



Черниш Роман Федорович,
кандидат юридичних наук,
доцент кафедри правознавства, Житомирський
національний агроекологічний університет,
Україна, м. Житомир
e-mail: ChernysRF@gmail.com
ORCID 0000-0003-4176-7569

doi: 10.21564/2414–990x.136.93352
УДК 342:004.738.5

СОЦІАЛЬНІ МЕРЕЖІ ЯК ОДИН ІЗ ІНСТРУМЕНТІВ НАКОПИЧЕННЯ ТА ПРОТИПРАВНОГО ВИКОРИСТАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН

Розглянуто окремі аспекти накопичення в соціальних мережах особистих даних користувачів. Проаналізовано негативні наслідки розміщення ідентифікуючих даних особи як для неї, так і для інтересів національної безпеки в цілому. Запропоновано конкретні кроки для вироблення принципово нових підходів до забезпечення захисту інтересів особи, суспільства та держави у інформаційній сфері.

Ключові слова: інформаційна безпека; Інтернет; соціальні мережі; накопичення персональних даних громадян; протиправне використання персональних даних громадян.

Черныш Р. Ф., кандидат юридических наук, доцент кафедры правоведения, Житомирский национальный агроэкологический университет, Украина, г. Житомир.
e-mail: ChernysRF@gmail.com ; ORCID 0000-0003-4176-7569

Социальные сети как один из инструментов накопления и противоправного использования персональных данных граждан

Рассмотрены отдельные аспекты накопления в социальных сетях личных данных пользователей. Проанализированы негативные последствия размещения идентифицирующих данных лица как для него, так и для интересов национальной безопасности в целом. Предложены конкретные шаги по выработке принципиально новых подходов к обеспечению защиты интересов личности, общества и государства в информационной сфере.

Ключевые слова: информационная безопасность; Интернет; социальные сети; накопления персональных данных граждан; противоправное использование персональных данных граждан.

Вступ. Загальновідомо, що протягом останніх років соціальні мережі перестали бути виключно інструментом для спілкування. Щоденно мільйони користувачів в усьому світі викладають інформацію (у тому числі й персонального характеру), яка у будь-який момент може бути використана або проти них, або

за певних обставин на шкоду національним інтересам. Особливо гостро окреслене питання постало для нашої держави в умовах фактичного її перебування у стані неоголошеної війни [16].

Наприклад, у серпні 2014 р. у таких соціальних мережах, як «ВКонтакте», «Однокласники», «Facebook» та «Twitter» було зареєстровано понад 40 млн українських акаунтів. Перше місце утримувала соціальна мережа «ВКонтакте» – більш ніж 27 млн облікових записів. Другу сходинку посіли «Однокласники» – близько 11 млн акаунтів (2012 р. – 5 млн акаунтів). У Facebook кількість українських облікових записів перевищила 3,2 млн [15].

При цьому, якщо проаналізувати кількість користувачів у Facebook, то лише з лютого по квітень 2016 р. кількість українських користувачів зросла на 400 тисяч. Станом на 25 квітня 2016 р. користувачами Facebook були 5,4 млн громадян України [8] на відміну від 3,2 млн у 2014 р. За наявними даними, 49,6 % молодих українців стверджують, що не уявляють життя без соціальних мереж. Якщо 71,9 % щодня користується загалом Інтернетом, то 65,8 % з них – переважно соціальними мережами [14].

Занепокоєння викликає той факт, що сучасний стан накопичення та збереження персональних даних громадян у соціальних мережах створює в тому числі й підґрунтя для їх залучення до протиправної діяльності на шкоду державним інтересам представниками спеціальних служб іноземних держав. Особливої актуальності досліджуване питання набуло в контексті ведення Російською Федерацією «гібридної війни» стосовно України. На жаль, розробка способів протидії вказаному виду злочинної діяльності значно відстає від потреб правоохоронної практики [18, с. 367].

