Це призведе до виникнення глобального руху за громадянські права в суспільстві роботів, а до 2038 року США стануть першою країною, що надала такі права андроїдам.

Давайте порахуємо, скільки залишилося до 2038 року – 16 років. Таким чином, переважна більшість сучасників буде свідками і учасниками цих подій.

Це, на перший погляд, може здаватися певною мірою футуристичним прогнозом. Але я б зауважив, що такий прогноз робить не дилетант або письменник-фантаст (як свого часу це робив відомий письменник-фантаст Г. Уелс у книгах «Машина часу» і «Боротьба світів»), але один з провідних фахівців у найсучаснішій технологічній галузі – робототехніці. І цей факт, на мій погляд, вимагає ставитися до його прогнозу з повагою і увагою.

Найважливішим результатом сучасних процесів у сфері високих технологій є усвідомлення правоохоронними органами розвинених країн необхідності зміни парадигми своєї діяльності – перехід від реактивного принципу до предикативного, що і відбувається в останні декілька років. І головним інструментом реалізації такої парадигми є застосування інтелектуальних аналітичних систем типу Palantir, ePOOLICE.

Ткач Ю. О.,
ад'юнкт
Дніпропетровського державного університету внутрішніх справ,
майор поліції
Науковий керівник:
Гребенюк А. М.,
завідувач кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету внутрішніх справ

СУЧАСНІ ПИТАННЯ ДЕЗІНФОРМАЦІЇ В УМОВАХ ВІЙНИ

Так, 24 лютого 2022 року російська федерація розпочала повномасштабне вторгнення в Україну. Щодня в інформаційному просторі з'являється багато інформації різного характеру, серед якої є недостовірна інформація, яка публікується у Facebook, Instagram, Twitter, Telegram та інших соціальних мережах. Поширення такої інформації тягне за собою дезінформацію населення, залякування, введення громадян в оману, при цьому здійснюється психологічний тиск на них за допомогою цієї інформації, яку використовує ворог у своїх цілях.

Так, дезінформація – це очевидно неправдива або така, яка вводить в оману, інформація, що в сукупності: створена, представлена і поширена з

метою економічної вигоди або умисного введення в оману громадськості; та може заподіяти шкоду суспільству через загрозу демократичним політичним процесам і процесам вироблення політики, а також таким суспільним благам, як захист здоров'я громадян, довкілля і безпека. Таке поняття як «дезінформація» не охоплює недостовірну рекламу, помилки у звітності, сатиру і пародію чи очевидні необ'єктивні новини й коментарі, та не є порушенням юридичних зобов'язань, кодексів саморегулювання рекламних послуг і стандартів щодо недостовірної реклами [1].

До дезінформації не можуть бути визнано: по-перше оціночні або критичні судження; по-друге сатира; по-третє недостовірна інформація про особу, яка не шкодить суспільним інтересам [1].

За поширення дезінформації відповідальність може бути як адміністративна або кримінальна залежності від дій осіб, які поширюють дезінформації.

Адміністративна відповідальність може настати у разі одноразового поширення дезінформації без ознак замовлення; відсутність вихідних даних про медіа [1].

Кримінальна відповідальність може настати у разі умисного, систематичного поширення дезінформації; умисного поширення дезінформації на замовлення третьої особи або якщо спричинено шкоду; втручання в діяльність журналіста або медіа, підкуп. Також необхідно звернути увагу, що відповідальність за дезінформацію настає виключно на підставі рішення суду [1].

Необхідно звернути увагу, як поводитися у мережі, щоб протидіяти дезінформації та фейкам під час війни:

1. Бажаєте бути корисними в інформаційному фронті? Знайдіть собі команду, яка вже зосередила сили на окремому напрямку боротьби з дезінформацією.
2. Не поширювати інформацію з не офіційних джерел. Навіть, якщо вам її надіслала близька людина, кум, сват або ще хтось. Не впевнені, то ж не робіть репост.
3. Не вірити сліпо в інформацію в інтернеті. Виключення – правила або вказівки, опубліковані на офіційних сторінках військового керівництва держави чи органів державної влади, або тих, які лунають в ефірі «Українського радіо» чи інших офіційних каналів оповіщення. Критично аналізуйте будь-яке джерело.
4. Намагатись не реагувати на масові розсилки та зупиняти за змогою їх поширення. Залиште в підписках лише офіційні сторінки та канали влади і місцевого уряду.
5. Не залишати свої дані у відкритому доступі – онлайн-форми, петиції та будь-які анкети є небезпечними наразі. Лише громадяни відповідальні за особисту конфіденційність.
6. Не відкривати сумнівних листів та повідомлень та не робити їх репост або пересилку.
7. Не захоплюватись історіями з неперевірених джерел – під час війни сарафанне радіо працює не на нашу користь, та інше [2-3].

Підсумовуючи вважаємо за необхідним проводити роз'яснювальну роботу з населенням щодо поведінки в мережі з метою протидії дезінформації та фейкам, пояснювати громадянам, що останні не повинні залишати свої дані у відкритому доступі – онлайн-форми, петиції та будь-які анкети, тощо. Правоохоронним органам необхідно посилити моніторинг для виявлення дезінформації та подальшого документування загрози та виправлення недоліків, які використовує агресор. Також необхідно посилити покарання за поширення дезінформації та вжити всіх необхідних заходів правоохоронними органами для стримування агресора в інформаційному просторі.

Список використаних джерел:

1. Ясність? Міністерство культури, молоді та спорту України: веб-сайт. URL: https://mkip.gov.ua/files/pdf/Ясність%20fin.pdf?__cf_chl_tk=Q65s0J_RVOlCJoKRbs_g01T5zNW.SJnPzdOWDSIOiVM-1668295307-0-gaNycGzNCKU.
2. Моє місто? Інформаційна війна: як вийти з нею переможцем: веб-сайт. URL: https://mycity.one/blog/faktcheking?utm_source=google&utm_medium=cpc&utm_campaign=inweb_My_City_Informatsijna_Vijna_Ukraine&utm_content=611396250363&utm_term=дезінформація%20це&gclid=EAIaIQobChMIxe2z16qj-wIV7kKRBR0J_AlSEAAYASAAEgKg6_D_BwE.
3. Плескачова В. С. Дезінформація як один із способів інформаційно-психологічного впливу на суспільство. *Міжнародна та національна безпека: теоретичні і прикладні аспекти*: матер. V Міжнар. наук.-практ. конф. (м. Дніпро, 12 березня 2021 р.). Дніпро: ДДУВС, 2021. С. 406-407. URL: http://er.dduvs.in.ua/jspui/handle/123456789/6262.

Форос Г. В.,
т. в. о. завідуча кафедри кібербезпеки та інформаційного забезпечення Одеського державного університету внутрішніх справ, кандидат юридичних наук, доцент

ОКРЕМІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ В СУЧАСНИХ УМОВАХ

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади. На сьогодні актуальність проблеми забезпечення кібернетичної безпеки не викликає жодних сумнівів. Щодня кожен з нас стикається із необхідністю користування інформаційними технологіями. Від соціальних мереж, розміщення інформації про свої персональні дані в інтернеті до користування банкоматами, банківськими рахунками і т.п.