УДК 316.77
DOI: 10.31733/2078-3566-2023-2-89-94

Олег ЛЕВІН©
кандидат історичних наук, доцент
(Дніпропетровський державний університет внутрішніх справ, м. Дніпро, Україна)

ВИКОРИСТАННЯ ФЕЙКОВИХ АКАУНТІВ ЯК ІНСТРУМЕНТУ ІПСО ПІД ЧАС УКРАЇНСЬКО-РОСІЙСЬКОЇ ВІЙНИ

Ця стаття присвячена відносно новому інструменту інформаційної війни проти України, а саме фейковим акаунтам та ботофермам як дієвому інструменту ІПСО під час повномасштабного вторгнення на нашу землю з боку росії, їхній загальній характеристиці та методам протидії цьому явищу на просторах мережі Інтернет. У дослідженні окреслено особливості утворення, впливу та роботи ботів і ботоферм, їхні ознаки та властивості, наведено приклади використання фейкової інформації, надано рекомендації щодо розпізнавання фейкових повідомлень та ресурсів. Звернено увагу на важливість боротьби з цим явищем, особливо коли наша країна веде героїчну боротьбу проти загарбників, які використовують всі види боротьби з нами: від збройної до інформаційної, використовуючи проти нас і недозволені прийоми.

Ключові слова: *ботоферми, фейкові акаунти, дезінформація, Інтернет-ресурси.*

Постановка проблеми. Глобалізація є найважливішою тенденцією сучасного світу, а в новому столітті ця тенденція стала визначальною для всієї галузі інформаційних технологій. Глобалізація інформаційного середовища та соціальних мереж призвела до безперервного розвитку різноманітних методів маніпулювання користувачами мережі Інтернет за допомогою мови, образів, звуків, способів та послідовності подачі матеріалів. Саме завдяки інформаційній силі мережі Інтернет нею стали користуватися різні політичні сили, щоб маніпулювати масами й розгортати курс країни в потрібному напрямі. Це дуже сподобалося російської владі.

Об'єкти маніпулювання дуже різні – від продажу товарів до інформаційної війни між державами. Так, понад дев'ять років росія, як країна-агресор, намагається дестабілізувати суспільну політику України, створюючи осередки напруги, щоб дискредитувати нашу державу, як усередині, так і на міжнародній арені, застосовуючи різноманітні методи ведення «гібридної війни», серед яких одним із найбільш дієвих є розповсюдження фейків у соціальних мережах, що з початком повномасштабного вторгнення у лютому 2022 року стали плацдармом для інформаційно-психологічного впливу на свої, ворожі та інші групи громадськості. Кількість фейків досягла рекордних результатів, їх розповсюджують більш ніж 250 сайтів, що не піддає сумніву актуальність обраної теми дослідження.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. З розповсюдженням такої практики соціальної дезінформаційної схеми дослідженням окремих її аспектів займалися такі наукові діячі, як: К. Молодецька [1], А. Марущак [2], С. Зелінський [3], О. Зінченко [4], М. Кіца [5], О. Курбан [6], та ін.

Метою статті є дослідження сучасної практики утворення фейкових акаунтів та ботоферм, окреслення їхньої загальної характеристики та методів протидії цьому явищу на просторах мережі Інтернет. Для досягнення поставленої мети було сформульовано такі завдання: ідентифікувати та розкрити соціальну природу ботів і ботоферм; визначити причини їх активного застосування; узагальнити правові засади протидії цьому явищу та його попередження.

Виклад основного матеріалу. Останньою тенденцією сучасності стало використання фейкових акаунтів, що керуються чат-ботами, призначеними для

© О. Левін, 2023
ORCID iD: https://orcid.org/0000-0003-3501-3509
docentagro55@gmail.com

повторення однотипних задач. Принагідно зазначимо, що в мережі Інтернет почали активно створювати так звані «ботоферми» – компаній, що модерують вигаданих користувачів із їхніми коментарями.

