Черниш Р. Ф.,
кандидат юридичних наук, доцент,
доцент спеціальної кафедри
Національної академії Служби безпеки України
ORCID ID:*0000–0003–4176–7569*

DOI: *https://doi.org/10.17721/2413-5372.2020.3-4/168-177*

УДК: *34:316.46.058.5:004.738.5*

ОРГАНІЗАЦІЙНІ ТА ПРАВОВІ МЕТОДИ ПРОТИДІЇ МАНІПУЛЮВАННЮ СВІДОМІСТЮ ГРОМАДЯН У СОЦІАЛЬНИХ МЕРЕЖАХ

«Жодна велич не приходить до світу людей без прокляття»
Софокл

Анотація. *У статті констатовано, що у XXI столітті мережа Інтернет та соціальні мережі все частіше використовуються на шкоду національним інтересам. Зважаючи на тотальну комп'ютеризацію та діджиталізацію людства, кіберпростір стає середовищем для вчинення кіберзлочинів. Одночасно актуальною є загроза надшвидкого поширення деструктивного контенту для маніпулювання свідомістю громадян.*

Зважаючи на викладене, ***метою статті*** *є питання розробки дієвих організаційних та правових методів протидії вказаному негативному явищу.*

Констатовано увагу на тому, що чинним законодавством закріплено винятковий перелік підстав для обробки (і як її складової – збору) персональних даних. Серед них однією із ключових, в контексті збору персональних даних у мережі Інтернет, за винятком окремих випадків, є саме згода суб'єкта персональних даних. Дійшли висновку, що не всі інтернет-ресурси чи мобільні додатки попереджають про обробку персональної інформації. Переважно про вказане можна дізнатися шляхом аналізу відповідного налаштування чи наданих дозволів (інколи й за замовчуванням). Також відповідно до політики конфіденційності соціальних мереж, мобільних додатків доступ до обробки персональних даних є обов'язковою умовою використання сервісів. Тобто, відсутня альтернатива, а сама згода за своєю правовою природою є умовно добровільною.

Стверджується, що проблемним є питання обробки інформації (персональних даних) про третіх осіб. Адже у випадку, коли користувач надає доступ до власної сторінки у соціальній мережі чи до телефонної книги, він автоматично надає доступ й до даних про третіх осіб без будь- якої їхньої персональної згоди. Тобто на практиці складається ситуація, за якої право на захист вказаної категорії осіб систематично порушується.

Проаналізовано правовий досвід країн Європейського Союзу у сфері забезпечення безпеки персональних даних громадян.

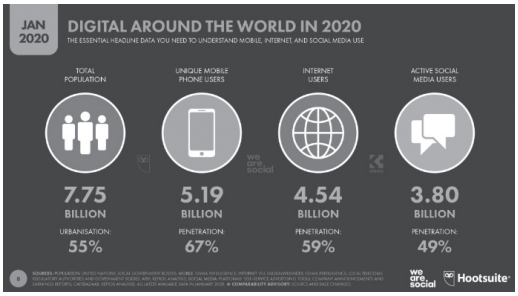
У заключній частині дослідження наголошено на тому, що користувачами мережі Інтернет та соціальних мереж є представники органів державної влади, місцевого самоврядуван-

ня, військовослужбовці, співробітники національних правоохоронних органів і спецслужб, інші суб'єкти з числа секретоносіїв. Відповідно подальшої наукової розробки потребує посилення правового забезпечення та цілеспрямованого застосування організаційних заходів, в першу чергу, у вказаному середовищі, яке може бути використане іноземними спецслужбами, зокрема Російською Федерацією, у своїх інтересах.

Ключові слова: *соціальна мережа, мережа Інтернет, деструктивний вплив, міжнародно-правовий досвід захисту персональних даних, кіберпростір.*

Постановка проблеми. У XXI столітті мережа Інтернет та соціальні мережі[1] все частіше використовуються на шкоду національним інтересам. Зважаючи на тотальну комп'ютеризацію та діджиталізацію людства (див рис. 1), кіберпростір[2] стає середовищем для вчинення кіберзлочинів[3]. Одночасно актуальною є загроза надшвидкого поширення деструктивного контенту для маніпулювання свідомістю громадян.

