Юлія Калюжна
Національний інститут стратегічних досліджень, Україна

ВПРОВАДЖЕННЯ ПОЛІТИКИ ЦИФРОВОЇ ГІГІЄНИ: ПОРІВНЯЛЬНИЙ ДОСВІД КАНАДИ ТА РОСІЇ

Yuliia Kaliuzhna
National Institute for Strategic Studies, Ukraine

CYBER HYGIENE POLICY'S IMPLEMENTATION: CANADA AND RUSSIA EXPERIENCE COMPARISON

The main purpose of the article is to underline the role of cyber hygiene for ordinary users and for social system and society in general. The invention of the Internet and other new communication means raise efficiency and speed of business and finance management. However, these technologies increase the risks of disinformation spreading, confidential data loss, and hacking and phishing attacks on government, business, and private sites. The author underlines key specific issues of modern social life and work connecting with Internet invention and the main consequences of cyber hygiene rule breaches. The paper research connected with implementation of cyber hygiene and cybersecurity policies in Canada and Russian Federation makes the comparative analysis of qualities of these practices in democratic and authoritarian societies and exposure of the most effective rules for secure Internet use.
Keywords: cyber hygiene, digital hygiene, information technologies, information security, cyber security, cyber crime.

Вступ. Питання цифрової гігієни набуває дедалі більшої ваги в епоху масштабного розвитку інформаційних технологій й переходу у цифровий формат політичного, економічного, соціального та культурного життя суспільства. Безпека особи та захист її персональних даних, інтересів та майна в інформаційній сфері мають винятково вагоме значення.

Виникнення мереж Інтернету та розвиток комунікаційних технологій підвищили ефективність та швидкість керування політикою, бізнесом та фінансами. Наявність ноутбуку або мобільного телефону з різноманітними додатками дозволяє людині дистанційно навчатися, працювати, здійснювати фінансові операції, спілкуватися з іншими людьми з усього світу. З кожним роком набирають обертів технології «розумного дому» та «розумного міста», електронна роздрібна торгівля, що значно спрощує життя суспільства. Проте, з розвитком подібних технологій злочинність також переміщується у віртуальний простір. Крадіжки персональних даних та даних підприємств, державних структур та інститутів, хакерські атаки, поширення недостовірної інформації для здійснення шахрайства та фінансових махінацій, розповсюдження інформації, яка деструктивно впливає на окремі групи населення є невід'ємною частиною віртуального життя суспільства.

Під загрозою є також національні інтереси держав, оскільки новітні технології істотно збільшують ризик витоку конфіденційної інформації, поширення дезінформації, що може призвести до внутрішніх та зовнішніх конфліктів, уможливлює хакерські атаки на державні сайти, а також внутрішні інформаційні системи. Саме тому питання цифрової гігієни та кібербезпеки набувають дедалі більшої актуальності. Адже недостатня поінформованість та неналежна увага до правил безпеки одного з користувачів, може призвести до інфікування всієї інформаційної системи.

Хід дослідження. Забезпечення безпеки особи або соціальної групи є, відповідно до загальновідомої «Піраміди Маслоу», однією з фундаментальних потреб людини, на якій базуються такі вищі потреби як приналежність до соціальної групи, повага та самореалізація[1]. Відповідно, недотримання правил та умов особистої та/або групової безпеки спричинює негативні наслідки для психологічного та соціального розвитку як окремої людини, так і суспільства

[1] Maslow, A.H. (1970). *Motivation and Personality (2nd ed.).* New York: Harper & Row.

загалом[1]. За подібних умов питання інформаційної безпеки є одновимірними з питаннями фізичної безпеки.

