

**Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»**

**Факультет соціології і права
Кафедра інформаційного, господарського та адміністративного права**

**Державна наукова установа «Інститут інформації, безпеки і права
Національної академії правових наук України»
Науковий центр національної безпеки і права**

**ПРОБЛЕМИ ЄВРОПЕЙСЬКОЇ ТА СВІТОВОЇ БЕЗПЕКИ:
ПРАВОВІ ВЕКТОРИ**

Матеріали круглого столу

**10 травня 2023
Київ, Україна**

**Київ
КПІ ім. Ігоря Сікорського
2023**

Рекомендовано до друку рішенням вченої ради
факультету соціології і права КПП ім. Ігоря Сікорського
(протокол № 11 від 29.06.2023 р.)

Рекомендовано до друку рішенням вченої ради
Державної наукової установи «Інформація,
безпека і права Національної академії правових наук України»
(протокол № 7 від 17.07.2023 р.)

Проблеми європейської та світової безпеки: правові вектори: матеріали
круглого столу (Київ, 10 травн. 2023 р.) / Упоряд: Бевз С.І., Бирса Н.О.,
Серебрякова Ю.О. – Київ: КПП ім. Ігоря Сікорського, 2023. – 234 с.

В збірнику подані тези доповідей учасників круглого столу «Проблеми
європейської та світової безпеки: правові вектори» (м. Київ, 10 травня 2023 р.),
які містять погляди відомих вчених, молодих науковців і студентів, що роблять
перші спроби наукових розвідок.

Висвітлено правові аспекти підтримки європейської та світової безпеки в
умовах цифровізації та розвитку економіки і забезпечення прав людини в
умовах протидії злочинності та кризовим явищам у сучасному суспільстві.
Розглянуто синергію правових систем, правової політики та законодавства
країн Європи і світу в умовах сталого розвитку, трансформацію правового
регулювання інформаційної безпеки, штучного інтелекту та високих технологій
в епоху цифрового суспільства. Досліджено правові проблеми глобальної
безпеки в умовах запобігання збройним конфліктам.

Для науковців, викладачів, аспірантів, студентів вищих навчальних
закладів, а також юристів-фахівців.

@ Автори статей, 2023
@ КПП ім. Ігоря Сікорського (ФСП), 2023
@ ДНУ ІБП НАПрН України, 2023

ЗМІСТ

Бевз С.І. ЗАКОНОДАВЧІ ВЕКТОРИ БЕЗПЕКИ В УКРАЇНІ	7
Корж І.Ф. БЕЗПЕКА ЛЮДСЬКОЇ ЦИВІЛІЗАЦІ В СУЧАСНИХ УМОВАХ	10
Мисливий В.А. ПРИНЦИПИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНОМУ ПРАВІ	17
Бабанін С.В. ОСНОВИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ ЯК ОБ'ЄКТ КОМП'ЮТЕРНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ	24
Попов К.Л. КРИМІНАЛЬНО-ПРАВОВА ОХОРОНА ПРАВОСУДДЯ: ПРАВАЗАСТОСОВНА РЕАЛЬНІСТЬ	29
Радзієвська О.Г. ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ТА БЕЗПЕКИ ОСОБИ В СУЧАСНИХ УМОВАХ	35
Лук'янчиков Є.Д., Лук'янчиков Б.Є., Микитенко О.Б. ПОПЕРЕДНЄ ДОСЛІДЖЕННЯ СЛІДОВОЇ ІНФОРМАЦІЇ В ПРОЦЕСІ РОЗСЛІДУВАННЯ	41
Дорогих С.О. ПИТАННЯ ПРОТИДІЇ ПЕРЕХОПЛЕННЮ ПЕРСОНАЛЬНИХ ДАНИХ ІНОЗЕМНИМИ ДЕРЖАВАМИ В УМОВАХ ГЛОБАЛЬНОГО ПРОТИСТОЯННЯ	47
Романенко А.О. КОНЦЕПЦІЯ ПЕРЕХІДНОГО ПРАВОСУДДЯ КРІЗЬ ПРИЗМУ УКРАЇНСЬКИХ РЕАЛІЙ	50
Стадник В.Я. ПРОБЛЕМА ВИЗНАННЯ КУЛЬТУРНОГО ГЕНОЦИДУ	58
Мухаммад А.Т. СУЧАСНИЙ СТАН КРИМІНАЛЬНОГО ПРАВА УКРАЇНИ ТА ПЕРСПЕКТИВИ ЙОГО ІНТЕГРАЦІЇ В РАМКАХ ЄВРОПЕЙСЬКОГО СОЮЗУ	61
Саградян А.Г. КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА ПОРУШЕННЯ НЕДОТОРКАНОСТІ ПРИВАТНОГО ЖИТТЯ	67
Гайдай Є.А. ДО ПИТАННЯ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ПРАВ ЗАСУДЖЕНИХ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ	73
Юров М.С. ЕЛЕКТРОННИЙ ДОКУМЕНТООБІГ В ТРУДОВИХ ВІДНОСИНАХ	78

