Адміністративне право і процес

УДК 004.8:34:351.746.1

DOI https://doi.org/10.5281/zenodo.20596393

Правове регулювання deepfake-технологій: виклики для інформаційної безпеки

Предместніков Олег Гарійович,
доктор юридичних наук, професор, заслужений юрист України, завідувач кафедри права, Мелітопольський державний педагогічний університет імені Богдана Хмельницького, м. Запоріжжя, Україна,
http://orcid.org/0000-0001-8196-647X

Любченко Станіслав Олегович,
начальник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України, м. Київ, Україна,
https://orcid.org/0009-0002-8212-4869

Пугач Дмитро Олексійович,
кандидат юридичних наук, викладач кафедри іноземної філології та перекладу,
Європейський Університет, м. Київ, Україна,
https://orcid.org/0009-0002-9178-7517

Прийнято: 19.05.2026 | Опубліковано: 30.05.2026

Анотація: Стаття розкриває особливості правового регулювання deepfake-технологій та їх вплив на стан інформаційної безпеки в умовах

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

цифровізації суспільства. Актуальність обраного питання зумовлена стрімким розвитком штучного інтелекту та поширенням технологій синтетичного створення аудіо-, відео- та зображувального контенту, який використовується не тільки для розваг, а й у політичних, інформаційних та комунікаційних процесах. Наголошується, що deepfake-контент здатний створювати високореалістичні продукти, які розмивають межу між правдою та цифровою імітацією, тим самим створюючи загрозу для інформаційної безпеки держави та прав людини.

У роботі головна увага зосереджена на застосуванні deepfake-технологій, а також пов'язаних із ними ризиків, зокрема поширення дезінформації, маніпулювання громадською думкою, цифрового шахрайства, дискредитації осіб та втручання у виборчі процеси тощо. Окрему увагу приділено міжнародним підходам до регулювання deepfake, зокрема положенням Artificial Intelligence Act Європейського Союзу, який передбачає обов'язкове маркування синтетичного контенту та використання технічних засобів його ідентифікації.

У межах дослідження встановлено, що національне законодавство України не містить спеціального правового регулювання deepfake-технологій, що створює прогалини у сфері притягнення до відповідальності за їх неправомірне використання. Обґрунтовано необхідність формування комплексного правового механізму регулювання, який поєднує нормативні, організаційні та технічні інструменти протидії дезінформації.

Окремо підкреслено значення інформаційного рівня захисту, що включає розвиток медіаграмотності населення та створення систем оперативного виявлення і спростування фейкового контенту. Запропоновані підходи спрямовані на підвищення стійкості інформаційного простору та зменшення ризиків маніпулятивного впливу deepfake-технологій. В умовах війни такі заходи набувають особливого значення, оскільки deepfake-контент може використовуватися як інструмент інформаційно-психологічного впливу,

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

спрямованого на дестабілізацію суспільства, поширення паніки, дискредитацію державних інституцій та підрив довіри до офіційних джерел інформації.

Ключові слова: дезінформація, deepfake, синтетичний контент, національна безпека, цифрова безпека, правовий вимір, штучний інтелект, AI Act, медіаграмотність, цифрові технології.

Legal regulation of deepfake technologies: challenges for information security

Oleh Predmestnikov,
Doctor of Law, Professor, Honored Lawyer of Ukraine, Head of the Department of Law, Bogdan Khmelnitsky Melitopol State Pedagogical University, Zaporizhia, Ukraine, http://orcid.org/0000-0001-8196-647X

Stanislav Liubchenko,
Head of the Center of Forensic and Special Expertise of the Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine, Kyiv, Ukraine, https://orcid.org/0009-0002-8212-4869

Dmytro Puhach,
Candidate of Law, Lecturer at the Department of Foreign Philology and Translation,
European University, Kyiv, Ukraine,
https://orcid.org/0009-0002-9178-7517

Abstract: The article reveals the features of the legal regulation of deepfake technologies and their impact on the state of information security in the context of the digitalization of society. The relevance of the chosen issue is due to the rapid development of artificial intelligence and the spread of technologies for synthetic

