DOI: 10.46340/eppd.2020.7.4.20

Ihor Ishchenko, ScD in Political Science
ORCID ID: https://orcid.org/0000-0001-5799-7364
Oles Honchar Dnipro National University, Ukraine

SOCIAL NETWORKS AS A SOCIAL SECURITY CHALLENGE: PERSONAL AND STATE-LEVEL DIMENSION

Ігор Іщенко, д. політ. н.
Дніпровський національний університет імені Олеся Гончара, Україна

СОЦІАЛЬНІ МЕРЕЖІ ЯК ВИКЛИК ДЛЯ СОЦІАЛЬНОЇ БЕЗПЕКИ: ОСОБИСТІСНИЙ ТА ДЕРЖАВНИЙ ВИМІР

The article considers specific characteristics of the process of communication via online social networks, which alongside with new possibilities also lead to emergence of new threats and destabilizing factors for the society in cyber-space. Within the article the nature and origins of these threats are examined, as well as their possible consequences for social and state security. Detected general tendencies are extrapolated on political reality of Ukraine which is forced to resist open acts of information aggression. Conclusions are drawn concerning existing points of connection between the fields of social and state security, on the basis of which the recommendations are given on creation of state strategy of security enforcement and introduction of efficient tools for governance and control over the cyber space.

Keywords: social security, state security, information warfare, social networks, communication.

Постановка проблеми. Природа будь-якого середовища, здатного виконувати роль платформи для суспільно-політичних процесів, різнорівневої комунікації та взаємодії між окремими індивідами і суспільними групами, має визначний вплив на те, яку форму приймають ці процеси, як саме наявними каналами зв'язку користуються суб'єкти комунікації. Мережа Інтернет як середовище суспільної комунікації визначається відсутністю єдиного центру, що контролював би комунікацію, за глобальної розгалуженості різноманітних зв'язків. Відповідно, «виникнення і розвиток соціальних мереж в Інтернеті за своєю суттю не має керівних центрів»[1]. Відносна неконтрольованість та розмитість комунікаційних процесів в мережі Інтернет спричиняє зникнення чітко окреслених граней між особистою та публічною сферою життєдіяльності. Ускладнюється також і політичний процес, оскільки в глобальній мережі будь-хто може стати джерелом політично значимого висловлювання або дії. Подібна трансформація відбувається і в сфері безпеки. Серйозна загроза може походити від окремих користувачів або невеличких груп, в той час як основний удар під час атаки у віртуальному просторі приймають на себе не збройні сили чи служби безпеки тієї чи іншої держави, а життєво важлива інфраструктура та усталені суспільні зв'язки. Окреслена проблема є особливо актуальною для України, враховуючи зовнішню агресію та пов'язаний із нею постійний зловмисний інформаційний вплив. Метою цієї статті є з'ясування взаємного впливу сфери соціальної та національної безпеки в Інтернеті, визначення специфіки й важливості захисту кожної окремої особи для безпеки всієї держави, із наданням відповідних рекомендацій щодо коригування державної стратегії контролю над мережею Інтернет.

Аналіз останніх досліджень і публікацій. Українська наука приділяє певну увагу суспільній та політичній ролі соціальних мереж. Найбільш ретельне дослідження цього питання надається в роботах О. Онищенка[2] та В. Горового[3], окремі аспекти розглядаються

[1] Іщенко, І.В. (2015). *Політичні інститути в нестабільному середовищі: функціональні особливості.* Дніпро: Дніпровський національний університет імені Олеся Гончара, 135.
[2] Онищенко, О.С. та ін. (2014). *Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства*. Київ: НАН України, Нац. б-ка України ім. В. І. Вернадського.
[3] Горовий, В.М. (2010). *Соціальні інформаційні комунікації, їх наповнення і ресурс*. Київ: НАН України, Нац. б-ка України ім. В. І. Вернадського.

