



Slovak international scientific journal

№47, 2020

Slovak international scientific journal

VOL.3

The journal has a certificate of registration at the International Centre in Paris – ISSN 5782-5319.

The frequency of publication – 12 times per year.

Reception of articles in the journal – on the daily basis.

The output of journal is monthly scheduled.

Languages: all articles are published in the language of writing by the author.

The format of the journal is A4, coated paper, matte laminated cover.

Articles published in the journal have the status of international publication.

The Editorial Board of the journal:

Editor in chief – Boleslav Motko, Comenius University in Bratislava, Faculty of Management

The secretary of the journal – Milica Kovacova, The Pan-European University, Faculty of Informatics

- Lucia Janicka – Slovak University of Technology in Bratislava
- Stanislav Čerňák – The Plant Production Research Center Piešťany
- Miroslav Výtisk – Slovak University of Agriculture Nitra
- Dušan Igaz – Slovak University of Agriculture
- Terézia Mészárossová – Matej Bel University
- Peter Masaryk – University of Rzeszów
- Filip Kocisov – Institute of Political Science
- Andrej Bujalski – Technical University of Košice
- Jaroslav Kovac – University of SS. Cyril and Methodius in Trnava
- Paweł Miklo – Technical University Bratislava
- Jozef Molnár – The Slovak University of Technology in Bratislava
- Tomajko Milaslavski – Slovak University of Agriculture
- Natália Jurková – Univerzita Komenského v Bratislave
- Jan Adamczyk – Institute of state and law AS CR
- Boris Belier – Univerzita Komenského v Bratislave
- Stefan Fišan – Comenius University
- Terézia Majercakova – Central European University

1000 copies

Slovak international scientific journal

Partizanska, 1248/2

Bratislava, Slovakia 811 03

email: info@sis-journal.com

site: <http://sis-journal.com>

CONTENT

ECONOMY

Kozachenko A. FEATURES OF ACCOUNTING VALUATION OF RECEIVABLES OF THE ENTERPRISE	3	Tokarchuk D., Prishlyak N., Palamarenko Y. METHODOLOGY FOR CALCULATING THE ECONOMIC EFFICIENCY OF WASTE USE FOR THE PRODUCTION OF BIOFUELS IN COMPARISON WITH THEIR TRADITIONAL USE	24
Pasemko G., Porokhniak N., Besedina G. NATURE AND CHARACTERISTICS OF INTELLECTUAL CAPITAL AS AN ECONOMIC PHENOMENON	10	Khaietska O. THE ROLE OF INNOVATION IN THE DEVELOPMENT OF ORGANIC PRODUCTION	34
Bairachna O. EFFICIENCY OF INTEGRATING FUNCTIONAL TRAINING TOOLS INTO ENTERPRISE PERSONNEL MANAGEMENT.....	15	Shevchuk H. CURRENT STATE OF THE FRUIT AND VEGETABLE INDUSTRY AND OVERCOMING THE COVID-19 PANDEMIC CONSEQUENCES	41

SOCIAL COMMUNICATION STUDIES

Kurban O. THE SPECIFICS OF THE CREATION AND OPERATION OF ILLEGAL LOCAL SOCIAL ONLINE NETWORKS	45
--	----

STATE AND LAW

Zyleva E. CONCEPT, ESSENCE AND SIGNIFICANCE OF VERIFICATION BY THE PROSECUTOR OF COMPLIANCE WITH THE REQUIREMENTS OF THE LAW IN THE PRETRIAL STAGES OF THE	52	Prokopiev R. LEGAL FEATURES OF THE CLUSTER APPROACH FOR FORMATION OF THE SYSTEM OF RAILWAY TRANSPORT ENTERPRISES.....	63
Malanchiy M. DIRECTIONS OF REFORM OF THE PERSONNEL MANAGEMENT SYSTEM OF THE STATE BORDER GUARD SERVICE OF UKRAINE.....	55	Serdiuk O., Myrna O., Sytnyk A., Myrnyi M. DEVELOPMENT OF E-DEMOCRACY IN THE UNITED TERRITORIAL COMMUNITIES OF UKRAINE.....	67
Ostapenko Y. EXPANSION OF THE SUBJECT OF ECONOMIC LAW (ON THE EXAMPLE OF THE SPHERE OF COMMERCIALIZATION OF PHYSICAL CULTURAL OR PHYSICAL AND HEALTH ACTIVITY).....	59		

SOCIAL COMMUNICATION STUDIES

СПЕЦИФІКА СТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ НЕЛЕГАЛЬНИХ ЛОКАЛЬНИХ СОЦІАЛЬНИХ ОН-ЛАЙН МЕРЕЖ

Курбан О.В.

