Скоморохов В. А.,
слухач магістратури,
Київський інститут Національної гвардії України
(м. Київ, Україна)

Науковий керівник:
Ковальова Т. І.,
кандидат юридичних наук, доцент,
Київський інститут Національної гвардії України
(м. Київ, Україна)

DEEPFAKE: ЗАГРОЗА ЦИФРОВОЇ ДЕЗІНФОРМАЦІЇ В СЕКТОРІ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

У сучасних умовах стрімкого розвитку технологій штучного інтелекту та зростання інформаційних загроз протидія deepfake-технологіям стає одним із ключових пріоритетів національної безпеки будь-якої держави. Україна, перебуваючи в умовах повномасштабної війни, постійно потерпає від дезінформаційних кампаній, які здійснюються ворогом з метою інформаційно-психологічних операцій та поширення фейкової інформації [1]. Deepfake-технології мають похитнути довіру українців до держави та ЗСУ, поширити паніку, дестабілізувати роботу державних органів, особливо гостро відчувається потреба в ефективному правовому регулюванні у сфері протидії синтетичним медіа, зокрема у контексті діяльності сектору безпеки і оборони [2].

Сектор безпеки і оборони України як система державних органів, що забезпечує національну безпеку, виконує важливу роль у захисті стратегічних об’єктів, охороні громадського порядку та протидії загрозам національній безпеці, що включає і інформаційні загрози типу deepfake [3]. Проте чинне законодавство лише частково визначає механізми протидії deepfake-технологіям у секторі безпеки, що створює правові прогалини та ускладнює реалізацію потенціалу держави в цій сфері.

Актуальність цього дослідження випливає з потреби вдосконалити нормативно-правову базу, що регулює протидію deepfake-технологіям у системі національної безпеки держави, і створення ефективної правової моделі взаємодії з іншими суб’єктами інформаційної безпеки.

Нормативно-правова база протидії дезінформації в Україні базується на низці національних законодавчих актів, котрі окреслюють головні напрямки діяльності державних органів у цій сфері. Основним документом є Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII [4]. У цьому законі вперше на законодавчому рівні було закріплено поняття кібербезпеки, визначено коло суб’єктів її забезпечення, а також встановлено правові засади взаємодії між ними у контексті протидії інформаційним загрозам.

Вагоме значення має Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII [5], у якому інформаційна безпека визнана складовою національної безпеки. Цим законом передбачено створення єдиної державної політики у сфері протидії інформаційним загрозам та впровадження відповідних механізмів контролю і координації з боку Ради національної безпеки і оборони України.

Важливу роль відіграє діяльність Центру протидії дезінформації при РНБО України, який здійснює моніторинг та аналіз дезінформаційних кампаній, включаючи deepfake-контент [6]. Як зазначається експертами ЦПД, "Мета фейку – дискредитація української армії та влади, розпалювання суспільної недовіри і провокування протестних настроїв серед громадян" - це стосується і deepfake-технологій, які використовуються російською пропагандою.

Повноваження сектору безпеки і оборони України у сфері протидії deepfake-загрозам на сьогодні не мають чіткого та однозначного нормативного закріплення. Відповідні закони не містять положень, які б безпосередньо регламентували участь органів сектору безпеки у протидії синтетичним медіа. Однак, з огляду на загальні завдання цих органів, такі як захист національних інтересів, забезпечення інформаційної безпеки, участь у боротьбі з інформаційними загрозами можна зробити висновок, що їх функціонал опосередковано включає компоненти, дотичні до протидії deepfake [7].

У контексті захисту критичної інфраструктури – зокрема стратегічно важливих підприємств оборонно-промислового комплексу, об’єктів державної влади та військових формувань – органи сектору безпеки можуть виконувати функції з забезпечення безпеки інформаційно-комунікаційних систем, які виступають потенційними цілями для deepfake-атак. Також, відповідно до чинного законодавства, субєктами забезпечення інформаційної безпеки можуть виступати різні державні органи, що взаємодіють у питаннях реагування на інформаційні інциденти [8].

Однією з ключових проблем у сфері правового регулювання протидії deepfake є недостатня визначеність статусу та функціонального призначення органів сектору безпеки у цій галузі. Нормативно-правова база не містить положень, що безпосередньо стосуються участі у протидії deepfake-загрозам, що зумовлює обмеженість залучення до реагування на такі загрози в межах національної системи безпеки. Проблемою також є відсутність спеціалізованих підрозділів, здатних здійснювати оперативне реагування на deepfake-інциденти.

