УДК 316.6:659.9]:004.7 (043.3)

ПРИЙОМИ ТА ЗАСОБИ ПРИХОВАННЯ Й ІДЕНТИФІКАЦІЇ АВТОРСТВА АКАУНТІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

О. В. Курбан

Київський університет імені Бориса Грінченка,
вул. М. Тимошенка, 13-Б, Київ, 02000

Досліджено питання маскування та демаскування персональних акаунтів у соціальних мережах, можливості та особливості реалізації цих завдань у форматах web 2.0 та web 3.0. Розглянуто механізм використання чужих інформаційних ресурсів через вербування їх та залучення до співпраці у прихованому та відкритому варіанті. На думку автора, в перспективі зазначені концептуальні аспекти мають бути адаптовані до ключових інформаційних процесів онлайн-середовища й активно застосовуватися під час розбудови національної системи інформаційної безпеки.

Ключові слова: *інтернет-технології, соціальні мережі, персональні акаунти.*

Постановка проблеми. Вже давно назріла потреба в науковому дослідженні комунікаційних принципів, психологічних механізмів і практичних інструментів роботи з авторськими й анонімними (фейковими) персональними сторінками (акаунтами) у соціальних мережах. Ці питання особливого значення набувають сьогодні, в контексті інформаційно-комунікаційних протистоянь, що відбуваються на міжнародному, політичному та корпоративному рівнях.

Аналіз останніх досліджень та публікацій. Вивчення практики маскування та демаскування персональних акаунтів у соціальних мережах є принципово новим питанням для профільних галузей наукового дослідження. Власне наукових розвідок, які б стосувалися зазначеної проблеми, ми не виявили. Окремі загальні аспекти цієї тематики розглянуті у працях Г. Почепцова, Д. Халілова, Д. Коника та С. Рендел [3–6, 9, 10]. У тематичних інтернет-виданнях окреслені питання досліджували в тематичних розслідуваннях українські фахівці з OSINT (розвідка у відкритих джерелах) — Д. Тимчук, Р. Бурко, І. Комахідзе, В. Гусаров, Ю. Карін, К. Машовець [1, 2, 8, 11]. Особливо важливими в цьому плані вважаємо розвідки в рамках таких проектів, як «InformNapalm», «Миротворець» та «Інформаційний спротив» [1, 2, 11].

Мета статті — дослідження сучасної практики маскування та демаскування персональних акаунтів у форматі інформаційних протистоянь у соціальних мережах. Реалізація задекларованої мети статті розкриватиметься в межах таких завдань:

1. Дослідити попередні розробки профільних фахівців у питаннях ідентифікації персоналій у соціальних мережах.

2. Розглянути сучасну практику маскування та демаскування персональних акаунтів у соціальних мережах.

3. Розробити рекомендації та визначити перспективи подальшого дослідження порушеної теми.

Виклад основного матеріалу дослідження. Однією з важливих компонент будь-яких інформаційних протистоянь є вміння маскуватися або розкривати замаскованого опонента. Це мистецтво особливо актуальне у протистояннях в соціальних мережах.

Зважаючи на те, що головним засобом боротьби у соціальних мережах є обмін інформацією та спілкування, успішною буде комунікація між тими, хто має однакові погляди або належить до близьких соціальних груп. Саме тому дуже важливо, щоб майданчик, з якого відбувається трансляція інформаційного послання, або персональний акаунт мали відповідний вигляд.

Обкладинка та інше оформлення в групах, на сторінках та акаунтах має відповідати образам і символам, характерним для тих цільових груп, на які вони орієнтовані. Аватарки (фото або графічно-символьне зображення автора) на блогах та акаунтах повинні виглядати також відповідно. Це аксіома, яка не потребує деталізації та обґрунтування.

