Глобальні соціальні мережі та кібербезпека особистості

Досліджуються глобальні соціальні мережі (*Facebook, LinkedIn* тощо) як нова віртуальна реальність XXI століття, яка може зашкодити кібербезпеці особистості. Аналізуються ситуації, коли громадянин не може висловлювати приватні думки без стеження з боку держави та порушуються права на приватність і людську гідність. Вивчаються порушення фундаментальних прав людини на думку, точку зору, висловлювання. Пропонуються правила безпеки в соціальних мережах.
Ключові слова: **глобальні соціальні мережі, кібербезпека особистості, Інтернет, фундаментальні права людини.**

Ольга ЗЕРНЕЦЬКА,
доктор політичних наук,
професор,
завідувач відділу глобальних
і цивілізаційних процесів
Державної установи
«Інститут всесвітньої історії
НАН України»

Global social network and cybersecurity of an individual

Olga ZERNETSKA, Doctor of Political Sciences, Professor, Head of Department of State Institution 'The Institute of World History at National Academy of Sciences of Ukraine'

Global social networks (Facebook, LinkedIn, etc.) as a new virtual reality of the 20th century that may harm cybersecurity of any individual is investigated. The situation of a citizen unable to communicate private thoughts without surveillance of a state is analyzed. The fundamental rights of freedom of thought, opinion and expression that are at the center of any democratic practice are detected. Some rules of behavior in social networks are recommended.
Keywords**: global social networks, cybersecurity of an individual, Internet, the fundamental rights.**

На початку XXI століття соціальні мережі стали дуже популярними. Люди використовують їх, щоб підтримувати зв'язки зі своїми родинами та друзями. Це такі глобальні соціальні мережі, як *MySpace, FriendWise, FriendFinder, Yahoo! 360, Facebook, Orkut, Classmates* та багато інших. У кожній країні є також свої соціальні мережі. У Сполучених Штатах, наприклад, багато юзерів користуються *LinkedIn*, щоб мати різні бізнесові контакти та відстежувати можливості щодо зростання своїх кар'єр.

Але не всі підозрюють, що користування Інтернетом у добу соціальних медіа чи, як її ще називають, *Web 2.0. (blogs, wikis, file sharing, social networking sites, microblogs)* несе в собі багато загроз для користувачів Інтернету. «Останніми роками він перетворився із системи, орієнтованої передовсім на постачання інформації, на медіум для комунікації та розбудови комунікації» [1].

Поняття *Web 2.0.*, соціальний софтвер, сайти соціального мережування, такі як *Facebook, Twitter, MySpace*, з'явилися в цьому контексті. Разом із цими платформами сформувалася й зберігається величезна кількість персональних даних, які систематично оцінюються та використовуються рекламодавцями для пошуку своїх таргетингових користувачів.

У світі глобальної економічної конкуренції, кризи та побоювання тероризму і корпорації, і державні установи мають дедалі більший інтерес до цих персональних даних. Тому особливо важливими стають такі питання:

- як змінюється ландшафт у цій сфері;
- як відбувається збирання комерційних персональних даних для реклами;
- як співвідносяться сайти для споживачів та інтерактивні медіа;
- як відбувається саморозкриття в соціальних мережах;
- як стежать за тими, хто обмінюється файлами;
- як трактується прайвесі в добу Інтернету;
- що таке громадянське самостеження за сайтами соціальних мереж та мережеве стеження в транснаціональному просторі.

Сайт «Що таке соціальне мережування?» [2] в доступній формі ознайомлює користувачів із тим, які небезпеки чекають необачних юзерів у соціальних мережах. Відчувається, що він спрямований на молодіжну групу. Розмова на ньому йде від першої особи: «Я впевнений, що ви обізнані про наявність небезпек, пов'язаних із соціальними мережами, включаючи крадіжку даних та віруси. Найбільшу небезпеку часто становлять он-лайн хижаки чи індиві-

думи, котрі видають себе за когось, ким вони насправді не є. Хоча в он-лайн мережуванні існує небезпека, вона існує й у реальному житті. Такі саме поради, як і ті, що стосуються ситуацій, коли ви зустрічаєте незнайомця в клубі чи барі, у школі чи на роботі, стануть вам у пригоді, щоб убезпечити себе он-лайн». Далі даються конкретні настанови щодо того, як треба поводитися в кіберпросторі:

• створи свій особистий медіа-прайвесі простір, аби лише друзі могли бачити твій профіль та контент;

• не приймай дружніх запрошень від незнайомців;

• не розголошуй свій щоденний розклад справ;

• не давай людям змоги дізнатися, коли тебе немає вдома;

• не використовуй локально базовані сервіси типу *Facebook Places* і *Foursquare*, які автоматично підказують твоє місце перебування;

• не публікуй фотографії членів своєї родини (особливо малят) або дорогих речей, що є у твоїй домівці;

• запропонуй *Google Maps* зробити розпливчастими фото твоїх будинку, машини або будь-чого, що для тебе є занадто приватним, аби бути висвітленим публічно.

Зрозуміло, що ці поради написані для молодого покоління, але вони стосуються кожного. Натомість поради американської впливової газети *Washington Post* розраховані передовсім на солідну публіку. Після скандалу 2014 року, коли хакери оприлюднили інтимні фотографії голлівудських зірок, які ті зберігали в сервісі *iCloud*, на сайті *Washington Post* виклали декілька порад, як захищати свої дані [3]:

1. Переконайтеся, що деякі з ваших фото не потрапили в *iCloud* без вашого відома.

Річ у тім, що деякі компанії на кшталт *Apple, Microsoft, Dropbox* пропонують автоматично зберігати в «хмарі» фотографії з ваших телефонів або планшетів.

2. Користуйтеся двоетапною автентифікацією.

Ця процедура допоможе вам підвищити захищеність акаунтів за допомогою додаткового короткого коду, крім паролю при вході.

3. Уникайте пасток хакерів.

Хакерні атаки часто-густо стають успішними не завдяки високим технологіям, а завдяки введенню в оману потерпілих, які в підсумку самі видають зловмисникам потрібні їм дані.

Але не тільки хакери прокладають собі шлях до розкриття даних американців. Це роблять і федеральні інститути США. Вони змусили відомий Інтернет-пошуковик *Yahoo* відкрити доступ до конфіденційних даних користувачів, погрожуючи щоденно штрафувати компанію на 250 тисяч доларів. Про це сповіщає адміністрація *Yahoo* в Інтернет-блозі своєї компанії.

Компанія, діставши дозвіл суду, опублікувала 1,5 тисячі сторінок документів, пов'язаних із судовим позовом проти Агентства національної безпеки (*NSA*). Юрисконсульт *Yahoo* Рон Белл додав до цієї публікації відповідні коментарі. З документів стає зрозуміло, що спроба Агентства національної безпеки отримати доступ до персональних даних стала можливою лише 2007 року після того, як у законодавство США були внесені зміни, які давали змогу владі вимагати від Інтернет-компаній інформацію про користувачів.

Спочатку *Yahoo*, як стверджує Р. Белл, відмовлялася виконувати накази Агентства національної безпеки, вважаючи їх антиконституційними. Компанія подала на агентство позов до суду, що займається наглядовою діяльністю над розвідками, вимагаючи скасувати таку антиконституційну вимогу. Але цей суд здебільшого стає на бік влади, тому компанія після півторарічної боротьби зазнала поразки.

Вимогою Агентства національної безпеки було отримання від компанії метаданих про користувачів її електронної пошти. Такі дані дають можливість відстежити, між ким і коли відбувається обмін посланнями. При цьому дозволу на доступ до листів, як стверджують у *Yahoo*, спецслужби ніколи не мали. Влітку 2013 року найбільші Інтернет-компанії США, які брали участь у передачі даних Агентству національної безпеки, звернулися до суду з вимогою дозволити публікацію статистичних даних щодо запитів спецслужб. Перша публікація таких даних відбулася в лютому 2014-го. Нині Інтернет-компанії намагаються провести через Конгрес закон, який захищав би конфіденційність приватного листування [4].