Пропаганда рф активно проводить ІПСО – інформаційно-психологічні операції, що спрямовані на вплив на настрої різних груп суспільства для досягнення певної мети з використанням пропаганди, дезінформації, приховування однієї інформації й роздмухування та перебільшення іншої. З такою проблемою зазвичай стикається населення, яке знаходиться на окупованій території, території країни-агресора, території країн ЄС, а також ті, хто знаходиться на підконтрольній території України. Представники спецслужб російської федерації, а також підконтрольні їм бойовики «ДНР/ЛНР» в останні роки активно користуються Інтернет-ресурсами (фейсбук, телеграм, вайбер, вконтакті, тікток, слек), створюючи вигаданих користувачів для поширення дезінформації, котра може призвести до суспільного резонансу за допомогою набутих фахових знань стосовно відповідних технічних та психологічних прийомів у процесі її підготовки та поширення. Це підсилюється також припиненням роботи українського зв'язку із застосуванням стільникових операторів на тимчасово окупованих територіях ДНР і ЛНР «Фенікс» та «Лугаком», що не підтримують зв'язок з українськими операторами, підтримуючи дзвінки та повідомлення за допомогою деяких Інтернет-сервісів. Однак роботу російських пропагандистів ускладнює відсутність електрики на більшій частині тимчасово окупованої території, а значить, і можливості приймати тут трансляцію російського телебачення.

Зазначимо, що дезінформації – це публічне поширення неперевіреної або визнаної неправдивою інформації, що може негативно вплинути на реалізацію конституційних прав громадян або загрожувати національній безпеці. Дезінформацію можна розглядати як процес (поширення) та його результат (різновид інформації, Завдяки якому набуває змісту словосполучення «поширення дезінформації»). Під фейком слід розуміти не тільки «жовту пресу», а й людей, які видають себе в Інтернеті за інших; фотографії, підроблені, змонтовані у відповідних програмах; несправжні сайти та / або сайти, підроблені під справжні («самозванці»); несправжні сторінки від імені відомих осіб тощо.

Слід зауважити, що боти – це програми, котрі керують фейковими обліковими записами в соцмережах. Ще так називають людей під фейковими акаунтами, які пишуть потрібні коментарі у потрібний час під потрібним постом. Класифікувати їх можна на такі групи:

1. Боти-одноденки – їхньою особливістю є незграбне створення облікових записів без фотографії профілю, лише з кількома друзями та порожньою або заповненою стрічкою. Зазвичай вони створюються автоматично за допомогою скриптів, знайдених у мережі Інтернет. Ці боти щодня виконують масу подібних дій, тому фейсбук може їх швидко знайти та заблокувати. Оскільки такі боти мають завдання доставляти повідомлення та зникати під впливом модераторів, творці спеціально не намагалися зробити їх схожими на реальних людей. Залежно від діяльності їхній цикл активності може варіюватися від одного дня до кількох місяців;

2. Класичні боти – відрізняються від ботів-одноденок тим, що мають обкладинки та фотографії профілю, проте фактично ніколи не використовують обличчя людей для цього. Такі облікові записи створюються більш просунутими версіями скриптів і лише подекуди – вручну. Краще заповнення сторінок може зробити такі облікові записи довше активними, ніж одноденні облікові записи;

3. Боти-іноземці – це акаунти з іноземними іменами, куплені за низькою ціною на іноземних «робофермах». Ціна товару обмежена. Загалом це досить поширена практика в багатьох країнах третього світу, де системи виробляються в промислових масштабах і коштують дешево. В іншому зовнішні характеристики такого бота повністю відповідають класичному роботу;

4. Боти нешаблонного прокачування – це робот, що поводиться як реальна людина. У таких акаунтах у стрічці використовуються різні типи публікацій, під якими стоять тільки лайки або коментарі. Переваги цих сторінок полягає в тому, що вони насправді мають вигляд немов сторінки реальних людей. Мінусом є те, що система не має чітко сегментованої аудиторії через розрізненість дописів;

5. Боти зі складною поведінкою – системи, створені складними програмами, що чітко імітують поведінку людей у соціальних мережах. З огляду на це вони не мають

підозр у фейсбук, оскільки існують невидимі алгоритми, що автоматично обчислюють спам-запити. Вони ретельно збирають і охороняють власних підписників. Згаданий тип цікавий і цінний тим, що за його допомогою клієнти можуть досягти реальних результатів. Ці машини здатні формувати або змінювати інформацію в соціальних мережах, впливати на думку звичайних людей, журналістів і політиків.