Аналіз початку та перебігу т.зв «кольорових революцій», протестних акцій, які систематично відбуваються на території Європейського Союзу, подій у районі проведення операцій об'єднаних сил (далі-ООС) свідчить, що поширення фейкового контенту (аналіз вказаного поняття було наведено у попередніх роботах[5,6,7,]) в ході проведення інформаційних операцій, призводить до вчинення громадянами антидержавних дій[8]. При цьому в контексті забезпечення інформаційної безпеки України потрібно враховувати, що наша держава у переліку країн, які найбільш піддаються



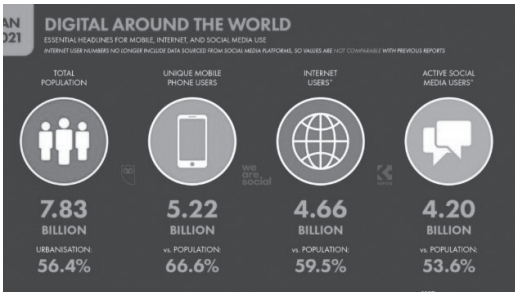


Рис. 1 Динаміка використання населенням мобільних гаджетів, мережі Інтернет та соціальних мереж[4]

[1] Roman F. Chernysh, Viktoriya L. Pogrebnaya, Iryna I. Montrin, Tetiana V. Koval and Olha S. Paramonova. Formation and application of communication strategies through social networks: legal and organizational aspects. *International Journal of Management*. Volume 11. Issue 06. June 2020. pp. 476–488. Article ID: IJM_11_06_041 <http://www.iaeme.com/ijm/issues.asp? JType=IJM&VType=11&IType=6> DOI: 10.34218/IJM.11.6.2020.041/ дата звернення 06.11.2020

[2] Погорецький М., Шеломенцев В. Поняття кіберпростору як середовища вчинення злочинів. (2009) 2 *Інформаційна безпека людини, суспільства, держави* 77–81.

[3] Погорецький М., Шеломенцев В. Кіберзлочини: до визначення поняття. (2012) *8 Вісник прокуратури* 89–96.

[4] DIGITAL 2020: GLOBAL OVERVIEW REPORT. <https://datareportal.com/reports/digital-2020-global-overview-report> дата звернення 06.11.2020

[5] Черниш Р, Юридична відповідальність за поширення фейкової інформації (2020) 1 *Електронне наукове фахове видання «Юридичний науковий електронний журнал»* 191–194 <http://lsej.org.ua/1_2020/47.pdf> дата звернення 06.11.2020.

[6] Черниш Р, Фейк, як один із інструментів негативного впливу на національну безпеку України в умовах ведення гібридної війни. (2019) 2 *Часопис Київського університету права.* <http://kul.kiev.ua/doc/chasopys2019/CHAS19_2.pdf> дата звернення 06.11.2020.

[7] Черниш Р, Правовий досвід країн Європейського Союзу у сфері протидії поширенню фейкової інформації (2019) 10 *Підприємництво, господарство і право* 123–128 <http://pgp-journal.kiev.ua/archive/2019/10/22.pdf> дата звернення 06.11.2020.

[8] Грищук Р, Основи кібернетичної безпеки: моногр; за заг. ред. проф. Ю. Г. Даника. Житомир: ЖНАЕУ, 2016. 636 с.

інформаційними маніпуляціями з боку країни-агресора[1].

Метою статті є критичний аналіз механізмів і способів маніпулювання свідомістю громадян у соціальних мережах та розробка організаційних та правових методів протидії вказаному негативному явищу. Окреслена тематика є мультидисциплінною і вимагає ґрунтовного теоретичного опрацювання науково-прикладних здобутків різних галузей: права, психології, кібербезпеки, інформаційної безпеки тощо.

Основні результати дослідження. У XXI столітті однією з найбільш «конвертованих валют» є персональні дані. В процесі отримання відповідних послуг в мережі Інтернет громадяни в переважній більшості випадків не витрачають грошових коштів, однак «розрахунок» відбувається шляхом добровільної передачі особистої інформації та відомостей про третіх осіб. Це відбувається в процесі використання соціальних мереж, користування мобільними додатками, перегляду онлайн відео тощо.

У ст. 11 Закону України «Про захист персональних даних» закріплено виключний перелік підстав для обробки (і як її складової – збору) персональних даних[2]. Серед них однією із ключових в контексті збору персональних даних у мережі Інтернет, за винятком окремих випадків, є саме згода суб'єкта персональних даних. У ст. 2 вказаного нормативно-правового акту зазначено, що згодою суб'єкта персональних даних є добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу дійти висновку про надання згоди[3].

Однак не всі інтернет-ресурси чи мобільні додатки попереджають про обробку персональної інформації. Переважно про вказане можна дізнатися шляхом аналізу відповідного налаштування чи наданих дозволів (інколи й за замовчуванням). Також відповідно до політики конфіденційності соціальних мереж, мобільних додатків доступ до обробки персональних даних є обов'язковою умовою використання сервісів. Тобто відсутня альтернатива, а сама згода за своєю правовою природою є умовно добровільною.

