такі заходи було прийнято заради забезпечення захисту національних інтересів та збереження територіальної цілісності країни. Доцільно в даному аспекті зазначають І.І. Голубенко та А.Г. Саградян: «Це дозволяє державі взяти під контроль інформаційний простір та забезпечити захист національних інтересів. Проте, разом з тим, подібні заходи можуть значно обмежити доступ громадян до публічної інформації. Це може відбуватися через обмеження доступу до деяких інформаційних джерел, а також шляхом введення комендантської години» [1, с. 145]. Тому відправною точкою для законного обмеження доступу до інформації є врахування принципу презумпції відкритості публічної інформації.