кандидат наук із соціальних комунікацій, доцент

Доцент кафедри реклами та зв'язків з громадськістю Інституту журналістики Київського університету імені Бориса Грінченка

Доцент кафедри військової журналістики Військового інституту Київського національного університету імені Тараса Шевченка

Докторант кафедри журналістики Філологічного факультету Харківського національного університету імені Василя Каразина

THE SPECIFICS OF THE CREATION AND OPERATION OF ILLEGAL LOCAL SOCIAL ONLINE NETWORKS

Kurban O.

PhD in Social Communications, Associate Professor

*Associate Professor of Advertising and Public Relations Department ,
Institute of Journalism of Kyiv Borys Hrinchenko University*

*Associate Professor of Military Journalism Department,
of Military Institute of Kyiv Taras Shevchenko National University*

*Doctoral student of the Department of Journalism,
Faculty of Philology, Kharkiv Vasyl Karazin National University*

Анотація

Стаття присвячена аналізу ситуації із використанням нелегальних локальних соціальних он-лайн мереж (ботоферм), при здійсненні управління інформаційними процесами у глобальних соціальних он-лайн-мережах. Аналізується поточна ситуація із використанням різноманітних незаконних прийомів та засобів роботи із контентом. Пропонується визначення змісту та сутності поняття «ботоферма», яке поступово переходить з площини сленгових професійних термінів у науково-дослідницьку сферу. Також представлена типологія та класифікація сучасних ботоферм, які використовують для просування комерційних проєктів а також в рамках інформаційних війн. Проведено аналіз інноваційних інтернет-технологій web 2.0 та 3.0, які використовуються для управління ботофермами. Наведено практичні приклади функціонування типових ботоферм. Представлено рекомендації щодо подальшого наукового та прикладного дослідження та протидії нелегальним локальним соціальним он-лайн мережам.

Abstract

The article is devoted to the analysis of the situation with the use of illegal local social online networks (bot farms), when managing information processes in global social online networks. The current one is analyzed in the context of the use of various illegal techniques and means of working with content. The definition of the content and essence of the concept of "bot farm" is proposed, which is gradually moving from the plane of slang professional terms to the research area. It also presents a typology and classification of modern bot farms, which are used to promote commercial projects as well as in the framework of information wars. The analysis of innovative Internet technologies web 2.0 and 3.0, which are used to manage bot farms, is carried out. Practical examples of the functioning of typical bot farms are given. Recommendations for further theoretical and practical research and counteraction to illegal local social online networks are presented.

Ключові слова: соціальні он-лайн мережі, ботоферма, управління інформаційними процесами, таргетинг.

Keywords: social online networks, bot farm, information process management, targeting.

Актуальність. Народження та поширення мережі Інтернет у форматі web 1.0 призвело до значного прискорення процесів глобалізації сучасного світу у планетарному масштабі. Із появою інтернет-технології наступного покоління, а саме web 2.0 – соціальних онлайн-мереж – серед користувачів глобальної інформаційної мережі відбулася широко-масштабна персоніфікація, яка розширила можливості кожної конкретної людини. Але разом із можливостями з'явилися й небезпеки. Сьогодні, створюючи свої персональні сторінки в соціальних онлайн-мережах, людина наражається на низку

серйозних проблем, серед яких однією з найважливіших є небезпека стати жертвою психологічних маніпуляцій через споживання недоброякісного контенту. Особливо важливу роль у цих процесах відіграє діяльність локальних субмереж персональних акаунтів, які професійною мовою визначаються як «ферми ботів» або «ботоферми».

В науковій літературі, питання визначення терміну «ботоферма», ще не опрацьовано в достатній мірі, й він має більше вигляд професійного сленгового поняття. На нашу думку, типову ботоферму, можна визначити, як локальне (субмережа)

мережеве об'єднання фейкових (фальшивих) персональних акаунтів на тлі глобальних соціальних мереж, що діє із порушенням етичних норм поведінки користувачів та принципів управління інформаційними процесами.

Етичні норми як засіб регулювання взаємовідносин у соціальних онлайн-мережах є важливим чинником та основою для самоорганізації легальних об'єднань акаунтів реальних користувачів. Ці норми є відносно простими і зрозумілими та спираються на загальнолюдські принципи. Наприклад, адміністрація соціальної онлайн-мережі Facebook серед своїх основних пріоритетів у комунікаціях акцентує такі: достовірність, безпека, конфіденційність, гідність [7]. Дотримання таких стандартів, на думку засновників мережі, має дати можливість понад 2 млрд. осіб «вільно самовиражатися десятками мов у різних країнах і культурних середовищах» [7].