Вказана згода може надаватися у письмовій формі або у формі, що дозволяє дійти висновку про її надання. При цьому вона повинна бути однозначною і дії користувача мають однозначно свідчити про те, що він дозволяє збирати та використовувати свої персональні дані. Вказане може забезпечуватися шляхом проставляння відповідних поміток в електронних формах, або ж в процесі натискання віртуальних вікон «погоджуюсь» чи «дозволяю». Однак частина електронних ресурсів, соціальних мереж, мобільних додатків не вимагають активних дій користувача щодо надання вказаної згоди, а лише попереджають про те, що сам факт подальшого користування за замовчуванням розцінюється як «згода». При цьому відсутні активні дії користувача, а йдеться про пасивне сприйняття, тобто наявність згоди не буде очевидною.

У деяких випадках дані про дозволи, які хоче отримати додаток чи будь-який соціальний ресурс, яку саме інформацію планується збирати та відомості про мету її використання є мінімальною, публікуються в окремому розділі. Вони є неповними, викладаються іноземною мовою і фактично є незрозумілими та тяжко доступними для конкретного користувача.

[1] Україна серйозно вражена інформаційним маніпуляціям РФ – дослідження Facebook. <https://petrimazepa.com/ukraina_serezno_porazhena_informmanipulyaciyami_rf_issledovanie_facebook?utm_source=gravitec&utm_medium=push&utm_campaign=News&fbclid=IwAR1mVNSEKe1K8kTWQsqdQbYUCB67ceOUt3GAjVAtrHcFDD2T3xGcpEMRQZY> дата звернення 06.11.2020

[2] Про захист персональних даних: Закон України від 01.06.10 <www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297–17> дата звернення 06.11.2020

[3] Про захист персональних даних: Закон України від 01.06.10 <www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297–17> дата звернення 06.11.2020.

Для усунення вказаних суперечностей на території Європейського Союзу на рівні нормативно-правових актів почали впроваджувати полодження, відповідно до яких операторів надання електронних послуг зобов'язали заздалегідь і в доступній формі інформувати користувачів про ті дозволи, які їм останні зобов'язані надати. Зокрема, вказане знайшло свій вираз у Загальному регламенті про захист даних (General Data Protection Regulation, GDPR), який почав діяти з 2018 року[1]. Зазначений акт регламентує питання, пов'язані з використанням персональних даних користувачів. Соціальні мережі Facebook, YouTube, Twitter, пошуковик Google та інші зберігають про користувачів великі масиви даних на основі їхньої поведінки онлайн, що дозволяє налаштовувати більш персоналізовану рекламу та мікротаргетинг рекламних дописів. Мікротаргетинг дозволяє налаштувати показ реклами, базуючись не лише на загальних даних про користувача (стать, вік, регіон перебування тощо), а й на інформації про інтереси, переконання, смаки користувача, отриманої, наприклад, з його/її історії пошуку в браузері, взаємодії з іншими рекламними дописами та ін. GDPR ділить персональні дані на дві категорії: звичайні (ім'я, освіта, місце проживання, місце робити, вік тощо) та чутливі дані (релігійна та етнічна належність, сексуальна орієнтація, політичні переконання тощо).

Відповідно до GDPR зберігання та використання персональних даних користувачів може відбуватися лише за їх інформованої згоди. Запит на згоду повинен бути простим і зрозумілим для користувача. Персональні дані можуть бути використані тільки у законний спосіб, прозорим шляхом, зберігатися лише для попередньо заявленої мети, мають залишатися конфіденційними та зберігатися протягом обмеженого періоду часу. При цьому користувачі можуть оскаржити спосіб зберігання та використання їхніх даних. На території кожної держави-члена ЄС діє спеціальний орган – Data Protection Authority (DPA), уповноважений контролювати вимоги GDPR. Зокрема, DPA може накласти штраф розміром до 20 тисяч євро на організацію, що займається збором, зберіганням і використанням персональних даних за порушення норм Регламенту. Протягом 2019 року сумарно на всій території ЄС було накладено штрафів сукупним розміром понад 711,5 мільйонів євро.

Проблемним є питання обробки інформації (персональних даних) про третіх осіб. Як вже зазначалося в ст. 11 Закону України «Про захист персональних даних», йдеться про необхідність отримання згоди конкретної особи на збирання та використання саме її персональних даних. Однак у випадку, коли користувач надає доступ до власної сторінки у соціальній мережі чи до телефонної книги, він автоматично надає доступ й до даних про третіх осіб без будь-якої їхньої персональної згоди (наприклад, йдеться про алгоритми функціонування додатків Getcontact, Truecaller тощо). Тобто на практиці виникає ситуація, за якої право на захист вказаної категорії осіб систематично порушується.