Улітку 2013 року в Інтернеті був опублікований лист організацій громадянського суспільства світу до Конгресу Сполучених Штатів про Інтернет- і телекомунікаційне стеження. У ньому йшлося: «Ми пишемо як коаліція організацій громадянського суспільства з усього світу для того, щоб висловити серйозну занепокоєність численними прикладами стеження за американськими й неамериканськими громадянами. Ми дуже занепокоєні тим, що дані, які збираються під час стеження в Сполучених Штатах, передаються іншим державам, зокрема Великій Британії, Нідерландам, Канаді, Бельгії, Австралії та Новій Зеландії. Багато американських компаній глобального значення роблять те саме».

Як бачимо, група могутніх глобальних Інтернет-компаній, що оперізують світ, співпрацює зі спецслужбами, хоча тоді, коли вони тільки виходили на ринок інформаційно-комунікаційних послуг, вони обіцяли повну приватність користувачам. На що це з часом перетворюється, простежмо на прикладі найбільшої у світі соціальної мережі *Facebook*.

Соціальна мережа *Facebook* перетнула межі країни, регіону й сягнула глобальних масштабів. У чому секрет її успіху в світі? *Facebook* принципово відмінна від усіх інших Інтернет-компаній, які їй передували, хоча б тим, що вона теоретично й практично ґрунтується на справжній інформації про особу. «Тут важливо бути собою. В Інтернеті всі давно вже звикли до анонімності, ролей, псевдонімів, нікнеймів... Але тут усе це зайве. Якщо ви вигадуєте собі образ чи надто штучно поводитеся, у *Facebook* вам робити нічого. Будьте собою, інакше друзі вас не впізнають чи не зафрендять. Тут швидко дізнаються, хто ви насправді, лише перевіривши список ваших друзів. Саме вони є вашим посвідченням особи», – відзначає Дональд Кіркпатрік, який написав книгу про цю компанію [5]. Він замислюється над соціальними й психологічними змінами, спричиненими ефектом *Facebook*. Розуміє, що ще замало наукових даних, аби з упевненістю говорити про такі зміни, але наголошує, що для багатьох *Facebook* – джерело оманливого почуття єдності (5000 осіб – максимально дозволена кількість друзів), яка з часом вироджується в глибоку самотність. До того ж він ставить запитання: чи не втрачають молоді люди, котрі днями сидять у *Facebook*, здатність радіти й дивуватися тому, що відбувається в реальному світі й оточує їх повсякденно?

З часом ейфорія від знаходження старих друзів та придбання нових зникає, а викладення у *Facebook* «прикольних» фотографій з вечірок, де витівки студентів часто-густо були зафіксовані їхніми товаришами без дозволу (тобто в соціальну мережу потрапляли кадри з пляшками чи келихами в руках друзів, сп'янілими обличчями, моментами, коли молодь бавилася легкими наркотиками, та інші компрометувальні фото), не лише почало дратувати тих, хто на них опинився, а й стало серйозною перешкодою в їх кар'єрному зростанні. Адже фірми, державні установи й компанії перед тим, як наймати на роботу претендентів, відстежують їхнє життя та поведінку в кіберпросторі, зокрема в соціальній мережі *Facebook*, де вони представлені в різних іпостасях під своїми справжніми іменем і прізвищем.

Опитування, проведене серед американських роботодавців 2009 року, показало, що 35% компаній відхилили претендентів на посади через інформацію, знайдену про них у соціальних мережах. Перша причина відмови: розміщення провокативних фотографій чи недостойної інформації [5, с. 276]. Те саме почали практикувати й університети, оскільки віковий ценз доступу до *Facebook* знизився до 13 років. Тепер під час вступних

кампаній члени приймальних комісій в університетах та коледжах також перевіряють соцмережі.

Марк Цукерберг є переконаним сповідачем «відкритого прозорого світу». Він вважає, що відкрито визнаючи свою сутність і однаково поводячись із усіма друзями, «ми творимо здорове суспільство». Але з часом зростає кількість людей, яким здається, що оприлюднення приватної інформації у *Facebook* стає надмірним. Насправді, як свідчить Д. Кіркпатрік, «Цукерберг теж не вірить у тотальну відкритість. Він не пише про конфіденційні зустрічі у своєму профілі» [5, с. 274].

Реальна політика його компанії доводить, що *Facebook* змушує користувачів ділитися власними даними, хоча приводом до цього є досить безневинне прагнення «створити безпечнішу, надійнішу версію Інтернету, де люди свідомі наслідків своїх учинків, де вони послуговуються справжніми іменами».