Натомість діяльність ботоферм зазвичай спрямована на те, щоб позбавити пересічних користувачів зазначених вище прав та можливостей і нав'язати їм певні наративи комерційного, політичного або суспільного характеру. Це ставить такі утворення поза етичними нормами онлайн-мережі та дає адміністраторам підстави переслідувати порушників на своїх майданчиках і підключати правоохоронні структури до вирішення ситуацій, в яких мали місце порушення.

Представлені вище аспекти потребують ретельного теоретико-методологічного дослідження з визначенням соціальної природи цього явища для формування дієвих інструментів і засобів протидії таким технологіям.

Мета статті. Розкрити специфіку та особливості функціонування типових ботоферм, в контексті загально-теоретичних наукових питань, а також, визначити основні напрямки роботи із боротьби з цим явищем.

Завдання статті:

- представити історіографічні аспекти дослідження проблеми боротьби із нелегальними локальними соціальними онлайн-субмережами;
- розкрити типову структуру та принципи управління ботофермами;
- подати пропозиції із протидії нелегальним ботофермам.

Рівень розробленості теми. На сьогодні проблема функціонування нелегальних соціальних онлайн-субмереж (ботоферм) у науковій площині майже не досліджена. Переважна більшість розробок у цьому напрямку має суто практичний характер. При тому у відкритому доступі є лише дані, що надаються громадськими структурами та окремими експертами, які не є представниками державних органів влади. Діяльність профільних державних структур у цьому напрямку здебільшого не стає предметом для публічної дискусії.

Серйозність визначеної проблеми в останні роки підтверджують провідні європейські фахівці. Зокрема, експерти компанії Safe Guard Cyber встановили, що з боку РФ проти інформаційного поля ЄС діє близько 6,7 тис. фейкових акаунтів (тролів

та ботів), які можуть охопити близько 241 млн. користувачів [11].

Нідерландські експерти Роберт ван де Ноордаа та Коен ван де Вен, дослідивши за допомогою програми Pyton близько 9 млн. твітів на тему MH17, створили власну дослідницьку базу російських ботоферм [9].

Системну роботу із виявлення та протидії нелегальним субмережам на тлі глобальних соціальних онлайн-мереж здійснюють і їх адміністрації. Зокрема, у період із жовтня 2018 р. по березень 2019 р., за повідомленням компанії Facebook, вона виявила та ліквідувала 3 млрд. фейкових акаунтів. На думку експертів Facebook, з 2,4 млрд. активних користувачів цієї соцмережі близько 5% складають саме фейкові акаунти [8; 10].

В Україні на недержавному рівні цими питаннями наразі опікуються переважно волонтерські проекти та окремі експерти, серед яких «StopFake», «InformNapalm», «Інформаційний спротив». Також ця проблематика висвітлюється у статтях журналістів у провідних українських ЗМІ.

Наукова новизна дослідження полягає в тому, що це одне з перших теоретико-методологічних досліджень проблеми функціонування локальних нелегальних субмереж фейкових акаунтів (ботоферм) у глобальних соціальних онлайн-мережах. Питання розглядається в контексті використання трьох типів інноваційних технологій – цифрових, гуманітарних та психотехнологій, – які інтегруються з метою формування ефективних алгоритмів управління інформаційно-комунікаційними процесами.

Основна частина.

Основним змістом діяльності ботоферм є розбудова ефективної соціальної комунікації, що формується за допомогою низки управлінських (гуманітарних) технологій. Саме соціальна комунікація є тією основою, навколо якої розбудовуються алгоритми управління інформаційними потоками в соціальних мережах. Типовими ознаками соціальної комунікації є [4, с. 29]:

- антропологічність – міжособистісне спілкування представників цільової аудиторії;
- соціальність – учасники комунікації переслідують певні цілі або інтереси;
- кодування – застосовуються визнані символи, образи, знаки;
- процесуальність – зміна змісту комунікації в процесі спілкування.

Саме ці ознаки визначають специфіку функціонування та використання управлінських інструментів та прийомів, які є в арсеналі тих, хто керує ботофермами.

Серед психотехнологій, які зазвичай використовуються в роботі ботоферм, то тут частіш за все фігурує маніпуляція, що базується на елементах нейролінгвістичного програмування (НЛП) або окремих прийомів та засобів психологічного впливу. За своєю сутністю ці методи не є апіорі поганими, але те, як їх використовують, дозволяє вести мову про них як про інформаційну зброю, особливо коли йдеться про роботу ботоферм. На

думку українського фахівця із НЛП В. Зеленіна, «Фактично нейролінгвістичне програмування не є зброєю. Але його вже давно використовують, як зброю масового впливу в інформаційно-пропагандистських війнах фактично в усьому світі» [1, с. 15].