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

creation of audio, video and image content, which is used not only for entertainment, but also in political, information and communication processes. It is emphasized that deepfake content is capable of creating highly realistic products that blur the line between truth and digital imitation, thereby creating a threat to the information security of the state and human rights. The work focuses on the use of deepfake technologies, as well as the risks associated with them, in particular the spread of disinformation, manipulation of public opinion, digital fraud, discrediting individuals and interference in electoral processes, etc. Special attention is paid to international approaches to regulating deepfake, in particular the provisions of the Artificial Intelligence Act of the European Union, which provides for the mandatory labeling of synthetic content and the use of technical means of its identification.

The study found that the national legislation of Ukraine does not contain special legal regulation of deepfake technologies, which creates gaps in the area of bringing to justice for their improper use. The need to form a comprehensive legal mechanism of regulation that combines regulatory, organizational and technical tools to combat disinformation is substantiated.

The importance of the information level of protection is especially emphasized, which includes the development of media literacy of the population and the creation of systems for the prompt detection and refutation of fake content. The proposed approaches are aimed at increasing the stability of the information space and reducing the risks of the manipulative influence of deepfake technologies. In times of war, such measures take on particular importance, as deepfake content can be used as a tool of informational and psychological influence aimed at destabilizing society, spreading panic, discrediting state institutions, and undermining trust in official sources of information.

Keywords: disinformation, deepfake, synthetic content, national security, digital security, legal dimension, artificial intelligence, AI Act, media literacy, digital technologies.

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Постановка проблеми. Розвиток штучного інтелекту (далі – ШІ) та цифрових засобів обробки аудіо- та відеоконтенту зумовив появу та швидке поширення deepfake-технологій, які дозволяють створювати високої якості зображення, відео- чи аудіоматеріали, котрі важко відрізнити від справжніх. Сфера застосування цих технологій з кожним днем невпинно розширюється не тільки у сфері медіа та розваг, а й у політичній, інформаційній та комунікаційній діяльності. Неконтрольоване поширення deepfake-контенту ускладнює забезпечення ефективного захисту інформаційного простору та перешкоджає притягненню винних осіб до юридичної відповідальності.

Вагомого значення окреслена проблема набуває в умовах цифровізації суспільства та гібридних інформаційних загроз, коли deepfake-технології можуть використовуватися для дезінформації, перекручування громадської думки, дискредитації осіб, втручання у виборчі процеси, шахрайства та поширення неправдивої інформації.

Незважаючи на активний розвиток міжнародних підходів до правового регулювання ШІ, в законодавстві України питання правового статусу deepfake-технологій, меж їх допустимого використання та механізмів протидії зловживаннями залишаються не в повній мірі врегульованими. Як наслідок, виникає необхідність комплексного наукового дослідження проблем правового регулювання deepfake-технологій та визначення ефективних правових механізмів забезпечення інформаційної безпеки в умовах сучасних цифрових викликів.

Аналіз останніх досліджень і публікацій. Правове регулювання ШІ, deepfake-технологій та протидії дезінформації активно досліджуються сучасними науковцями. У працях О.В. Козлової [1], С.С. Драбюк [2], Ю.Б. Ірхи [3], О.В. Турути та О.П. Турути [4] розглядаються проблеми використання ШІ, інформаційних маніпуляцій, цифрових загроз і впливу цифрових технологій на права людини й суспільну свідомість. Питання інформаційної безпеки, дезінформації та гібридних загроз досліджуються А.П. Крапом [5], С.М.

 ISSN: 3041-2110

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Грищенко [6], М.О. Шевчук [7], А.А. Завадським [8], П.М. Присяжним [9] та Л.І. Братах [10], які зосереджують увагу на необхідності розвитку механізмів фактчекінгу та захисту інформаційного простору. Безпосередньо проблеми deepfake-технологій та їх впливу на комунікації, інформаційну безпеку й інформаційну боротьбу аналізуються в працях Л.І. Братах [10], Т.В. Іванової, О.В. Єфремової, А.І. Чулкова [11], Н.П. Литвиненко та М.І. Атаманчука [12]. Дослідники А.А. Муровицький [13], О.Г. Череп разом із С.В. Марковим та А.А. Лещенком [14] приділяли увагу дослідженню використання deepfake як інструменту дезінформації та інформаційної війни.