У свою чергу, під ботофермами слід розуміти місце роботи реальних людей, якими були створені фейкові акаунти в соціальних мережах, що використовуються для виконання певних завдань.

Слід зауважити, що ботоферми створюються за двома напрямами або призначені для виконання двох завдань:

1. Дезінформація, пропаганда, популяризація певних новин, наративів, поглядів та думок серед суспільства;

2. Генерація фейкового трафіка та «відкрутки» реклами на рекламних акаунтах бота у різних соцмережах для отримання заробітку.

Проаналізувавши цю проблему, ми виокремили основні причини створення фейкових сторінок під час військових дій в Україні: просування в соціальних мережах політичних парадигм та наративів; продукування бажаної суспільної думки маніпулятором; шахрайство з метою інвестування; завантаження ботами особистої інформації для проведення різних махінацій та можливого шантажу.

Задля дієвості фейкових сторінок зловмисники звичай використовують певні методи їх реалізації, а саме: розповсюдження великою кількістю користувачів інформації, аналогічної за змістом, протягом нетривалого проміжку часу; використання заголовків, що підвищують інтерес, наприклад, «термінова новина», «увага» тощо; наповнення більшої частини тексту, що поширюється, лінками на «псевдонаукові дослідження»; провокативне наповнення тексту; нав'язливе прохання про репости; поширення інформації з невідомих ресурсів або першоджерел зі сторінок вигаданих людей.

В Україні діє Центр протидії дезінформації при РНБО, що утворився 11 березня 2021 року. Метою цієї організації є проведення роботи у таких напрямах, як: військова сфера, боротьба зі злочинністю та корупцією, внутрішня та зовнішня політика, економіка, інфраструктура, екологія, охорона здоров'я, соціальна сфера, науково-технологічний напрям. Але основну увагу приділено протидії поширенню дезінформації у мережі Інтернет та медіа. Центр не має каральних функцій за дезінформацію і не може застосовувати санкції, але може вносити подання до РНБО щодо певних порушень [8]. Причому механізм законодавчої протидії цьому явищу відбувається за допомогою трьох рівнів, залежно від ступеня суспільної небезпечності поширення такої інформації:

1. Цивільно-правова відповідальність – передбачена Конституцією України (ч. 4 ст. 32) [7], Цивільним кодексом України (ст. 278) [8], Законом України «Про інформацію» [9] тощо;

2. Адміністративна відповідальність – передбачена Кодексом України про адміністративні правопорушення (ст. 173-1) [10];

3. Кримінальна відповідальність – передбачена Кримінальним кодексом (ст. ст. 109, 110, 250, ч. 2 ст. 361 та ін.) [11].

Так, наші правоохоронні органи активно працюють у напрямі ліквідації так званих ботоферм. Від початку повномасштабного вторгнення СБУ закрила таких 5, що налічували понад 100 000 фейкових акаунтів. Вони активно дезінформували населення Тернопільщини, Харківщини, Полтавщини, Черкащини та Закарпаття. Їх створювали на різних платформах, у тому числі тих, що поширюють ідеологію країни-агресора і є забороненими на території нашої держави. Під час обшуку представниками СБУ були виявлені: майже 100 комплектів GSM-шлюзів; майже 10 тис. сім-карток різних мобільних операторів, котрі використовувалися для маскування злочинної діяльності; чорна бухгалтерія; комп'ютерне обладнання з доказами протиправних дій. На основі вищезазначеного відкрили кримінальне провадження для притягнення винних до відповідальності, кваліфікація дій яких відбувається за ст. 110 Кримінального кодексу України (посягання на територіальну цілісність і недоторканність України), якою передбачено покарання у виді позбавлення волі до 15 років [12].