Л. Іващук[1], Ю. Якименком[2] та С. Коноплицьким[3]. Перелічені дослідники розглядають соціальні мережі переважно в позитивному контексті, як інструмент сприяння політичній комунікації, організації та мобілізації прогресивних суспільних рухів. Соціальні мережі як джерела загроз ще не стали предметом детального розгляду в складі об'ємних досліджень, дисертацій чи монографій. Однак, окремі статті, що торкалися цієї проблеми, були опубліковані в останні декілька років. Це, зокрема, публікації К. Молодецької 2016[4] та 2017[5] рр., А. Пелещишина та Р. Гумінського [6]. Серед закордонних авторів, які розглядали наслідки розвитку соціальних мереж в Інтернеті для соціальної або національної безпеки, можна виділити Ч. Чжана[7], М. Файра, Р. Голдшмидта та Ю. Еловічі[8], А. Сквічаріні, М. Шехаба та Ф. Пачі[9], Н. Хаджлі та С. Ліна[10] тощо. Однак наявні публікації, близькі до теми представленого дослідження, розглядають різні сфери безпеки дискретно, у відриві одна від одної. Завданням цієї статті є з'ясування вмісту різних складових дискурсу безпеки соціальних мереж та природи їхнього опосередкованого чи прямого впливу на безпеку держави.

Виклад основного матеріалу дослідження. Розвиток засобів та платформ для встановлення нових соціальних зв'язків та ведення діалогу онлайн спричинив певні когнітивні зміни в мисленні осіб, що користуються послугами цих сервісів. Люди, які в повсякденному житті з пересторогою ставляться до нових знайомств, не відчувають таких обмежень у віртуальному просторі, з легкістю розширюють коло онлайн-знайомств. Частково цьому сприяє і політика самих соціальних мереж. Потрапляння у відкритий доступ інформації особистого характеру, може спровокувати її використання зі злочинною метою у фізичному та віртуальному просторі. Такі злочини можуть приймати різні форми, серед яких персоналізована розсилка спаму та фішинг, переслідування та наклепи тощо. Зрозуміло, що оцінка наслідків публікації чутливої інформації про особу має в першу чергу здійснюватися самим користувачем, але провайдер онлайн-послуг також має вживати певні заходи з нівелювання ризиків, пов'язаних із вільним розповсюдженням інформації в мережі Інтернет. Втім, незважаючи на наявні ризики, більшість діючих механізмів забезпечення конфіденційності даних та контролю доступу до них в соціальних мережах є навмисно слабкими, для полегшення процесу приєднання до цих мереж та розповсюдження інформації за допомогою цих сервісів та платформ[11].

Однак велике значення має також поведінка користувачів. Соціальні мережі не лише сприяють підтримці вже існуючих стосунків, вони заохочують користувачів до встановлення нових зв'язків та подальшої соціалізації. Таким чином, ключовим компонентом будь-якої соціальної мережі є механізм пошуку користувачів та ознайомлення з тою інформацією, яку вони вважають за потрібне публікувати. Результати попередніх досліджень свідчать про те. що гендерний фактор має суттєвий вплив на регулювання та контроль власної діяльності в Інтернеті та розуміння ризиків, пов'язаних

---

[1] Іващук, Л. (2011). Соціальні мережі Інтернету в сучасній політичній комунікації. *Наукові праці Національної бібліотеки України ім.. В. І. Вернадського, 32,* 63-70.

[2] Якименко, Ю. (2012). Соціальні мережі та соціальні рухи. *Наукові праці Національної бібліотеки України ім. В. І. Вернадського, 33,* 524-531.

[3] Коноплицький, С.М. (2007). *Соціальні аспекти комунікації в мережі Інтернет: феноменологічний аналіз*: автореферет дисертації кандидата соціологічних наук. Київ.

[4] Молодецька, К. (2016). Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави. *Information Technology and Security, 4, 1(6),* 13-20.

[5] Молодецька-Гринчук, К. (2017). Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах. *Автоматизація технологічних і бізнес-процесів, 9, 2,* 36-42. <doi: 10.15673/atbp.v9i2.560>.

[6] Пелещишин, А., Гумінський, Р. (2012). Загрози інформаційної безпеки держави в соціальних мережах. *Наука і техніка Повітряних Сил Збройних Сил України, 11, 2,* 192-199.

[7] Zhang, C. et al. (2010). Privacy and Security for Online Social Networks: Challenges and Opportunities. *IEE Network, 24, 4,* 13-18. <doi: 10.1109/MNET.2010.5510913>.