Герасименко О. І., ПРАВОВІ ЗАСОБИ ПРОТИДІЇ ЗЛОЧИННОСТІ У СФЕРІ ЗАХИСТУ ПРАВ ЛЮДИНИ В УМОВАХ РОЗВИТКУ ТЕХНОЛОГІЙ: СУЧАСНІСТЬ І ПЕРСПЕКТИВИ	82
Грачова О.Ю., ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ЕЛЕКТРОННОЇ КОМЕРЦІЇ В УМОВАХ ВОЄННОГО СТАНУ	88
Дубняк М.В., ПРАВОВЕ РЕГУЛЮВАННЯ В ГІГ-ЕКОНОМІЦІ: КОМПЕТЕНЦІЇ ПРАВНИКА	93
Завада Р.С., ПЕРЕВАГИ ЕЛЕКТРОННОГО УРЯДУВАННЯ ДЛЯ ПУБЛІЧНО- УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ	96
Ільченко І.П., ПРАВО СПОЖИВАЧІВ НА ІНФОРМАЦІЮ ЩОДО ХАРЧОВИХ ПРОДУКТІВ ТА ЙОГО ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ	99
Ковний Ю.Є., РЕАЛІЗАЦІЯ ПРАВА НА ВИБІР МІСЦЯ ПРОЖИВАННЯ РОМСЬКОЇ ЕТНІЧНОЇ ГРУПИ: БЕЗПЕКОВІ ВЕКТОРИ	104
Макарчук В.В., ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ	107
Масалітін В.В., СТРУКТУРА ТА ЕЛЕМЕНТИ АДМІНІСТРАТИВНО-ПРАВОВОГО СТАТУСУ ГРОМАДЯН УКРАЇНИ	110
Міщук Є.В., ЄВРОПЕЙСЬКА ІНТЕГРАЦІЯ ТА ЗАХИСТ НАЦІОНАЛЬНИХ ІНТЕРЕСІВ: ВИКЛИКИ ТА ШЛЯХИ ЇХ ПОДОЛАННЯ	113
Найда І. В., ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ ТА ЇЇ ВПЛИВ НА ПАТРІОТИЧНЕ ВИХОВАННЯ	118
Нікітін Ю.В. ЗАГАЛЬНІ ЗАСАДИ РОЗВИТКУ СЕК'ЮРИТОЛОГІЇ ЯК НАУКИ	122
Нікітін Д.Ю. КОРУПЦІЯ, ЯК ЗАГРОЗА ЕКОНОМІЧНОМУ РОЗВИТКУ ТА ЖИТТЄДІЯЛЬНОСТІ СУСПІЛЬСТВА І, ЯК НАСЛІДОК, НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ	124
Петрів С. Ю. МОНІТОРИНГ ПРАВОВОЇ ІНФОРМАЦІЇ ЯК УМОВА ЕФЕКТИВНОСТІ СИСТЕМИ ПРАВОВОЇ ІНФОРМАЦІЇ	131
Політова А.С. ДОТРИМАННЯ ПРАВА НА СТАТЕВУ СВОБОДУ ТА СТАТЕВУ НЕДОТОРКАНИСТЬ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ	136