Складнішим та специфічним є питання функціонування так званих ботів та тролів — фейкових акаунтів, які застосовуються як атакуючі одиниці в класичній війні формату web 2.0–3.0. Негативне ставлення інтернет-спільноти до таких суб'єктів — загальновідоме. Ідентифікація як троля автоматично викликає недовіру до трансльованої інформації, робить марними всі зусилля та навіть може допомогти зрозуміти плани противника. Тому особливо важливо мати навички маскування власних фейкових акаунтів та вміння вирахувати акаунти опонентів.

Для надання власним акаунтам більшої правдивості необхідно:

1. Обирати реалістичне ім'я, яке є типовим для представників відповідних цільових груп.

2. Ставити на аватарку реалістичне фото — обирати фотографію будь-якої реальної людини.

3. Робити акаунт реальним — створювати персоніфіковані альбоми, підписуватися на різнопланові (не тільки за призначенням троля) сторінки і групи, розміщати поряд з тематичними пости, що мають розважальний або персональний характер.

Загальне правило: такі акаунти не повинні надто виокремлюватися серед інших, вони мають бути типовими, стандартними на фоні відповідних представників цільових груп. Тим, хто реєструє такі акаунти у тематичних групах, треба виявляти активність: лайкати чужі пости, ставити нейтральні коментарі. Активність фейкових акаунтів, крім маскування, має ще одне завдання: налагодження корисних контактів, здобування важливої інформації та вербування прибічників (безпосередньо або опосередковано).

Демаскування фейкових акаунтів, відповідно, відбувається за такими самими трьома ознаками, але одночасно фіксується їх відсутність або не повна відповідність.

Серед класичних ознак, за якими можна ідентифікувати типового троля, можна визначити такі (рис. 1):

– шаблонність формулювань та висловлювань, що виникає внаслідок використання кількох варіацій на один меседж;
– демонстративна лояльність до головної теми, занадто палка підтримка офіційної влади, окремих персоналій;
– висока агресивність, використання ненормативної лексики, персональні образи, знущання, погрози.