[8] Fire, M., Goldschmidt, R., Elovici, Yu. (2014). Online Social Networks: Threats and Solutions. *IEEE communication surveys & tutorials*, *16, 4,* 2019-2036. <doi:10.1109/COMST.2014.2321628>.

[9] Scuicciarini, A., Shehab, M., Paci, F. (2009). Collective Privacy Management in Social Networks. *WWW '09: Proceedings of the 18th international conference on World wide web (April 2009, Madrid),* 521-530. <doi: https://doi.org/10.1145/1526709.1526780>.

[10] Hajli, N., Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics, 133, 1,* 111-123.

[11] Zhang, C. et al. (2010). Privacy and Security for Online Social Networks: Challenges and Opportunities. *IEE Network, 24, 4,* 13. <doi: 10.1109/MNET.2010.5510913>.

із поширенням інформації в соціальних мережах. В цілому, жінки приділяють більше уваги конфіденційності особистих даних в Інтернеті, ніж чоловіки[1]. Однак достатньо велика кількість користувачів не знає про загрози, пов'язані із використанням онлайн-комунікацій, або не звертає на них увагу. Дослідження західних науковців свідчать про те, що більшість користувачів довіряє як самим соціальним мережам, особливо мережі Facebook, так і контактам, які встановлюються за допомогою цих засобів комунікації[2], що зумовлює активне розповсюдження інформації та встановлення нових соціальних зв'язків. Відповідно, ці користувачі не опікуються конфіденційністю самостійно, повністю покладаючись на захисні механізми онлайн-платформ, які не завжди спроможні забезпечити захист від усіх наявних ризиків, що включають в себе крадіжку та злочинне використання особистих даних, розсилку злочинного програмного забезпечення, розповсюдження ворожнечі та різні форми дискримінації і знущання над особистістю. Відомо, що користувачі Facebook зазвичай охоче приймають запити на додання в список контактів від незнайомих людей, з якими їх поєднує лише наявність спільних друзів. При цьому, навіть якщо учасники процесу онлайн-комунікації усвідомлюють факт доступності їхніх особистих даних для сторонніх осіб та пов'язану з цим небезпеку, можливість проконтролювати це та відповідним чином налаштувати доступ до власних особистих даних зазвичай є обмеженою[3]. Доступ до особистих даних відкривається широкій аудиторії також у непрямий спосіб, шляхом публікації фотографій та відомостей про власне місцезнаходження[4]. Отримана таким чином інформація може бути використана зі злочинною метою, а, отже, надмірна відкритість в соціальних мережах може завдати серйозної шкоди у віртуальному та реальному світі, особливо коли жертвами злочинів стають найбільш вразливі категорії населення, наприклад, підлітки. В особливо критичних випадках цілеспрямована або випадкова віртуальна атака на людську гідність та конфіденційність особистих даних може привести до летального випадку, наприклад, спровокувавши суїцид[5].

Однак віртуальні загрози часто виходять за рамки суто соціальних відносин та наповнюються політичним контекстом. По-перше, із поступовим вкоріненням соціальних мереж в повсякденному житті суспільства завдання цільового збирання особистих даних полегшується не лише для злочинців, але і для модераторів соціальних мереж, комерційних організацій та урядових органів. Автономна або скоординована агрегація даних всіма переліченими акторами відкриває нові можливості для політичних маніпуляцій, війни компроматів, шантажу тощо.

По-друге, представники урядових структур, користуючись соціальними мережами для висвітлення своєї політичної діяльності та ретрансляції власних точок зору на ті чи інші події, мало чим відрізняються від звичайного користувача в контексті вміння розпізнавати можливі загрози онлайн-комунікації та протистояти ним. А отже, теж можуть стати жертвами технічно більш обізнаних злочинців. Прикладом цього може слугувати випадок «клонування» сторінки адмірала НАТО Дж. Ставрідіса у Facebook, точна копія якої була використана для збирання інформації про високопоставлених чиновників з міністерств оборони країн-членів НАТО та інших урядовців[6]. Тактика створення копій сторінок в соціальних мережах може застосуватися і для атаки у зворотному напрямку: не лише для дискредитації урядовців та отримання інформації про них, а і для аналогічних дій з боку уряду по відношенню до опозиціонерів. Зокрема, тактику «клонування» сторінок активістів використовував уряд Філіппін під час протестів проти прийняття суперечливого

[1] Hajli, N., Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics, 133, 1,* 112.

