Маленко Андрій Олександрович
Студент 2 н.гр. 4-КВ курсу ІЗДН НАВС

Науковий керівник:
Кудінов Вадим Анатолійович
кандидат фізико-математичних наук, доцент, завідувач кафедри інформаційних технологій ННІ права та психології НАВС

ПРОТИДІЯ ДІПФЕЙКАМ ЯК СУЧАСНІЙ ФОРМІ КІБЕРЗАГРОЗ

Представлено дослідження сучасних загроз, пов'язаних із використанням діпфейк-технологій у контексті гібридної війни. Метою роботи є аналіз технічних, організаційних і правових засобів протидії діпфейкам як формі кіберзброї. Розглянуто потребу у нормативному регулюванні, міжвідомчій координації та підвищенні медіаграмотності населення, інтеграції протидії діпфейкам в систему національної кібербезпеки.

З розвитком синтезу високоякісного штучного медіаконтенту діпфейки стали потужним інструментом інформаційної маніпуляції. Удосконалення технологій призвело до дедалі важчого відрізнення таких матеріалів від справжніх, що ускладнює їх виявлення [1], діпфейки перетворились на «кіберзброєю» – інструмент, що комбінується з соціальними мережами, хакерськими атаками та психологічними операціями.

В умовах гібридної війни діпфейк-технології застосовуються для створення контенту з метою підриву довіри до державних інституцій та дестабілізації суспільства; на початок збройної агресії у цифровому просторі виявлено діпфейки нібито із заявами уряду про капітуляцію. Використання діпфейку із зображеннями авторитетних осіб може викликати справедливі сумніви у достовірності серед частини громадян, проте не слід нехтувати впливом навмисної шкідливої інформації, який призводить до тривалих негативних наслідків [2].

Тема протидії діпфейкам є не лише технологічним викликом, але й елементом національної безпеки, інформаційної стійкості та кіберзахисту. Маючи технічну природу, діпфейки чітко зорієнтовані у соціально-психологічному векторі: вони не просто підробка, а потужний засіб маніпуляції, що впливає на рішення громадян та адекватну роботу інституцій.

Разом із тим урядовими структурами ще не приділено достатньої уваги зменшенню ризику загроз, викликаних діпфейками.

Одною з причин цього, на наш погляд, є віднесення діпфейків до суто кібернетичних загроз, серед яких за кількістю інцидентів лідирують: шкідливий програмний код, спроби втручання та несанкціонований збір інформації (згідно річних звітів Держспецзв'язку за 2022-2024 рр.), отже пріорітет надано відверненню саме таких загроз. Ефективна протидія діпфейкам передбачає застосовування комплексного підходу із залученням технологічних та організаційно-правових заходів в оперативному режимі.

Технологічними заходами є розробка і впровадження засобів виявлення діпфейків: алгоритми детекції медіа на основі штучного інтелекту, цифрові водяні знаки, біометрія, багатофакторна аутентифікація тощо.

До *організаційних-правових заходів* належать організаційні/управлінські (підвищення рівня медіаграмотності населення, навчання служб реагування, створення схем перевірки медіаконтенту у державних та приватних структурах, побудова порядків верифікації інформації) та нормативно-правові (удосконалення законодавства, яке визначає відповідальність за створення та поширення шкідливих діпфейків, регулювання цифрових платформ, співпраця між державою й технологічними компаніями) [3].

Оперативність протидії забезпечують такі заходи, як використання аналітики для виявлення діпфейків у режимі реального часу, інтеграція їх моніторингу у системи інформаційної безпеки, швидке оприлюднення спростувань, координація із ЗМІ та соціальними мережами.

В Україні наявний специфічний контекст: поєднання збройного конфлікту і інформаційної війни, що зумовлює високу потребу в захисті цифрового простору. Тобто, заходи протидії діпфейкам повинні бути адаптовані до умов воєнного стану, включати взаємодію із Збройними Силами, спецслужбами та медіа.

Інформаційна безпека країни потребує врахування сучасних методів інформаційно-психологічних атак [4]. Водночас, в Україні проводяться тематичні дослідження, де діпфейк розглянуто як новий вид кіберзброї в інформаційній війні [5], що означає подальшу потребу у мовній локалізації відповідних технологій, забезпеченні партнерства із технологічними компаніями, врахуванні і удосконаленні законодавчих чинників, підготовці кадрів, підвищенні обізнаності населення про технології психологічних маніпуляцій.

Висновки. Діпфейки – не маргінальна технологія, а серйозна кіберзагроза, здатна впливати на хід подій у військовому конфлікті. Протидія діпфейкам має охоплювати технологічні, організаційні й правові складові, і повинна інтегруватись до національної концепції кібербезпеки, особливо в умовах воєнного стану. Вкрай важливо сформувати власну систему оперативного виявлення та реагування із урахуванням особливостей національного медіапростору в умовах триваючої гібридної війни.

З цією метою слід здійснити низку взаємопов'язаних заходів: створення урядової платформи моніторингу медіаконтенту на предмет діпфейків; впровадження обов'язкових цифрових водяних знаків для офіційного медіаконтенту; розробку методології швидкої верифікації медіа у кризових ситуаціях; удосконалення законодавства про відповідальність за створення/поширення діпфейків. Також варто посилити масову просвітницьку роботу щодо вмінь розпізнавання підробленого контенту, критичного ставлення до аудіовізуальних матеріалів та джерел їхнього походження.

Список використаних джерел:

1. K.T.Mai, S.Bray, T.Davies, L.D.Griffin. Warning: Humans cannot reliably detect speech deepfakes // *PLoS ONE* 18(8): e0285333 – 02.08.2023. [Електронний ресурс]. URL: https://doi.org/10.1371/journal.pone.0285333 (дата звернення: 21.10.2025).
2. J.J.Twomey, C.Linehan, G.Murphy. Deepfakes in warfare: new concerns emerge from their use around the Russian invasion of Ukraine // *The Conversation* – 26.10.2023. [Електронний ресурс]. URL: https://doi.org/10.64628/AB.mqvh4tx3x (дата звернення: 21.10.2025).
3. Вальорска М. Аґнєшка. Діпфейк та дезінформація : практ. посіб. / Академія української преси ; Центр Вільної Преси, 2020 [Електронний ресурс]. URL: https://www.aup.com.ua/ uploads/DEEPFAKES_FNF_AUP_2020.pdf (дата звернення: 21.10.2025).
4. Колосовський Є.Ю., Круць Е.М. Сучасний стан кібербезпеки України в умовах воєнного періоду // *Юридичний науковий електронний журнал*. – 2023. – №12. – С. 402-405. [Електронний ресурс]. URL: https://doi.org/10.32782/2524-0374/2023-12/100 (дата звернення: 21.10.2025).
5. Прищепа М.О. Deepfake як новий небезпечний вид кіберзброї : дипломна робота ... бакалавра. – Київ, 2023. – 76 с. [Електронний ресурс]. URL: https://ela.kpi.ua/server/api/core/ bitstreams/d062597f-1fb5-4662-a01b-8a02c2b98d13/content (дата звернення: 21.10.2025).