

URL: <https://www.osce.org/osce-secretariat-exb-support-programme-for-ukraine/570414> (дата звернення: 12.05.2025).

5. Federal Bureau of Investigation. Hogan's Alley [Електронний ресурс]. URL: <https://www.fbi.gov/investigate/how-we-investigate/hogans-alley> (дата звернення: 15.05.2025).

6. Brissel L., Morel L., Dupont L. Contribution to setting up a sustainable learning in an eco-neighborhood development plan based on "Serious game" // 2013 International Conference on Engineering, Technology and Innovation (ICE) & IEEE International Technology Management Conference, The Hague, Netherlands, 2013. – P. 1–14. – DOI: 10.1109/ITMC.2013.7352607.

Пендюра Максим Миколайович,
*завідувач кафедри теорії, історії та
філософії права навчально-наукового
інституту права та психології
Національної академії внутрішніх справ,
кандидат юридичних наук, доцент*

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В УМОВАХ ПРАВОВОГО РЕЖИМУ ВОЄННОГО СТАНУ ТА ПІСЛЯВОЄННИЙ ПЕРІОД

У ХХІ столітті людство вступило в епоху інформаційного суспільства, у якому знання та інформація стали ключовими ресурсами. Однак з розвитком цифрового середовища зростає і вразливість до нових викликів, особливо в умовах правового режиму воєнного стану. Інформаційна безпека ще більше набуває пріоритетного значення не лише як складова національної безпеки, а як основа стійкості держави, її обороноздатності та суспільної стабільності.

Метою статті є проаналізувати правові та організаційні аспекти забезпечення інформаційної безпеки суспільства в умовах правового режиму воєнного стану та післявоєнний період, окреслити проблеми та напрями їх подолання в контексті розвитку інформаційного суспільства в Україні.

Інформаційне суспільство, як нова стадія цивілізаційного розвитку, характеризується зростанням ролі інформації, цифрових технологій, знань та інформаційної взаємодії в усіх сферах життєдіяльності держави. Концепція інформаційного суспільства була сформована у працях Д. Белла, З. Бжезинського, М. Кастельса, М. Порат, А. Тоффлера, А. Турена, Ю. Хабермаса та інших дослідників, які акцентували увагу на переході від індустріальної до постіндустріальної епохи.

Однак саме в умовах воєнного стану інформаційна сфера стає вразливою до низки загроз: інформаційно-психологічних операцій, дезінформації, кібератак, порушення доступу до критичних інфраструктур, поширення паніки через соціальні мережі тощо. На тлі цих викликів особливої актуальності набуває інформаційна безпека як цілісна система заходів для захисту інтересів держави, суспільства й особи в інформаційній сфері.

Відповідно до Закону України «Про правовий режим воєнного стану», під час його запровадження можливе тимчасове обмеження конституційних прав і свобод громадян, зокрема свободи слова, діяльності ЗМІ, права на інформацію. Основною метою є протидія ворожим інформаційним впливам, охорона стратегічної інформації, блокування каналів деструктивного контенту [1].

Однак ці обмеження повинні бути пропорційними, законними та такими, що відповідають принципам міжнародного права. Водночас воєнний стан вимагає не лише обмеження, а й ефективної стратегії інформаційної протидії, зокрема:

1. нейтралізації пропагандистських кампаній;
2. забезпечення інформаційної гігієни суспільства;
3. розбудови системи стратегічних комунікацій;
4. протидії кіберзлочинності;
5. гарантування захисту персональних даних.

Інформаційна безпека як складова національної безпеки України закріплена в Конституції України, Законах України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», а також у Стратегії кібербезпеки та інших нормативних актах. В умовах збройної агресії РФ, значного поширення фейкових наративів та кібератак з боку ворожих структур, забезпечення цілісності національного інформаційного простору є ключовим [2; 3, с. 182].

З 2014 року Україна активно розвиває системи протидії гібридним загрозам, зокрема створено Центр протидії дезінформації при РНБО, посилено взаємодію з Європейським Союзом та НАТО у сфері кібербезпеки та стратегічних комунікацій.

Особливу роль відіграє державна політика у сфері медіаграмотності, оскільки суспільна спроможність до критичного сприйняття інформації безпосередньо впливає на рівень загальної безпеки.