За даними міжнародних агенцій We Are Social та Hootsuite станом на початок 2019 року кількість інтернет-користувачів зросла більше ніж на 1 мільйон у порівнянні з попереднім роком і склала 4,39 мільярдів користувачів, що становить 57% від загального населення планети. З них 3,48 мільярди є активними користувачами соціальних мереж. Якщо розглянути дані щодо кількості інтернет-користувачів за регіонами світу, то найбільший процент – близько 95% населення, залученого до глобальної мережі, припадає на країни Північної Америки, а також Північної і Західної Європи[2]. На другому місці Південна Європа – 88%, Східна Європа (в тому числі, Росія) – 80% та Південна Америка – 73% від загалу населення даного регіону[3]. Найнижчий рівень залучення користувачів до мережі Інтернет у Центральній Африці – всього 12 %[4]. З огляду на зазначені статистичні дані вимальовується картина більшої / меншої актуальності питань забезпечення інформаційної безпеки особистості у мережі Інтернет та дотримання людиною норм цифрової гігієни.

Вперше поняття «цифрової гігієни» застосував американський вчений у галузі теорії обчислювальних систем та один з «батьків-основоположників» Інтернету Вінт Серф у Заяві до Спільного економічного комітету Конгресу США[5], у якій він зазначав, що більшість загроз інформаційній безпеці виникає в процесі роботи інтернет-користувачів, які, незалежно від їх статусу, нехтують правилами гарної кібер-гігієни[6].

Поняття «цифрової гігієни» включає практики та кроки, до яких мають вдаватися користувачі, незалежно від їх соціального статусу та професії, яких вони мають дотримуватися для підтримання нормального функціонування системи та забезпечення її інформаційної безпеки під час онлайнових сесій в мережі Інтернет[7]. Адже точки з'єднання та канали передачі даних, які використовує пристрій для зв'язку з іншими інформаційними системами, для встановлення окремих додатків та послуг, можуть бути використані для злочинного зовнішнього проникнення у систему[8]. До таких точок входу належать всі електронні пристрої та сигнали, такі як Wi-Fi, Bluetooth і у сумі сигнали 5G, різноманітні додатки та платформи тощо.

Прикладами порушення правил цифрової гігієни слід вважати використання одного пароля для всіх web-ресурсів та додатків, або використання слабкого пароля, невчасне оновлення програмного забезпечення та баз антивірусів, передача робочих файлів за допомогою особистої пошти, користування незашифрованими USB-накопичувачами та ін.[9] Ці безневинні на перший погляд практики порушення правил цифрової гігієни при користуванні інформаційними ресурсами можуть призвести до викрадення або втрати даних, порушення конфіденційності інформації, виникнення загроз безпеці не тільки окремої особи або групи осіб, але і безпеці соціальної системи загалом. Теоретично, відповідальність за безпеку даних користувачів мають нести розробники та постачальники web-сайтів та додатків, проте на практиці притягнення їх до відповідальності є досить складним та малоймовірним процесом, до того ж особисті дані вже буде втрачено.

Підсилює необхідність розв'язання даної проблеми те, що більшість держав або мають обмежене законодавче забезпечення щодо цього питання, або не мають його взагалі через

[1] Войскунский, А.Е. (2010). Информационная безопасность: психологические аспекты. *Национальный психологический журнал, 1(3),* 48-53.
[2] Global Digital 2019 reports. *We Are Social.* <https://wearesocial.com/global-digital-report-2019>. (2019, січень, 30).
[3] Global Digital 2019 reports. *We Are Social*. <https://wearesocial.com/global-digital-report-2019>. (2019, січень, 30).
[4] Global Digital 2019 reports. *We Are Social*. <https://wearesocial.com/global-digital-report-2019>. (2019, січень, 30).
[5] Cerf, V.G. (2000). *Statement to the United States Congress Joint Economic Committee.* <https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm>.
[6] Cerf V.G. (2000). *Statement to the United States Congress Joint Economic Committee.* <https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm>.
[7] What is cyber hygiene? *CyberSecurity Forum.* <https://cybersecurityforum.com/cybersecurity-faq/what-is-cyber-hygiene.html>. (2019, березень, 04).
[8] Depow, J. Poor personal cyber hygiene is putting your fellow Canadians at risk. *iPOLITICS* <https://ipolitics.ca/article/poor-personal-cyber-hygiene-is-putting-your-fellow-canadians-at-risk>. (2018, вересень, 28).
[9] Depow, J. Poor personal cyber hygiene is putting your fellow Canadians at risk. *iPOLITICS* <https://ipolitics.ca/article/poor-personal-cyber-hygiene-is-putting-your-fellow-canadians-at-risk>. (2018, вересень, 28).