Зовнішні експерти не підтримують ці міркування Цукерберга. От думка одного з них – Марка Ротенберга, виконавчого директора Центру електронної приватності інформації (*EPIC*) і досвідченого «сторожового пса Інтернету», який пише, що з кожним роком *Facebook* створює дедалі більше перешкод на шляху до захисту приватності користувачів. Вони позбавлені можливості просто контролювати приватність інформації, а сам *Facebook*, попри переконання й сповідування прозорості, не надто прозоро показує, що він робить із нашими даними.

Порушення конфіденційності з боку *Facebook* шкодить не тільки абітурієнтам і випускникам університетів. Велику загрозу становить він для політиків та офіційних осіб вищого рангу, оскільки може зруйнувати їхні кар'єри. Так, політичний кандидат з канадського Ванкувера зняв свою кандидатуру, коли в газеті з'явилася фотографія, де двоє людей натягують його труси. Йона Фавро, спічрайтера Барака Обами, публічно осудили, коли в блозі з'явилася фотографія, де він на одній із вечірок мацає груди картонної Гілларі Клінтон. На *Facebook* знімок вивісив хтось із друзів... Можливо, Б. Обама думав якраз про інцидент з Фавро, виступаючи перед старшокласниками у Вірджинії навесні 2009-го: «Будьте обережні з тим, що ви розміщуєте на *Facebook*, – попередив він, – оскільки в еру *YouTube* усе, що ви робите, колись може неочікувано вигулькнути на поверхню. А доки ви молоді, ви робите багато дурниць».

Із розвитком соцмережі дедалі гостріше постають проблеми конфіденційності. Від її прозорості постраждали люди, посади яких потребують таємниці. Приміром, після того як у Великій Британії в середині 2009 року оголосили, що сер Джон Соерс очолить управління контррозвідки – Таємну розвідувальну службу (колись відому як *MI6*), газета *Daily Mail* знайшла публічні фотографії його з дружиною, розміщені нею на *Facebook*. Там були знімки зі свят, зображення друзів сім'ї й подробиць про те, де він жив і чим займався.

Прикладом знаменитості світового калібру, яка порушила модель *Facebook*, можна назвати Білла Гейтса, котрий закрив свій особистий профіль у соцмережі на початку 2008 року.

Отже, існує дилема: люди прагнуть поширювати особисту інформацію скрізь, набувати популярності, але при тому хотіли би бути захищеними від неочікуваного розголошення, яке може завдати їм шкоди. Проблема в тому, що нашкодити небажаним розголошенням інформації може лише людина, котру користувач «додав у друзі», – таке собі дружнє порушення приватності. Для запобігання появі провокативних фотографій у соцмережі в Сполучених Штатах останніми роками заборонено користуватися фотоапаратом на університетських вечірках, а в деяких закладах є навіть спеціальні темні кімнати, де ніхто не зможе зафіксувати розпивання алкоголю чи куріння трави. Однак такі застережні заходи примушують замислитися: чи насправді *Facebook* сприяє розвитку «прозорого відкритого суспільства», якщо стають потрібні темні кімнати для втаємничення не найкращих людських проявів? Чи не призводить це натомість до вкорінення подвійних стандартів моралі?

Початкове призначення *Facebook* як місця, де можна знайти своїх друзів з реального світу, постійно відсувалося на другий план. Важлива віха в розвитку сайта – поява сторінок компаній (а не друзів). Тепер їхні оновлення з'являються в стрічці новин поряд із новинами від друзів. Хоч би як намагалися маркетологи з *Facebook* позитивно схарактеризувати цей крок, очевидним є одне – комерціалізація, монетизація компанії. Вона отримує величезні прибутки саме завдяки рекламі – єдиному шляху стати справжньою бізнес-компанією. Завдяки цьому *Facebook* перетворилася на одне з найкращих рекламних середовищ сучасності. До того ж інформація, яку вона має про своїх користувачів, – «золота жила» для ринкових досліджень, для створення таргетингової реклами. Саме ці стратегії дали змогу *Facebook* спокійно пережити глобальну фінансово-економічну кризу 2008 року й стати публічною компанією.