Полякова І.В. ПОРІВНЯЛЬНИЙ АНАЛІЗ ВПРОВАДЖЕННЯ ЕЛЕКТРОННОГО РЕЦЕПТУ В НІМЕЧЧИНІ, ЕСТОНІЇ ТА УКРАЇНІ	140
Попович К.Г. ПІДТРИМКА ЄВРОПЕЙСЬКОЇ ТА СВІТОВОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ ТА РОЗВИТКУ ЕКОНОМІКИ	145
Самотуга А.В. КОНСТИТУЦІЙНА СВОБОДА ЗМІ, ІНФОРМАЦІЙНА БЕЗПЕКА І ЄВРОПЕЙСЬКІ ТА ЄВРОАТЛАНТИЧНІ ПЕРСПЕКТИВИ УКРАЇНИ	148
Самчинська О.А. ШТУЧНИЙ ІНТЕЛЕКТ – ІНСТРУМЕНТ ДЛЯ ЧИ ПРОТИ ДЕЗІНОФРМАЦІЇ?	155
Сердечна А.Ю. ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ПОШИРЕННЮ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ	162
Соха С.С. ОГЛЯД ПРАВОВОГО ПІДГРУНТЯ ВПЛИВУ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА НА МІСЦЕВЕ САМОВРЯДУВАННЯ В УКРАЇНІ	166
Старжинський В.В. ПРОБЛЕМНІ ПИТАННЯ ЗАПОБІГАННЯ ВЧИНЕННЮ РЕЙДЕРСЬКИХ ДІЙ ЩОДО АГРАРНИХ ПІДПРИЄМСТВ В УМОВАХ ВОЄННОГО СТАНУ	170
Фурашев В.М. РЕАЛЬНІ ТА ПОТЕНЦІЙНІ ЗАГРОЗИ ПРОЦЕСАМ УТВОРЕННЯ СИСТЕМИ ГЛОБАЛЬНОЇ БЕЗПЕКИ: ПРАВОВОЇ АСПЕКТ	175
Хашев В.Г. ДЕЯКІ ПИТАННЯ КВАЛІФІКАЦІЇ ЗАПОДІЯННЯ ШКОДИ ВОДНИМ ОБ'ЄКТАМ, ЩО ВЧИНЯЮТЬ РОСІЙСЬКІ ВІЙСЬКОВІ В УКРАЇНІ	178
Простаков О.Д. ВЗАЄМНЕ ВИЗНАННЯ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ МІЖ УКРАЇНОЮ ТА ЄС	184
Гончарова Є.М. ШТУЧНИЙ ІНТЕЛЕКТ ТА АВТОРСЬКЕ ПРАВО: ПРАВОВІ ВИКЛИКИ	189
Дудкін О.М. СОЦІОКУЛЬТУРНИЙ КОНТЕКСТ ЄВРОІНТЕГРАЦІЇ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ: АНАЛІЗ ПОТОЧНОЇ СИТУАЦІЇ ТА ПЕРСПЕКТИВИ РОЗВИТКУ	193
Ніколюк М.Р. ШТУЧНИЙ ІНТЕЛЕКТ ЯК ІНСТРУМЕНТ МАНІПУЛЮВАННЯ	198