[2] Dwyer, C., Hiltz, S., Passerini, K. (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. *Reaching New Heights. 13th Americas Conference on Information Systems, AMCIS (9-12 August 2007, Keystone, Colorado, USA), 339,* 13.

[3] Scuicciarini, A., Shehab, M., Paci, F. (2009). Collective Privacy Management in Social Networks. *WWW '09: Proceedings of the 18th international conference on World wide web (April 2009, Madrid)*, 521. <doi: https://doi.org/10.1145/1526709.1526780>.

[4] Fire, M., Goldschmidt, R., Elovici, Yu. (2014). Online Social Networks: Threats and Solutions. *IEEE communication surveys & tutorials*, *16, 4,* 2019.

[5] Pearce, M. (2013). Florida girl, 12, found dead after bullies said 'Kill Yourself'. *Los Angeles Times*. <http://articles.latimes.com/2013/sep/12/nation/la-nann-florida-cyberbullying-20130912>.

[6] Lewis, J. (2012). How spies used facebook to steal NATO chiefs' details. *The Telegraph.* <https://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html> (2012, March, 10).

Закону про боротьбу з тероризмом, що мало місце в червні 2020 року[1]. Сторінки урядовців в Facebook також можуть використовуватися для розповсюдження дезінформації, компрометуючих відомостей про політичних опонентів, що мало місце в Молдові напередодні парламентських виборів 2019 року[2]. В свою чергу, перебуваючи під впливом тривалої та постійної інформаційної агресії, Україна відчуває на собі недосконаліть архітектури безпеки соціальних мереж, що проявляється як в формі діяльності проросійських ботів[3], так і у випадках видалення проукраїнських публікацій модераторами мережі Facebook[4]. Такі методи зловмисного впливу в соціальних мережах та зловживання наявними комунікаційними можливостями і регулятивними повноваженнями виходять за рамки звичайних хакерських та DDoS-атак на урядові сайти та публічні сторінки чиновників, мають більш прихований, маніпулятивний характер, а, отже, наслідки подібних деструктивних дій складніше відстежити та виявити.

Наведені приклади ілюструють загальну тенденцію використання напрацьованих методів тиску на соціум в мережі Інтернет для досягнення більш масштабних політичних цілей. Ця тенденція проявляється ще яскравіше в умовах прямої зовнішньої агресії. К. Молодецька виділяє низку можливих шляхів дестабілізації суспільства за допомогою соціальних мереж, від особистісно орієнтованих, таких як маніпуляції психологічним та емоційним станом користувачів, до спрямованих безпосередньо проти держави. Це, зокрема, розповсюдження в соціальних мережах закликів до сепаратизму, порушення територіальної цілісності держави, дії, спрямовані на дискредитацію уряду, підтримка та сприяння діяльності кримінальних або терористичних угрупувань тощо[5]. Низка характеристик соціальних мереж як засобу комунікації сприяє створенню підґрунтя для такої деструктивної діяльності. Виділяючи важливі для дискурсу безпеки якості соціальних мереж, А. Пелещишин та Р. Гумінський приділяють особливу увагу таким характеристикам як комплексність подачі і сприйняття інформації в соціальних мережах та прихованість джерела впливу[6], який не завжди є сприятливим та корисним. Перша з цих характеристик окреслює можливість застосовувати декілька тактик впливу та тиску на користувачів, одночасно залучаючи до цього процесу одразу декілька сучасних мультимедійних технологій. Таким чином, складний та багаторівневий наратив подається у зручному для сприйняття вигляді, із можливістю приховування певних мотивів та контекстів і акцентування уваги на інших, маніпулюванням емоціями та почуттями користувача. Все це ускладнює задачу розпізнавання злочинних намірів (якщо такі є) та вчасного застосування контр-заходів як для державних служб безпеки, так і для внутрішніх механізмів моніторингу і захисту безпеки онлайн-платформ та, тим більше, для пересічних користувачів.