Аналіз літературних даних і постановка задачі дослідження. Безпосередньо науковим дослідженням проблемних питань у інформаційній сфері займалися В. М. Брижко, О. О. Баранов, К. І. Беляков, В. Д. Гавловський, Д. В. Ланде, А. І. Марущак, В. С. Цимбалюк, М. Я. Швець та ін. Однак переважна більшість їх наукових праць стосувалася виключно глобальних питань забезпечення інформаційної безпеки без ґрунтового аналізу функціонування соціальних мереж, їх впливу на свідомість громадян, специфіки накопичення персональних даних та можливого протиправного використання всупереч волі останніх.

Метою статті є ґрунтовний аналіз специфіки накопичення персональних даних громадян у найбільш популярних у нашій країні соціальних мережах і вироблення конкретних пропозицій щодо необхідності внесення змін до національного законодавства з метою врегулювання окремих проблемних питань у вказаній сфері.

Основна частина. Передумовою створення соціальних мереж стала розробка в 1951 р. Р. Соломоноффим та А. Рапортом т. зв. «теорії про соціальні мережі» [6]. Уперше термін «соціальна мережа» було вжито представником Манчестерської школи англійським соціологом Джеймсом Барнсом для визначення зразків соціальних зв'язків, які йшли у розріз традиційних для багатьох

соціологів понять: обмежені групи (племена, сім'ї) або такі соціальні категорії, як стать чи етнічна належність тощо. Одначе соціальна мережа в Інтернеті у класичному вигляді з'явилася лише через понад 40 років – у 1995 р. Це був американський портал *classmates.com* (соціальна спільнота «Однокласники» є аналогом вказаного сайта).

Проте офіційним початком їх «життя» прийнято вважати 2003–2004 рр. Саме у цей період було запущено такі ресурси, як *LinkedIn*, *MySpace* і *Facebook* [20].

Зараз соціальні мережі, зважаючи на задекларовану мету їх створення – спілкування, надають користувачам усі можливі для цього інструменти – відео, чати, зображення, блоги, форуми тощо. Але поряд з цим вони наповнені непотрібною рекламою (спамом). Стає зрозумілим, що засновники соціальних мереж створюють їх, перш за все, з комерційною метою (рекламодавці платять гроші за показ контекстної реклами), а вже потім для спілкування людей.

Не викликає сумнівів той факт, що у соціальних мереж є технічні можливості відслідковувати інформацію про своїх користувачів, їх активність у мережі Інтернет незалежно від того, чи перебувають вони в соціальній мережі, тобто після виходу зі сторінок соціальної мережі, а також про користувачів мережі Інтернет, які взагалі не мають акаунта в соціальній мережі, шляхом створення профілів незареєстрованих користувачів [3]. Але ж значну частину персональних даних користувачі соціальних мереж повідомляють добровільно. Соціальні сервіси передбачають розміщення в Інтернеті відомостей, які так чи інакше (через реєстраційні дані, особливості поведінки у віртуальному просторі) дозволяють ідентифікувати особу користувача. Зокрема, більшість соціальних мереж передбачає розміщення на персональній сторінці прізвища та ім'я, дати народження, статі, місця народження (проживання), місця навчання/роботи, посади, інформації про сімейне становище, відомостей про батьків, братів/сестер, дітей тощо [10]. Після введення загальних відомостей у ході змістового наповнення відповідної сторінки можуть додаватися дані про факти зі свого особистого життя, рід занять, захоплення, національність, віросповідання, світлини, номер ICQ, Skype-ідентифікатор, партійну належність, коло друзів, колег, ділових партнерів тощо. Здебільшого акаунт користувача містить різні статистичні характеристики його перебування в системі: дату, час і тривалість останнього входу та перебування в системі, адреси, використані при підключенні комп'ютера тощо. Світлини, завантажені через смартфон із вбудованим GPS-модулем, містять точний час і GPS-координати місця, в якому було зроблено фото, а спеціальні сервіси дозволяють визначити, яким саме пристроєм ви фотографували та чи було відредаговано зображення у редакторі *Photoshop*.