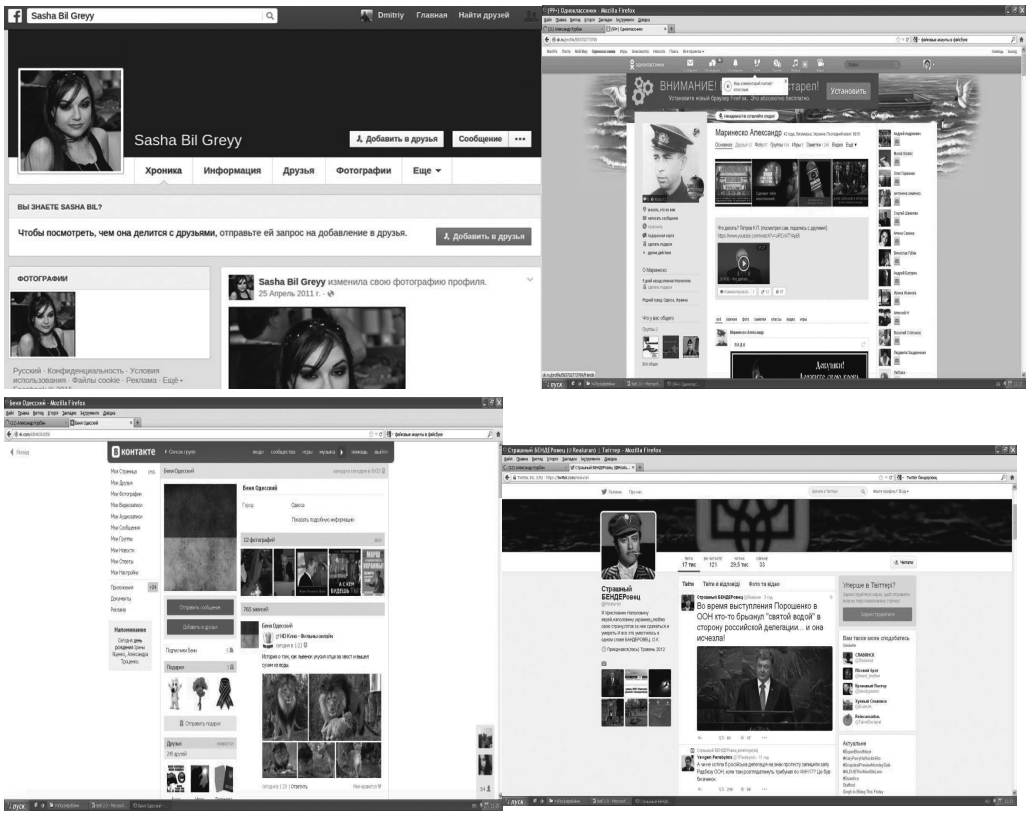

Рис. 1. Типові фейкові акаунти

Практичний приклад.

Типовим прикладом вдалого маскування та доволі успішного виконання завдань із інформаційно-психологічної диверсії може слугувати діяльність групи, очолюваної мережевим активістом, колишнім бойовиком ДНР Сергієм Жуком, що діяв як медіаактивіст під ніком Степан Мазур і позиціонував себе у провідних соціальних мережах як український націоналіст [7].

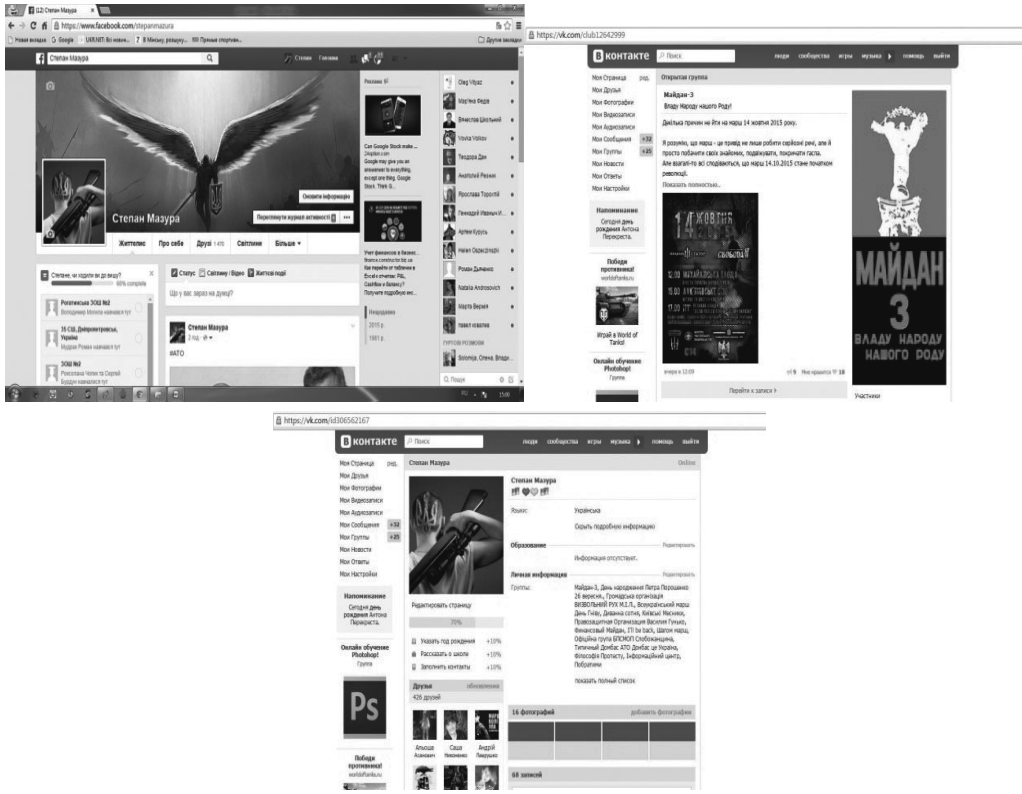

Рис. 2. Акаунти Степана Мазура

Головним завданням цього агента впливу було підбурення населення проти влади, для чого було створено групи «Майдан-3» у провідних соціальних мережах. Головним меседжем стали заклики до організації нового Майдану *(рис. 2)*.