В свою чергу, друга з наведених характеристик означає можливість проведення прихованої, масштабної за своїми наслідками атаки, здійсненої актором, який не має в своєму розпорядженні значних людських та матеріальних ресурсів. Прихованість джерела атаки також означає відносну безкарність нападника, наявність в нього можливості для швидкого знищення слідів своєї діяльності, миттєвого маскування або зміни місця дислокації, з метою можливого здійснення повторної атаки в майбутньому. Ці можливості є корисними і для держави-агресора, яка може використовувати комунікаційні технології соціальних мереж для поширення деструктивних посилів у віртуальних спільнотах, групах, на публічних сторінках соціальних мереж, з метою підвищення рівня соціальної напруженості, підігрівання протестних настроїв, незадоволення діяльністю уряду[7].

---

[1] Beltran, M. (2020). Philippine Activists: 'Cloned' Facebook Account Attacks Possibly Linked to Government. *The News Lens.* <https://international.thenewslens.com/article/136297>. (2020, June, 10).

[2] Necsutu, M. (2019). Facebook Shuts Moldova Officials' 'Fake News' Accounts. *The Balkan Insight.* <https://balkaninsight.com/2019/02/14/facebook-shuts-moldova-officials-fake-news-accounts/>(2019, February, 14).

[3] Дрогомирецький, Б. (2018). Україно-російська кібервійна: невидимий фронт. *Українська Правда.* <https://www.pravda.com.ua/columns/2018/02/22/7172439/>.

[4] Середа, С. (2018) Facebook видаляє українські публікації про Росію та російську агресію. Інформаційна війна чи збій?. *Радіо Свобода.* <https://www.radiosvoboda.org/a/29624092.html>.

[5] Молодецька-Гринчук, К. (2017). Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах. *Автоматизація технологічних і бізнес-процесів, 9, 2,* 37. <doi: 10.15673/atbp.v9i2.560>.

[6] Пелещишин, А., Гумінський, Р. (2012). Загрози інформаційної безпеки держави в соціальних мережах. *Наука і техніка Повітряних Сил Збройних Сил України, 11, 2,* 192.

[7] Молодецька, К. (2016). Соціальні інтернет-сервіси як суб'єкт інформаційної безпеки держави. *Information Technology and Security, 4, 1(6),* 13.

При цьому ситуація ускладнюється через відсутність ефективних механізмів державного контролю та регулювання безпеки в соціальних мережах. Блокування доступу до інтернаціональних соцмереж з міркувань безпеки може привести до різноманітних непередбачуваних наслідків від погіршення репутації держави на міжнародній арені до провокування масових виступів всередині країни. В свою чергу, більш тонкі та помірковані засоби забезпечення суспільного порядку та протистояння зловмисному інформаційному впливу в соціальних мережах потребують безпрецедентної координації та концентрації зусиль різноманітних державних органів та ланок управління, залучення суттєвої частки матеріальних ресурсів держави.

Можливо, відповідні ресурси та методи слід шукати на міждержавному рівні. Зокрема К. Молодецька вказує на успішний досвід протистояння кібер-загрозам, наявний в об'єднаного центру передових технологій з кібер-оборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence). Діяльність центру базується на низці аналітичних алгоритмів, таких як Індекс національної кібер-безпеки (NCSI), який розраховується для кожної держави окремо та враховує низку показників, таких як загальний та базові показники інформаційної безпеки, здатність до управління інцидентами і кризами, рівень міжнародного впливу[1]. Як партнер НАТО з розширеними можливостями, Україна цілком може приєднатися до євроатлантичних проектів з кібер-безпеки, взяти участь у їхній розробці та імплементації, поділитися власним унікальним досвідом протистояння інформаційній агресії.

Висновки. Комплексна та глобальна природа соціальних мереж, їхня екстериторіальність та інтернаціональність відкриває нові можливості для суспільної комунікації та встановлення нових соціальних зв'язків. З іншого боку, ті ж фактори слугують підґрунтям для виникнення та розвитку специфічних для віртуального простору загроз для соціальної безпеки. В просторі соціальних мереж наявні методи зловмисного впливу можуть бути адаптовані як для здійснення протиправних дій проти окремих осіб, так і для тиску на суспільні та державні органи й інститути. Це зумовлює актуальність питання захисту соціальної безпеки та забезпечення суспільного порядку в соціальних мережах для державних інтересів та, відповідно, державної безпеки.