На нашу думку, на увагу заслуговує випадок, що трапився із комп'ютерним винахідником Джоном Макафі. Його оголосили в розшук та арештували у Гватемалі завдяки exif-данним із фотографій, які його приятелі виклали в Інтернеті. Саме таким чином поліція визначила місцезнаходження підозрюваного [5].

Як бачимо, кожна із сторінок користувача в соціальній мережі – це необмежений та відносно легкодоступний архів його персональних даних. При цьому потрібно розуміти, що зважаючи на розвиток сучасних технологій, навіть у тому разі, коли вищевказана інформація буде знеособленою чи «рейковою», за певних умов (зв'язки, статистика перебування в мережі, зміст інформації, що «поститься» тощо) особу вдасться ідентифікувати.

Особливої актуальності набуває окреслена проблема з огляду на тенденцію до інтеграції соціальних сервісів. Так, на сьогодні Google забезпечує об'єднання даних про користувачів різних своїх сервісів: соціальної мережі Google+, служби електронної пошти Gmail, відеохостингу YouTube, фотосервісу Picasa, сервісу читання RSS-каналів Google Reader, сервісу оповіщення Google Alerts тощо [9]. Тобто стане зрозуміло, що різними сервісами користується одна і та ж особа. Та переважна більшість користувачів навіть не здогадується, наскільки широкому колу осіб може стати відомою надана ними інформація. Зазначене обумовлено тим, що власники переважної більшості соціальних мереж запевняють користувачів у закритості особистих даних від третіх осіб чи передбачають можливість її часткового відкриття лише за згодою.

Реалії ж сьогодення свідчать про інше: наприклад, коли користувач відкриває на ту чи іншу Інтернет-сторінку, то у контекстній рекламі розміщено саме ті товари чи послуги, якими напередодні він цікавився. Іншим прикладом може слугувати те, що переважна більшість соціальних мереж після введення інформації про місце проживання, навчання, електронну адресу тощо, автоматично пропонує додати друзів, однокласників та однокурсників.

Науковці, інші представники світової спільноти наголошували на порушенні власниками Інтернет-ресурсів (у першу чергу соціальних мереж) низки європейських законів про захист приватного життя, оброблення і використання даних користувачів без їх згоди. З метою припинення протиправної діяльності у вказаній сфері було ініційовано ряд судових позовів. Зокрема, Бельгійською Комісією із захисту даних (Belgian Privacy Commission) було подано позов до засновників Facebook, а судовий розгляд проти цілого ряду американських компаній ще кілька років тому ініціював австрійський бізнесмен Марк Шрамс, який занепокоївся про збереження особистих даних європейців після викриттів колишнього контрактика АНБ Едварда Сноудена про масове стеження американських спецслужб [1].

При цьому не варто себе тішити ілюзіями, що якщо користувач видалив будь-яку інформацію чи, наприклад, фото, то доступу до неї чи можливості відновлення вже не буде. Більшість громадян не замислюється над тим, що інформація, яку опубліковано на загальнодоступних ресурсах (в тому числі й у соціальних спільнотах), за певних умов може залишитися там назавжди, навіть після того, як її було видалено. Вважається, що таке поняття як «анонімність» у сучасних умовах є фікцією. Аналогічної думки дотримується й власник великого детективного агентства Pallorium (США) С. Рамбам. Зокрема, у своїй доповіді на конференції хакерів Hackers On Planet Earth у 2010 р. у Нью-Йорку

він зазначив: «Більше нічого не видаляється, не стирається й не забувається. Нічого з того, що ви розмістили в мережі, ні твіту, ні блогу, ні СМС, ані веб-сторінки, ані веб-сторінки, яку ви видалили через 15 секунд після публікації, ви вже не зміните. Нічого. Як тільки ви це розмістили, все всмоктується в систему, індексується, прив'язується до вашого імені і я можу це отримати. І ви вже не заженете джина назад у пляшку» [19].

Так, один із користувачів соціальної мережі «Facebook» звернувся з офіційним зверненням з проханням надати всі відомості щодо свого акаунту і виявив серед них дані трирічної давнини, які були видалені ним на персональній сторінці [11].