Незважаючи на значну кількість наукових праць, питання комплексного правового регулювання deepfake-технологій в Україні, визначення їх правового статусу та механізмів юридичної відповідальності за неправомірне використання залишаються недостатньо дослідженими, а відтак – потребують додаткового опрацювання.

Виділення невирішених раніше частин загальної проблеми. Незважаючи на посилену увагу науковців до проблем правового регулювання ШІ, кібербезпеки та захисту інформації, питання правового врегулювання deepfake-технологій залишаються недостатньо дослідженими і потребують подальшого комплексного аналізу. Низка наукових праць насамперед зосереджується на загальних аспектах функціонування технологій ШІ, проблемах цифровізації суспільства та інформаційних загрозах, однак недостатньо уваги приділяється саме особливостям правового статусу deepfake-контенту та механізмам юридичної відповідальності за його неправомірне використання.

Окрім того, потребують уваги питання визначення поняття deepfake-технологій у правовому полі, їх класифікація та співвідношення з інформаційними правопорушеннями. Наукового опрацювання потребують також проблеми встановлення меж допустимого використання deepfake, захисту персональних даних, честі, гідності та ділової репутації особи в

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

умовах поширення викривленої цифрової інформації. Окремої уваги потребує дослідження впливу deepfake-технологій на стан інформаційної безпеки держави, зокрема в період інформаційної війни, поширення дезінформації та гібридних загроз.

Разом з тим, у вітчизняному законодавстві відсутній цілісний механізм правового регулювання створення, використання й поширення deepfake-контенту, що ускладнює процес виявлення правопорушень та притягнення винних до відповідальності. Потребують додаткового опрацювання питання імплементації міжнародного досвіду правового регулювання ШІ та адаптації міжнародних правових механізмів до національної системи забезпечення інформаційної безпеки України.

Мета статті полягає в комплексному дослідженні особливостей правового регулювання deepfake-технологій та у визначенні їх впливу на стан інформаційної безпеки та обґрунтування необхідності вдосконалення механізмів правового забезпечення протидії загрозам, пов'язаним із використанням deepfake-контенту. Для досягнення визначеної мети необхідно розкрити низку ключових **завдань**, а саме:

- провести аналіз особливостей deepfake-технологій як сучасного цифрового явища і джерела загроз інформаційній безпеці;
- дослідити сучасний стан національного та міжнародного правового регулювання використання deepfake-технологій;
- визначити основні напрями вдосконалення правових механізмів протидії неправомірному використанню deepfake-контенту в умовах цифровізації суспільства.

Виклад основного матеріалу дослідження. Сучасний розвиток суспільства відзначається стрімкою цифровізацією всіх сфер суспільного життя, активним впровадженням інформаційних технологій та широким використанням систем штучного інтелекту. Інноваційні технології впливають на процеси комунікації, обробки інформації, функціонування державних

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

інституцій та забезпечення суспільних потреб людини. Розвиток технологій ШІ зумовлює виникнення нових викликів та загроз, пов'язаних насамперед із використанням цифрових засобів впливу на інформаційний простір.

Deepfake – це технологія, що використовує ШІ для створення реалістичних фальшивих зображень та відео. Для цього використовуються нейронні мережі, зокрема генеративно-змагальні мережі (GAN). Deepfake-технології можуть мати як позитивні так і негативні аспекти (таблиця 1):

