МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНА КОНФЕРЕНЦІЯ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

(ATICE'2025)

ОДЕСА, УКРАЇНА, 18 ЛИПНЯ 2025 Р.

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

ОДЕСА

2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

INTERNATIONAL HUMANITARIAN UNIVERSITY

INTERNATIONAL CONFERENCE

ADVANCED TECHNOLOGY IN INFORMATION AND COMMUNICATION ENGINEERING

(ATICE'2025)

ODESA, UKRAINE, JULY 18, 2025

CONFERENCE PROCEEDINGS

ODESA

2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ПЕРЕДОВІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ ІНЖЕНЕРІЇ

МАТЕРІАЛИ КОНФЕРЕНЦІЇ

Одеса, Україна, 18 липня 2025 р.

Видавничий дім
«Гельветика»
2025

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
INTERNATIONAL HUMANITARIAN UNIVERSITY

International Conference "Advanced Technology in Information and Communication Engineering" (ATICE'2025)

Odesa, Ukraine, July 18, 2025

Conference Proceedings

Видавничий дім
«Гельветика»
2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ПТІКІ'2025)

Одеса, Україна, 18 липня 2025 р.

Матеріали конференції

Видавничий дім
«Гельветика»
2025

International Conference “Advanced Technology in Information and Communication Engineering” (ATICE’2025): Conference Proceedings. Odesa : International humanitarian university, 2025, 123 p.

DOI:

Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2025): Матеріали конференції. Міжнародний гуманітарний університет, 2025. – Одеса: Видавничий дім «Гельветика», 2025. – 123 с.

ISBN 978-617-554-582-9

Збірка містить праці Міжнародної конференції з інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова

КІВАЛОВ С.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

Співголови

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

Члени організаційного комітету

БЕРКМАН Л.Н. – д.т.н., проф., Державний університет телекомунікацій, м.Київ, Україна.

КЛИМАШ М.М. – д.т.н., проф., Національний університет «Львівська політехніка», м.Львів, Україна.

ЛЕМЕШКО А. В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.

РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

РИХЛІК А. – к.т.н., Лодзький технічний університет, м.Лодзь, Польща

СЕМЕНКО А.І. – д.т.н., проф ., Національний авіаційний університет, Київ, Україна.

СІМЕНС Е. – д.т.н., проф., Анхальтський університет прикладних наук, м.Кетен, Німеччина.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СУНДУЧКОВ К.С. – д.т.н., проф., Національний авіаційний університет, м. Київ, Україна.

РЕДАКЦІЙНИЙ КОМІТЕТ

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

РОЗЕНВАССЕР Д.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

КОМІТЕТ МІЖНАРОДНИХ ЗВ'ЯЗКІВ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГЛОБА Л. С . – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ВЧЕНИЙ СЕКРЕТАР

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

ТЕХНІЧНО-ПРОГРАМНИЙ КОМІТЕТ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

СЕКЦІЇ

СЕКЦІЯ 1. ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

СТРЕЛКОВСЬКА І.В. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

ГЛОБА Л.С. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ГРИГОР'ЄВА Т.І. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 2. КОМП'ЮТЕРНІ НАУКИ ТА КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

МІРОШНИК М.А. – д.т.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СОЛОВСЬКА І.М. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

РУСУ О.П. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 3. КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

ЛУНТОВСЬКИЙ А.О. – д.т.н., проф., Державна академія Саксонії «Беруфсакадемія», м. Дрезден, Німеччина.

ЙОНА Л.Г. – к.т.н., доц., Міжнародний гуманітарний університет, Одеса, Україна.

МАНЬКО Д.Г. – д.ю.н., проф., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 4. ЕЛЕКТРОННІ КОМУНІКАЦІЇ ТА РАДІОТЕХНІКА

УРИВСЬКИЙ Л.О. – д.т.н., проф., Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, Україна.

ЛЕМЕШКО А.В. – д.т.н., проф., Харківський національний університет радіоелектроніки, м. Харків, Україна.

ПЕДЯШ В.В. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

СЕКЦІЯ 5. ІНФОРМАТИКА ТА ПРОГРАМУВАННЯ В ОСВІТІ

КУЧАЙ О.В. - д.п.н., проф., Національний університет біоресурсів і природокористування України.

ЖИГУЛІН О.А. – д.е.н., проф., Міжнародний гуманітарний університет, Одеса, Україна

ГОРБАЧОВ В.Е. – к.т.н., доц., Міжнародний гуманітарний університет, м.Одеса, Україна.

