***Сірик А. В., магістрант***
***Єфіменко А. А., к.т.н., доцент***
*Державний університет «Житомирська політехніка»*

**DEEPFAKE У ФІШИНГОВИХ АТАКАХ: АНАЛІЗ ЗАГРОЗ ТА ЗАСОБІВ ВИЯВЛЕННЯ**

Сучасні технології штучного інтелекту суттєво змінюють ландшафт кібербезпеки, створюючи як нові можливості для захисту даних, так і загрози. Одним із найбільш небезпечних проявів цих загроз є використання deepfake – методів генерації підробленого аудіо, відео та зображень за допомогою нейронних мереж. Deepfake-технології, які спочатку розглядалися як інструменти для розваг та кіноіндустрії, сьогодні активно використовуються кіберзлочинцями у фішингових атаках для маніпуляції жертвами, обходу засобів автентифікації та компрометації корпоративних мереж.

Фішингові атаки, що використовують deepfake, можуть мати різні форми, зокрема:

– **Аудіофішинг** (voice phishing, vishing): Кіберзлочинці синтезують голос керівників компаній або знайомих осіб, щоб переконати жертву виконати певні дії, наприклад, здійснити грошовий переказ або передати конфіденційні дані.

– **Відеофішинг:** Використання підроблених відеозаписів, які створюють ілюзію реальної присутності людини. Такі відео можуть застосовуватися для обману співробітників або дискредитації осіб у суспільному та корпоративному середовищі.

– **Соціальна інженерія через фальшиві відеодзвінки:** Зловмисники можуть проводити відеоконференції, використовуючи deepfake, щоб видавати себе за керівників або працівників організацій та маніпулювати жертвами.

– **Компрометація особистих акаунтів:** Створення підроблених профілів у соціальних мережах із згенерованими зображеннями для отримання довіри та подальшого використання у шахрайських схемах.

Варто наголосити, що deepfake-фішинг становить значну загрозу, оскільки традиційні методи перевірки автентичності, такі як голосова ідентифікація чи відеозв'язок, стають ненадійними. Сучасні алгоритми deepfake дозволяють створювати надзвичайно реалістичні підробки, які важко відрізнити від справжніх навіть за допомогою професійних інструментів, що значно ускладнює їхнє виявлення. Окрім цього, автоматизація deepfake-застосувань сприяє розширенню масштабів атак, адже зловмисники швидко генерують великі обсяги персоналізованого фішингового контенту, орієнтованого на конкретних осіб або організації. Такі атаки можуть мати далекосяжні наслідки не лише для корпоративної безпеки, а й для суспільства в цілому, оскільки deepfake активно використовуються у політичних маніпуляціях, дезінформаційних кампаніях та навіть у фінансових махінаціях, впливаючи на довіру до публічних осіб і ринків.

Ба більше, deepfake-фішинг є однією з найбільш витончених кіберзагроз, що вимагає комплексного підходу до виявлення та запобігання. Сучасні методи боротьби з такими атаками поєднують технологічні та організаційні заходи. Зокрема, ефективним способом є аналіз аномалій, коли алгоритми машинного навчання виявляють нестандартні рухи губ, невідповідність між звуком і відео, а також відхилення в тінях та освітленні. Важливу роль відіграє біометрична автентифікація, яка доповнює традиційні методи перевірки особи за допомогою аналізу мімічних мікровиразів обличчя та поведінкових особливостей голосу. Додатковий рівень безпеки забезпечують криптографічні методи перевірки контенту, що передбачають використання цифрових підписів для аудіо- та відеофайлів, дозволяючи підтвердити їхню автентичність. Не менш значущим є підвищення рівня обізнаності серед користувачів і співробітників компаній, що включає навчання методам розпізнавання deepfake-загроз і дотримання основних принципів інформаційної безпеки.

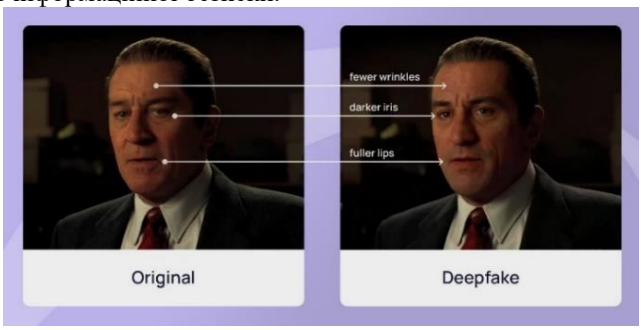


Рис 1. Порівняння оригінального зображення та deepfake

Таким чином, зосередимося на аналізі сучасних методів використання deepfake у фішингових атаках, їхній загрозі для інформаційної безпеки та ефективних способах протидії.

**Список використаних джерел:**

1. What is Deepfake Phishing: Deepfake Phishing Explained. - Keepnet. Keepnet Labs. URL: https://keepnetlabs.com/blog/what-is-deepfake-phishing.

2. Peters J. Deepfake phishing example: Protect your employees from deepfake scams. infosecinstitute. URL: https://www.infosecinstitute.com/resources/phishing/deepfake-phishing-example/.