Окрім видимої шкоди, соціальні мережі містять невидимі загрози, які особливо активізувалися в ході проведення АТО на сході України – це накопичення і протиправне використання інформації про користувачів представниками спецслужб Російської Федерації. На нашу думку, така діяльність здійснюється з метою впливу на свідомість і підсвідомість громадян (насамперед молоді) та формування у них антигромадської позиції (недовіри до чинної влади, правоохоронних органів тощо), а також спонукання до вчинення актів непокори чи інших протиправних дій, які можуть призвести як до дестабілізації суспільно-політичної ситуації всередині країни, так і до нанесення шкоди іміджу держави у сфері зовнішньополітичних відносин.

Ще з 2010 р. у ФСБ РФ почали працювати інформаційно-аналітичні системи для моніторингу інтернет-ЗМІ, блогосфери і соцмереж. Перші роки вони вмiли працювати лише з відкритою інформацією. Тобто, якщо інтернет-користувач приховував про себе інформацію за допомогою налаштувань соцмережі, інтернет-робот ці дані не міг обробити. Зазначена проблема була вирішена зміною ліцензійних умов: кожного провайдера зобов'язали встановити обладнання, що дозволяє спецслужбам перехоплювати веб-трафік (тобто моніторити інформацію на етапі її додавання). Однак дані, розміщені на закордонних серверах, все одно були недоступні. У зв'язку з цим найбільші російські соцмережі (Mail.ru, «Однокласники», «ВКонтакте») в 2012-2013 рр. були поглинуті бізнес-групами, власників яких російські ЗМІ пов'язують із вищим керівництвом РФ (самі вони цей зв'язок заперечують).

У 2012 р., як свідчать офіційні дані, Служба зовнішньої розвідки Російської Федерації почала використовувати новітні інформаційні технології з метою моніторингу Інтернет-мережі. Так, було оголошено три закриті тендери на суму понад 30 мільйонів рублів із задекларованою метою вироблення нових методик моніторингу блогосфери (дослідження з кодовими позначеннями «Шторм-12», «Монітор-3» і «Диспут»). Однак, на думку експертів, уже тоді існувала ймовірність використання розробок на отримання персональних даних користувачів у російських та іноземних соціальних мережах [12].

Із 01.08.2016 р. у РФ набрав чинності так званий «антитерористичний пакет» законів, який складається із трьох нормативно-правових актів – один дозволяє обшукувати громадян лише за першої підозри поліції, другий кон-

тролює електронні платежі, а третій контролює обмін інформації в Інтернеті. Експерти переконані, що саме закон про інформацію може зашкодити українцям, адже відтепер ФСБ має безперешкодний доступ до приватного листування та персональних даних українських користувачів [13]. Уряд РФ зобов'язав власників соціальних мереж встановити обладнання і програмне забезпечення, за допомогою якого спецслужби можуть в автоматичному режимі отримувати інформацію про дії користувачів, дистанційно знімати інформацію і здійснювати стеження «в режимі реального часу». Відомості про діяльність учасників тієї чи іншої спільноти (учасниками якої є громадяни РФ) повинні зберігатися безпосередньо на території країни-агресора.

Зважаючи на викладене, з метою максимального захисту особистих персональних даних сформулюємо загальні правила користування соціальними мережами (насамперед тими, що зареєстровані на території РФ):

- заходячи в Інтернет-мережу, обов'язково використовуйте проксі сервери, анонімайзери, TOR і подібні сервіси;
- ознайомтеся з політикою приватності соцмережі;
- не інтегруйте акаунт в одній соцмережі з акаунтом в іншій;
- не додавайте до друзів незнайомих осіб;
- не встановлюйте легкодоступні паролі та намагайтеся їх періодично змінювати;
- з пересторогою ставтеся до матеріалів, які викладаєте у соціальні мережі;
- пам'ятайте: все, що ви постите онлайн, може бути розповсюджене набагато ширше, навіть за межами даної соцмережі;
- інстальуйте антивірусне програмне забезпечення тощо.