У кожного із суб'єктів персональних даних (будь-якого користувача онлайн-сервісів) є передбачене ст. 8 Закону України «Про захист персональних даних» право на відкликання згоди на обробку персональних даних. Однак у тому випадку, коли користувач, наприклад, видалив профіль з соціальної мережі, відсутні гарантії, що персональні дані буде видалено з відповідних серверів. У випадку, коли йдеться про дані, які стосуються третіх осіб, можемо констатувати, що вони взагалі втрачають контроль над власними персональними даними.

[1] General Data Protection Regulation (EU GDPR). <https://gdpr-text.com/?col=2&lang1=ukr&lang2=en&lang3=rumain> дата звернення 06.11.2020; Про захист персональних даних: Закон України від 01.06.10 <www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297–17> дата звернення 06.11.2020

Соціальні мережі Facebook, YouTube, Twitter тощо зберігають значні масиви даних (формується т.зв. «цифровий слід») про користувачів на основі їхньої поведінки онлайн. Вказане зумовлено комерційною складовою – налаштовування персоналізованої реклами та мікротаргетинг рекламних дописів. Це може використовуватися для подальшого впливу на свідомість користувачів з боку представників спеціальних служб у своїх інтересах.

В основу функціонування соціальної мережі закладено такий алгоритм: чим частіше взаємодіємо з іншим (ми) акаунтами (пости, репости, перегляд фотографій, вподобання тощо), тим частіше бачимо інформацію конкретного користувача (чів). Якщо окресленого зв'язку немає або він фрагментарний, відповідно один акаунт не бачитиме публікації іншого.

Будь-яка наша активна дія в соціальній мережі дозволяє сформувати «цифрову копію» реального користувача та на системній основі наповнювати її масивами необхідних даних. Як наслідок, буде сформовано т.зв. «цифрову бульбашку» з контентом, який з найбільшою вірогідністю викличне інтерес у конкретного користувача.

Аналіз вказаної вище інформації дозволяє констатувати, що для маніпулювання свідомістю громадян у соціальній мережі необхідно зберігати дані про зв'язок між обліковими записами користувачів (далі акаунтами) шляхом системної та послідовної взаємодії.

Зважаючи на те, що згідно з положеннями політики конфіденційності соціальної мережі, яка формується відповідно до вимог, що висуваються представниками міжнародної спільноти, її адміністрація вживає заходів щодо суттєвого зменшення випадків передачі персональних даних користувачів (конфіденційної інформації)[1,2,3] третім особам.

Вказане зумовлює для зацікавлених суб'єктів незалежно від мети (комерційна (продаж товарів) чи маніпулятивна (вплив на свідомість)) необхідність пошуку шляхів отримання зазначеної інформації, в тому числі й шляхом розробки нових способів та інструментів для маніпуляцій.

Щоб реалізувати наміри з конструювання маніпуляцій чи інформаційних вірусів, потрібно вирішити хоча б одне з таких завдань:

– отримати прямий чи опосередкований доступ до персонального акаунту (тобто мати можливість показувати інформацію);

– взаємодіяти з маніпулятивним чи інформаційним дописом, у тому числі й шляхом поширення певних «постів», які здатні викликати «емоцію» – гнів, несприйняття, переживання, співчуття тощо;

– використати ботів для активації «поведінки натовпу», тобто збільшити аудиторію шляхом створення штучної популярності для певних сторінок або створення штучної популярності під певними дописами. Як свідчить практика, за таких обставин користувачі самостійно та безкоштовно поширять відповідні дописи у середовищі своїх друзів і підписників (створюється т. зв. «піраміда поширення інформації;

– використати ботів для поширення інформації.

Більш детально проаналізуємо кожне із наведених вище завдань.

Зокрема, аналіз вітчизняного сегменту мережі Інтернет свідчить про наявність наступних найбільш поширених ***способів заволодіння акаунтами***:

Копіювання акаунта. Вказаний спосіб використовується, як правило, по від-

[1] Про доступ до публічної інформації: Закон України від 13.01.11 № 2939-VI < https://zakon.rada.gov.ua/laws/show/2939–17#Text > дата звернення 06.11.2020

[2] Про інформацію: Закон України від 02.10.92 № 2657-XII (із змінами та доповненнями) <https://zakon.rada.gov.ua/laws/show/2657–12#Text> дата звернення 06.11.2020

[3] Про захист персональних даних: Закон України від 01.06.10 <www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297–17> дата звернення 06.11.2020

ношенню до персональних сторінок лідерів громадської думки. Полягає в тому, що зловмисники дублюють усі дані, які містяться на офіційній сторінці, і пересічний користувач у повну міру довіряє інформації, що ширитиметься з акаунта-клона.