Важливим складником розбудови комунікаційних процесів у форматі діяльності ботоферм є інтернет-лінгвістика як інтегроване явище, що узагальнює правила та принципи цифрових технологій, психотехнологій та гуманітарних технологій. На думку Л. Компанцевої, об'єктом інтернет-лінгвістики є комунікативна взаємодія в мережі інтернет, а предметом – організація інтернет-комунікації [3, с. 21].

Для управління діями таких незаконних локальних мережових структур, як ботоферми зазвичай використовуються специфічні методи автоматизованого (програмно-апаратного) або ручного керування.

Автоматизоване управління ботофермами передбачає використання алгоритмів інтернет-технологій формату web 3.0. Це означає застосування таких легальних програмних засобів (послуг, що надаються адміністраторами соцмереж), як:

- автоматизований таргетинг (он-лайн сервіс поширення контенту);
- пошукова оптимізація (автоматизована система просування сайту на основі його семантичного ядра);
- чат-боти (он-лайн сервіси комунікації із користувачами);
- програмні додатки (ігри, сервіси із оплати, он-лайн карти та ін.).

Поруч із легальним програмним забезпеченням, яке використовується для управління інформаційними процесами в соцмережах, адміністратори ботоферм використовують й нелегальні програми. Серед таких:

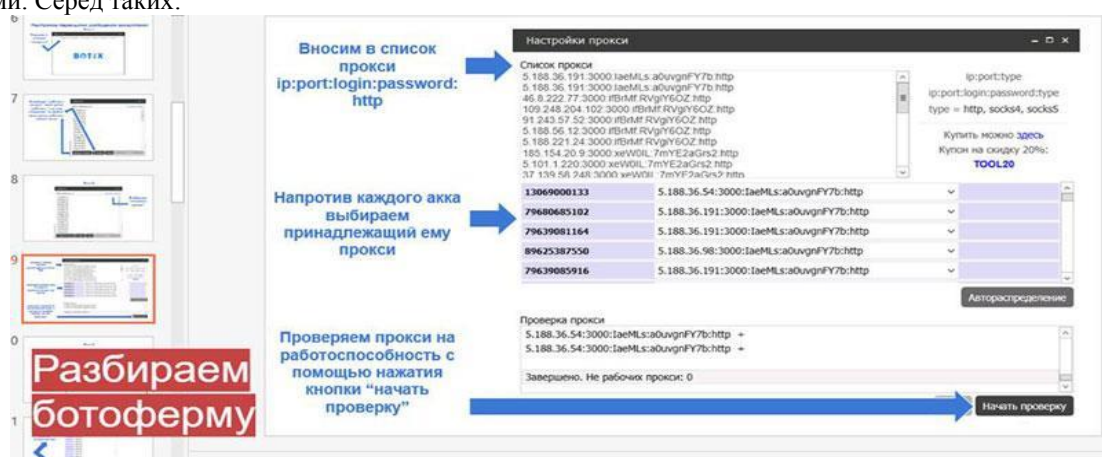
- мережеві віруси (програми для зламу та проникнення на акаунти, рекламні кабінети та он-лайн-кабінети управління сайтами);

