Конопля В. В.,
здобувач вищої освіти факультету службово-бойової діяльності НГУ, Київський інститут Національної гвардії України
(м. Київ, Україна)

Науковий керівник:
Бейкун А. Л.,
кандидат юридичних наук, доцент, доцент кафедри правового забезпечення та правоохоронної діяльності факультету забезпечення державної безпеки,
Київський інститут Національної гвардії України
(м. Київ, Україна)

ПРОБЛЕМАТИКА ЗАКОНОДАВЧОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ В УМОВАХ ПОВНОМАСШТАБНОЇ ЗБРОЙНОЇ АГРЕСІЇ

Сучасні глобальні виклики, зумовлені війнами, що мають гібридні складові, зокрема, інформаційні маніпуляції та кібератаки, висувають на перший план проблему ефективного правового забезпечення протидії дезінформації як складової гібридних загроз повномасштабного збройного конфлікту. Україна, перебуваючи на передовій інформаційної війни, потребує системного законодавчого реагування на деструктивні впливи, спрямовані на підрив державного суверенітету, національної безпеки та демократичних інститутів [1, с. 35-36].

Поняття «гібридні загрози» охоплює сукупність воєнних, інформаційно-психологічних, політичних, економічних та кібернетичних дій, спрямованих на дестабілізацію держави. На нормативному рівні це поняття закріплено у Стратегії національної безпеки України «Безпека людини - безпека країни» від 2020 року, де зазначено, що до гібридних загроз належать: дії держав чи недержавних акторів, спрямовані на деструкцію суспільної свідомості, розкол громадської думки, підрив довіри до влади та інституцій [2].

Нормативно-правове забезпечення протидії гібридним загрозам в Україні формує комплекс взаємопов’язаних актів: від Конституції до спеціального законодавства у сфері інформаційної безпеки, кіберзахисту та державної безпеки. Основою є Конституція України, яка визначає захист суверенітету та інформаційного простору як обов’язок держави (статті 17, 34). Розвиток конституційних положень відбувається у Законі України «Про національну безпеку України» від 21.06.2018 № 2469-VIII, який встановлює систему

забезпечення національної безпеки, включно з інформаційною, кібернетичною та військовою складовими [3].

Особливе місце серед інструментів протидії гібридним загрозам посідає законодавство про інформаційний простір. Закон України «Про інформацію» визначає принципи інформаційної діяльності, права громадян на достовірну інформацію та механізми її захисту [4]. Закон «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII закріплює повноваження державних органів у сфері протидії кіберзагрозам, що часто є компонентом гібридних операцій [5]. Важливою є також діяльність Ради національної безпеки і оборони України, яка координує заходи із забезпечення інформаційної стійкості держави.

В аспекті протидії дезінформації ключовим напрямом є розвиток правових механізмів захисту інформаційного простору від фейкових повідомлень, маніпуляцій і пропаганди. Відповідно до Доктрини інформаційної безпеки України (Указ Президента України №47/2017), дезінформація розглядається як загроза національній безпеці, оскільки вона може впливати на формування суспільних настроїв, генерувати зневіру у спротив агресорові, підривати довіру до влади та міжнародних партнерів. Доктрина передбачає створення системи моніторингу інформаційного простору, удосконалення законодавства щодо протидії інформаційній агресії та посилення співпраці з ЄС і НАТО у сфері стратегічних комунікацій [6].

У європейському вимірі правові підходи до боротьби з дезінформацією реалізуються через Директиву (ЄС) 2018/1808 про аудіовізуальні медіа-послуги та Кодекс практик ЄС щодо дезінформації (2022). Україна поступово імплементує ці стандарти, зокрема через оновлення Закону України «Про медіа» (в редакції червня 2025 року), що встановлює вимоги до прозорості власності медіа, недопущення поширення матеріалів, що містять дезінформацію або виправдовують агресію російської федерації [7].

Під час повномасштабної агресії росії проти України інформаційна безпека набула статусу пріоритетного елементу державної політики. Держава застосовує комплекс правових заходів: від обмеження доступу до ресурсів, що поширюють російську пропаганду, до посилення відповідальності за інформаційне пособництво агресору. Так, у 2022 р. було внесено зміни до Кримінального кодексу України (статті 111-1, 111-2), якими встановлено відповідальність за колабораційну діяльність, у тому числі за поширення пропаганди держави-агресора [8].

Окремо варто відзначити роль стратегічних комунікацій як інструменту протидії дезінформації. Відповідно до Концепції розвитку стратегічних комунікацій у секторі безпеки і оборони (затвердженої рішенням РНБО від 27.12.2021), держава повинна формувати ефективну систему інформаційної взаємодії між органами влади, ЗМІ та громадськістю, що сприятиме підвищенню стійкості суспільства до маніпуляцій. Відповідно до означеної Концепції повинні бути розроблені і відомчі нормативи суб’єктів оборонно-безпекового сектору.[9].

Таким чином, законодавче забезпечення протидії гібридним загрозам і дезінформації в Україні базується на інтегрованому підході, який охоплює конституційні гарантії, спеціальні закони, доктринальні документи, а також імплементацію європейських стандартів. У подальшому розвиток цієї системи має бути спрямований на удосконалення механізмів інформаційного моніторингу, запровадження стандартів медіаграмотності, підвищення прозорості діяльності медіа та посилення кримінально-правових інструментів відповідальності за дезінформацію. В умовах гібридної війни саме правові механізми стають фундаментом інформаційної безпеки держави.

Список використаних джерел:

1. Городецький В. П. Інформаційна безпека в умовах гібридної війни: правовий вимір. *Науковий вісник публічного та приватного права.* 2023. № 2. С. 35–42.
2. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». Указ Президента України від 14.09.2020 № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 30.09.2025).
3. Про національну безпеку України. Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради (ВВР)*, 2018, № 31, ст.241. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 30.09.2025).
4. Про інформацію. Закон України від 02.10.1992 № 2657-XII. (*Відомості Верховної Ради України (ВВР*), 1992, № 48, ст.650). URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 30.09.2025).
5. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII. (*Відомості Верховної Ради (ВВР)*, 2017, № 45, ст.403). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.09.2025).
6. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ Президента України від 25.02.2017 № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 30.09.2025).
7. Про медіа. Закон України від 13.12.2022 № 2849-IX. (*Відомості Верховної Ради України (ВВР)*, 2023, №№ 47-50, ст.120). URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 30.09.2025).
8. Кримінальний кодекс України. (*Відомості Верховної Ради України (ВВР)*, 2001, № 25–26. ст. 131). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 30.09.2025).
9. Деякі питання реалізації стратегічних комунікацій у системі Міністерства оборони України. Наказ Міністерства оборони України від 02.10.2025 № 653-нм. URL: https://zakon.rada.gov.ua/rada/show/v0653322-25#n6 (дата звернення: 30.09.2025).