Висновки. Проблематика збереження в таємниці персональних даних користувачів є досить актуальною і вимагає подальших наукових пошуків. Зважаючи на необхідність забезпечення належного захисту конституційних прав громадян і національних інтересів від протиправних посягань, у рамках виконання планових заходів, передбачених Указом Президента України №32/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації»», вищі органи державної влади зобов'язані вжити невідкладних кроків для вироблення принципово нових підходів до забезпечення захисту інтересів особи, суспільства та держави у інформаційній сфері. Насамперед увага має бути спрямована на:

- внесення змін до національного законодавства в частині зобов'язання власників відповідних соціальних мереж зберігати установчі та інші особисті дані громадян України виключно на території нашої держави;
- удосконалення системи заходів правового регулювання доступу до персональної інформації в соціальних мережах шляхом чіткої регламентації права та обов'язків власників, адміністрації та технічного персоналу соціальних мереж, які функціонують на території України, щодо використання, зберігання та захисту персональної інформації;

- посилення відповідальності за незаконне розголошення, розповсюдження та використання персональної інформації, що накопичується в інформаційних масивах соціальних мереж;
- проведення відповідної роз'яснювальної роботи серед пересічних користувачів, насамперед молоді;
- залучення до розробки систем захисту персональних даних, відповідного програмного забезпечення вітчизняних ІТ фахівців;
- вироблення єдиного підходу до формування і закріплення на відповідному рівні обмежень щодо використання соціальних мереж деякими спеціальними категоріями громадян (військовослужбовці, співробітники правоохоронних органів тощо).

Список літератури:

1. Google и Facebook угрожают европейцам [Електронний ресурс]. – Режим доступу : <http://internetua.com/Google-i-Facebook-ugrojuat-evropeicam>.
2. Бельгийские регуляторы призывают суд «не бояться» Facebook [Електронний ресурс]. – Режим доступу : <http://internetua.com/belgiiskie-regulyatori-prizivauat-sud--ne-boyatsya--Facebook>.
3. Гавловський В. Д. До питання захисту персональних даних у соціальних мережах [Електронний ресурс] / В. Д. Гавловський. – Режим доступу : <http://pravoznavec.com.ua/period/article/26876/%C3>.
4. Гавловський В. Д. До питання несанкціонованого збору та систематизації персональних даних користувачів через соціальні мережі [Електронний ресурс] / В. Д. Гавловський. – Режим доступу : http://www.nbuv.gov.ua/old_jrn/soc_gum/bozk/2011_25-26/25_26text/g36.pdf.
5. Журналістика епохи соціальних мереж: виклики та небезпеки [Електронний ресурс]. – Режим доступу : <http://imi.org.ua/analytics/41174-jurnalistika-epohi-sotsialnih-merej-vikliki-ta-nebezpeki.html>.
6. Історія терміна «соціальна мережа» [Електронний ресурс]. – Режим доступу : <http://www.socialnetwork.com.ua/2012/07/istoriya-terminu-sotsialna-merezha/>.
7. Как следят за пользователями соцсетей [Електронний ресурс]. – Режим доступу : <http://vesti-ukr.com/infografika/64391-kak-sledjat-za-polzovateljami-socsetej>.
8. Кількість користувачів Facebook в Україні почала рости швидше [Електронний ресурс]. – Режим доступу : http://osvita.mediasapiens.ua/web/social/kilkist_koristuvachiv_facebook_v_ukraini_pochala_rosti_shvidshe/.
9. Куприков А. Интернет теряет анонимность. Сохранится ли свобода в сети: мнения [Електронний ресурс] / А. Куприков, Д. Штайсслингер. – Режим доступу : <http://www.iarex.ru/interviews/23120.html>.
10. Марущак А. І. Проблеми правового захисту персональних даних в умовах соціалізації інтернет-сервісів [Електронний ресурс] / А. І. Марущак, В. М. Панченко // Інформація і право. – Режим доступу : <http://ippi.org.ua/sites/default/files/12mais.pdf>.
11. Приватне життя в мережі // Euronews [Електронний ресурс]. – Режим доступу : <http://ua.euronews.net/programs/right-on/privatne-zhyttya-merezhi>.
12. Російські соціальні мережі та їх небезпека [Електронний ресурс]. – Режим доступу : <http://navkolonas.com/archives/16028>.
13. Спецслужби штурмують блогосферу (перепост) [Електронний ресурс]. – Режим доступу : <http://blog.i.ua/user/696590/1059940/>.
14. Украинская молодежь ежедневно пользуется Интернетом, – исследование / [Електронний ресурс]. – Режим доступу : http://institute.gorshenin.ua/news/1004_ukrainskaya_molodezh_ezhednevno.html.

