суспільство, органи влади відіграватимуть вирішальну роль у цих зусиллях» (2), а отже, інструментарієм боротьби з інформаційним викликом сучасним демократіям є розвиток сталості суспільства й підвищення поінформованості, цифрової освіти громадян, оскільки темпи розвитку цифрових технологій і надалі посилюватимуться, змінюючи суспільні процеси.

Список використаних джерел

1. Anderson Janna, Rainie Lee. Many Tech Experts Say Digital Disruption Will Hurt Democracy. Pew Research Centre. 2020. 118 p. URL: https://eloncdn.blob.core.windows.net/eu3/sites/964/2020/02/Elon-Pew-Future-of-Democracy-2-21-20.pdf (last accessed: 03.04.2024)

2. Mathias Gyselen. International institute for Democracy and Electoral Assistance (International IDEA). 2018. URL : https://www.idea.int/news/challenges-and-opportunities-democracy-21st-century (last accessed: 04.03.2024)

Литвиненко Наталія Павлівна
Кандидат економічних наук, доцент кафедри міжнародної інформації.
Київський національний університет імені Тараса Шевченка
ORCID: 0009-0008-7125-5496
Атаманчук Марія Ігорівна
Здобувач другого рівня вищої освіти.
Київський національний університет імені Тараса Шевченка

ДІПФЕЙКИ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА СУЧАСНИХ ДЕРЖАВ

Бурхливий розвиток технологій призвів до потужних зрушень у різних сферах життєдіяльності сучасного суспільства, але саме у військовій сфері вони набули найбільш суперечливого характеру. Серед технологій, які суттєво змінили стратегії протиборства, експерти визначають діпфейки. Саме поняття «діпфейк» передбачає поєднання технологій глибинного навчання та генерування фейкових відео, що імітують реальні аудіо- та відеозображення. Програми, які використовуються для створення діпфейків, постійно удосконалюються, тобто «вчяться», завдяки штучним нейронним мережам, що робить результати їх використання все більш реалістичним, а отже – небезпечними. Як зазначає американський експерт Е. Грото, ці технології будуть й надалі розвивати і вже через кілька років людині буде важко відрізнити реальне відео від підробного [1; 2].

Отже, технології, що спочатку використовувалися у кіноіндустрії та сфері розваг, нині почали активно застосовуватися у внутрішньополітичній конкуренції та в інформаційному протиборстві між державами, що перетворює їх на сучасну високотехнологічну інформаційну зброю [1]. Наприклад, у США ще у 2018 р. було продемонстровано можливості підробки відеозвернень до населення відомих американських політиків, зокрема, колишнього президента Б. Обами, який у фейковому відео, зробленому за допомогою програми Fakeapp і графічного редактора Adobe After Effects, образив Д. Трампа, що в умовах загострення конфронтації між прибічниками республіканців та демократів потенційно могло б спровокувати внутрішньополітичну кризу [3].

Слід зазначити, що незважаючи на зростання занепокоєння можливостями використання генеративного штучного інтелекту у передвиборчій кампанії у 2020 в цілому ці технології не були масово застосовані. Водночас, це не означало, що небезпека була переоцінена. Технології набули подальшого розвитку і ставали дедалі більш досконалими, що додало стурбованості правоохоронним органам та розвідці, які постійно попереджали про використання країнами-противниками США підробних відео з метою впливу на внутрішньополітичну ситуацію та національну безпеку держави.

Технології діпфеків використовувалися в рамках ізраїльсько-палестинського конфлікту з метою поглиблення кризи та провокації відкритого збройного протистояння, але далі, ніж поширення відео у формі мемів або історій та відео, вирваних з контексту, учасники протистояння не пішли. А у 2020 р. у Мережі з’явилися підроблене відео з кадрами розмови Кім Чен Ина, метою якого було поглибити кризу у відносинах між США та Північною Кореєю, звинувативши в цьому саме Дж. Байдена [4].

У жовтні 2023 р. представники служб розвідки Великої Британії та США зауважили, що подальший розвиток технологій діпфейків може стати «загрозою для демократії» та спричинити спалах розбрату, насильства і хаосу в суспільстві. Так, К. МакКалум, керівник британської розвідки MI5, висловив занепокоєння щодо можливого застосування цих технологій для впливу на майбутні загальні вибори. А його американський колега, директор ФБР К. Рей зазначив, що слід також враховувати загрози застосування технологій штучного інтелекту та діпфейків терористами для створення більш досконалих видів озброєнь [5].