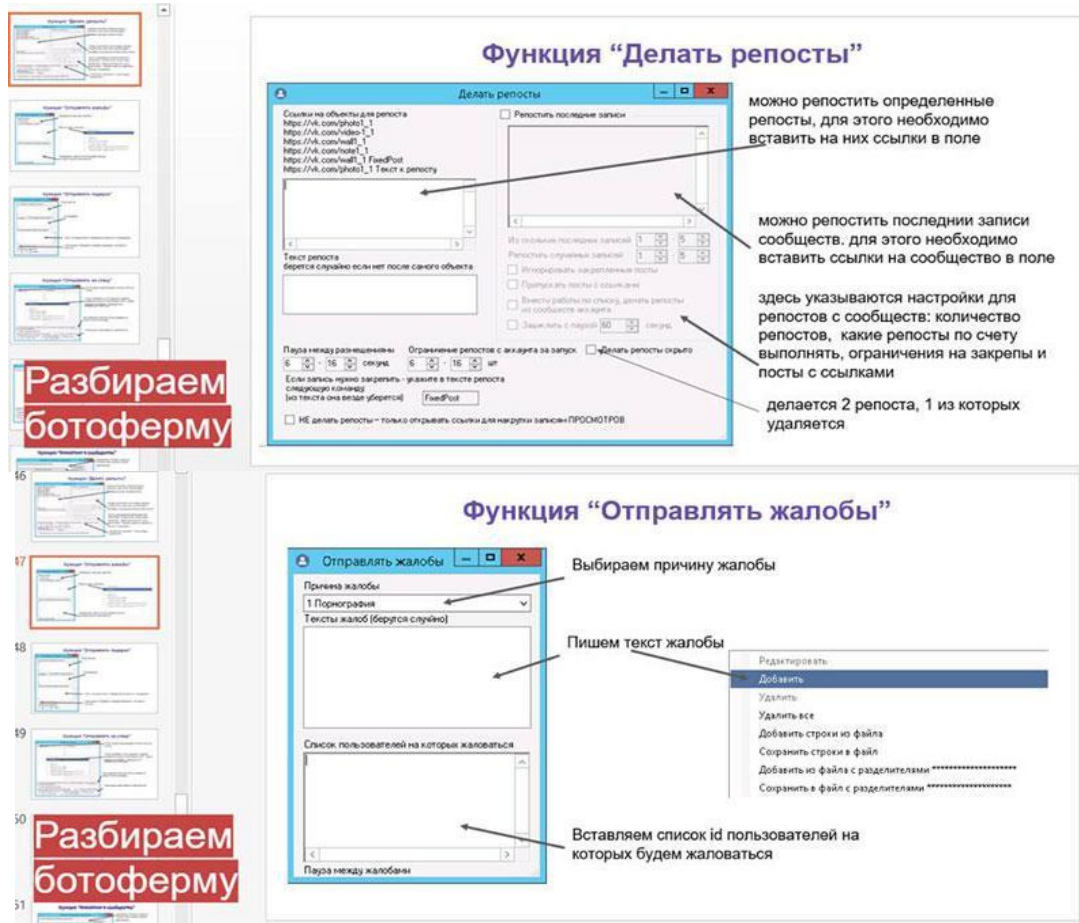
- www-боти (програми автоматизованого управління акаунтами).

Глобальні соціальні онлайн-мережі мають достатньо програмно-апаратних засобів для відстеження фактів використання чужорідного програмного забезпечення, яке заходить до їх мережевого простору. Втім, мережеві шахраї постійно вдосконалюють інструменти та підходи, тому сьогодні у світі не існує соцмереж, абсолютно захищених від автоматизованих ботоферм.

Автоматизовані інструменти управління використовуються тільки великими ботофермами, в яких на одного працівника припадає управління більш ніж 30–40 фейковими акаунтами. Для контролю та управління процесами у таких структурах, доволі часто створюються індивідуальні програми. Прикладом є представлена на мал. 1 схема роботи однієї з українських ботоферм, виявлена експертом компанії DATAS Technology Є. Папишевим і прокоментована у статті О. Карпенко «Як виглядає з середини робота ботоферми» [2].

Оцінюючи роботу програми управління ботофермою, Є. Папишев зазначає, що у її адміністраторів «...детально налагоджені процеси роботи та обліку, звітності, налаштована інфраструктура і спеціалізований софт. Вони управляють своїм ресурсом, постійно актуалізують його і оперативно перемикають на виконання різних завдань. Вони займаються навчанням своїх співробітників. Вони можуть реєструвати сотні акаунтів, створювати пости, лайкати, репостити, скаржитися на інші акаунти, писати в співтовариства, змінювати інформацію в своїх профілях, і все це – масово, всього за кілька кліків» [Цит. за: 2].





Мал. 1. Робочі вікна програми управління ботофермами (схема С. Папишева, за статтею О. Карпенко) [2]

Одним зі шляхів легального використання сторонніх програм автоматизованого управління великою кількістю акаунтів, сторінок та груп у соцмережах є спеціалізовані онлайн-сервіси моніторингу та постингу. Найбільш відомі з них та найбільш популярні сьогодні, це:

- «Buffer reply» – сервіс моніторингу та підтримки контактів із фоловерами у Twitter, Facebook и Instagram;
- «Zoho social» – моніторинг, планування та розміщення постів у Twitter, Facebook, Instagram, LinkedIn, Google+;
- «Sendible» – сервіс управління локальними субмережами акаунтів, сторінок та груп у Facebook, Twitter, Instagram, YouTube, Google+;
- «Falcon.io» – сервіс управління мережевими проектами у Twitter, Facebook, Instagram, LinkedIn, Google+ и YouTube.

Зазначені вище онлайн сервіси мають офіційні угоди із адміністраціями глобальних соціальних онлайн-мереж, що дозволяє їх користувачам створювати відповідні майданчики управління локальними субмережами акаунтів, сторінок та груп. Як свідчить практика, типові ботоферми не часто користуються послугами таких онлайн-сервісів, бо там робота відбувається прозоро, а всі форми порушення унеможливаються через численні програмні запобіжники. Фактично, використовуючи такі системи, ботоферми потрапляють під подвійний фільтр – онлайн-сервісу та соціальної мережі, в

якій вони працюють.