Таблиця 1

Напрями застосування deepfake-технологій та їх функціональні можливості

№ п/п	Сфера застосування	Можливості використання deepfake-технологій
1	Розваги та кіноіндустрія	Використання штучних технологій для створення реалістичних візуальних ефектів, відновлення образів акторів, дублювання голосів та вдосконалення кінематографічного контенту
2	Маркетинг та реклама	Створення персоналізованих рекламних кампаній, інтерактивного контенту та цифрових образів відомих осіб для просування продукції чи популяризації послуг
3	Освіта та професійні тренінги	Формування інтерактивних навчальних методів, відео, цифрового контенту, навчального матеріалу із використанням ШІ
4	Соціальні мережі	Створення відеоповідомлень, цифрових аватарів, засобів візуальної комунікації з використанням голосу та зовнішності користувача
5	Мистецтво і творчість	Розроблення нових форм цифрового мистецтва, інтерактивних проєктів, творчого контенту із застосуванням технологій ШІ
6	Медицина	Використання ШІ для відновлення мовлення пацієнта, створення навчальних матеріалів для медичних працівників тощо

Джерело: укладено авторами

Застосування deepfake-технологій характеризується значними ризиками для інформаційної безпеки, прав і свобод людини. Такі технології часто використовуються для поширення дезінформації, цифрового шахрайства, характеризуються порушенням прав на приватність, дискредитацію осіб та спотворення громадської думки. Щоб цього уникнути, необхідно формувати ефективні правові механізми регулювання deepfake-технологій та впроваджувати засоби протидії, щоб зменшити їх неправомірне застосування

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

[1, с. 45]. На думку С.С. Драбюк, поряд із перевагами розширення інформаційних потоків зростають і ризики, найперше пов'язані із маніпуляцією суспільною свідомістю через застосування таких інструментів як пропаганда, дезінформація, фейкові повідомлення, стереотипи та упередження [2].

Вчений Ю.Б. Ірха зазначає, що на відміну від людини ШІ здатний обробляти величезні масиви інформації за короткі проміжки часу. Однак швидкий розвиток технологій ШІ потребує пильної уваги у питаннях безпеки, надійності і прозорості, етики та рівності. Вказані проблеми несуть ризики для основних прав людини, особливо коли неможливо передбачити наслідки застосовування такої нової технології [3, с. 100].

Вчені О.В. Турута та О.П. Турута зазначають, що швидкий розвиток технологій ШІ шкодить людині набагато більше, ніж технології, які з'явилися раніше. Проникаючи у повсякденне життя, схильність ШІ до порушення прав людини стає дедалі серйознішою. Головною проблемою розвитку ШІ є недостатній рівень ефективності правових, інституційних та програмно-технічних механізмів контролю за їх створенням, функціонуванням та поширенням. Окреслена ситуація зумовлена тим, що темпи розвитку сучасних цифрових технологій значно випереджають можливості державних інституцій та суспільства щодо своєчасного формування належних механізмів правового регулювання й реагування на новітні технологічні виклики. Додатковими причинами цього процесу є складність архітектури й непрозорість функціонування багатьох систем ШІ. Значна частина сучасних нейромереж функціонує за принципом так званої «чорної скриньки», коли алгоритми прийняття рішень залишаються недостатньо зрозумілими не лише для користувачів, а й для самих розробників. Як наслідок, виникають труднощі, пов'язані з визначенням механізмів відповідальності, забезпеченням контролю за діяльністю таких систем та оцінкою правових наслідків їх використання [4, с. 51].

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Сучасні технології здатні впливати на поведінку та свідомість людини, формуючи інформаційну залежність, здійснюючи психологічний та дезінформаційний вплив, створюючи ризики втручання у права і свободи громадян. Використання ШІ у цифровому середовищі сприяє розширенню можливостей збору та аналізу персональних даних, підсиленню контролю за поведінкою користувачів та прийняттю автоматизованих рішень, механізми яких часто залишаються непрозорими [5].

Технології ШІ здатні розмивати межу між достовірною інформацією та цифровими фальсифікаціями, негативно впливаючи на рівень суспільної довіри до інформаційного простору. Негативні наслідки ШІ можуть виникати як на основі автономного функціонування алгоритмів, так і в результаті їх навмисного використання розробниками, операторами чи іншими суб'єктами з протиправною метою. Подальший розвиток технологій ШІ зумовлює появу нових викликів, пов'язаних насамперед із можливим виходом окремих систем за межі первинно визначених алгоритмів та моделей функціонування. Як наслідок, це створює ризики формування непередбачуваних механізмів прийняття рішень, здатних впливати на суспільні процеси, інформаційну безпеку та розвиток сучасного суспільства в цілому [4, с. 54].