Злам акаунта. Є одним із найбільш масових способів заволодіння персональною сторінкою. Як правило, відбувається шляхом підбору паролів, або ж за результатами спеціальної акції із спонукання користувача перейти за посиланням, що містить вірусне програмне забезпечення.

Купівля акаунта або ж його оренда. Полягає в тому, що персональну сторінку передають третій особі за кошти. Як правило, у більшості випадків йдеться про короткострокову оренду. Однак аналіз наявної інформації свідчить, що власник сторінки майже завжди у всіх випадках втрачає над нею контроль назавжди.

У випадку, коли постає завдання ***домогтися взаємодії з акаунтом***, то розміщується допис, що здатний викликати «емоцію», або ж із загальноприйнятою тезою, з якою неможливо не погодитися. Наприклад, права і свободи людини і громадянина є невід'ємними. У той момент, коли починаємо взаємодіяти із вказаним постом (лайк, репост, коментар тощо), вмикаються алгоритми соціальної мережі та автоматично нам пропонуються новини чи інша інформація користувача, який його опублікував.

Вказана взаємодія досягається й за результатами аналізу «емоційних гачків користувача».

Упроваджено кілька популярних способів їх збору. Зокрема, йдеться про проходження користувачами різноманітних тестів у соціальній мережі (пропонується безкоштовний контент, який має розважальний характер і викликає емоції; у разі згоди з обробкою інформації персональні дані конкретного користувача, його друзів у соціальній мережі та підписників стають доступними для третіх осіб).

Інший спосіб реалізується в процесі поширення різноманітних флешмобів, суть яких полягає в реакції користувача на пост («+», будь-яке слово тощо) з подальшим копіюванням в себе на сторінці. У результаті вдається збільшити охоплення аудиторії за рахунок тих осіб, які реагують та коментують. Занепокоєння викликає факт того, що у вказаних діях досить часто беруть участь т.зв. лідери громадської думки, адже за змістом контенту, який копіюється, неможливо визначити суспільну шкоду від вказаних дій. У зазначеному випадку негативні наслідки полягають у створенні т. зв. «піраміди поширення інформації».

Аналіз вітчизняного сегменту мережі Інтернет свідчить, що використання ботів (для активації «поведінки натовпу» або поширення інформації) є часто застосованою технологією.

У своїх наукових дослідженнях К. Молодецька-Гринчук поділяє ботів на 5 видів. Критерієм класифікації є завдання, що вони виконують. Зокрема, на технічних ботів, бойових ботів, тролів, дезінформаторів, ботів-спамерів[1]. Погоджуючись із вказаною класифікацією, охарактеризуємо види ботів, які є, на нашу думку, притаманними саме для українського сегменту мережі Інтернет. В основу кваліфікації покладено критерій наповнення персональної сторінки в соціальній мережі. Зокрема, це:

Примітивний бот. Характеризується відсутністю фотографій, стрічки новин та мінімальною кількістю друзів і підписників (як правило, також ботів).

Бот початкового рівня. Характеризується наявністю мінімальної кількості фотографій на нетральну тематику. Стрічка новин і кількість друзів відсутні або ж є незначними.

Бот середнього рівня. Характеризується наявністю абстрактних фотографій, стрічки новин, яка формується з од-

[1] Молодецька-Гринчук К, Соціальні боти як інструмент деструктивного інформаційного впливу на акторів соціальних інтернет-сервісів. (2017) *Современные инновационные технологии подготовки инженерных кадров для горной промышленности и транспорта*: сб. науч. тр. междунар. конф., 13–14 апреля 442–447.

нотипних джерел за допомогою репостів. До друзів може бути додано незначну кількість акаунтів реальних користувачів.

Шаблонний бот. Характеризується наявністю незначної кількості однотипних персональних фотографій, частковим заповненням персональної інформації та публікаціями у новинній стрічці. У вітчизняному сегменті мережі Інтернет вказані боти досить поширені.

Бот-аналог існуючого користувача. Характеризується наявністю різноманітних фотографій, публікацією особистих дописів у стрічці новин тощо. Для непідготовленого користувача досить складно його відрізнити від «реальної» людини.

Перші три охарактеризовані категорії переважно використовуються з метою активації «поведінки натовпу». Четверта й п'ята для поширення відповідного контенту з метою маніпулювання свідомістю громадян у соціальних мережах.

На нашу думку, аналіз активності ботів з поширення саме конкретного меседжа може свідчити про його маніпулятивний характер і намагання вплинути на свідомість громадян у вигідному для конкретної особи (групи осіб) ракурсі.