Авторство акаунта «Степан Мазур» доволі швидко вирахували за IP-адресою і встановили місце його базування *(рис. 3)*, яким виявилася Москва.

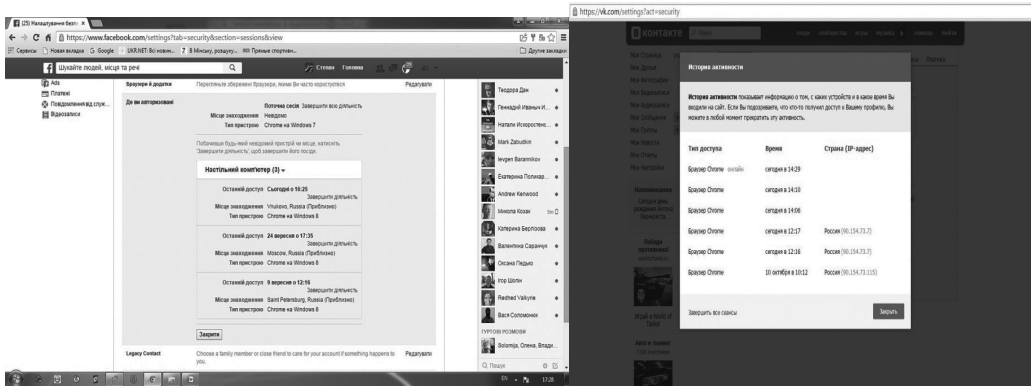

Рис. 3. IP-адреси фейкових акаунтів

Сергій Жук та його команда створили доволі потужну систему, яка протягом певного періоду успішно працювала, здійснюючи інформаційно-психологічний тиск на користувачів українського сегмента соціальних мереж (рис. 4).

Окрім візуальних засобів ідентифікації фейкових акаунтів, існує низка технічних інструментів та сервісів, що дають можливість отримувати конкретнішу інформацію, зокрема [12]:

- знайти сторінку конкретної особи одразу в усіх соцмережах (Yandex);
- знайти останні дописи конкретної особи одразу в усіх соцмережах (Facebook, Instagram, Flickr, Tumblr, Vimeo, Reddit);
- дізнатися, що конкретна особа писала на своєму акаунті в певний день (Twitter);
- дізнатися тематику та зміст постів мешканців конкретного населеного пункту (Twitter);
- дізнатися, що про конкретну особу пишуть у соцмережах (Social Mention);
- отримати інформацію про нещодавно розміщені та відзняті фото в конкретному місці (Yomapic);
- отримати інформацію про відеоматеріали, в яких фігурує конкретна особа (YouTube);
- ідентифікувати осіб на фото (Google);
- визначати, в якому районі придбано сім-карту мобільного зв'язку (gsm-inform.ru);
- вирахувати місцезнаходження через IP (ipfingerprints.com).

Окремим питанням у процесі інформаційної війни web 2.0–3.0 є технології пошуку друзів та залучення їх до кола власних інтересів, а також використання на дружній основі чужих ресурсів. Мовою професійної розвідки це називається ***вербування*** — процес залучення до співпраці на добровільній основі або за певну винагороду (матеріальну чи нематеріальну) персони, яка володіє цінною інформацією або корисними організаційними ресурсами.

В основі процесу вербування у соціальних мережах є класична схема, але з певною корекцією на специфіку середовища. Зокрема, визначаються такі етапи:

1. ***Пошук*** — моніторинг у тематичних групах активних та авторитетних блогерів, що мають максимальну кількість друзів та підписників.

2. ***Встановлення первинного контакту*** — лайки і розміщення улесливих коментарів під авторськими постами, згадування при розміщенні цікавих постів (вказання імені акаунта в статусі та в тексті поста).