Як зазначає Центр стратегічних комунікацій, "росія використовує інформаційний вплив як зброю, а західний світ уже шукає системні рішення для протидії FIMI" (Foreign Information Manipulation and Interference – іноземні маніпуляції інформацією та втручання), що включає і deepfake-технології.

Мета таких дій – переконати українську та міжнародну аудиторії, що опір України російській агресії марний.

З огляду на поточні виклики, доцільним є внесення змін до відповідних законів України. Ці зміни повинні розширити компетенції органів сектору безпеки у сфері протидії deepfake-технологіям та забезпечити законодавче

підґрунтя для активної участі у захисті від синтетичних медіа, особливо в умовах воєнного стану. Окрім цього, доречним є розробка низки підзаконних нормативних актів, які визначатимуть механізм взаємодії різних відомств під час протидії deepfake-загрозам. Важливим кроком є також формування спеціалізованих технічних підрозділів чи груп швидкого реагування, які будуть спроможні ефективно протистояти синтетичним медіа загрозам.

Значну роль у протидії deepfake відіграють інформаційні ресурси держави. Зокрема, Центр стратегічних комунікацій та протидії дезінформації активно працює над виявленням та спростуванням deepfake-контенту, як це було у випадку з фальшивим відео командира Третього армійського корпусу ЗСУ [1].

Таким чином, участь сектору безпеки і оборони України у протидії deepfake-загрозам має значний потенціал, однак наразі залишається недостатньо врегульованою на нормативно-правовому рівні. Чинне законодавство не містить прямого зв'язку "deepfake – кіберінцидент", що вимагає додаткового юридичного тлумачення. Враховуючи сучасні виклики у сфері національної безпеки, особливо в умовах воєнного стану, актуальним є створення правових механізмів, які б забезпечили ефективну протидію deepfake-технологіям та захист від дезінформаційних кампаній у цифровому просторі.

Deepfake-атака, може бути кваліфікована не лише як дезінформація, а й як складова частина кібератаки або інформаційний вплив, що призводить до порушення роботи об'єктів критичної інфраструктури. Це дозволяє задіяти розширений інструментарій та повноваження органів сектору безпеки, які визначені для протидії кіберзагрозам та захисту критичної інфраструктури.

Список використаних джерел:

1. Роспропагандисти зробили deepfake з командиром Третього армійського корпусу ЗСУ Андрієм Білецьким. Центр стратегічних комунікацій. 2025. URL: https://spravdi.gov.ua/rospropagandysty-zrobyly-deepfake-z-komandyrom-tretogo-armijskogo-korpusu-zsu-andriyem-bileczkym/
2. Штучний інтелект і дезінформація: можливості та ризики в умовах війни. Центр стратегічних комунікацій. 2023. URL: https://spravdi.gov.ua/shtuchnyj-intelekt-i-dezinformacziya-mozhlyvosti-ta-ryzyky-v-umovah-vijny/ .
3. FIMI-атаки: як Росія веде інформаційну війну проти України та Заходу. Центр стратегічних комунікацій. 2025. URL: https://spravdi.gov.ua/fimi-ataky-yak-rosiya-vede-informaczijnu-vijnu-proty-ukrayiny-ta-zahodu/ .
4. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 р. № 2163-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 17.09.2025).
5. Про національну безпеку України : закон України від 21.06.2018 р. № 2469-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 19.09.2025).

6. Що таке діпфейк і як його використовує російська пропаганда. Центр протидії дезінформації при РНБО України. 2023. URL: https://cpd.gov.ua/en/безтегории/ccd-explains-the-term-deepfake/.
7. Як захиститися від фейків і дезінформації. Дія. Цифрова освіта. URL: https://osvita.diia.gov.ua/courses/how-to-protect-yourself-from-fakes-and-disinformation.
8. Спам, реклама, фейки. Як російська пропаганда атакує українців у соцмережах. Центр стратегічних комунікацій. 2024. URL: https://spravdi.gov.ua/spam-reklama-fejky-yak-rosijska-propaganda-atakuye-ukrayinczіv-u-soczmerezhah/.