15. Українці в соціальних мережах: нове дослідження від Яндексa [Електронний ресурс]. – Режим доступу : <http://watcher.com.ua/2014/08/21/ukrayintsi-v-sotsialnyh-merezhah-nove-doslidzhennya-vid-yandeksa/>.

16. Черниш Р. Ф. Протидія зловживанням з боку вимушених переселенців в ході отримання соціальних виплат [Електронний ресурс] / Р. Ф. Черниш // Порівняльно-аналітичне право: електронне наукове фахове видання юридичного факультету ДВНЗ «Ужгородський національний університет». – Режим доступу : http://pap.in.ua/2_2016/27.pdf.

17. Черниш Р. Ф. Щодо необхідності правової регламентації процедури внесення подання про усунення причини та умов, які сприяли вчиненню злочину / Р. Ф. Черниш // Досудове розслідування: актуальні проблеми та шляхи їх вирішення : матер. постійно діючого наук.-практ. семінару, 27 лист. 2015 р. / редкол. : С. Є. Кучерина (голов. ред.), В. В. Федосєєв (заст. голов. ред.) та ін. – Харків : Право, 2015. – Вип. № 7. – С. 158–160.

18. Черниш Р. Ф. Щодо окремих аспектів протидії інформаційному тероризму в сучасних умовах / Р. Ф. Черниш, І. М. Осауленко // Протидія терористичній діяльності: міжнародний досвід і його актуальність для України : матері. міжнар. наук.-практ. конф. (30 вересня 2016 р.). – Київ : Національна академія прокуратури України, 2016. – С. 367.

19. Чулівська І. Журналістика епохи соціальних мереж: виклики та небезпеки [Електронний ресурс] / І. Чулівська, Д. Снопченко. – Режим доступу : http://osvita.mediasapiens.ua/web/cybersecurity/zhurnalistika_epokhi_sotsialnikh_merezh_vikliki_ta_nebezpeki/.

20. Шахненко О. Вплив соціальних мереж на підлітків [Електронний ресурс] / О. Шахненко. – Режим доступу : <http://konf.koippo.kr.ua/blogs/index.php/blog2/title-50>.

References:

1. Google y Facebook uhrozhaiut evropejsam [Google and Facebook threaten the Europeans]. Retrieved from: <http://internetua.com/Google-i-Facebook-ugrojuat-evropeicam> [in Russian].

2. Bel'hyjskye rehulyatory przyvaiut sud «ne boiat'sia» Facebookhttp [The Belgian regulators urged the court «not to fear» with Facebook]. *internetua.com*. Retrieved from: <http://internetua.com/belgijskie-regulyatori-prizivauat-sud--ne-boyatsya--Facebook> [in Russian].

3. Havlovs'kyj, V.D. (2011). Do pytannia zakhystu personal'nykh danykh u sotsial'nykh merezhakh [On the issue of protection of personal data in social networks]. *pravoznavec.com.ua*. Retrieved from: <http://pravoznavec.com.ua/period/article/26876/%C3> [in Ukrainian].