Поряд із ботами для швидкого поширення інформації серед представників різних соціальних груп використовують лідерів громадської думки. Вказане відбувається в тому випадку, коли вони є першоджерелом, або ж значимість інформації є штучно перебільшеною і викликає значний суспільний резонанс, а вказана категорія осіб починає її ширити та коментувати.

Щоб зусилля у вказаному напрямі були мінімальними, інформація має бути завуальованою та поширеною у формі «інформаційної пастки», тобто у такий спосіб, який однозначно викличе інтерес у конкретного користувача і на підсвідомому рівні спонукатиме його до взаємодії із дописом.

Проаналізувавши наявні «інформаційної пастки», які ширяться у вітчизняному сегменті мережі Інтернет, ми їх класифікували таким чином:

Конспірологічні. Суть полягає в тому, що зважаючи на специфіку менталітету та інші суб'єктивно – об'єктивні чинники, в Україні існує тенденція до недовіри меседжам, які озвучуються представниками органів державної влади. Зважаючи на викладене, з певною періодичністю з'являються маніпуляційні дописи, в основі яких міститься суспільно значима інформація, яку нібито поширюють від імені першоджерела (близької особи, колеги, сусіда тощо). Наприклад, вказане стосується постів, пов'язаних з COVID-19. Протягом квітня 2020 р. модератори соціальної мережі Facebook виявили 50 мільйонів дописів[1], які містили фейкову інформацію, що стосувалася певних аспектів пандемії («теорія про небезпеку 5G для здоров'я людини», «кропління вулиць з гелікоптера смертельно небезпечними хімікатами для дезінфекції від коронавірусу», «дистанційне поширення вірусу представниками іноспецслужб за допомогою радіохвиль» тощо)[2].

Прогнозні. Поширення прогнозів на розвиток подій, складених нібито астрологами, екстрасенсами, езотерикаки, експертами тощо. Більшість користувачів не перевіряє кваліфікацію вказаних вище суб'єктів. У переважній більшості випадків вони взагалі не мають відношення до інформації, яка поширюється від їхнього імені.

Благодійність. Використовується тематика надання фінансової допомоги (може бути поєднана з кібершахрайством) або ж просто репосту чи реакції у коментарях («+», будь-яке слово тощо).

Наявність «жертви». Інформація публікується від імені «звичайної» людини, яку було ображено представником органів державної влади чи місцевого самоврядування. В переважній більшості випадків використовується для дискредитації політиків, громадських активістів, лідерів громадської думки тощо.

[1] Модератори Facebook за місяць виявили 50 мільйонів дописів із фейками про коронавірус. <https://novynarnia.com/2020/05/12/facebook-fakes/> дата звернення 06.11.2020

[2] «Дай 5!» Звідки взялися теорії про зв'язок технології 5G з коронавірусом і чому це ФЕЙК. <https://novynarnia.com/2020/05/15/5g/> дата звернення 06.11.2020

Емоційні пастки. Спрямовані на штучний поділ українців (мова, війна, релігія, територія проживання тощо). Специфікою є те, що вони викликають значний суспільний інтерес та містять посили, які є «близькими». Зважаючи, що до вказаного виду «інормаційних пасток» потрапляють активні групи користувачів з різними поглядами – поширюються досить швидко. Застосовуються зацікавленими суб'єктами для дестабілізації суспільно-політичної ситуації та у випадку наявності нагальної потреби для відволікання уваги від актуальних питань.

Зважаючи на те, що користувачами мережі Інтернет та соціальних мереж є представники органів державної влади, місцевого самоврядування, військовослужбовці[1], співробітники національних правоохоронних органів[2] і спецслужб, інші суб'єкти з числа секретоносіїв, подальшої наукової розробки потребує посилення правового забезпечення та цілеспрямованого застосування організаційних заходів, у першу чергу, у вказаному середовищі, яке може бути використане іноземними спецслужбами, зокрема Російською Федерацією, у своїх інтересах.

Висновки. Враховуючи мультидисциплінарний характер досліджуваної проблематики, вважаємо, що способи протидії маніпулюванню свідомістю громадян у соціальних мережах повинні бути «гібридними» з обов'язковою інтеграцією міжнародного правового та організаційного досвіду щодо мінімізації окресленого негативного явища. Вказану інтеграцію необхідно здійснювати після адаптації до національних реалій сьогодення.

Правові методи протидії повинні бути спрямовані на розробку нових та вдосконалення чинних нормативно-правових актів у сфері забезпечення інформаційної безпеки держави з урахуванням міжнародного досвіду. Важливим аспектом у вказаному напрямі є організація дієвої співпраці зі світовими інформаційними лідерами (Google, Facebook, Twitter тощо) щодо виявлення та блокування маніпулятивних дописів, які впливають на свідомість користувачів соціальних мереж та підвищення інформаційної і цифрової грамотності громадян.