3. ***Встановлення дружніх стосунків*** — спілкування у коментарях з поступовим переходом на особисте листування у «лічку».

4. ***Залучення до спільних дій*** — запрошення до власних груп та сторінок, віртуальних заходів або до чатів, створених у «лічці». Як варіант, можна надати людині статус модератора у власній групі.

5. ***Стимулювання —*** надання цікавої інформації, корисних посилань, порад за потребою.

6. ***Утримання —*** підтримка постійного інформаційного контакту із цікавим об'єктом, привітання з персональними, загальними та професійними святами. Звернення за порадами та консультаціями.

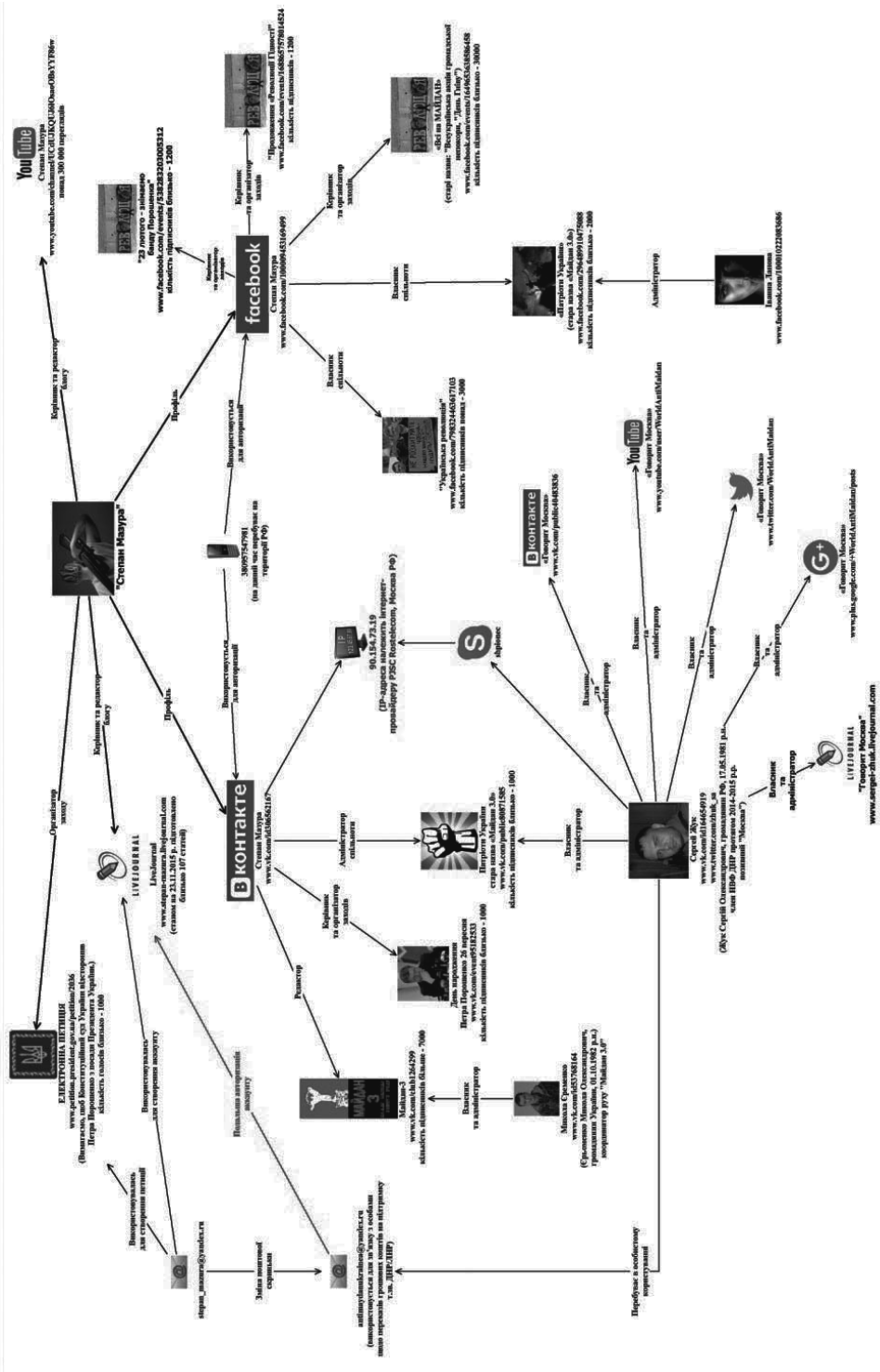

Рис. 4. Карта інформаційного поля діяльності Степана Мазура

Головним полем для вербування у соцмережах є пости та коментарі під ними у групах, пабліках і на тематичних сторінках.

Базовими засобами, що використовуються під час вербування, є:

– вияв зацікавленості до конкретної персони та сфери її інтересів;
– «безкорисливе» надання певних власних інформаційних ресурсів;
– промоція об'єкта вербування за рахунок власних ресурсів.

Висновки. З огляду на відсутність ґрунтовних наукових досліджень цієї тематики, у пропонованій статті подано первинну теоретичну базу до прикладних авторських досліджень. Зокрема, ми класифікували наявні методи і засоби подання інформації у закамуфльованому варіанті та ідентифікації таких інформаційних «вкидів». Було визначено головні принципи інформаційного маскування, серед яких є надання базовим майданчикам, з яких поширюють інформацію, типового для профільних цільових груп вигляду. Також було наголошено на потребі виконання певних обов'язкових обсягів роботи із розміщення нейтральної інформації та так званої «персоніфікації» акаунтів, розглянуто таку технологію боротьби в рамках інформаційних протистоянь, як вербування, що призначена для збирання важливої інформації та посилення ефекту від окремих інформаційних «вкидів».