Точки взаємозв'язку між смисловими полями соціальної та державної безпеки формуються під впливом в наступних чинників:

1. Орієнтація внутрішніх механізмів регулювання соціальних мереж на забезпечення відкритості процесу обміну інформацією та ведення діалогу в умовах відсутності усталених державних стратегій управління та контролю над мережею Інтернет.

2. Однакова вразливість та відкритість до зловмисного впливу публічних сторінок та профілів пересічних користувачів, працівників державних установ, діючих політиків та урядовців.

3. Наявність широкого спектру можливостей для здійснення прихованого впливу через соціальні мережі, диверсифікація можливих джерел небезпеки, можливість проведення багатоцільових атак.

4. Схильність суб'єктів політичного процесу до зловживання новими засобами комунікації, їхнього використання для маніпулювання суспільною думкою, розповсюдження дезінформації та пропаганди, впровадження репресивних заходів тощо.

Державна стратегія протистояння наявним кібер-загрозам та регулювання соціальних мереж для України має бути розроблена із врахуванням перелічених чинників та включати в себе наступні складові:

1. Участь у міждержавних проектах з регулювання мережі Інтернет, застосування міжнародних норм та правил, що забезпечить необхідну ефективність управління та контролю онлайн-комунікацій без репутаційних ризиків для держави.

2. Ведення роз'яснювальної роботи серед населення з питання збереження конфіденційності особистих даних в соціальних мережах, медіа-грамотності та вміння розпізнавати маніпулятивний або недостовірний контент.

3. Створення механізмів моніторингу та відстеження загроз в соціальних мережах, із можливим залученням до цього процесу не лише державних служб безпеки, але і добровольців та громадянських активістів.

4. Приділення уваги підривній діяльності держави-агресора, що здійснюється не лише через російські соціальні мережі, але і через проросійські центри впливу в західних соціальних мережах.

[1] Молодецька-Гринчук, К. (2017). Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах. *Автоматизація технологічних і бізнес-процесів, 9, 2,* 37.

Якщо перша проблема в цілому вирішується шляхом простого блокування відповідних інтернет-ресурсів, то вирішення другої проблеми потребує діалогу та координації зусиль українського уряду, міжнародної спільноти та управлінських структур самих соціальних мереж.

References:

1. Beltran, M. (2020). Philippine Activists: 'Cloned' Facebook Account Attacks Possibly Linked to Government. *The News Lens*. <https://international.thenewslens.com/article/136297>. (2020, June, 10). [in English].
2. Drogomyreczkyi, B. (2018). Ukrayino-rosiiska kibervijna: nevydymyj front [Cyber-war between Ukraine and Russia: the inwisible front]. *Ukrainska Pravda* [Ukrainian Truth]. <https://www.pravda.com.ua/columns/2018/02/22/7172439/>(2018, February, 22). [in Ukrainian].
3. Dwyer, C., Hiltz, S., Passerini, K. (2007). Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace. *Reaching New Heights. 13th Americas Conference on Information Systems, AMCIS (9-12 August 2007, Keystone, Colorado, USA), 339,* 1-13. [in English].
4. Fire, M., Goldschmidt, R., Elovici, Yu. (2014). Online Social Networks: Threats and Solutions. *IEEE communication surveys & tutorials*, *16, 4,* 2019-2036. <doi: 10.1109/COMST.2014.2321628>. [in English].
5. Gorovyi, V.M. (2010). *Socialni informacijni komunikaciyi, yih napovnennya i resurs* [Social information communications, their content and resources]. Kyiv: NAN Ukrayiny, Nacz. b-ka Ukrayiny im. V. I. Vernadskogo. [in Ukrainian].
6. Hajli, N., Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics, vol. 133, no. 1,* 11-123. <doi: 10.1007/s10551-014-2346-x>. [in English].
7. Ishhenko, I.V. (2015). *Politychni instytuty v nestabilnomu seredovyshhi: funkcionalni osoblyvosti* [Political institutions in unstable environment: functional characteristics]. Dnipro: Dniprovskyi nacionalnyi universytet imeni Olesya Gonchara. [in Ukrainian].
8. Ivashhuk, L. (2011). Social`ni merezhi Internetu v suchasnij politychnij komunikaciyi [Internet social networks in modern political communication]. *Naukovi praci Nacionalnoyi biblioteky Ukrayiny im. V. I. Vernadskogo* [Scientific publicatins of Vernadsky National Library Of Ukraine], *no. 32,* 63-70. [in Ukrainian].
9. Konoplyczkyi, S.M. (2007). *Socialni aspekty komunikaciyi v merezhi Internet: fenomenologichnyj analiz*. [Social aspect of comunication in the Internet: fenomenological analysis]. Kyiv. [in Ukrainian].
10. Lewis, J. (2012). How spies used facebook to steal NATO chiefs' details. *The Telegraph.* <https://www.telegraph.co.uk/technology/9136029/How-spies-used-Facebook-to-steal-Nato-chiefs-details.html>. (2012, March, 10). [in English].
11. Molodeczka, K. (2016). Socialni internet-servisy yak subyekt informacijnoyi bezpeky derzhavy [Social Internet-services as a subject of state information security]. *Information Technology and Security*, *vol. 4, no. 1(6),* 13-20. [in Ukrainian].
12. Molodecka-Grynchuk, K. (2017). Metod ocinyuvannya oznak zagroz informacijnij bezpeci derzhavy u socialnyh internet-servisax [The method of evaluation of the signs of danger in social internet services]. *Avtomatyzaciya texnologichnyx i biznes-procesiv* [Automation of technological and business processes], *vol. 9, no. 2,* 36-42. <doi: 10.15673/atbp.v9i2.560>. [in Ukrainian].
13. Necsutu, M. (2019). Facebook Shuts Moldova Officials' 'Fake News' Accounts. *The Balkan Insight.* <https://balkaninsight.com/2019/02/14/facebook-shuts-moldova-officials-fake-news-accounts/>. [in English].
14. Onyshhenko, O.S. ta in. (2014). *Socialni merezhi yak instrument vzayemovplyvu vlady ta gromadyanskogo suspilstva* [Social networks as a tool for mutual influence between the government and civil society]. Kyiv: NAN Ukrayiny, Nacz. b-ka Ukrayiny im. V. I. Vernadskogo. [in Ukrainian].
15. Pearce, M. (2013). Florida girl, 12, found dead after bullies said 'Kill Yourself'. *Los Angeles Times.* <http://articles.latimes.com/2013/sep/12/nation/la-nann-florida-cyberbullying-20130912>. [in English].
16. Peleshhyshyn, A., Guminskyi, R. (2012). Zagrozy informacijnoyi bezpeky derzhavy v socialnyh merezhax [Threats for state information security in social networks]. *Nauka i texnika Povitryanyx Syl Zbrojnyx Syl Ukrayiny* [Science and technology of Ukrainian air force], *vol. 11, no. 2,* 192-199. [in Ukrainian].
17. Scuicciarini, A., Shehab, M., Paci, F. (2009). Collective Privacy Management in Social Networks. *WWW '09: Proceedings of the 18th international conference on World wide web (April 2009, Madrid),* 521-530. <doi: https://doi.org/10.1145/1526709.1526780>. [in English].
18. Sereda, S. (2018). Facebook vydalyaye ukrayins`ki publikaciyi pro Rosiyu ta rosijs`ku agresiyu. Informacijna vijna chy zbij? [Facebook deletes ukrainian publications on Russia and Russian aggression: Information warfare or just a failure?] *Radio Svoboda* [Radio Liberty]. <https://www.radiosvoboda.org/a/29624092.html>. [in Ukrainian].
19. Yakymenko, Yu. (2012). Socialni merezhi ta socialni ruxy [Social Networks and social Movements]. *Naukovi praci Nacionalnoi biblioteky Ukrainy im. V. I. Vernadskogo* [Scientific publicatins of Vernadsky National Library Of Ukraine], *vol. 33,* 524-531. [in Ukrainian].
20. Zhang, C. et al. (2010). Privacy and Security for Online Social Networks: Challenges and Opportunities. *IEE Network*, *vol. 24, no. 4,* 13-18. <doi: 10.1109/MNET.2010.5510913>. [in English].