Могутність *Facebook*, її потенціал і амбіції щодо контролю над користувачами й платформою щонайменше такі самі, як були колись у *Microsoft*, але *Facebook* контролює власну платформу більше, ніж *Microsoft*. «*Facebook* може натиснути кнопку й вимкнути вас. Усіх вас. Будь-коли» [5, с. 446]. Автор відзначає: якщо розмірковувати радикально, *Facebook* може перебрати на себе ключові функції урядів. Він наводить слова Ю. Мільнера, російського інвестора компанії: «*Facebook Connect* – це загалом ваш паспорт, ваш он-лайновий паспорт. Паспорти видає уряд. Тепер з'явилася ще одна інституція, яка цим займається. Так народжується конкуренція. Але хто сказав, що видавати паспорти конче має уряд? Ми просто перейдемо до глобального громадянства». Питання в тому, чи всі користувачі *Facebook* прагнуть мати глобальне громадянство? Чи це кінцева мета М. Цукерберга, який з початку запуску сайта був більше зацікавлений у зростанні кількості користувачів, ніж у зростанні прибутків? Чи зацікавлені уряди країн світу делегувати *Facebook* свої повноваження? І все ж таки, коли одна приватна компанія глобального масштабу має інформацію про переважну більшість населення Землі, чи це не ознака її м'якого панування (монополії) в сучасному світі, панування, багато з ефектів якого нікому, крім Цукерберга, не відомі, а може, навіть і йому?

Мабуть, про ці глобальні ефекти Марк Цукерберг усе ж добре знає. Станом на 2015 рік його статок становив 33,4 мільярда доларів США. Зміни за рік додали йому 3,4 мільярда доларів. За рейтингом *Forbes* він посідає 16 місце серед найбагатших людей планети. Так-от, засновник і генеральний директор *Facebook* і далі веде компанію до ринкових рекордів, хоча для частини молодої аудиторії соціальна мережа поступово стає анахронізмом. 2014 року дохід Цукерберга зріс на 58% завдяки кращій віддачі від мобільної реклами. Аудиторія компанії – близько 1,4 мільярда осіб у всьому світі, які дивляться в день 3 мільярди відеороликів. 300 мільйонів користувачів акумулюють «фотоаплікацію» *Instagram*, що належить цій мережі, і ще 700 мільйонів використовують месенджер *WhatsApp*, який був придбаний 2014 року за рекордні 19 мільярдів доларів.

Куди ж подівся юний Марк, котрий мріяв про прозорий Інтернет і про відсутність реклами в створеній ним соціальній мережі? Безжальні закони ринкової конкуренції привели його до пулу маленької групи величезних Інтернет-компаній, де він опинився в лідерах.

Ден Гіллмор у статті «Нові редактори Інтернету» запитує: «Хто дав їм таку владу? Ми з вами. І якщо ми не заберемо те, що віддали – і що в нас віднімають, – то цілком заслуговуватимемо на нові реалії: концентрацію медійної влади, яка шкодитиме, якщо їй не завадити, нашій традиційній свободі вираження» [6].

Отже, складна ситуація зі збереженням прайвесі в соціальних мережах і при користуванні Інтернет-пошуковиками, а також інтерактивними мультимедійними додатками ставить складні запитання як перед творцями Інтернету, так і перед глобальною Інтернет-спільнотою: як зберегти право на свободу слова, право на комунікацію в глобальній громадській комунікаційній сфері, уособленням якої сьогодні великою мірою є Інтернет, як не перетворитися на об'єкт для стеження, аналізу та використання різними інституціями – від спецслужб до маркетологів і рекламодавців.

Можна підсумувати, що введення механізмів стеження в серцевину глобальних диджитальних комунікацій серйозно загрожує правам людини в диджитальну еру. **Всі нові форми децентралізованої влади відбивають фундаментальні зсуви структури інформаційних систем у модерних суспільствах.** І кожен крок у цьому напрямі повинен бути розглянутий і широко, і глибоко, і транспарентно.

Список використаних джерел:

1. Internet and Surveillance / Ed. by C. Funch, K. Boersma, A. Albrechtslund and M. Sandoval. – New York: Routledge, 2011. – 332 p.