Зенченко О.Д. СПІВПРАЦЯ ЄС ТА УКРАЇНИ У СФЕРІ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ	203
Кушнірук Т.О. ВИКЛИКИ ЄВРОІНТЕГРАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ: ДОСВІД КРАЇН ЄС	210
Сорока М. БЕЗПЕКОВІ ГАРАНТІЇ ПРАВОВОГО РЕЖИМУ ДІЯ СІТІ	215
Захарчук Є.М. ВИКОРИСТАННЯ ВІРТУАЛЬНОЇ ТА ДОПОВНЕНОЇ РЕАЛЬНОСТІ ДЛЯ ОБОРОННО-ПРОМИСЛОВОГО КОМПЛЕКСУ УКРАЇНИ В УМОВАХ ЄВРОІНТЕГРАЦІЇ: ДОСВІД ЄВРОПЕЙСЬКИХ КРАЇН	219
Сугулов Є.С. ЯК ВЕКТОР ЄВРОІНТЕГРАЦІЇ ПІД ЧАС ВОЄННОГО СТАНУ	224
Заславська Л.В. ПРОБЛЕМИ ПРИТЯГНЕННЯ ДО ВІДПОВІДАЛЬНОСТІ ЗА РОЗПОВСЮДЖЕННЯ ПРОПАГАНДИ В УКРАЇНІ	229
Терещенко О.В. ДО ПИТАННЯ ЦИФРОВІЗАЦІЇ У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ	233

цілісності»: Указ Президента України від 30.09.2022 № 679/2022. URL : <https://www.rnbo.gov.ua/ua/Ukazy/5785.html>.

12. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL : https://zakon.rada.gov.ua/laws/show/984_011#Text.

13. Хартія про особливе партнерство між Україною та Організацією Північно-Атлантичного договору від 09.07.1997. URL : https://zakon.rada.gov.ua/laws/show/994_002#Text.

14. Чи сумісна свобода інформації з інформаційною безпекою? URL : <https://ms.detector.media/utiski-zhurnalistiv-u-sviti/post/9515/2011-05-24-chy-sumisna-svoboda-informatsii-z-informatsiynoyu-bezpekoyu/>.

15. Як росія створює потужну пропаганду з фейками: пояснення на прикладі RT. 17.11.2022. URL : https://lb.ua/blog/infosecurity_institut/536213_yak_rosiya_stvoryuie_potuzhnu_propagandu_z.html.

ШТУЧНИЙ ІНТЕЛЕКТ – ІНСТРУМЕНТ ДЛЯ ЧИ ПРОТИ ДЕЗІНОФРМАЦІЇ?

Самчинська О.А.,
аспірантка, викладач кафедри інформаційного,
господарського та адміністративного права
КПІ ім. Ігоря Сікорського

Сьогодні штучний інтелект став невід’ємною частиною повсякденного життя людей з різних куточків земної кулі. Це не просто тренд, а невідворотне майбутнє. Підприємницька діяльність, кінематограф, мистецтво, журналістика, наука, освіта, охорона здоров’я, юридичні послуги, правоохоронна діяльність, судова система та військова сфера – це лише невеликий перелік галузей, у яких активно використовується дана технологія з метою оптимізації та підвищення ефективності різних процесів та їх результатів. Можна навести багато прикладів позитивного застосування штучного інтелекту, які не лише спрощують життя

сучасній людині, а й підвищують його якість та рівень безпеки. Зокрема, вже сьогодні саме ця технологія лежить в основі засобів діагностики, раннього виявлення та лікування різних захворювань, що у майбутньому, за різними прогнозами дозволить збільшити середню тривалість життя людини на 10-15 років.

Водночас, як практично будь-яке інше явище, широке використання та стрімкий розвиток даного досягнення науково-технічного прогресу має не лише плюси, а й мінуси. Так, разом із низкою захоплюючих думок щодо ефективності, необхідності подальшого удосконалення можливостей та збільшення масштабів застосування штучного інтелекту, існує абсолютно полярна позиція, що ця технологія є більш небезпечною за ядерну зброю (зокрема, таку думку висловив відомий підприємець у сфері новітніх технологій – Ілон Маск) та може становити серйозну загрозу для існування людства.

