Овсянніков Д.В., магістрант,
Бродський Ю.Б., к.т.н., доцент,
Державний університет «Житомирська політехніка»

ВПЛИВ DEEPFAKE-ТЕХНОЛОГІЙ НА КІБЕРБЕЗПЕКУ

У сучасному цифровому середовищі технології deepfake, які поєднують методи глибокого навчання з підробкою, набули значного поширення. Вони дозволяють створювати реалістичні фальшиві зображення, відео та аудіо, які важко відрізнити від справжніх. Це викликає серйозні занепокоєння у сфері кібербезпеки, оскільки deepfake-технології активно використовуються зловмисниками для дезінформації, шантажу, шахрайства та інших злочинних дій. Особливу увагу привертають їхній вплив на соціальну інженерію, політичну дезінформацію, фінансове шахрайство та порушення приватності.

Метою дослідження є аналіз загроз, пов'язаних із використанням технологій deepfake, та розробка рекомендацій для підвищення рівня кібербезпеки. Дослідження включає оцінку сучасних технологій виявлення deepfake, таких як аналіз артефактів зображень, перевірка біометричних ознак та використання алгоритмів штучного інтелекту, а також розробку практичних заходів щодо запобігання злочинам на основі deepfake. Особлива увага приділяється методам генеративно-змагальних мереж (GAN), які демонструють здатність створювати реалістичний підроблений контент, і розробці стандартів цифрової автентифікації.

Результати дослідження свідчать, що впровадження нових підходів до виявлення та протидії deepfake, зокрема на основі машинного навчання, може суттєво знизити ризики використання цих технологій у злочинних цілях. Практична значущість роботи полягає у розробці рекомендацій для покращення захисту інформаційних систем, вдосконаленні законодавства у сфері кібербезпеки та проведенні освітніх програм, спрямованих на підвищення обізнаності про ризики використання deepfake. Таким чином, дослідження сприяє формуванню комплексного підходу до протидії цим загрозам, що забезпечує безпеку інформаційного простору.

Теоретична значущість: Дослідження сприяє поглибленню розуміння впливу технологій deepfake на кібербезпеку, формуючи базу для подальших наукових розробок. Виявлені закономірності допомагають вдосконалювати моделі виявлення deepfake, зокрема за допомогою методів машинного навчання для аналізу даних. Також підкреслено соціальні та етичні аспекти технологій deepfake, їхній вплив на суспільну довіру та приватність, що дозволяє розробляти нові підходи до цифрової етики та правового регулювання.

Практична значущість: Рекомендації, розроблені в межах дослідження, можуть бути застосовані для підвищення захисту інформаційних систем від загроз, пов'язаних із deepfake. Це включає впровадження технологій виявлення, освітніх програм для обізнаності громадськості, а також вдосконалення законодавчих та політичних підходів. Практичні заходи спрямовані на зменшення ризиків дискредитації, фінансового шахрайства та маніпуляцій у соціальних мережах.

Рекомендації:

- Розробка та впровадження технологій виявлення deepfake на основі аналізу артефактів зображень та аудіо.
- Підвищення обізнаності громадськості про ризики, пов'язані з використанням deepfake, через освітні програми та інформаційні кампанії.
- Вдосконалення законодавства у сфері кібербезпеки з урахуванням нових загроз, пов'язаних із технологіями deepfake.
- Створення міжнародних стандартів та протоколів для протидії використанню deepfake у злочинних цілях.

Висновки: технології deepfake становлять значну загрозу для кібербезпеки, оскільки дозволяють створювати фальшиві відео та аудіо, які важко відрізнити від справжніх. Це спричиняє ризики дезінформації, шантажу та інших злочинних дій. Для протидії цим загрозам необхідно впроваджувати сучасні методи виявлення deepfake і підвищувати обізнаність суспільства про пов’язані ризики.

Список використаних джерел

1. Deepfake та право на образ URL: https://polikarpov.legal/blogposts/deepfake-ta-pravo-na-obraz/.
2. Діпфейки: чому це так небезпечно? URL: https://cybercalm.org/novyny/dipfejky-chomu-tse-tak-nebezpechno/.
3. 10 найкращих генераторів AI Deepfake для фото та відео у 2023 році URL: https://mpost.io/uk/top-ai-deepfake-generators/.
4. 4 ways to future-proof against deepfakes in 2024 and beyond URL: https://www.weforum.org/stories/2024/02/4-ways-to-future-proof-against-deepfakes-in-2024-and-beyond/.