

Міністерство освіти і науки України
Український державний університет залізничного транспорту



МАТЕРІАЛИ

двадцять другої науково-практичної міжнародної конференції
*«Міжнародна транспортна інфраструктура,
індустріальні центри та корпоративна логістика»*

(4-5 червня 2026 р. м. Харків, Україна)



MT.KART.EDU.UA

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МІНІСТЕРСТВО РОЗВИТКУ ГРОМАД ТА ТЕРИТОРІЙ УКРАЇНИ
ТРАНСПОРТНА АКАДЕМІЯ УКРАЇНИ
АТ «УКРАЇНСЬКА ЗАЛІЗНИЦЯ»
CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS (FRANCE)
INSTITUTE OF AUTOMATIC CONTROL TELEMATICS OF
TRANSPORT (POLAND)
УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ЗАЛІЗНИЧНОГО
ТРАНСПОРТУ
ІНСТИТУТ ЕКОНОМІКИ ПРОМИСЛОВОСТІ НАН УКРАЇНИ

Матеріали

*Двадцять другої науково-практичної
міжнародної конференції*

**«МІЖНАРОДНА ТРАНСПОРТНА
ІНФРАСТРУКТУРА,
ІНДУСТРІАЛЬНІ ЦЕНТРИ ТА
КОРПОРАТИВНА ЛОГІСТИКА»**

(4 – 5 червня 2026 р., м. Харків)

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова: *Панченко С. В.*, д.т.н., проф., ректор Українського державного університету залізничного транспорту (Харків).

Заступники голови: *Каграманян А. О.*, к.т.н., доц., проректор з науково-педагогічної роботи Українського державного університету залізничного транспорту (Харків);
Дикань В. Л., д.е.н., проф., завідувач кафедри економіки та управління виробничим і комерційним бізнесом Українського державного університету залізничного транспорту (Харків).

Секретаріат:

Толстова А. В. к.е.н., доц., доцент кафедри економіки та управління виробничим і комерційним бізнесом Українського державного університету залізничного транспорту (Харків);

Шаповал Г. В. к.т.н., доц., заступник декана з денної форми навчання факультету управління процесами перевезень Українського державного університету залізничного транспорту (Харків);

Примаченко Г. О. к.т.н., доц., доцент кафедри транспортних систем та логістики Українського державного університету залізничного транспорту (Харків).

[3] IMO Resolution MSC.232(82). Adoption of the Revised Performance Standards for Electronic Chart Display and Information Systems (ECDIS). International Maritime Organization, 2006. Adopted on 5 December 2006.

[4] OpenStreetMap contributors. OpenStreetMap geographic data. OpenStreetMap Foundation, ODbL 1.0. Accessed: 30 May 2026.

[5] Bowditch, N. The American Practical Navigator. National Geospatial-Intelligence Agency, Pub. No. 9, 2019 edition.

УДК 004.056.5

DEERFAKE ЯК ІНСТРУМЕНТ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ В СУЧАСНИХ КІБЕРАТАКАХ

DEERFAKES AS A SOCIAL ENGINEERING TOOL IN MODERN CYBERATTACKS

А. Онтіверо-Валлс

Державний університет інтелектуальних технологій і зв'язку (м. Одеса)

А. Ontivero-Valls

State University of Intellectual Technologies and Communications (Odessa)

Стрімкий розвиток інформаційно-комунікаційних технологій, високий рівень відкритості інформаційного простору та активне використання соціальних мереж сприяють швидкому поширенню дезінформації, що створює не лише інформаційні загрози, але й суттєві репутаційні ризики.

Це питання набуває особливої актуальності в умовах розвитку технологій штучного інтелекту, зокрема технологій deepfake, які дають змогу створювати фальшиві аудіо-, відео- та графічні матеріали, які важко відрізнити від справжніх. Поширення такого контенту становить загрозу для репутації організацій, цифрової довіри та інформаційної безпеки, що зумовлює необхідність розвитку медіаграмотності та вдосконалення методів виявлення технологій deepfake.

Технологія deepfake базується на використанні нейронних мереж, зокрема генеративно-змагальних мережах (GAN). Генеративно-змагальна мережа складається з двох нейронних мереж – генеруючої та дискримінуючої. Генеруюча мережа створює фальшиві зображення, аудіо або відео матеріали намагаючись їх максимально наблизити до реального контенту, а дискримінуюча мережа, у свою чергу, намагається аналізувати отримані результати та визначає, чи є вони справжніми.

У процесі постійної взаємодії і «змаганнях» між цими мережами якість згенерованого контенту поступово підвищується, що дозволяє створювати високореалістичні deepfake-матеріали, які складно відрізнити від оригіналу.

Про зростаючу серйозність цієї загрози свідчать реальні кіберінциденти. У 2019 році шахраї використали технологію клонування голосу на основі штучного інтелекту, щоб видати себе за керівника компанії, і таким чином успішно змусили співробітника переказати 243 000 доларів США [1]. Перенесімося у 2024 рік, коли сталася ще більш масштабна атака з використанням відеоконференції, створеної за допомогою штучного інтелекту [2]. Під час цього інциденту співробітника компанії Arup обдурили, змусивши переказати приблизно 20 мільйонів фунтів стерлінгів. До 2026 року голоси, створені за допомогою технології deepfake, стали звичним явищем у шахрайських схемах, спрямованих проти окремих осіб, де використовуються емоційний тиск та маніпуляції [3].