Зазначені вище чинники є однією з вагомих підстав для того, що управління ботофермами сьогодні здебільшого здійснюється в ручному форматі. При такому підході залучається значно більша кількість людей, відбувається розподіл на три виконавчі групи, що відповідають за моніторинг, виробництво та поширення контенту. Найбільшою групою є саме поширювачі контенту, блогери, яких професійною мовою ботоферми називають «тролями» (від англ. trolling). Саме вони поширюють пости, пишуть коментарі, атакують конкурентів (шляхом тролінгу та адресних скарг).

Управління діями функціональних груп назначених ботоферм здійснюється через чати, месенджери або закриті групи. Структура та принципи взаємодії підрозділів ботоферми моделюється залежно від завдання. Основними об'єктами спрямування зусиль є: окремі організації (комерційні, політичні, громадські), персоналії (політики, бізнесмени, поп-зірки, громадські діячі), території (країни, регіони), події (політичні, громадські, комерційні).

В переважній більшості випадків поняття «ботоферма», «тролінг», «троль», «бот» асоціюються із негативними аспектами активності в соціальних онлайн-мережах. Втім, в якості альтернативного руху, спрямованого на поширення позитивної інформації, існують так звані мережеві ельфи, а цей рух має назву ельфінг. За визначенням, ельфінг – це

інтернет-комунікація, різновид тролінгу, поширення позитивної та правдивої інформації [6]. Вперше цей термін почали використовувати у онлайн-мережових іграх в стилі фентезі ще на початку 2000-х років. Втім, у зв'язку із початком широкої інформаційної агресії з боку РФ проти її геополітичних опонентів, під ельфами стали розуміти борців із російськими тролями. У 2014 році саме під цим брандом розгорнули свою діяльність литовські інтернет-активісти [5].

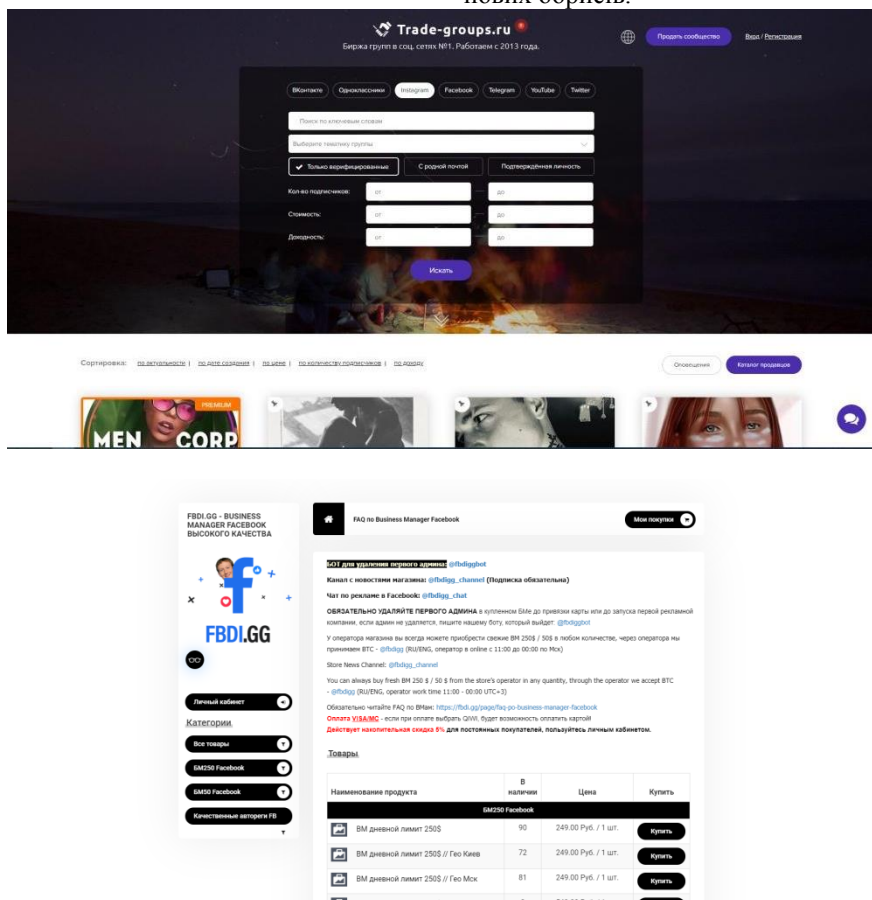
Аналізуючи питання структури та системи управління ботофермами неможна оминати увагою механізми формування таких локальних субмереж. Одним із основних питань у цих процесах є формування бази фейкових акаунтів, що здійснюватимуть основну роботу із поширення контенту. Є два основних шляхи – офіційна реєстрація нових із прив'язкою до легальної Sim-картки та купівля на спеціалізованих онлайн-майданчиках.