Особливо дискурсивним це питання є з правової та етичної точки зору. Порушення основоположних прав та свобод людини, зокрема, права на приватність, свободу слова та волевиявлення, права на отримання повної, точної та достовірної інформації, на повагу до честі, гідності та ділової репутації, дискримінація – це лише частина реальних та потенційних ризиків застосування ШІ. У даній роботі ми розглянемо штучний інтелект як інструмент дезінформації, – з одного боку, та водночас як засіб протидії та запобігання даному виду деструктивного інформаційно-психологічного впливу - з іншого. Під дезінформацією мається на увазі цілеспрямований процес створення, модифікації та поширення інформації, як недостовірної, так і достовірної, з метою введення осіб (групи осіб) в оману для досягнення політичної, економічної або ідеологічної мети, внаслідок якого порушуються або можуть бути порушені права людини та громадянина та/або суспільства та держави [1].

Розпочнемо розгляд даного питання з характеристики використання технологій ШІ для здійснення обраного виду деструктивного інформаційно-психологічного впливу. У даному контексті хочемо виділити три основні

напрями застосування можливостей штучного інтелекту, які дозволяють підвищити ефективність дезінформації: створення, масове поширення та цільове поширення.

1. Створення недостовірної інформації. Цілеспрямоване виробництво інформації, завданням якої є введення в оману не є чимось новим. Напевне, ще з початку виникнення комунікації люди почали застосовувати прийоми інформаційного впливу для досягнення різних цілей, що з поміж усього, передбачало підготовку «спеціальних відомостей». Проте, не можна заперечувати той факт, що використання технологій штучного інтелекту, по-перше, значно пришвидшують процес масового виробництва інформації, яка не відповідає дійсності (особливо у текстовому вигляді) та, по-друге, надають можливості зробити її більш «правдоподібною» та «переконливою» (особливо коли це стосується зображення, аудіо та відео). Розглядаючи останнє, варто згадати про тенденцію підвищення популярності використання дипфейку (deep-fake) як інструменту дезінформації. Так, саме за допомогою цієї технології у березні 2022 року було створено відео-звернення Володимира Зеленського «про капітуляцію», а у червні цього ж року мери кількох європейських столиць проводили онлайн-зустріч з нібито з мером столиці України - Віталієм Кличко, який насправді виявся фейком. І якщо перший приклад був виконаний «недосконало», а його фальшивість не викликала сумніву, то встановити несправжність другого виявилось не так просто.

2. Масове поширення. Розвиток інформаційних технологій, зокрема мережі Інтернет значно пришвидшив процеси обміну інформацією, що дозволило оперативно поширювати важливу інформацію широкому колу осіб. Водночас, саме новітні технології дозволяють розповсюджувати «шкідливу» інформацію у небачених масштабах, що значно ускладнює протидію її негативному впливу. Розглядаючи даний пункт, варто приділити увагу ботам, які сьогодні стали невід'ємним інструментом деструктивної пропаганди та дезінформації. Ці програми, в основі діяльності яких зазвичай лежать технології штучного інтелекту, дозволяють, зокрема: масово, а головне досить

оперативно розповсюджувати інформацію, яка використовується для маніпуляції та введення в оману; генерувати та поширювати велику кількість дописів та коментарів, що підтримують певний наратив; залишати вподобання та «репостити» публікації. Зазвичай такі дії дозволяють створити ефект популярності та масовості підтримки певної ідеї, що впливає на формування «потрібного» ставлення громадськості до неї.

Крім просування недостовірної інформації, досить часто боти використовуються для здійснення так званих «атак» на профілі та канали, які поширюють достовірні відомості. Це призводить до блокування таких ресурсів з боку адміністраторів онлайн-платформ через «підозрілу» активність або ж самотійного обмеження власниками профілів та каналів можливості коментування дописів, що має наслідком зниження їх популярності серед аудиторії.

3. Цільове поширення. У даному контексті хочемо розглянути два напрями використання особливостей роботи алгоритмів соціальних мереж та онлайн-платформ, в основі яких лежить штучний інтелект, з метою здійснення інформаційного впливу, зокрема дезінформації.