Підбиваючи підсумки авторського дослідження, наголосимо на важливості та перспективності порушеного питання. Насамперед це стосується теоретико-методологічного аспекту. Зокрема, вже в найближчій перспективі галузь потребуватиме розвідок і ґрунтовних досліджень у психологічному, технічному та соціокомунікативному напрямах, які ідентифікуються як хай-сенсоро, хай-тек та хай-х'юм технології.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «InformNapalm» (Про нас) [Електронний ресурс] // InformNapalm. — Режим доступу : https://psb4ukr.org.
2. «Информационное сопротивление» (О нас) [Електронний ресурс] // Информационное сопротивление. — Режим доступа: http://sprotyv.info.
3. Коник Д. Расставьте сети. Как использовать Интернет в интересах вашего бизнеса / Д. Коник, С. Рендел. — К. : ЛИК, 2011. — 120 с.
4. Почепцов Г. Г. Від Facebook'у і гламуру до Wikileaks: медіакомунікації / Г. Г. Почепцов. — К. : Спадщина, 2012. — 464 с.
5. Почепцов Г. Новые подходы в сфере «жестких» инфовойн [Электронный ресурс] // Media sapiens [сайт]. — Режим доступа : http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkikh_infovoyn.
6. Почепцов Г. Г. Информационные войны. Новый иснтрумент политики / Г. Г. Почепцов. — М. : Алгоритм, 2015. — 256 с.
7. Самохвалова Л. Московський слід колорадського Жука, або хто і як готує «Майдан-3» [Електронний ресурс] / Л. Самохвалова // Укрінформ [сайт]. — Режим доступу: http://www.ukrinform.ua/rubric-politycs/1948496-moskovskij-slid-koloradskogo-zuka-abo-hto-i-ak-gotue-majdan3.html.