У першому варіанті процедура не складна, але вимагає певного часу для підготовки фейкового акаунту до роботи. Зазвичай перед тим, як створені таким чином акаунти починають працювати, їх розвивають, або, професійною мовою, «прокачують». Створюють певну історію особи, яку акаунт представляє. Це передбачає створення щонайменше кількох фотоальбомів, підписку на нейтральні групи та сторінки, підбирання адекватного фото на

заставку (аватарку) та імені (нікнейм). Також протягом певного часу та вже в процесі роботи фейковий акаунт потрібно наповнювати нейтральними постами та спілкуванням у месенджері. Таке «олюднення» фейкового акаунту здійснюють для того, щоб не потрапити під фільтри соцмереж, які мають власні алгоритми розпізнавання фейкових акаунтів.

Другий шлях є простішим, але більш затратним. Він передбачає звернення до послуг різноманітних онлайн-майданчиків, на яких можна здійснити купівлю вже зареєстрованих акаунтів. Відповідно до запиту покупця, адміністратори таких інтернет-магазинів можуть запропонувати як новостворені акаунти, так і акаунти з історією. Вартість одного акаунту залежить від кількості підписників, історії, наявності попереджень та блокувань з боку адміністрації соцмереж (мал. 2).

Типологізування ботоферм є доволі складним завданням, бо закони їх функціонування є доволі гнучкими і непередбачуваними. Краще всього для їх аналізу використовувати алгоритми ройового інтелекту, але це тема окремого дослідження і навіть низки спеціалізованих досліджень. Структура будь-якої ботоферми формується під конкретні завдання, які необхідно вирішувати. Відповідно зі змінами завдань або ситуації структура ботоферми змінюється та набуває принципово нових обрисів.



Мал. 2. Онлайн-сервіси із продажу акаунтів (скріншоти)

За видами ботоферми можна поділити на три варіанти – корпоративні, агентські та персональні. Перший варіант реалізується, коли організація самотужки формує команду, яка створює та керує локальною субмережею акаунтів, сторінок та груп із метою супроводження діяльності організації у онлайн середовищі її цільових груп. Другий варіант передбачає собою певний центр (SMM-агенцію) із надання послуг супроводження проектів або виконання окремих завдань замовника в соціальних онлайн-мережах. Третій варіант подекуди близький до корпоративного з тією різницею, що виконавцем є досвідчений блогер, який просуває власні проекти або надає послуги під замовлення.

За типами (розмірами) досить умовно ботоферми можна поділити на три варіанти – великі, середні та малі.

Великі ботоферми зазвичай налічують від однієї і до десятків, а іноді й сотень тисяч акаунтів. Вони керуються за допомогою автоматизованих систем управління, мають чітку внутрішню структуру із прив'язкою акаунтів до конкретних сторінок або груп та каналів, а також формування тролінгових команд. Кількість обслуговуючого персоналу може складати кілька десятків фахівців.

Середні ботоферми можуть мати у своєму складі до кількох сотень акаунтів та кількох десятків сторінок і груп. Їх робота достатньо легко координується в ручному форматі, за наявності достатньої кількості персоналу, що може складати в межах 10-15 осіб.

Малі ботоферми керуються у ручному режимі й потребують мінімальної кількості персоналу (1-3 особи). Загальна кількість робочих одиниць складає до сотні фейкових акаунтів, кілька сторінок та груп.

Види та типи ботоферм чітко корелюються між собою. Корпоративні ботоферми можуть бути трьох видів – великі, середні, малі. Агентські, зазвичай бувають великими та середніми. А персональні, за типами, зазвичай є середні та малі.

Як уже зазначалося вище, локальні субмережі на тлі глобальних соціальних онлайн-мереж є, по суті, нелегальним засобом досягнення комунікаційного ефекту, який порушує певні етичні норми, які декларуються адміністраціями соцмереж. Проте однозначно визначити це явище як негативне не можна, бо учасники цих процесів можуть ставити перед собою як негативні, так і позитивні цілі. Це означає, що до питання боротьби із тролінгом та ботофермами потрібно підходити більш системно. Заборона як засіб регулювання в цьому випадку не є абсолютно доцільною, бо на кожну дію завжди знайдеться контрдія. Найбільш ефективним є контроль за дотриманням етичних норм та правил поведінки користувачів, а також моніторинг щодо використання стороннього програмного забезпечення.