2. What is Social Networking? [Електронний ресурс]. – Режим доступу: http://www.whatissocialnetworking.com

3. Как повысить безопасность ваших фоторгафий в «облаке»? [Електронний ресурс]. – Режим доступу: http://www.inosmi.ru/world/20140904/222797438.html

4. Федеральные власти и *Yahoo* [Електронний ресурс]. – Режим доступу: http://www.russian-bazar.com/ru/mnews/156958.htm

5. *Кіркпатрік Д.* Ефект *Facebook*. Внутрішня історія компанії, що об'єднує світ / Д. Кіркпатрік. – К.: Темпора, 2013. – 488 с.

6. *Gillmor D.* The New Editors of the Internet / D. Gillmore // The Atlantic. – 2014. – 24 August.

Global Social Network and Cybersecurity of an Individual

At the beginning of the XX century social networks became very popular. People use them to keep in touch with their families and friends. These are such global social networks as *MySpace, FriendWise, FriendFinder, Yahoo! 360, Facebook, Orkut, Classmates*, etc. There are also own social network services in every country. In the United States, for example, many users have LinkedIn to have different business contacts and to follow the possibilities in their career developments.

But not all understand that using the Internet in the times of social media, or like it is already called *Web 2.0.* (*blogs, wikis, file sharing, social networking sites, microblogs*), carries in itself many threats for the users of the Internet. "During the recent years it has transformed from the system, which was oriented foremost on the supply of information, to the medium for communication and development of communication" [1].

Concept *Web 2.0.*, social software, sites of social web such as *Facebook, Twitter, MySpace*, appeared in this context. Together with these platforms the enormous amount of personal information was formed and is stored, and which is systematically estimated and used by advertisers to look for their target users.

In the world of global economic competition, crisis and fear of terrorism and corporations, the state institutions have all greater interest to this personal data as well. Therefore the following questions become of great importance:

- how the environment changes in this sphere;
- how the gathering of commercial personal data for advertising is done;
- how the sites for users and interactive medias are correlated;
- how self-revealization is done in social networks;
- how those who make exchange of the files are watched;
- how privacy is interpreted in the time of the Internet;
- what the civil surveillance after the sites of social networks and the network surveillance in the transnational space mean.

Site "What is social network?" [2] acquaints the users in an intelligible form with the dangers that are waiting for imprudent users in the social networks. It is felt that its target audience is the youth. The conversation goes from the first person: "I am sure that you all are well-informed about the presence of dangers related to the social networks, including the theft of information and viruses. The most dangerous are on-line predators or individuals who pretend to be someone whoever they are not in actual fact. Exactly the same pieces of advice as those which relate to the situations when you meet a stranger in a club or bar, at school or at work, will be useful in order to feel safe on-line". Further you will find the concrete rules on how you should behave in the cyberspace:

- create your personal media-privacy space so that only your friends could see your profile and content;
- do not accept invitations to become friends from the strangers;
- do not make your daily curriculum of businesses public;
- do not give people the possibility to know when you are not at home;
- do not use the locally based services as *Facebook Places* and *Foursquare* which show your place of stay automatically;
- do not show the pictures of your family (especially kids) or expensive things which you have in your house;
- ask *Google Maps* to make the vague photos of your house, car or anything that is private for you in order to be shown in public.

It's clear that these pieces of advice are written for the young generation but they concern everyone. But the pieces of advice published by the American influential newspaper *Washington Post* are foremost for solid audience. After the scandal in 2014, when hackers made public the intimate pictures of the Hollywood stars which were stored in *iCloud* service, the *Washington Post* newspaper published on its site a few pieces of advice how to protect the information [3]:

1. Make sure that any of your photos did not get in iCloud without your consent.

The thing is that some companies like *Apple, Microsoft, Dropbox* offer to store the pictures from your telephones or tablets in "cloud" automatically.

2. Use two level auto identification.

This procedure will help you to protect your accounts better with the help of additional short code, in addition to the password at the entrance.

3. Avoid the traps of hackers.

Hacker attacks often become successful not due to high technologies but due to cheating the victims who finally give the necessary data to abusers.

But not only hackers pave the way to disclose the data of Americans. It is also done by the federal institutions of the USA. They compelled the known Internet-searcher *Yahoo* to give them access to the confidential data of its users,