На такі протиправні дії відреагувала і світова спільнота, а саме корпорацією Meta (материнською організацією фейсбук, інстаграм, вотсап та окулус) були закриті російські та китайські фальшиві акаунти відомих ЗМІ з фейками про війну в Україні. Мова йде про розвинену мережу 60 сайтів рф, що видавали себе за платформи для поширення новин й

публікували інформацію за допомогою облікових записів вигаданих користувачів у фейсбук, телеграм, ютуб, твіттер, а інші сайти соціальних мереж розповсюджували її. Поширення фейкової інформації було спрямоване на такі країни, як Німеччина, Великобританія, Франція, Італія та Україна. Крім того, китайська мережа фальшивих акаунтів налічувала у фейсбук 80 акаунтів, одні з яких видавали себе за консервативних американців, а інші – за лібералів, які проживають у Флориді, Техасі та Каліфорнії. Цими акаунтами була поширена неправдива інформація про політичні переконання США (неправдивість виборів) та Чехію (дискредитація уряду стосовно зусиль щодо підтримки України у війні, котру розв'язала росія) [13].

З вищезазначеного випливає, що для кожної людини дуже важливо вміти розпізнавати фейкові акаунти та боротися з їх поширенням, як під час різних екстремальних ситуацій, так і у мирний час. Ми сформували низку правил, що спрямовані на виявлення таких акаунтів та протидію ним:

1. Зверніть увагу на фотографії профілю, адже зазвичай у фейкових облікових записах розміщені випадкові стокові фотокартки, тому зображення можна перевірити за допомогою функції «пошук картинки» в Google;

2. Однією з однак фейкового акаунта є наявність випадкових друзів та/або відсутність друзів за місцем проживання;

3. Перевірте регулярність розміщення публікацій;

4. Вивчіть особисту інформацію, що розміщена на сторінці в розділі «ABOUT» ;

4. Зверніть увагу на дату створення профілю;

5. Варто не додавати в друзі незнайомців або ж інших осіб із сумнівним наповненням облікового запису;

6. Якщо представники державних органів у соціальних мережах просять вас сплатити штраф чи пропонують платні послуги, зверніться на «гарячу лінію» та уточніть, чи дійсно вони пропонують громадянам послуги такого формату.

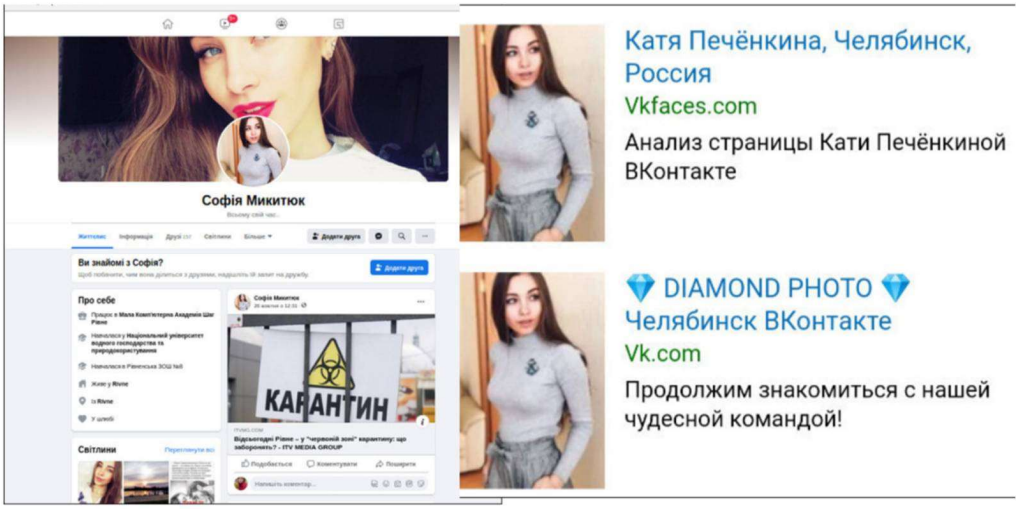

Рис. 1. Типовий фейковий обліковий запис російських пропагандистів

Висновки. Таким чином, на основі вищезазначеного можна дійти висновку, що створення фейкових акаунтів є дієвим методом поширення дезінформації на державному рівні та дискредитації міжнародного іміджу України, тому кожному з нас варто звертати увагу на це. Щодо чинного законодавства України, то воно є досить розгалуженим саме у сфері протидії розповсюдженню фейкової інформації і потребує удосконалення та приведення у відповідність до вимог сьогодення, а також до міжнародних стандартів. У будь-якому випадку боти та ботоферми не слід сприймати легковажно. Гроші, час, зусилля та інші ресурси, витрачені на його створення, на задум авторів фейків, повинно повернутися з користю для них і, відповідно, завдати втрат для нас.