Варто розпочати з того, що згадані алгоритми дозволяють збирати велику кількість персональних даних користувачів цих мереж та платформ, які сьогодні стали важливим інструментом маркетингової діяльності, зокрема підвищення ефективності рекламних оголошень, які поширюються користувачам за певними критеріями (вік, стать, регіон проживання, уподобання тощо). Водночас, такі відомості можуть бути незаконно зібрані, проаналізовані та використані з метою формування «психологічного портрету» об'єкта інформаційно-психологічного впливу, визначення його так званих «емоційних гачків», що дозволяє налаштовувати не лише рекламу, а й «персоналізовану» маніпуляцію, пропаганду та дезінформацію та підвищити рівень їх впливовості. У даному випадку яскравим прикладом може слугувати кейс незаконної обробки персональних користувачів соціальної мережі Facebook, британською компанією Cambridge Analytica, яку звинувачують у втручанні у вибори та інші

політичні процеси, шляхом маніпуляції думкою потенційного електорату (зокрема, президентські вибори у США в 2016 році та процедуру Brexit).

Напевне кожен хоча б раз помічав, що після уподобання, коментування або іншої реакції на ролик на YouTube, допису у Tiktok, або сториз в Instagram через певний час власні рекомендації починають наповнюватися контентом схожого характеру. У цьому полягає суть наступної загрози використання штучного інтелекту у контексті дезінформації, адже алгоритми соціальних мереж та онлайн-платформ налаштовані таким чином, що зазвичай користувача оточує інформація, яка відповідає його переконанням та уподобанням. Власне небезпека полягає у тому, що якщо такі ресурси використовуються не з розважальною метою, а є основним джерелом отримання інформації про навколишній світ, людина потрапляє у так звану «інформаційну бульбашку» або ж «бульбашку фільтрів», яка містить відомості та дані, які висвітлюють події лише з однієї точки зору. Це підсилює ефект підтвердженого упередження, що досить часто є причиною формування деформованого уявлення про дійсність та перешкоджає сприйняттю відомостей, що його спростовують.

Розглядаючи реальні та потенційні загрози використання технологій штучного інтелекту з метою впливу на масову свідомість не можна не згадати ChatGPT, який останнім часом став предметом низки дискусій. Перш за все, варто зазначити, що даний чат може використовуватися як інструмент умисного створення маніпулятивного чи недостовірного контенту. Підтвердженням цьому може слугувати дослідження, яке у січні 2023 року провели аналітики NewsGuard. Зміст експерименту полягав у тому, що чат попросили відповісти на 100 запитань із вибірки фейків та маніпулятивних повідомлень, зібраних упродовж 2022 року (серед яких були конспірологічні теорії, фейки щодо COVID-19 і вакцинації, а також події війни в Україні), а результати підтвердили, що він може бути використаний для створення недостовірних наративів. Схоже дослідження, яке дозволило дійти до того ж висновку, провели і представники національної громадської організації «Опора» [2].

Крім цього, через недосконалість роботи алгоритмів, цей чат може й «неумисно» вводити в оману. У даному випадку доречно згадати нещодавній випадок, коли один із популярних українських телеканалів вирішив за допомогою ChatGPT зробити добірку цікавих «маловідомих» фактів про українського письменника Олеса Гончара, проте які насправді виявилися фейковими. І хоча за своєю сутністю та через відсутністю умислу введення в оману даний приклад є саме поширенням помилкової інформації (misinformation), а не дезінформацією, він ще раз підтверджує загрозу хоча й не цілеспрямованого, проте ж введення людей в оману. Варто відзначити, що перед початком роботи з чатом, розробники попереджують користувачів про можливість недостовірності та «обмеженість» актуальності інформації, якою він (чат) оперує, проте, через недостатній рівень медіаграмотності населення, такі застереження не мають передбачуваного ефекту.

Узагальнюючи перелічені вище чинники, можна зазначити, що в сукупності використання технологій штучного інтелекту підвищує ефективність деструктивного інформаційного впливу та ускладнює процес його виявлення та протидії, що звісно не може не викликати занепокоєння.