Література

1. Гришко, С.М. Інформаційна безпека та захист інформації: Навчальний посібник. Київ: Видавничий дім «Кондор», 2020.

2. Лаптєв, В.М., Євдокименко, В.К., Рибалко, О.Ю. Комплексний підхід до захисту інформації: Підручник. Харків: ХНУРЕ, 2018.

3. Шахов, В.В. Основи кібербезпеки. Київ: Академія, 2019

4. Bishop, M. Computer Security: Art and Science. Boston: Addison-Wesley, 2003.

5. Stallings, W. Cryptography and Network Security: Principles and Practice. 7th edition. Upper Saddle River: Pearson, 2017.

6. Alpaydin, E. Introduction to Machine Learning. 4th edition. Cambridge: MIT Press, 2020.

7. Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd edition. New York: Wiley, 2020.

Димов Максим Віталійович
Студент факультету Кібербезпеки, програмної інженерії та комп'ютерних наук,
Спеціальність: 125 Кібербезпека
Міжнародний гуманітарний університет
mak.dymov@gmail.com
Керівник: к.т.н.,доцент Йона Лариса Григорівна,
yonalarisa66@gmail.com

РИЗИКИ ДЛЯ БЕЗПЕКИ В ЦИФРОВОМУ ПРОСТОРІ

Анотація. Досліджуються сучасні ризики кібербезпеки, пов'язані з використанням штучного інтелекту для створення фішингового контенту. Проаналізовано класифікацію AI-підсилених атак, методи генерації синтетичного контенту та їх застосування в дезінформаційних кампаніях. Запропоновано підходи до виявлення та протидії таким загрозам в умовах гібридних конфліктів.

Ключові слова: кібербезпека, штучний інтелект, фішинг, синтетичний контент, дезінформація, цифрові загрози.

Сучасне цифрове середовище характеризується швидким зростанням технологій розумних комп'ютерів що відкриває нові шанси як для розвитку суспільства так і для зловмисних осіб. Використання AI-технологій для створення підробленого контенту стала однією з найбільших загроз безпеки Інтернету у останніх роках [1]. Звичайні способи обману урізноманітнилися від простих текстових повідомлень та до складних мультимедійний атак із використанням deepfake-технології, AI-створеними картинками та фальшивими текстами.

Актуальність роботи пов'язана із зростанням кількості кібер-інцидентів з використанням контенту, який було створено AI, особливо під час змішаних конфліктів та боїв за інформацію [2]. По даним аналізу цифр, більше 75% організацій зустрічали нові типи фішингових атак, що використовують елементи штучного уміння для покращення соціальної інженерії.

Дослідження показує, що атаки на основі штучного інтелекту можна розділити на три головні групи згідно з типом контенту:

Перша група включає створення підроблених профілів та особистостей, де злочинці використовують мережі для генерування синтетичних фотографій, які важко відрізнити від справжніх. Такі картинки застосовуються для формування довірчих профілів у соцмережах, що дозволяє злочинцям налагоджувати зв'язки з можливими жертвами. У той же час автоматично створюються біографії і дані про осіб, яких використовують для створення фальшивих акаунтів у соціальних медіа, а також формування ботнетів.

Друга група говорить про фальшування паперів та офіційних матеріалів. Сучасні AI-програми дають змогу робити дуже хороші копії документів посвідчення особи, банківських і фінансових документів, а також офіційних листів від держави. Технічна майстерність таких підробок досягла така рівня, що візуальне впізнавання стає практично неможливим без спеціальних засобів для знаходження їх.

Третя група є найнебезпечнішою, до якої потрапляють маніпуляції з медіа-контентом голов. Технології Deepfake дають змогу виготовляти відео, на яких керівники фірм або чиновники віддають накази про переведення грошей або передачу секретної інформації [3]. Такі удари дуже дієві у випадках BEC-ударів , оскільки використовують довіру робітників до глави.

Практичні приклади AI-підсилених атак

1. **Приклад 1: Корпоративне шахрайство з використанням deepfake**

   У 2019 році британська енергетична компанія стала жертвою атаки з використанням AI-синтезованого голосу. Зловмисники створили голосову імітацію керівника німецької материнської компанії та переконали співробітника перевести 220 000 євро на рахунок в Угорщині. Атака була настільки переконливою, що жертва впізнала характерний німецький акцент та інтонації свого босса.