Список використаних джерел

1. Молодецька К. В. Технологія виявлення організаційних ознак інформаційних операцій у соціальних інтернет-сервісах. *Проблеми інформаційних технологій.* 2016. № 2. С. 84–93. URL:

http://nbuv.gov.ua/UJRN/Pit_2016_2_12.

2. Марущак А. І. Міжнародно-правові підходи та національно-правове регулювання протидії дезінформації. *Інформаційна безпека людини, суспільства, держави*. Вип. 1–3(31–33). 2022. С. 64–71. URL: http://journals.uran.ua/ispss/article/view/260235.

3. Зелінський С. Дидактичні принципи особистісно орієнтованого навчання з використанням інформаційно-комунікаційних технологій. *Молодь і ринок.* 2015. № 6. С. 141–144. URL: http://nbuv.gov.ua/UJRN/Mir_2015_6_32.

4. Зінченко О. В. Мережеві фейки як психологічна проблема. URL: https://www.newlearning.org.ua/system/files/sites/default/files/zagruzheni/zinchenko_olexandr_2020.pdf.

5. Кіца М. О. Фейкова інформація в українських соціальних медіа: поняття, види, вплив на аудиторію. *Наукові записки Української академії друкарства.* 2016. № 1. С. 281–287. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nz_2016_1_37.

6. Курбан О. Фейки у сучасних медіа: ідентифікація та нейтралізація. *Бібліотекознавство. Документознавство. Інформологія.* 2018. № 3. С. 96–103. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=bdi_2018_3_15.

7. Конституція України від 28 червня 1996 року. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.

8. Цивільний кодекс України : Закон України від 16.01.2003. URL: https://zakon.rada.gov.ua/laws/main/435-15#Text.

9. Про інформацію : Закон України від 02.10.1992. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.

10. Кодекс України про адміністративні правопорушення : Закон України від 10.01.2002. *Відомості Верховної Ради України.* 1984. Додаток до № 51. Ст. 1122.

11. Кримінальний кодекс України : Закон України від 05.04.2001. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

12. З початку війни СБУ ліквідувала 5 ворожих ботоферм потужністю понад 100 тис. фейкових акаунтів. *Служба безпеки України.* URL: https://ssu.gov.ua/novyny/z-pochatku-viiny-sbu-likviduvala-5-vorozhykh-botoferm-potuzhnistiu-ponad-100-tys-feikovykh-akauntiv.

13. Meta закрила російські та китайські фальшиві акаунти відомих ЗМІ з фейками про війну в Україні. *Радіо Свобода.* URL: https://www.radiosvoboda.org/a/news-meta-feyky-viyna/32056257.html.

Надійшла до редакції 30.05.2023

References

1. Molodetska, K. V. (2016) Tekhnolohiia vyiavlennia orhanizatsiinykh oznak informatsiinykh operatsii u sotsialnykh internet-servisakh [Technology for identifying organisational features of information operations in social Internet services]. *Problemy informatsiinykh tekhnolohii*. № 2. pp. 84–93. URL: http://nbuv.gov.ua/UJRN/Pit_2016_2_12. [in Ukr.].

2. Marushchak, A. I. (2022) Mizhnarodno-pravovi pidkhody ta natsionalno-pravove rehuliuvannia protydii dezinformatsii [International legal approaches and national legal regulation of countering disinformation]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy.* Issue 1–3(31–33), pp. 64–71. URL: http://journals.uran.ua/ispss/article/view/260235. [in Ukr.].

3. Zelinskyi, S. (2015) Dydaktychni pryntsypy osobystisno oriientovanoho navchannia z vykorystanniam informatsiino-komunikatsiinykh tekhnolohii [Didactic principles of personality-oriented learning with the use of information and communication technologies]. *Molod i rynok.* № 6, pp. 141–144. URL: http://nbuv.gov.ua/UJRN/Mir_2015_6_32. [in Ukr.].

4. Zinchenko, O. V. Merezhevi feiky yak psykholohichna problema [Network fakes as a psychological problem]. URL: https://www.newlearning.org.ua/system/files/sites/default/files/zagruzheni/zinchenko_olexandr_2020.pdf. [in Ukr.].