4. Havlovs'kyj, V.D. (2012). Do pytannia nesanktsionovanoho zboru ta systematyzatsii personal'nykh danykh korystuvachiv cherez sotsial'ni merezhi [On the issue of unauthorized collection and systematization of personal data of users through social networks]. *nbuv.gov.ua*. Retrieved from: http://www.nbuv.gov.ua/old_jrn/soc_gum/bozk/2011_25-26/25_26text/g36.pdf [in Ukrainian].

5. Zhurnalistyka epokhy sotsial'nykh merezh: vyklyky ta nebezpeky [Journalism era of social networks: challenges and risks]. *imi.org.ua*. Retrieved from: <http://imi.org.ua/analytics/41174-jurnalistika-epohi-sotsialnih-merezh-vikliki-ta-nebezpeki.html> [in Ukrainian].

6. Istoriia terminu «sotsial'na merezha» [History of the term «social network»]. *socialnetwork.com.ua*. Retrieved from: <http://www.socialnetwork.com.ua/2012/07/istoriya-terminu-sotsialna-merezha/> [in Ukraine].

7. Kak slediat za pol'zovateliamy sotssetej [How to monitor the users of social networks]. *vesti-ukr.com*. Retrieved from: <http://vesti-ukr.com/infografika/64391-kak-sledjat-za-polzovateljami-socsetej> [in Russian].

8. Kil'kist' korystuvachiv Facebook v Ukraini pochala rosty shvydshe [The number of Facebook users in Ukraine began to grow faster]. *osvita.mediasapiens.ua*. Retrieved from: http://osvita.mediasapiens.ua/web/social/kilkist_korystuvachiv_facebook_v_ukraini_pochala_rosti_shvidshe/ [in Ukrainian].

9. Kuprykov, A., Shtaisslynher, D. Ynternet teriaet anonymnost'. Sokhranytsia ly svoboda v sety: mnenyia [Internet loses its anonymity. Does the freedom of the network will continue: Opinions]. *iarex.ru*. Retrieved from: <http://www.iarex.ru/interviews/23120.html> [in Russian].

10. Maruschak, A.I., Panchenko, V.M. (2012). Problemy pravovoho zakhystu personal'nykh danykh v umovakh sotsializatsii internet-servisiv [Problems of legal protection of personal data

in terms of socialization Internet services]. Information and Law Informatsiia i pravo. *ippi.org.ua*. Retrieved from: <http://ippi.org.ua/sites/default/files/12maisis.pdf> [in Ukrainian].

11. Pryvatne zhyttia v merezhi [Life Network]. *ua.euronews.net*. Retrieved from: <http://ua.euronews.net/programs/right-on/privatne-zhyttya-merezhi> [in Ukrainian].

12. Rosijs'ki sotsial'ni merezhi ta ikh nebezpeka [Russian social networks and their risk]. *navkolonas.com*. Retrieved from: <http://navkolonas.com/archives/16028> [in Ukrainian].

13. Spetssluzhby shturmuiut' blohosferu (perepost) [Special forces stormed the blogosphere (perepost)]. *blog.i.ua*. Retrieved from: <http://blog.i.ua/user/696590/1059940/> [in Ukrainian].

14. Ukrainskaia molodezh' ezhednevno pol'zuetsia Ynternetom, – yssledovanye [Ukrainian youth use the Internet every day – study]. *institute.gorshenin.ua*. Retrieved from: http://institute.gorshenin.ua/news/1004_ukrainskaya_molodezh_ezhednevno.html [in Russian].

15. Ukraintsi v sotsial'nykh merezhakh: nove doslidzhennia vid Yandeksa [Ukrainian social networks, a new study by Yandex]. *watcher.com.ua*. Retrieved from: <http://watcher.com.ua/2014/08/21/ukrayintsi-v-sotsialnyh-merezhah-nove-doslidzhennya-vid-yandeksa/> [in Ukrainian].