8. Тымчук Д. Вторжение в Украину: хроника российской агрессии / Д. Тымчук, Ю. Карин, К. Машовец, В. Гусаров. — К. : Брайт Стар Паблишинг, 2016. — 240 с.
9. Халилов Д. Маркетинг в социальных сетях / Д. Халилов. — М. : Ман, Иванов и Фербер, 2013. — 240 с.
10. Халилов Д. Мониторинг социальных сетей и блогов [Електронний ресурс] / Д. Халилов // Энциклопедия маркетинга. — Режим доступа: http://www.marketing.spb.ru/lib-omm/internet/smm_monitoring.htm?printversion.
11. Центр «Миротворец» [Електронний ресурс] // Миротворец. — Режим доступа: https://informnapalm.org.
12. Чернова И. 15 фишек для сбора информации о человеке в интернете [Електронний ресурс] / И. Чернова. — Режим доступа : https://www.iphones.ru/iNotes/533552.

REFERENCES

1. «InformNapalm» (Pro nas). InformNapalm. Retreived from https://psb4ukr.org (in Ukrainian).
2. «Informacionnoe soprotivlenie» (O nas). Informacionnoe soprotivlenie. Retreived from http://sprotyv.info (in Russian).
3. Konyk, D., & Rendel, S. (2011). Rasstav'te seti. Kak ispol'zovat' Internet v interesah vashego biznesa. Kiev: LIK (in Russian).
4. Pochepcov, G. G. (2012). Vid Facebook'u i glamuru do Wikileaks: mediakomunikaciї. Kiev: Spadshhina (in Russian).
5. Pochepcov, G. Novyepodhody v sfere «zhestkih» infovojn. Media sapiens. Retreived from http://osvita.mediasapiens.ua/trends/1411978127/novye_podkhody_v_sfere_zhestkikh_infovoyn/ (in Russian).
6. Pochepcov, G. G. (2015). Informacionnye vojny. Novyj instrument politiki. Moskva: Algoritm (in Russian).
7. Samokhvalova, L. Moskovskyi slid koloradskoho Zhuka, abo khto i yak hotuie «Maidan-3». Ukrinform. Retrieved from http://www.ukrinform.ua/rubric-politycs/1948496-moskovskij-slid-koloradskogo-zuka-abo-hto-i-ak-gotue-majdan3.html (in Ukrainian).
8. Tymchuk, D., Karin, Ju., Mashovec, K., & Gusarov, V. (2016). Vtorzhenie v Ukrainu: hronika rossijskoj agressii. Kiev: Brajt Star Pablishing (in Russian).
9. Halilov, D. (2013). Marketing v social'nyh setjah. Moskva: Man, Ivanov i Ferber (in Russian).
10. Halilov, D. Monitoring social'nyh setej i blogov. Entsiklopedija marketinga. Retreived from http://www.marketing.spb.ru/lib-comm/internet/smm_monitoring.htm?printversion (in Russian).
11. Centr «Mirotvorec». Mirotvorec. Retreived from https://informnapalm.org (in Russian).
12. Chernova, I. 15 fishek dlja sbora informacii o cheloveke v internete. Retreived from https://www.iphones.ru/iNotes/533552 (in Russian).

METHODS AND MEANS OF CONCEALMENT AND IDENTIFICATION OF ACCOUNTS AUTHORSHIP IN SOCIAL NETWORK

O. V. Kurban

Borys Hrinchenko Kyiv University,
13-B, M. Tymoshenko St., Kyiv, 02000, Ukraine
bairam1970@bk.ru

The article deals with the problem of masking and de-masking personal accounts in online social networks, possibilities and features of these tasks implementation in format of web 2.0 and web 3.0. We also consider the mechanism of using information resources of others through their recruitment and cooperation involvement in the hidden and open form. The author believes that in the future these conceptual aspects should be adapted to key information processes of online network environment and actively used in the development of national system of information security.

Keywords: *Internet technology, social networking, personal accounts.*

Стаття надійшла до редакції 19.07.2016.
Received 19.07.2016.