- аналізатори трафіку,
- системи резервного копіювання,
- системи захисту інформації від несанкціонованого доступу, в тому числі засоби шифрування,
- системи розмежування доступу і авторизації.

Кожен тип з перерахованих відповідає за своє коло завдань, вимагає відповідної настройки і інтеграції в загальну інфраструктуру підприємства. Реалізувати глобальне завдання з вибудовування програмно-апаратної частини ІБ корпорації під силу спеціалізованим компаніям.

Найкращий ефект досягається за рахунок поєднання програмних рішень для запобігання інцидентів безпеки, тому що інакше тримати під контролем складну розподілену структуру майже неможливо.

Для вирішення комплексу ІБ-задач необхідно:

1. Контролювати місця зберігання і маршрути руху інформації по всіх каналах зв'язку, які використовуються в компанії (пошта, Skype, месенджери, форуми, хмарні сховища та ін.)
2. Виявляти дані в мережі підприємства в будь-який момент часу. Аналізувати дані будь-якого формату: текстового, графічного, аудіо.
3. Фіксувати дії співробітників, їх активність на підприємстві, за робочими ПК і поведінку в колективі.
4. Відстежування небезпечних рис характеру. Як правило, фахівці з безпеки роблять це «вручну», що вкрай важко на величезних підприємствах. Але на ринку з'являються IT-рішення, які дозволяють автоматизувати цю роботу. Це робить автоматизований профайлинг, наприклад. Він показує цінності і характер людини, схильності до авантюризму, наприклад, демонструє в динаміці, якщо в особистостях людини відбуваються значні зміни.

Список використаних джерел

1. Роль людського чинника у питаннях захисту інформаційних систем [Електронний ресурс] 2. Режим доступу до ресурсу: http://www.vestipb.ru/articles8561.html

3. Роль людського фактора {Електронний ресурс} – Режим доступу до ресурсу: http://softline.rbc.ru/page/rol-chelovecheskogo-faktora/

4. Людський фактор та інформаційна безпека підприємства {Електронний ресурс] – Режим доступу до ресурсу: http://softline.rbc.ru/page/rol-chelovecheskogo-faktora/

УДК 004.855.5

МЕТОДИКА ПРОТИДІЙ СИНТЕЗУ ЗОБРАЖЕННЯ, ЗАСНОВАНА НА ШТУЧНОМУ ІНТЕЛЕКТІ (DEEPFAKE)

Чулінда О. С., здобувач вищої освіти, гр. МКБп-201
Науковий керівник: **Ткач Ю. М.**, д.пед.н., проф.
Національний університет «Чернігівська політехніка»

На даний момент в мережі настає велика проблема підробки відео, тобто підставлення або анімація обличчя людини. Це здійснюється за допомогою штучного інтелекту. Також за допомогою штучного інтелекту обробляються і підміняються не лише відео файли а і фотографії, на яких звичайна людина не може розпізнати підробку.

Методика синтезу зображення або ще називають діпфейки (deepfake), заснована на штучному інтелекті, використовується для з'єднання і накладення існуючих зображень і відео на вихідні зображення або відеоролики[4]. Що може призвести до шантажу або розповсюдженні злоякісної інформації від людини яка не подавала цю інформацію.

У переважній більшості випадків, для створення таких відео використовують генеративно-змагальні нейромережі (GAN) алгоритм машинного навчання без учителя, побудований на комбінації з двох нейронних мереж, одна з яких (мережа G) генерує зразки, а інша (мережа D) намагається відрізнити правильні «справжні» зразки від неправильних.

У 2018 році з'явилася перша публічна програма для підміни осіб під назвою FakeApp, яка відкрила діпфейк-інструменти простому користувачу. Набори для створення такого контенту знаходяться з тих пір у вільному доступі і легкі в освоєнні. Будь-яка людина, яка має доступ до інтернету, вільний час, цілі та мотивацію, може в режимі реального часу створювати фальшивий контент і наповнювати їм канали соціальних мереж.

Діпфейки представляють собою серйозну загрозу, оскільки подібного роду контент є, по суті, інформаційною атакою. IT-аналітики заявляють, що технологія Deepfake може стати найнебезпечнішою в цифровій сфері за останні десятиліття. З поширенням діпфейків з'явилися випадки дискредитації відомих людей, чиїх фотографій багато в мережі «Інтернет». У світі політики технологія Deepfake може бути використана як зброя проти окремих діячів і цілих партій, щоб маніпулювати громадською сприйняттям.

Крім політичних інформаційних війн Deepfake створює і ризики в області інформаційної безпеки корпоративного сектора. Діпфейкі виявилися непоганим інструментом в руках шахраїв.

Проблема діпфейків здається дуже складною. Оскільки вони створюються за допомогою штучного інтелекту, для боротьби з ними потрібно використовувати щось аналогічне. Завдання розробників таких як Facebook, Microsoft і Amazon полягає в тому, щоб створити технологію, яку кожен зможе використовувати, щоб краще визначати, коли штучний інтелект був використаний для зміни відео, щоб ввести глядача в оману.