Безперечно, засоби пропаганди, залякування та спотворення інформації є реальною загрозою для сучасного суспільства. Одним із найнебезпечніших інструментів поширення недостовірної інформації та цифрових фальсифікацій є технологія deepfake. Вказана технологія здатна створювати надзвичайно реалістичний аудіо- та відеоконтент, імітує зовнішність, міміку, голос людини, створює матеріали, у яких особа нібито виголошує заяви або вчиняє дії, які фактично не мали місця. Це значно підвищує ризики поширення дезінформації, введення суспільства в оману, використання цифрового контенту з маніпулятивною метою [6, с. 126].

Технологія deepfake створює цифровий контент, який реалістично відтворює дії, мову, зовнішній вигляд людини. Сучасні алгоритми здатні

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

генерувати зображення та відеоматеріали, використовуючи для цього вигадані образи людей, яких не існує насправді. Висока якість цього контенту ускладнює процес розпізнання цифрових фальсифікацій, тим самим підвищуючи ризик поширення дезінформації.

Як зазначалося раніше, технологічною основою більшості deepfake-технологій є генеративно-змагальні мережі (GAN), головна мета яких полягає у створенні контенту, максимально наближеного до реального. Використання таких алгоритмів вплинуло на підвищення якості реалістичності та доступності deepfake-технологій серед широкого кола користувачів. Додатковою небезпекою є поєднання deepfake із розвитком так званої моделі «злочинність як послуга», що сприяє поширенню інструментів цифрового шахрайства та кіберзлочинності. У зв'язку з цим актуалізується необхідність вдосконалення механізмів правового регулювання та протидії неправомірному використанню deepfake-контенту [7, с. 162].

Нині в суспільстві все більш поширеним стає використання deepfake-технологій як інструментів вчинення різних видів протиправної діяльності, в першу чергу створюючи загрози для інформаційної безпеки, прав людини та суспільства. Їх застосування насамперед пов'язано із ризиками цифрового переслідування, приниженням честі та гідності особи в мережі Інтернет, також використання сфальсифікованого контенту для шантажу, здирництва та інших форм шахрайства. Особливою небезпекою використання deepfake-контенту є підробка документів, цифрової ідентифікації особи та обходу механізмів верифікації користувачів. Визначені технології можуть застосовуватися з метою поширення незаконного контенту та інших форм цифрової експлуатації. Значним ризиком є також використання deepfake-технологій для фальсифікації чи викривлення достовірності цифрової інформації, що створює серйозну загрозу для забезпечення об'єктивності судового розгляду. Небезпечним є вплив deepfake на суспільно-політичні процеси. Так, поширення сфальсифікованих аудіо- та відеоматеріалів може використовуватися як

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

дезінформаційний вплив на громадську думку, дестабілізацію суспільних відносин, посилення політичної поляризації й формування соціальної напруги. Такі технології можуть підірвати довіру до державних інституцій, політикуму чи ЗМІ [8].

Безперечно, шкода від deepfake для інформаційної безпеки досить значна, оскільки багато людей можуть сприйняти відео, зняте із використанням цієї технології, як оригінальне, навіть якщо це просто пародія. Невідповідне позначення чи відсутність попереджень може дезінформувати аудиторію та призвести до маніпулятивних дій з громадською думкою, нівелюючи таким чином політичну та суспільну довіру.

Для сучасного суспільства deepfake це, насамперед, виклик, який потребує негайного втручання. У США боротьба з deepfake ведеться як на федеральному рівні, так і на рівні окремих штатів. У рамках боротьби із deepfake прийнято закони, які забороняють розповсюджувати сфабрикований аудіо- та відеоконтент про кандидата протягом 60 днів до виборів без чіткого розкриття. В ЄС головним актом, який регулює функціонування системи ШІ, є Artificial Intelligence Act (далі – AI Act) [9, с.258].