REFERENCES

LIST OF LEGAL DOCUMENTS

LEGISLATION

1. General Data Protection Regulation (EU GDPR). <https://gdpr-text.com/?col=2&lang1=ukr&lang2=en&lang3=rumain> data zvernennia 06.11.2020 [in Ukrainian].

2. Pro dostup do publichnoi informatsii: Zakon Ukrainy vid 13.01.11 r. № 2939-VI [About access to public information] <https://zakon.rada.gov.ua/laws/show/2939–17#Text> data zvernennia 06.11.2020 [in Ukrainian].

3. Pro informatsiiu: Zakon Ukrainy vid 02.10.92 r. № 2657-KhII [About information] <https://zakon.rada.gov.ua/laws/show/2657–12#Text> data zvernennia 06.11.2020 [in Ukrainian].

4. Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 01.06.10 r. [About personal data protection] <www.zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297–17> data zvernennia 06.11.2020 [in Ukrainian].

BIBLIOGRAPHY

AUTHORED BOOKS

5. Hryshchuk R. Osnovy kibernetychnoi bezpeky [Fundamentals of cyber security]: monohr; za zah. red. prof. Yu. H. Danyka. Zhytomyr: ZhNAEU, 2016. 636 s. [in Ukrainian].

[1] Черниш Р, Міжнародно-правовий досвід використання соціальних мереж військовослужбовцями збройних сил та співробітниками правоохоронних органів (2016) 6 *Порівняльно-аналітичне право* – електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет» <http://pap.in.ua/6_2016/64.pdf> дата звернення 06.11.2020.

[2] Погорецький М, Організована злочинність в Україні: тенденції розвитку та заходи протидії (2007) 16 *Боротьба з організованою злочинністю і корупцією* 99–111.

JOURNAL ARTICLES

6. Roman F. Chernysh, Viktoriya L. Pogrebnaya, Iryna I. Montrin, Tetiana V. Koval and Olha S. Paramonova. Formation and application of communication strategies through social networks: legal and organizational aspects. *International Journal of Management*. Volume 11. Issue 06. June 2020. pp. 476–488. Article ID: IJM_11_06_041 <http://www.iaeme.com/ijm/issues.asp? JType=IJM&VType=11&IType=6> data zvernennia 06.11.2020

7. Pohoretskyi M. A. Orhanizovana zlochynnist v Ukraini: tendentsii rozvytku ta zakhody protydii. Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu. Kyiv, 2007. № 16. S. 99–111. [in Ukrainian].

8. Pohoretskyi M., Shelomentsev V. Kiberzlochyny: do vyznachennia poniattia [Cybercrime: to define the concept]. Visnyk prokuratury. 2012. № 8.S. 89–96. [in Ukrainian].

9. Pohoretskyi M., Shelomentsev V. Poniattia kiberprostoru yak seredovyshcha vchynennia zlochyniv [The concept of cyberspace as an environment for committing crimes]. Informatsiina bezpeka liudyny, suspilstva, derzhavy. 2009. № 2. S. 77–81. [in Ukrainian].

10. Chernysh R. F. Pravovyi dosvid krain Yevropeiskoho Soiuzu u sferi protydii poshyrenniu feikovoi informatsii [Legal experience of the European Union in the field of combating the dissemination of fake information]. Pidpryiemnytstvo. hospodarstvo i pravo. № 10. 2019. S. 123–128 <http://pgp-journal.kiev.ua/archive/2019/10/22.pdf> data zvernennia 06.11.2020 [in Ukrainian].

11. Chernysh R. F. Feik, yak odyn iz instrumentiv nehatyvnoho vplyvu na natsionalnu bezpeku Ukrainy v umovakh vedennia hibrydnoi viiny. [Fake, as one of the tools of negative impact on the national security of Ukraine in a hybrid war] Chasopys kyivskoho universytetu prava. № 2. 2019. S. 109–114 <http://kul.kiev.ua/doc/chasopys2019/CHAS19_2.pdf>. data zvernennia 06.11.2020 [in Ukrainian].

12. Chernysh R. F. Mizhnarodno-pravovyi dosvid vykorystannia sotsialnykh merezh viiskovosluzhbovtsiamy zbroinykh syl ta spivrobitnykamy pravookhoronnykh orhaniv. Porivnialno-analitychne pravo – elektronne naukove fakhove vydannia yurydychnoho fakultetu DVNZ «Uzhhorodskyi natsionalnyi universytet». 2016. Vyp. 6. S. 216–218. <http://pap.in.ua/6_2016/64.pdf>. data zvernennia 06.11.2020 [in Ukrainian].