5. Kitsa, M. O. (2016) Feikova informatsiia v ukrainskykh sotsialnykh media: poniattia, vydy, vplyv na audytoriiu [Fake information in Ukrainian social media: concept, types, impact on the audience]. *Naukovi zapysky Ukrainskoi akademii drukarstva.* № 1. pp. 281–287. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nz_2016_1_37. [in Ukr.].

6. Kurban, O. (2018) Feiky u suchasnykh media: identyfikatsiia ta neitralizatsiia [Fakes in modern media: identification and neutralisation]. *Bibliotekoznavstvo. Dokumentoznavstvo. Informolohiia.* № 3. pp. 96–103. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=bdi_2018_3_15. [in Ukr.].

7. Konstytutsiia Ukrainy [The Constitution of Ukraine] vid 28 chervnia 1996 roku. *Vidomosti Verkhovnoi Rady Ukrainy.* 1996. № 30. Art. 141. [in Ukr.].

8. Tsyvilnyi kodeks Ukrainy [Civil Code of Ukraine] : Zakon Ukrainy vid 16.01.2003. URL:

https://zakon.rada.gov.ua/laws/main/435-15#Text. [in Ukr.].

9. Pro informatsiiu [On information] : Zakon Ukrainy vid 02.10.1992. *Vidomosti Verkhovnoi Rady Ukrainy.* 1992. № 48. Art. 650. [in Ukr.].

10. Kodeks Ukrainy pro administratyvni pravoporushennia [Code of Ukraine on Administrative Offences] : Zakon Ukrainy vid 10.01.2002. *Vidomosti Verkhovnoi Rady Ukrainy.* 1984. Dodatok do № 51. Art. 1122. [in Ukr.].

11. Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine] : Zakon Ukrainy vid 05.04.2001. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. [in Ukr.].

12. Z pochatku viiny SBU likviduvala 5 vorozhykh botoferm potuzhnistiu ponad 100 tys. feikovykh akauntiv [Since the beginning of the war, the SSU has eliminated 5 enemy bot farms with a capacity of more than 100,000 fake accounts]. *Sluzhba bezpeky Ukrainy*. URL: https://ssu.gov.ua/novyny/z-pochatku-viiny-sbu-likviduvala-5-vorozhykh-botoferm-potuzhnistiu-ponad-100-tys-feikovykh-akauntiv. [in Ukr.].

13. Meta zakryla rosiiski ta kytaiski falshyvi akaunty vidomykh ZMI z feikamy pro viinu v Ukraini [Meta shut down russian and Chinese fake accounts of well-known media with fake news about the war in Ukraine]. *Radio Svoboda.* URL: https://www.radiosvoboda.org/a/news-meta-feyky-viyna/32056257.html. [in Ukr.].

ABSTRACT

Oleh Levin. The use of fake accounts as a tool of special information and psychological operation during the Ukrainian-russian war. The 21st century has been marked by new methods of information warfare. Manipulation of consciousness and influence on the thoughts and decisions of the population successfully support armed methods of warfare. A distorted and deliberately false portrayal of events affects their acceptance by the population and, as a consequence, sows doubt and mistrust in the victory in the war, generates aggression and hatred towards other nations and strengthens discrimination. At the same time, the information may be presented in such a way that those affected by the information influence will consider its consequences to be those caused by their own decisions, the only possible and correct ones.

Fake news (from the English word «fake») is false information that is purposely disseminated by interested parties who pursue their (usually political) goals or who want to earn money from Internet traffic.

This article is devoted to a relatively new tool of information warfare against Ukraine – fake accounts and bot farms, their general characteristics and methods of counteracting this phenomenon on the Internet as an effective tool of SIPO during russia's full-scale invasion of our land. The study regulates the peculiarities of the formation, impact and operation of bots and bot farms, their signs and properties, provides examples of the use of fake information, and provides recommendations for recognising fake messages and resources. Attention is drawn to the importance of combating this, especially when our country is waging a heroic struggle against the invaders who use all types of struggle against us: from armed to informational, using against us and not allowed methods.

Keywords: *bot farms, fake accounts, disinformation, Internet resources.*