2. **Приклад 2: Дезінформаційна кампанія під час виборів**

   У 2020 році під час виборчих кампаній у кількох країнах було виявлено мережу фейкових акаунтів, що використовували AI-генеровані фотографії профілів. Більше 15 000 синтетичних облич були створені для поширення політичної дезінформації. Ці акаунти діяли координовано, поширюючи однакові меседжі в різних соціальних мережах.

3. **Приклад 3: Маніпуляції в фінансовій сфері**

   У 2021 році зафіксовано випадок використання deepfake-технологій для створення фальшивих відео-інтерв'ю з CEO фінансової компанії. Відео використовувалося для маніпуляцій на фондовому ринку, призвівши до короткострокового, але суттєвого коливання курсу акцій компанії.

Слід звернути увагу на дослідження використання AI-створеного контенту в дезінформаційних кампаніях під час гібридних конфліктів. Дослідження показує, що коли є військовий стан, зростає використання штучного контенту для впливу на думку людей. Зловмисники роблять фейкові фото з місць подій, вигадують неіснуючих свідків і експертів а також створюють документи та неправдиві джерела інформації. Це веде до появи альтернативної реальності, яка може дуже вплинути на прийняття важливих рішень як у індивідуальному так і у державному рівнях.

Підрив довіри до офіційних джерел інформації відбувається через створення фальшивих відео з словами політиків, підробок офіційних новин і документів, а також вигадки неправдивих новин. Скоординовані атаки за допомогою інформації використовують

сітки синтетичних акаунтів для автоматичної генерації дезінформаційного контенту та їх цілеспрямованої подачі різним групам в залежності від психології користувачів.

Для боротьби з загрозами, що посилені штучним інтелектом, потрібен комплексний підхід який поєднує технічні та організаційні заходи. Технічні способи виявлення базуються на аналізі цифрових об'єктів у синтетичних малюнках, знаходженні несумісностей метаданих файлів та застосуванні алгоритмів машинного навчання для детекції фейків [4]. Важливим елемент є аналіз поведінки підозрілих акаунтів що дозволяє знаходити координовані мережі для поширення дезінформації.

Організаційні заходи включають підвищення рівня кіберграмотності користувачів, впровадження багаторівневої верифікації важливих рішень і розробку протоколів реагування на підозрілий контент. Створення систем швидкого обміну інформацією про нові загрози між організаціями дозволяє оперативно реагувати виникнення нових типів атак.

Освітній компонент протидії включає навчання розпізнаванню ознак синтетичного контенту, підвищення критичного мислення при оцінці інформації та популяризацію методів верифікації джерел інформації. Це особливо важливо за умов інформаційних війн, коли швидкість поширення дезінформації може значно перевищувати можливості її спростування.

Висновки

Проведене дослідження показує, що використання штучного інтелекту в кіберзлочинності представляє якісно новий рівень загроз для безпеки цифрового простору. Запропонована класифікація AI-фішингових атак дозволяє систематизувати сучасні загрози та розробити цільові методи протидії.

В умовах гібридних конфліктів AI-генерований контент стає потужним інструментом дезінформаційних кампаній, що потребує розробки спеціалізованих методів виявлення та нейтралізації. Ефективна протидія можлива лише за комплексного підходу, що поєднує технічні рішення, організаційні заходи та підвищення рівня цифрової грамотності населення.

Література

1. Chesney R., Citron D. Deep fakes: a looming challenge for privacy, democracy, and national security // California Law Review. 2019. Vol. 107. P. 1753-1820. [Електронний ресурс]. – Режим доступу: https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security/ (дата звернення: 06.07.2025).

2. Kietzmann J., Lee L. W., McCarthy I. P., Kietzmann T. C. Deepfakes: Trick or treat? // Business Horizons. 2020. Vol. 63, № 2. P. 135-146. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/338144721_Deepfakes_Trick_or_treat (дата звернення: 06.07.2025).

3. Vaccari C., Chadwick A. Deepfakes and disinformation: exploring the impact of synthetic political video on deception, uncertainty, and trust in news // Social Media + Society. 2020. Vol. 6, № 1. [Електронний ресурс]. – Режим доступу: https://journals.sagepub.com/doi/full/10.1177/2056305120903408 (дата звернення: 06.07.2025).

4. Wang S. Y., Wang O., Zhang R., Owens A., Efros A. A. CNN-generated images are surprisingly easy to spot... for now // Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2020. P. 8692-8701. [Електронний ресурс]. – Режим доступу: https://openaccess.thecvf.com/content_CVPR_2020/papers/Wang_CNN-Generated_Images_Are_Surprisingly_Easy_to_Spot..._for_Now_CVPR_2020_paper.pdf (дата звернення: 06.07.2025).