13. Chernysh R. F. Yurydychna vidpovidalnist za poshyrennia feikovoi informatsii [Legal responsibility for the dissemination of fake information]. Elektronne naukove fakhove vydannia «Iurydychnyi naukovyi elektronnyi zhurnal». № 1. 2020. S. 191–194. <http://lsej.org.ua/1_2020/47.pdf> data zvernennia 06.11.2020 [in Ukrainian].

CONFERENCE PAPERS

14. Molodetska-Hrynchuk K. V. Sotsialni boty yak instrument destruktyvnoho informatsiinoho vplyvu na aktoriv sotsialnykh internet-servisiv [Social bots as a tool of destructive informational influence on the actors of social Internet services]. Sovremennыe ynnovatsyonnыe tekhnolohyy podhotovky ynzhenernыkh kadrov dlia hornoi promыshlennosty y transporta 2017: sb. nauch. tr. mezhdunar. konf., 13–14 aprelia 2017 h., 2017. S. 442–447. [in Ukrainian].

ARTICLES

15. «Dai 5!» Zvidky vzialysia teorii pro zviazok tekhnolohii 5G z koronavirusom i chomu tse FEIK [«Give 5!» Where did the theories about the connection between 5G technology and coronavirus come from and why is it FAKE?] <https://novynarnia.com/2020/05/15/5g/> data zvernennia 06.11.2020 [in Ukrainian].

16. Moderatory Facebook za misiats vyiavyly 50 milioniv dopysiv iz feikamy pro koronavirus. [Facebook moderators found 50 million fake posts about the coronavirus in a month] <https://novynarnia.com/2020/05/12/facebook-fakes/> data zvernennia 06.11.2020 [in Ukrainian].

17. Ukraina seriozno vrazhena informatsiinym manipuliatsiiam RF – doslidzhennia Facebook. <https://petrimazepa.com/ukraina_serezno_porazhena_informmanipulyaciyami_rf_issledovanie_facebook?utm_source=gravitec&utm_medium=push&utm_campaign=News&fbclid=IwAR1mVNSEKe1K8kTWQsqdQbYUCB67ceOUt3GAjVAtrHcFDD2T3xGcpEMRQZY> data zvernennia 06.11.2020 [in Ukrainian].

WEBSITES

18. DIGITAL 2020: GLOBAL OVERVIEW REPORT. Recovered from <https://datareportal.com/reports/digital-2020-global-overview-report> data zvernennia 06.11.2020

Chernysh R.,
Candidate of Law, Associate Professor,
Associate Professor special department
of the National Academy of Security
Service of Ukraine
***ORCID:** 0000–0003–4176–7569*

DOI: *https://doi.org/10.17721/2413-5372.2020.3-4/168-177*

ORGANIZATIONAL AND LEGAL METHODS OF COMBATING MANIPULATION OF CITIZENS 'CONSCIOUSNESS IN SOCIAL NETWORKS

Annotation. *The article states that in the XXI century the Internet and social networks are increasingly used to the detriment of national interests. Due to the total computerization and digitalization of humanity, cyberspace is becoming an environment for cybercrime. At the same time, the threat of excessive distribution of destructive content to manipulate the minds of citizens is urgent.*

In view of the above, ***the purpose of the article*** *is to develop effective organizational and legal methods to combat this negative phenomenon.*

It is noted that the current legislation establishes an exclusive list of grounds for processing (and as its component – collection) of personal data. Among them, one of the key, in the context of the collection of personal data on the Internet, except in some cases, is the consent of the personal data subject. However, it was concluded that, currently, not all Internet resources or mobile applications warn about the processing of personal information. Preferably, you can find out by analyzing the appropriate settings or permissions (sometimes by default).

Also, according to the privacy policy of social networks, mobile applications, access to the processing of personal data is a prerequisite for the use of services. That is, there is no alternative, and the consent itself by its legal nature is conditionally voluntary.

It is alleged that the issue of processing information (personal data) about third parties is problematic. After all, in the case when a user provides access to his own page on a social network or a phone book – he automatically provides access to data about third parties without any of their personal consent. That is, in practice there is a situation in which the right to protection of this category of persons is systematically violated.

The legal experience of the European Union countries in the field of ensuring the security of personal data of citizens is analyzed.

The final part of the study emphasizes that the users of the Internet and social networks are representatives of public authorities, local governments, servicemen, employees of national law enforcement agencies and special services, and other secret agents. Accordingly, further scientific development requires strengthening of legal support and purposeful application of organizational measures, first of all, in the specified environment which can be used by foreign special services, in particular by the Russian Federation, in the interests.

Key words: *social network, Internet, destructive influence, international legal experience of personal data protection, cyberspace.*