16. Chernysh, R.F. (2016). Protydiia zlovzhyvanniam z boku vymushenykh pereselentsiv v khodi otrymannia sotsial'nykh vyplat [Combating abuse of the internally displaced persons in the receiving social benefits]. Comparative Analytical right. Porivnial'no-analitychne pravo – elektronne naukove fakhove vydannia iurydychnoho fakul'tetu DVNZ «Uzhhorods'kyj natsional'nyj universytet [Electronic scientific specialized edition of the Law Faculty SHEE «Uzhhorod National University]. *pap.in.ua*. Retrieved from: http://pap.in.ua/2_2016/27.pdf [in Ukrainian].

17. Chernysh, R.F. (2015). Schodo neobkhidnosti pravovoi rehlementatsii protsedury vnesennia podannia pro usunennia prychny ta umov, iaki spryialy vchynenniu zlochynu [Regarding the need for legal regulation of procedure of introducing the idea of eliminating the causes and conditions that contributed to the commission of the crime]. Dosudove rozsliduvannia: aktual'ni problemy ta shliakhy ikh vyrishennia [Pre-trial investigation: current problems and solutions: materials nauk. permanent and practical. workshop]. Kharkiv: Pravo, 2015. Issue 7, 158–160 [in Ukrainian].

18. Chernysh, R.F., Osaulenko, I.M. (2016). Schodo okremykh aspektiv protydyi informatsijnomu teroryzmu v suchasnykh umovakh [Regarding certain aspects of counter terrorism information in modern conditions]. Protydiia terorystychnij diial'nosti: mizhnarodnyj dosvid i joho aktual'nist' dlia Ukrainy [Combating terrorism: international experience and its relevance to Ukraine: materials of international scientific conference (30 September 2016)]. Kiev: Natsional'na akademiia prokuratury Ukrainy, 2016, 367 [in Ukrainian].

19. Chuliv's'ka, I., Snopchenko, D. Zhurnalistyka epokhy sotsial'nykh merezh: vyklyky ta nebezpeky [Journalism era of social networks: challenges and risks]. *osvita.mediasapiens.ua*. Retrieved from: http://osvita.mediasapiens.ua/web/cybersecurity/zhurnalistyka_epokhy_sotsialnykh_merezh_viklyki_ta_nebezpeki/.

20. Shakhnenko, O. Vplyv sotsial'nykh merezh na pidlitkiv. *konf.koippo.kr.ua*. Retrieved from: <http://konf.koippo.kr.ua/blogs/index.php/blog2/title-50>.

Chernysh R. F., PhD in Law, Associate Professor, Law Zhytomyr National Agroecological University, Ukraine, Zhytomyr.

e-mail: ChernyshRF@gmail.com ; ORCID 0000-0003-4176-7569

Social networks as one of the instruments of accumulation and illegal use of personal data of citizens

It is well known that in recent years, social networks have ceased to be exclusively a tool for communication. Every day, millions of users around the world provide information (including personal data), which at any moment can be used either against them or, in certain circumstances, to the detriment of national interests. Especially sharply delineated issues raised for our country in terms of its actual stay in a state of undeclared war.

However, attention should be paid to the fact that a significant part of the personal data of users of social networks reported voluntarily. Most social networks involves placing personal page on name, date of birth, gender, place of birth (residence) place of study / work, office, information about family position, information on parents, brothers / sisters, children and so on. In most, the user account contains different statistical characteristics of his stay in the system, date, time and duration of the last entry and stay in the system, the address used when connecting a computer and more.

We can conclude that each page of a user's social network – is readily available and relatively unlimited archive of his personal data.

The issue of preserving a secret personal given users is important and requires its further scientific development. Given the need to ensure adequate protection of constitutional rights and national interests from illegal encroachments, within the framework of the planned measures provided for by the Decree of the President of Ukraine №32 / 2017 «On the decision of the National Security and Defense of Ukraine of 29 December 2016» On the state and threats cyber security urgent measures to neutralize them», it seems necessary at the highest state authorities to take immediate steps for the development of innovative approaches to protecting the interests of individuals, society and the state in the information sphere.

Keywords: information security; internet; social networks; storage of personal data of citizens; illegal use of personal data of citizens.

Надійшла до редколегії 17.02.2017 р.