Масштабність та небезпечність цієї нової тенденції підтверджуються результатами досліджень, проведених у всьому світі [4, 5]. Встановлено, що використання штучного інтелекту значно підвищує ефективність фішингових атак: у 54 % випадків користувачі переходять за шкідливими посиланнями, якщо текст був адаптований нейронними мережами відповідно до їхніх особистих інтересів. Наразі 62 % підприємств у всьому світі повідомляють про кібератаки, в яких використовується технологія «дідфейк». Найбільш швидко розвивається сфера аудіошахрайства (зокрема, спрямована на обхід процедур біометричної аутентифікації та верифікації у фінансових установах), де кількість зареєстрованих інцидентів зростає на вражаючі 1300%. Крім того, технічні перешкоди для зловмисників значно зменшилися: сучасні моделі штучного інтелекту потребують лише 3 секунди запису справжнього людського мовлення (який можна отримати, наприклад, із соціальних мереж), щоб створити високоточну голосову копію.

Підсумовуючи результати дослідження та аналізу емпіричних даних, можна з упевненістю стверджувати, що впровадження штучного інтелекту в арсенал засобів соціальної інженерії призвело до критичного зростання кіберзагроз. Наведені статистичні дані свідчать про значну математичну ефективність фішингу на основі штучного інтелекту.

[1] Damiani J. A Voice Deepfake Was Used To Scam A CEO Out Of \$243,000 // Forbes. 2019. URL: <https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/>

[2] Milmo D. UK engineering firm loses £20m in deepfake video call scam // The Guardian. 2024. URL: <https://www.theguardian.com/technology/article/2024/may/17/uk-engineering-arup-deepfake-scam-hong-kong-ai-video>

[3] Deepfake call cheats Roorkee farmer of Rs 6 lakh // The Times of India. 2026. URL: <https://timesofindia.indiatimes.com/city/dehradun/deepfake-call-cheats-roorkee-farmer-of-rs-6-lakh/articleshow/128124805.cms/>

[4] 2025 Data Breach Investigations Report // Verizon. URL: <https://www.verizon.com/business/resources/reports/dbir/>

[5] Voice Intelligence & Security Report // Pindrop. URL: <https://www.pindrop.com/resource-type/report/>

Зміст

Секція «Розвиток індустріальних центрів в умовах глобалізації»

С. В. Панченко Трансформація залізничного транспорту України: логістична стійкість та європейська інтеграція в умовах воєнних викликів	3
В. Л. Дикань Інституційне забезпечення розвитку індустріальних парків в Україні: виклики та перспективи	7
Yu. Prus Cluster approach to ensuring the protection of critical infrastructure objects	10
Л. М. Алексеєнко, О. І. Тулай Вплив управління публічними фінансами на розвиток індустріальних центрів: регіональний та міжнародний виміри	12
Е. Р. Бекіров Туризм як драйвер економічного зростання Дніпровського регіону: шляхи удосконалення	14
К. В. Гарькавенко Фінансові механізми повоєнного відновлення індустріальних центрів України в умовах глобалізації	16
Л. Л. Калініченко Цифрова трансформація промислових екосистем: нові архітектури індустріального розвитку	19
В. В. Коваль, І. М. Гончарова Новітні стандарти розвитку індустріальних парків України як чинник глобальної конкурентоспроможності	21
М. А. Мироненко, Т. І. Лисенко Розвиток індустріального центру в умовах глобальних викликів на прикладі міста Дніпра	23
М. Р. Новіцький Проблематика екологічної безпеки в умовах розвитку індустріальних центрів: системні виклики, технологічні ризики та стратегії модернізації	25

А. Онтіверо-Валлс Deerfake як інструмент соціальної інженерії в сучасних кібератаках	438
Г. Є. Острроверх, Ю. В. Калініченко Цифровізація та автоматизація виробничих процесів у транспортному машинобудуванні в умовах Індустрії 4.0: роль людського капіталу та економічна ефективність	440
В. В. Попкевич, В. А. Волохов Вплив цифрових технологій на логістику вантажних перевезень	443
М. С. Псуй, Я. О. Шаровський Автоматизування управлінських рішень у зовнішньоекономічній діяльності на основі ШІ-алгоритмів	445
А. П. Резнік, Т. М. Бороденко Роль автоматизованої системи аналізу ризиків (АСУР) у мінімізації людського фактора під час митного контролю	447
К. С. Сердюков Попередження кіберзагроз в сучасних організаціях як функція управління: аналіз та критичні складові	449
П. О. Харламов, М. Д. Федик Прогнозне обслуговування як інструмент оптимізації операційних витрат та підвищення безпеки залізничного транспорту	452
В. В. Хрустальова Інформаційні технології на транспорті як ключовий елемент у спрощенні процедур торгівлі за умов глобалізації	454
І. В. Чередько, Є. В. Срібна Інформаційні технології та штучний інтелект у розвитку міжнародної транспортної інфраструктури та корпоративної логістики	456
В. І. Чобіток, І. О. Чобіток Інноваційно-інформаційні технології в управлінні ризиками підприємств критичної інфраструктури в умовах сталого розвитку	458

МАТЕРІАЛИ
ДВАДЦЯТЬ ДРУГОЇ НАУКОВО-ПРАКТИЧНОЇ
МІЖНАРОДНОЇ КОНФЕРЕНЦІЇ
«МІЖНАРОДНА ТРАНСПОРТНА ІНФРАСТРУКТУРА,
ІНДУСТРІАЛЬНІ ЦЕНТРИ ТА КОРПОРАТИВНА ЛОГІСТИКА»

(4 – 5 ЧЕРВНЯ 2026 РОКУ)

Відповідальний за випуск А. В. Толстова

Підписано до друку 12 червня 2026 р.
Формат паперу 60x84 1/16. папір писальний.
Умовн.-друк. арк. **36,2**. Обл.– вид. арк. **36,8**.
Замовлення № Тираж 300. Ціна договірна

Видавництво УкрДУЗТу, свідоцтво ДК № 6100 від 21.03.2018 р.