Вказаний нормативно-правовий акт встановлює нові правила для поширення deepfake, які визначаються як згенерований або змінений штучним інтелектом контент, який не відрізнити від справжнього. AI Act встановлює вимоги щодо обов'язкового маркування deepfake-контенту та інших матеріалів, створених з допомогою ШІ. Провайдери системи ШІ мають забезпечувати позначення такого контенту у машино-зчитуваному форматі, а користувачі – чітко інформувати про його штучне створення. Головна мета цих вимог – забезпечення прозорості інформаційного середовища, протидія дезінформації, захист громадян від введення в оману. Для ідентифікації штучно створеного контенту AI Act передбачає використання технічних засобів підтвердження автентичності, зокрема й за допомогою цифрових водяних знаків, метаданих, інших технологічних механізмів. Разом з тим AI

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Act передбачає розробку кодексів поведінки та механізмів контролю за дотриманням встановлених вимог, спрямованих насамперед на підсилення рівня довіри до цифрового інформаційного поля та мінімізацію ризиків неправомірного використання deepfake-технологій [10].

Розроблені з метою розвитку цифрової творчості та імітації реалістичного відео, аудіо та зображень, deepfake-технології несуть суттєву загрозу для споживачів інформації на різних рівнях. Використання цих технологій створює ризики поширення дезінформації, введення суспільства в оману та викривлення сприйняття реальних подій. Особлива небезпека полягає у можливості застосування deepfake-контенту з метою дискредитації осіб, цифрового шахрайства та інформаційного впливу на громадську думку. За умов стрімкого розвитку цифрових технологій це актуалізує необхідність вдосконалення механізмів правового регулювання й забезпечення належного рівня інформаційної безпеки [11].

Дослідниці Н.П. Литвиненко та М.І. Атаманчук наголошують на тому, що в Україні стрімкий розвиток deepfake-технологій сприяв появі нових інструментів ведення інформаційної війни та здійснення дезінформаційного впливу. Поширення під виглядом реалістичних фальсифікованих відео- й аудіоматеріалів формує значні ризики для міжнародної та національної безпеки, оскільки їх використання може ввести суспільство в оману, дестабілізуючи політичну ситуацію, загострюючи конфлікти та посилюючи суспільні протистояння. Досить небезпечним є також поступове розмивання меж між достовірною інформацією та цифровими можливостями [12].

Вчений А.А. Муровицький зазначає, що дезінформація завжди маскується під правдиву інформацію. Основним методом боротьби є фактчекінг (перевірка фактів) та моніторинг інформаційних джерел з метою виявлення анонімних чи фальшивих повідомлень. Так, у низці європейських країн впроваджено закони, які зобов'язують видаляти неправдиві повідомлення протягом 24 годин після їх виявлення. Це зокрема відбувається

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

в Німеччині, де рівень поширення діпфейків нижчий у порівнянні з іншими європейськими країнами. У Франції уряд наділений повноваженнями самостійного блокування фейкових новин під час виборчих кампаній. Міжнародні організації, такі як Рада Європи та ООН, безперервно працюють над розробленням стандартів із запобігання й поширення дезінформації. Шкода, яку завдає дезінформація суспільству, – колосальна. Це й негативний вплив на економіку та політику, особисте життя громадян тощо. Наразі дезінформація поширюється через соціальні мережі, де вона може миттєво досягати великих аудиторій і викликати наплив реакцій [13].

Отже, опрацьовані матеріали дослідження встановили, що використання deepfake-технологій потрібно врегульовувати на законодавчому рівні. Наразі у вітчизняному просторі законодавство намагається регулювати інформацію, персональні дані, фейки, однак не сам механізм синтетичного відтворення людини. З огляду на це, deepfake фактично створює новий цифровий об’єкт – «синтетичну ідентичність». Важливо наголосити, що deepfake руйнує довіру до відео, електронних (цифрових) доказів, медіа та офіційних звернень представників політикуму і державних органів [14].