В статі «In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking» розповідається про те, як аналіз частоти моргання може допомогти виявити діпфейків. Ідея така: зазвичай у відкритому доступі важко знайти фотографії людини в момент моргання, так що нейронні мережі просто нема на чому вчитися генерувати подібні кадри. Крім того, у оригіналу і підробці можуть відрізнятися деякі примітні частини обличчя (підборіддя, брови, вилиці, вуса і борода, веснянки і родимі плями); будь-яка невідповідність - свідоцтво діпфейка[1].

Також в даний момент є аналіз діпфейка за допомогою якого можна розпізнати підробку по неправильного відображенню в очах людей на фото або відео.

Дослідники з Університету Буффало розробили інструмент для майже безпомилкового визначення діпфейков на цифрових зображеннях людей. Новий алгоритм помиляється всього в шести випадках зі ста. Це може допомогти в боротьбі з неправдивою інформацією, але алгоритм має ряд обмежень. Запропонований дослідниками алгоритм досліджує відображення в очах людей на цифрових фотографіях. На справжніх зображеннях відображення в очах, як правило, однакові, тоді як нейромережа в процесі створення діпфейків оперують безліччю цифрових зображень людей з великої бази даних, що веде до синтезу різних відображень на одній і іншій рогівці ока.

Зокрема, аналіз бази даних згенерованих нейромережею StyleGAN2 зображень несправжніх людей показав, що алгоритм здатний виявити діпфейк в 94% випадків портретних зображень людей, зроблених з хорошим освітленням і з досить великою роздільною здатністю. У той же час точність стрімко падала, якщо роздільна здатність знижувалося або освітлення було недостатньо для формування відображення від рогівки.

Також слід визнати, що при певному освітленні відображення в очах можуть відрізнятися, як і не можна даний алгоритм застосувати для випадків, коли друге око не видно або знаходиться в тіні[2].

Для того щоб мінімізувати ризики цільових фішингових атак за допомогою діпфейков в корпоративному середовищі, необхідно інформувати користувачів про нові типи шкідливої активності і бути напоготові в ситуаціях, коли поведінка співрозмовника в телефонній розмові або голосовому повідомленні здається незвичним. Крім того, рекомендується:

– використовувати багатофакторну аутентифікацію співробітників, електронний підпис для захисту повідомлень електронної пошти;

– відслідковувати факти наявності програм для створення діпфейків на комп'ютерах користувачів і спроби пошуку таких додатків в мережі «Інтернет», звертати особливу увагу на подібних працівників і проводити в їх відношенні внутрішні перевірки;

– забезпечити узгоджене поширення інформації;

– обмежити фото- і відео контент за участю керівних осіб підприємства;

– розробити план реагування на дезінформацію (по аналогії з інцидентами безпеки);

– мінімізувати число каналів комунікацій компанії;

– всередині компанії і для зв'язку з контрагентами застосовувати практику введення усних паролів, кодових слів або контрольних питань, відповідь на які відомий лише двом сторонам;

– стежити за новими способами виявлення діпфейків і методами боротьби з ними.

В даний час ринок ІБ не пропонує спеціалізованих рішень для захисту від діпфейків. Розвиток інструментів, здатних розпізнати підроблений контент, поки знаходиться в зародковому стані. Єдине рішення, яке існує в даний час, полягає в тому, щоб інформувати користувачів про нові типи атак і бути насторожі щодо будь-якої поведінки, яка здається незвичайною.

Список використаних джерел

1. In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://arxiv.org/pdf/1806.02877.pdf.

2. New Deepfake Spotting Tool Proves 94% Effective – Here's the Secret of Its Success [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://scitechdaily.com/new-deepfake-spotting-tool-proves-94-effective-heres-the-secret-of-its-success/.

3. Creating a dataset and a challenge for deepfakes [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://ai.facebook.com/blog/deepfake-detection-challenge.

4. Deepfake [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Deepfake.

5. DeepFaceLab [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/iperov/DeepFaceLab.

6. Unsupervised image-to-image translation [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/mingyuliutw/unit.

УДК 004.318

МЕТОД ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ

Шамара Н. В., здобувач вищої освіти гр.КБ-191
Науковий керівник: **Петренко Т. А** , викладач
Національний університет «Чернігівська політехніка»

Комп'ютер давно вже став частиною життя майже всіх людей. Він використовується для роботи, навчання, розваг, спілкування, в тому числі і кіберзахисту Для багатьох комп'ютер або ноутбук є єдиним джерелом доходу. Тож його продуктивність є однією з найголовніших складових вдалої роботи. Це сприяє швидкості та якості виконання технічних задач в сфері КіберБезпеки.

Не дивно, що на сьогодні все більше зростає потреба у наявності продуктивного комп'ютера. На жаль, люди зіштовхуються з проблемою невідповідності ціни та характеристик товару. Опис може відрізнятися від реальності, або взагалі вводити в оману