Водночас, як було зазначено вище, використання технологій ШІ є інструментом не лише дезінформації, а й протидії та запобігання їй здійсненню. Так, наприклад, саме використання штучного інтелекту надає можливість:

- здійснювати моніторинг та аналіз великого масиву даних на предмет наявності шкідливого контенту, в тому числі недостовірної інформації та у деяких випадках автоматизовано блокувати її;
- виявляти основні «тренди» та тенденції інформаційно-психологічних впливів та реакцію суспільства на них;
- здійснювати експертизу інформації у різній формі вираження (текст, зображення, фото, відео) на предмет її достовірності. Так сьогодні є низка програм, які працюють на основі штучного інтелекту, та які дозволяють встановити факт створення контенту за допомогою технологій або ж наявність у ньому модифікацій;

- розпізнавати ботів та автоматизовану поведінку в мережі, а також блокувати її. Проте, варто зазначити, що алгоритми виявлення та блокування шкідливого контенту та «підозрілої» поведінки в мережі не є ефективними на 100 % та можуть помилково ідентифікувати активність як шкідливу, коли насправді вона такою не є. Це, в свою чергу, призводить не до захисту, а до порушення прав та законних інтересів людини, зокрема свободи слова. Особливо ця проблема стала актуальною сьогодні, коли саме робота алгоритмів соціальних мереж стала перешкодою у донесенні достовірної інформації про події в Україні.

Розглядаючи позитивні аспекти застосування ІІІ, варто зазначити, що технології, які побудовані на основі його використання, вже давно зарекомендували себе як ефективний засіб журналістики, високий рівень якої також є невід'ємним елементом системи протидії та запобігання дезінформації.

Узагальнюючи, можна зробити висновок, що використання технологій штучного інтелекту дозволяє оптимізувати та підвищити ефективність фактчекінгової діяльності та моніторингу інформаційного середовища з метою виявлення загроз.

Дезінформація, як й інші види інформаційно-психологічного впливу, не є ноу-хау ХХІ століття чи наслідком використання штучного інтелекту. Споконвіку люди використовували цей інструмент для досягнення різних цілей, а нові відкриття науки і техніки лише змінювали його форму.

Штучний інтелект не спричинив виникнення нового виду впливу, не змінив його сутність, а лише оптимізував та підвищив його ефективність, як і у той же час підвищив ефективність механізмів протидії та запобігання різним загрозам в інформаційному просторі, включаючи дезінформацію. Це вкотре підтверджує ідею, що технологія сама про собі немає ціннісного змісту, є нетральною та виступає лише інструментом, який слугує для задоволення цілей її користувачів» [3, 104]. Сьогодні не штучний інтелект, а людина, яка його створює й використовує, визначає напрям його застосування та відповідальна за конструктивні чи деструктивні наслідки його функціонування.

Список використаних джерел

1. Самчинська О.А. Дезінформація: поняття та сутність. *Адміністративне право і процес*. 2022. № 3(38). С. 32-45. DOI: <https://doi.org/10.17721/2227-796X.2022.3.03>.
2. Штучний інтелект як суперінструмент для дезінформації та пропаганди. URL: https://www.oporaua.org/blog/polit_ad/24507-shtuchnii-intelekt-iak-superinstrument-dlia-dezinformatsiyi-ta-propagandi (дата звернення: 25.04.2023).
3. Білоцерковець Н. Технологічна нейтральність та заборона дискримінації як ключові принципи державного регулювання електронних довірчих послуг: поняття та ознаки. *Підприємництво, господарство і право*. 2018. № 1. С. 103–109. URL: http://pgp-journal.kiev.ua/archive/2018/1/1_2018.pdf. (дата звернення: 26.04.2023).

ПРАВОВІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ПОШИРЕННЮ ІНФОРМАЦІЇ В УМОВАХ ВОЄННОГО СТАНУ

Сердечна А.Ю.,
ст. викладач кафедри кримінального права та кримінології
Національної академії Служби безпеки України

Інформаційна безпека України є складовою частиною національної безпеки України, стан захищеності державного суверенітету, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом. Про