Для України неконтрольоване поширення deepfake в умовах війни становить особливу загрозу національній та інформаційній безпеці держави. Використання сфальсифікованого аудіо- та відеоконтенту спрямоване насамперед на дестабілізацію суспільно-політичної ситуації, поширення панічних настроїв серед населення, дискредитацію органів влади та військового керівництва, а також підрив довіри до офіційних джерел інформації. Наразі ефективна протидія поширенню deepfake-технологій неможлива на рівні правового регулювання чи технічних засобів виявлення. Важливим компонентом системи інформаційної безпеки є інформаційний рівень, що охоплює формування критичного мислення населення, підвищення рівня медіаграмотності, забезпечення належного реагування на випадки поширення дезінформації.

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Одним із головних превентивних механізмів протидії deepfake-контенту наразі є медіаграмотність. Загалом медіаграмотність є одним із ключових інструментів підвищення стійкості суспільства до маніпулятивного інформаційного впливу в умовах стрімкого розвитку цифрових технологій. Споживачі медіаконтенту повинні вміти критично оцінювати достовірність відео- та фотоматеріалів, розпізнавати ознаки фальсифікації та перевіряти інформацію.

Окрім того, впровадження системи медіа-освіти у закладах середньої та вищої освіти сприятиме підвищенню цифрової грамотності, інформаційної безпеки, критичного мислення. Такі заходи сприяють формуванню у молоді стійких навичок аналізу інформації, усвідомленню принципів роботи ШІ та ризиків, пов'язаних із deepfake-технологіями. Важливо залучити ЗМІ, громадські організації та державні інституції до реалізації просвітницької діяльності, спрямованої на підвищення рівня обізнаності населення щодо цифрових фальсифікацій. Окреслені заходи сприяють формуванню стійкого інформаційного поля, яке буде менш вразливим до маніпулятивного впливу.

Не менш важливим елементом інформаційного рівня є система оперативного виявлення та спростування дезінформації, яка містить deepfake-контент. Умови інформаційної війни та гібридних загроз потребують максимально-швидкої реакції на появу фальсифікованих матеріалів, оскільки затримка у поширенні або спростуванні офіційної інформації може призвести до значного суспільного резонансу та панічних настроїв. Ефективна система спростування повинна ґрунтуватися на наявності спеціалізованих державних структур, аналітичних центрів та фактчекінгових механізмів, які здійснюють моніторинг інформаційного простору, виявляють потенційні deepfake-матеріали, а також забезпечують їх належну перевірку. У цьому аспекті важливу роль відіграє взаємодія державних органів із соціальними мережами та медіа для швидкого обмеження поширення неправдивого контенту. Також важливо інформувати населення через офіційні канали комунікації. Своєчасне

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

спростування, роз'яснення та інформування здатні зменшити негативний вплив deepfake-контенту на суспільну свідомість та запобігти його подальшому поширенню. Поєднання медіаграмотності з ефективною системою оперативного реагування є важливою складовою комплексного захисту інформаційного простору держави від загроз, пов'язаних із використанням deepfake-технологій.

Висновок. На основі проведеного дослідження здійснено комплексний аналіз правового регулювання deepfake-технологій та їх впливу на стан інформаційної безпеки в умовах цифровізації суспільства, що дозволило зробити такі висновки. Deepfake є сучасним інформаційним інструментом, що поєднує в собі технологічні можливості ШІ та маніпулятивні впливи на суспільну свідомість. Наразі вітчизняне законодавство не містить спеціального регулювання deepfake-контенту, що створює правові прогалини в процесі його ідентифікації або притягнення до відповідальності. Проаналізований міжнародний досвід, зокрема положення AI Act Європейського Союзу, свідчить про формування ефективних механізмів забезпечення прозорості цифрового інформаційного середовища.

На основі дослідженого матеріалу обґрунтовано необхідність вдосконалення національного законодавства шляхом впровадження правових, організаційних та технічних механізмів протидії дезінформації. У рамках цього запропоновано основні напрями підвищення ефективності інформаційної безпеки, які включають розвиток експертизи цифрового контенту, правове закріплення відповідальності та підвищення медіаграмотності населення. Отримані результати можуть використовуватися для подальшого вдосконалення правової політики України у сфері регулювання технологій ШІ.