Для здійснення контролю над інформаційними процесами у глобальних соціальних онлайн-мережах необхідно залучати інструменти аналізу та управління інформаційними процесами інтернет-технологій формату web 3.0. Це стосується в першу

чергу автоматизованих систем пошуку та моніторингу контенту, які базуються на алгоритмах штучних нейронних мереж та ройового інтелекту. Також важливим аспектом боротьби із негативними наслідками функціонування ботоферм є широке залучення до співпраці різних груп інтернет-громадськості. В першу чергу мова йде про блогерів, які є лідерами громадської думки та засновниками різноманітних трендів.

Висновок. Підбиваючи підсумки проведеного дослідження функціонування нелегальних локальних соціальних субмереж, маємо зазначити, що сьогодні вони є однією з найважливіших проблем і небезпек для користувачів інтернет-середовища. Порушуючи морально-етичні норми спілкування, такі структури нав'язують конкретні наративи та меседжі, які вигідні замовникам або власникам. Порушуючи цілісність національного інформаційного поля, вони також перетворюються в ситуації інформаційної війни на фактор національної безпеки і таким чином стають серйозним викликом для держави та суспільства.

Аналіз ситуації дає підстави типологізувати ботоферми за кількома критеріями. За тематичною спрямованістю ботоферми є корпоративні, агентські та персональні (якісні показники). За розмірами – великі, середні та малі ботоферми (кількісні показники). Залежно від цих параметрів ботоферми можуть керуватися в автоматизованому або ручному режимі.

Масовість та кількісні показники цього явища свідчать про те, що проблема потребує комплексного вирішення із залученням зусиль та ресурсів держав, міжнародних організацій та суспільних інституцій.

Зважаючи на те, що засновники ботоферм користуються найсучаснішими розробками у сфері цифрових, управлінських та психотехнологій, програми боротьби з цим явищем мають також містити інтегровані рішення, зокрема пов'язані зі створенням відповідного програмного забезпечення та механізмів суспільного контролю.

Список літератури

1. Зеленін В. В. По той бік правди: нейролінгвістичне програмування, як зброя інформаційно-пропагандистської війни / В. Зеленін. – Вінниця : ТОВ «Віндрук», 2014. – 348 с.
2. Карпенко О. Как выглядит изнутри работа ботофермы [Електронний ресурс] / О. Карпенко // AIN.UA. – Режим доступу : <https://ain.ua/2018/11/20/rabota-botofermy/> (дата звернення: 08.10.2020)
3. Компанцева Л. Ф. Лінгвістична експертиза соціальних мереж: підручник / Л. Ф. Компанцева. – Київ : Аграр Медіа Груп, 2018. – 318 с.
4. Коник Д. Стратегічні комунікації : посібник для державних службовців / Д. Коник. – Київ : ТОВ «Обнова компанії», 2016. – 256 с.
5. Малинка В. Ботоферми, тролі, фейки: як виявити і протидіяти [Електронний ресурс] / В. Малинка // Media Sapiens. – Режим доступу : <https://ms.detector.media/maister->

klas/post/22388/2019-01-31-botofermi-troli-feiki-yak-viyaviti-i-protidiyati/ (дата звернення: 10.10.2020)

6. Подосокорский Н. Эффективный эльфинг [Електронне джерело] / Н. Подосокорский // Green. - Режим доступу : <https://blog.greensmm.ru/?p=755>.

7. Стандарти спільноти [Електронний ресурс] // Facebook. - Режим доступу : <https://www.facebook.com/communitystandards/> (дата звернення: 18.11.2020)

8. An Update on How We Are Doing At Enforcing Our Community Standards [Електронний ресурс] // FACEBOOK. - Режим доступу : <https://about.fb.com/news/2019/05/enforcing-our-community-standards-3/> (дата звернення: 15.10.2020)

9. Robert van der Noordaa, Coen van de Ven Ное Russische trollen inspelen op westerse angsten [Електронний ресурс] // De Groene Amsterdamer. -

Режим доступу : <https://www.groene.nl/artikel/hoe-russische-trollen-inspelen-op-westerse-angsten> (дата звернення: 08.10.2020)

10. Facebook видалила понад три мільярди фейкових акаунтів за пів року [Електронний ресурс] // Media Sapiens. - Режим доступу : <https://ms.detector.media/sots-merezhi/post/22934/2019-05-24-facebook-vidalila-ponad-tri-milyardi-feikovikh-akauntiv-za-piv-roku/> (дата звернення: 08.10.2020)

11. 241m Europeans 'may have received Russian-linked disinformation' [Електронний ресурс] // The Guardian. - Режим доступу : <https://www.theguardian.com/world/2019/may/08/241m-europeans-may-have-received-russian-linked-disinformation> (дата звернення: 08.10.2020)