Воєнний стан, на відміну від традиційних уявлень, сьогодні є не лише збройним протистоянням, а й боротьбою в інформаційному просторі. Російська агресія проти України супроводжується потужною інформаційною війною, яка включає:

- масштабне поширення фейкових новин;
- психологічне тиснення через соцмережі;
- дестrukцію внутрішньої довіри до інституцій влади;
- кампанії з деморалізації ЗСУ та цивільного населення;
- кібератаки на об'єкти критичної інфраструктури.

Відповіддю на ці виклики має бути інтеграція інформаційної політики з національною безпекою, формування сталої цифрової ідентичності, розвиток власного наративу, який об'єднує суспільство та зміцнює його стійкість.

Завершення активної фази бойових дій не означає автоматичного припинення інформаційної агресії. У післявоєнний період Україна буде стикатися з низкою складних завдань у сфері інформаційної безпеки, зокрема:

1. Реінтеграція інформаційного простору деокупованих територій. Багаторічне перебування під впливом ворожої пропаганди потребує комплексної

програми інформаційної реабілітації - від відновлення інфраструктури до відновлення довіри населення до українських інституцій.

2. Контроль за розповсюдженням деструктивних наративів. У післявоєнний період можлива активізація внутрішніх і зовнішніх деструктивних сил, які використовуватимуть «посттравматичний» стан суспільства для поширення паніки, реваншистських або сепаратистських настроїв.

3. Ризики політичної поляризації. В умовах зміни політичного ландшафту після завершення воєнного стану загострюються суспільні суперечності, що можуть бути використані в інформаційних кампаніях для розколу суспільства.

4. Вплив іноземних медіа. Після послаблення воєнних обмежень активізується присутність іноземних інформаційних платформ, не завжди лояльних до України, що вимагає посилення інформаційного суверенітету.

Отже, післявоєнна інформаційна політика повинна поєднувати демократичні принципи свободи слова з безпековими пріоритетами, дотримуючись балансу між відкритістю та стійкістю.

Для формування сталого та безпечного інформаційного середовища в умовах трансформації безпекового контексту необхідна реалізація цілісної стратегії. Вона має ґрунтуватися на нашу думку на таких базових напрямках:

1. Законодавче удосконалення:

Потрібно адаптувати нормативно-правову базу до нових викликів цифрової доби. Особливо актуальними є:

- розмежування понять «інформаційна безпека» і «свобода слова» в умовах особливих режимів;
- закріплення механізмів захисту критичної інформаційної інфраструктури;
- визначення правових основ цифрової ідентичності;
- створення єдиного реєстру інформаційних інцидентів у сфері нацбезпеки.

2. Інституційна координація:

Забезпечення міжвідомчої взаємодії між Радою Національної безпеки і оборони України, Міністерством оборони України, Службою безпеки України, Держспецзв'язку, Міністерством цифрової трансформації, медіарегулятором та громадянським суспільством є критично важливим. Особливу роль у цьому має відігравати Центр протидії дезінформації, який може стати центральним координатором державної інформаційної політики.

3. Розвиток національного інформаційного продукту:

Інформаційна безпека неможлива без створення якісного національного контенту – українськомовного, патріотичного, інтелектуального. Це стосується:

- розвитку суспільного мовлення;
- підтримки незалежних медіа;
- стимулювання виробництва українських документальних та художніх фільмів, серіалів, освітніх платформ;
- протидії монополізації інформаційного ринку іноземними технологічними гігантами.

4. Освітні ініціативи:

Підвищення рівня цифрової грамотності населення – один із ключових чинників запобігання маніпуляціям. Потрібно:

- запровадити системну медіаосвіту у дошкільних закладах, школах (ліцєях, коледжах) та університетах (академіях);
- створити державні і приватні платформи для навчання кібергігієні;
- проводити загальнонаціональні і регіональні (місцеві) кампанії з інформування щодо інформаційної безпеки.

5. Міжнародна співпраця:

Україна має інтегруватися в європейські та трансатлантичні механізми інформаційної безпеки. Участь у відповідних програмах ЄС, НАТО, співпраця з кіберкомандуваннями партнерських країн, особливо закладів вищої освіти дозволять підвищити ефективність вітчизняної системи захисту.