Діпфейки активно використовуються у війні РФ проти України. Діапазон застосування таких технологій є надзвичайно широким. Так, від самого початку військової агресії проти української держави Центр інформаційної безпеки попереджав щодо високої ймовірності поширення фейків про капітуляцію України, у тому числі, з використанням технологій діпфейку. Особливого

занепокоєння у експертів викликав інцидент у березні 2022 р., коли внаслідок російської хакерської атаки на телеканалі «Україна 24» та сайті «Сегодня» певний час транслювалося фейкове повідомлення та відео, що містило звернення президента В. Зеленського із нібито закликом припинити опір і скласти зброю. Президент України одразу виступив із спростуванням цього фейку, але подібні інциденти траплялися і пізніше [6; 7]. Так, після подій 7 жовтня 2023 р. в Ізраїлі та початку масштабної військової операції у Секторі Гази, в глобальному інформаційному просторі поширювалося відео низької якості в стилі репортажу BBC News, де стверджувалося, що Україна надсилає зброю, отриману від західних союзників, ХАМАСу [4].

Таким чином, розвиток технологій діпфейку призвів до появи нових інструментів ведення інформаційної війни. Введення в оману шляхом створення і поширення реалістичних фейкових відео може призвести до серйозних політичних наслідків як для окремих країн, так і світу в цілому, зруйнувати систему безпеки, спричинити ескалацію конфлікту та громадянського протистояння, оскільки відбувається поступове розмивання межі між реальністю та вигадкою. Це усвідомлюється урядами багатьох країн та їх структурами у сфері безпеки, які закликають не нехтувати новими можливостями у сфері генеративного штучного інтелекту. Водночас, як свідчить практика, дедалі більше компаній включилися у розробку програм, що здатні виявляти діпфейки, і таким чином ефективно протистояти можливостям використання цих технологічних інновацій у сфері внутрішньої та зовнішньої політики.

Список використаних джерел

1. Радіо Свободи. Технологія діпфейку стане найсучаснішою інформаційною зброєю. *Радіо Свободи.* 05 липня 2018 URL: https://cutt.ly/3w31DqCe. (дата звернення 03.01.2024 р.).

2. Associated Press. Fake News May Take New Form in Doctored Videos. *Associated Press*. July 2, 2018. URL: https://cutt.ly/Jw31Fqvq. (дата звернення 03.01.2024 р.).

3. BuzzFeedVideo. You Won’t Believe What Obama Says In This Video! *BuzzFeedVideo.* April 17, 2018. URL: https://cutt.ly/Gw31FLcu. (дата звернення 03.01.2024 р.).

4. Carlyon P. Deepfakes Aren't the Disinformation Threat They're Made Out to Be. *DC Journal An InsideSources Publication*. 2023. URL: https://cutt.ly/Gw31GfSR. (дата звернення 03.01.2024 р.).

5. Mendick R.‘Deep fake’ AI could threaten next general election, MI5 chief warns *The Telegraph.* 18 October 2023. URL: https://cutt.ly/nw31GKzK. (дата звернення 03.01.2024 р.).

6. Бойко І. В ефірі "Україна 24" показали фейкове повідомлення Зеленського про "капітуляцію", президент його спростував. *УНІАН. Інформаційне агентство.* 16 березня 2022. URL: https://cutt.ly/1w31HpoV. (дата звернення 03.01.2024 р.).

7. Інститут Масової Інформації. Хакери зламали рухомий рядок каналу «Україна 24» та транслюють фейк про «капітуляцію». 2022. URL: https://cutt.ly/Yw31HYc4. (дата звернення 03.01.2024 р.).

Ліцук Богдан Вікторович
Здобувач кафедри національної безпеки.
Волинський національний університет імені Лесі Українки
Стрелков Владислав Володимирович
Ph. D., старший викладач кафедри національної безпеки.
Волинський національний університет імені Лесі Українки

ГАЛУЗІ ЗАСТОСУВАННЯ РОЗВІДКИ ВІДКРИТИХ ДЖЕРЕЛ ДАНИХ (OSINT)

Розвідка відкритих джерел даних (з англ. – Open Source Intelligence, далі – OSINT) може бути помічною для різних організацій, включаючи: уряди, бізнес, наукові установи; а також може допомогти журналістам та фахівцям із кібербезпеки отримувати важливу інформацію про конкурентів, партнерів, клієнтів, ринки, загрози, можливості тощо. OSINT також може допомогти звичайним людям перевіряти факти, захищатися від дезінформації, підвищувати свою обізнаність та навички. Проте OSINT також може бути використаний для зловмисних цілей, таких як соціальна інженерія, шпигунство, крадіжка даних тощо. З огляду на це, дослідження теми OSINT викликає значну зацікавленість у вчених, які працюють у різних галузях: військовій, політичній, соціологічній, психологічній та ін., задля підвищення наукового рівня та якості його застосування.

Збір, аналіз та поширення інформації, доступної для громадськості та не захищеної грифами секретності, становлять основу OSINT. У сучасний час цей метод використовується різними установами, включаючи урядові структури, бізнес та неприбуткові організації. OSINT може бути використаний задля гарантування різноманітних інтересів тих чи інших суб’єктів, таких як забезпечення кібербезпеки, проведення досліджень ринку, підтримка журналістської діяльності, а також для потреб розвідки тощо. На ринку існує велика кількість інструментів та ресурсів для застосування OSINT у різних галузях, таких як OSINT Framework, OSINT Dojo та інші. Для успішного