ISSN: 3041-2110
Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

Список використаних джерел

1. Козлова О. В. Протидія дезінформації у маркетингових комунікаціях в умовах інформаційної війни. *Маркетинг і менеджмент інновацій*. 2022. № 3. С. 45–52. URL: https://mmi.fem.sumdu.edu.ua/article/view/2022_3_kozlova

2. Драбюк С.С. Штучний інтелект і пропаганда та дезінформація: основні виклики. *Науковий вісник Ужгородського Національного Університету*. 2025. Випуск 90, частина 5. С. 348-356. https://visnyk-pravo.uzhnu.edu.ua/article/view/341116/329128

3. Ірха Ю.Б. Загрози правам і свободам людини в епоху штучного інтелекту. *Інформація і право*. 2025. № 4(55). С. 95-109. DOI: https://doi.org/10.37750/2616-6798.2025.4(55).346356

4. Турута О. В., Турута О. П. Штучний інтелект крізь призму фундаментальних прав людини. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2022. № 71. С. 49-54. DOI: https://doi.org/10.24144/2307-3322.2022.71.7

5. Крап А.П. Дезінформація як загроза демократії та державному управлінню. *Український політико-правовий дискурс*. 2025. № 9. URL: https://zenodo.org/records/15108404

6. Грищенко С.М. Правове регулювання кібербезпеки в умовах цифрової трансформації суспільства. *Інформація і право*. Випуск 3(54). 2025. С. 122-130. DOI: https://doi.org/10.37750/2616-6798.2025.3(54).340519

7. Шевчук М.О. Сучасні виклики і загрози в сфері інформаційної безпеки держави. *Актуальні проблеми вітчизняної юриспруденції*. 2024. № 6. С. 160–166. URL: http://www.apnl.dnu.in.ua/6_2024/6_2024.pdf#page=160.

8. Завадський А.А. До питання правового регулювання штучного інтелекту для глибокого синтезу контенту та діпфейків: європейський досвід та перспективи його застосування в Україні. *ХНПУ імені Г.С. Сковороди*. 2023.

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license

https://dspace.hnpu.edu.ua/server/api/core/bitstreams/777a2872-e106-457e-9387-a3f073cd00ff/content

9. Присяжний П.М. Правове регулювання використання штучного інтелекту: виклики для України в контексті імплементації AI ACT ЄС. *Вісник Львівського університету*. 2026. Серія Журналістика. Випуск 59. С. 252-261. https://publications.lnu.edu.ua/bulletins/index.php/journalism/article/download/13964/14488

10. Братах Л.І. Інформаційна безпека України в умовах дезінформаційного впливу: загрози, виклики, механізми реагування. *Вісник Прикарпатського університету. Серія: Політологія.* 2025. Випуск 21. DOI: https://doi.org/10.32782/2312-1815/2025-21-6

11. Іванова Т.В., Єфремова О.В., Чулков А.І. Deepfake як технологія сфери соціальних та масових комунікацій: можливості та загрози. *Наукові записки Інституту журналістики*. 2025. Випуск 86, № 1. С. 21-34. URL: https://nz.knu.ua/uk/article/view/3617/3327

12. Литвиненко Н.П., Атаманчук М.І. Діпфейки як інструмент інформаційного протиборства сучасних держав. *Збірник матеріалів конференції – 2024.* С. 133- 136. URL: https://jppasa.donnu.edu.ua/article/view/15732

13. Муровицький А.А. Дезінформація та методи боротьби з нею. *Матеріали II науково-практичної конференції «Формування сучасного наукового простору: теорія і практика» (25-26 жовтня* 2024.). Ужгород; Одеса: Молодий вчений, 2024. С. 58-60. URL: https://molodyivchenyi.ua/omp/index.php/conference/catalog/download/118/1680/3500-1?inline=1

14. Череп О.Г., Маркова С.В., Лещенко А.А. Штучний інтелект у протидії дезінформації у системі маркетингового менеджменту в умовах війни та відновлення економіки України. *Підприємництво та інновації.* Випуск 37. 2025. DOI: https://doi.org/10.32782/2415-3583/37.4

Увесь контент ліцензовано за умовами Creative Commons BY 4.0 International license