6. Людина в центрі інформаційної безпеки:

Особливість сучасного підходу до інформаційної безпеки – зміщення акценту з державоцентризму на людиноцентризм. Основна мета – не просто захистити державу, а гарантувати безпечне і гідне інформаційне середовище для кожного громадянина. Це означає:

1. забезпечення доступу до достовірної інформації;
2. недопущення інформаційної дискримінації;
3. захист персональних даних і приватності;
4. можливість громадян реалізувати право на відповідь, спростування, доступ до правди.

Інформаційна безпека у цьому контексті – не лише технічний чи військовий захист, а передусім – умова якісного демократичного розвитку.

Інформаційна безпека в умовах воєнного стану та в післявоєнний період – це довгостроковий різнорівневий процес, який вимагає системності, адаптивності та активної участі держави, суспільства і кожного громадянина. Від ефективності державної інформаційної політики залежить не лише захищеність від зовнішніх впливів, а й здатність нації до самозбереження, відновлення та розвитку після війни.

Після перемоги Україна потребуватиме не лише фізичної, а й інформаційної реконструкції. Сформований під час воєнного стану досвід має бути інтегрований у довготривалу політику інформаційної стійкості, що ґрунтується на цінностях прав людини, демократичного розвитку та технологічного суверенітету.

Список використаних джерел

1. Закон України «Про правовий режим воєнного стану» від 12.05.2015 №389-VIII // *Відомості Верховної Ради України*. 2015. № 28. Ст. 250. URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text>

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII // *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

3. Милосердна І.М. Інформаційна безпека як елемент національної безпеки: теоретичний вимір та особливості впровадження / І.М. Милосердна // *Політикус* : наук. журнал. 2024. № 4. С. 179-185. URL: http://politicus.od.ua/4_2024/28.pdf

4. Посібник з протидії дезінформації. URL: <https://cpd.gov.ua/announcement/posibnyk-z-protydiyi-dezinformacziyi/>

Пендюра Максим Миколайович,
завідувач кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат юридичних наук, доцент

Пилипенко Вікторія Вікторівна,
доцент кафедри теорії, історії та філософії права навчально-наукового інституту права та психології Національної академії внутрішніх справ, кандидат історичних наук, доцент

ФОРМУВАННЯ НАВИЧОК МЕДІАГРАМОТНОСТІ ЯК ОСНОВА ПРОФЕСІЙНОЇ ПІДГОТОВКИ ЮРИСТІВ В УМОВАХ ВІЙНИ

В умовах війни інформація є зброєю, яку у вигляді фейків, дезінформації, маніпуляцій використовують для морального та психологічного придушення опору населення. За результатами проведеного протягом травня-червня 2024 року на замовлення Громадянської мережі ОПОРА опитування, було встановлено, що 73,4% українців використовують соцмережі як джерело новин. Серед них найпопулярніші – Telegram (78.1%), YouTube (59.5%) та Facebook (44.6%) [1]. Виходячи з такої популярності заявлених соцмереж й не представленого в опитуванні, але стрімко набираючого темпи популярності TikTok, юристи, особливо початківці, намагаються зайняти серед них свою нішу. Дедалі частіше можна зустріти коментарі юристів з приводу тієї чи іншої урядової ініціативи, законопроєкту або оголошення правової оцінки проведеним заходам. З одного боку така доступність покращує правову обізнаність населення, а з іншого, юрист сам того не усвідомлюючи, стає популяризатором фейків та неправдивих новин. Останнє особливо стосується численних коментарів щодо заявлених законопроєктів, які ще навіть не пройшли перше читання. Ось чому сьогодні загострилася проблема формування в юристів навичок медіаграмотності та основ критичного мислення під час їх професійної підготовки та перепідготовки.

Медіаграмотність являє собою сукупність мотивів, знань, умінь і можливостей, що сприяють добиранню, використанню, критичному аналізу, оцінюванню, створюванню та передаванню медіатекстів різних форм, жанрів, а також аналізу складних процесів функціонування медіа в суспільстві. Іншими