відсутність технічних засобів і можливостей для розробки та реалізації відповідного законодавства[1], що призводить, зрештою, до того, що кіберзлочинці можуть отримати доступ до мережі Інтернет анонімно або безкарно здійснювати правопорушення з-за кордону[2].

Саме тому, з кожним роком дедалі більше держав світу надають увагу розробці політики кібербезпеки держави та формуванню загальних правил та рекомендацій щодо користування мережею Інтернет для власних громадян. До таких держав, які більш-менш ефективно впроваджують політику кібербезпеки та цифрової гігієни слід віднести Канаду та Російську Федерацію.

За даними міжнародного агентства Global Web Index середньостатистичний канадець проводить близько 5:51 годин в день в мережі Інтернет. Водночас кожен житель Росії витрачає близько 6:29 свого щоденного часу на користування Інтернетом[3].

Починаючи з 2004 року, кожного жовтня Канада за прикладом США проводить Місяць поінформованості про кібербезпеку, спрямований на інформування громадян щодо заходів та ресурсів, які допомагають забезпечити власну онлайн-безпеку та протистояти кіберзагрозам[4,5].

У 2018 році для захисту політичної, економічної, соціальної та культурної сфер життя суспільства та боротьби з ризиками кіберпростору Канада оновила власну Національну стратегію кібербезпеки відповідно до рекомендацій міністрів оборони, інновацій, інфраструктури, державних послуг та Ради казначейства[6]. Відповідно до цієї Стратегії уряд Канади інвестує понад 500 мільйонів доларів протягом 5 років на розвиток системи кібербезпеки держави. Водночас, для розробки ефективної політики Уряд Канади запровадив кампанію «Cyber Review» для отримання рекомендацій від федерального уряду, цифрової спільноти, експертів з кібербезпеки, бізнес-лідерів, урядових чиновників, правоохоронних органів, науковців та зацікавлених громадян.

Політика Національної кібербезпеки Канади передбачає створення нового Кіберцентру під керівництвом Канадської організації безпеки, основною метою якого є координація та співпраця з приватним сектором та громадянами держави для протидії інформаційним загрозам державі та суспільству[7]. Важливою у плані розширення можливостей переслідування кіберзлочинності є роль Національної групи з координації протидії кіберзлочинності. Дана Група є також координаційним центром щодо взаємодії з внутрішніми та міжнародними партнерами[8]. Федеральний уряд Канади ініціював впродовж останнього періоду фінансування проектів, спрямованих на впровадження інновацій, економічне зростання та розвиток проектів для молоді, пов'язаних з кібербезпекою та цифровою гігієною[9]. Наприклад, у зв'язку зі зростанням попиту на кваліфікованих фахівців у галузі кібербезпеки уряд Канади пропонує заохочувати студентів до переходу в галузі науки, техніки, інженерії та математики, а також розширювати спеціалізацію фахівців у галузях гуманітарних наук з урахуванням навичок, необхідних для роботи у сфері кібербезпеки[10].

Одним з основних положень даної політики є також допомога канадцям в онлайновому захисті. Завдяки кампанії «Get Cyber Security» у 2010 році уряд Канади підтримав ініціативу щодо

[1] Овчинников, С.А., Русакова, Н.А. (2013). Демократические проблемы обеспечения информационной безопасности. *Информационная безопасность регионов*, *1(12),* 5-12.
[2] Овчинников, С.А., Русакова, Н.А. (2013). Демократические проблемы обеспечения информационной безопасности. *Информационная безопасность регионов*, *1(12),* 5-12.
[3] Global Digital 2019 reports. *We Are Social.* <https://wearesocial.com/global-digital-report-2019>. (2019, січень, 30).
[4] National Cybersecurity Awareness Month. *Official website of the Department of Homeland Security.* <https://www.dhs.gov/national-cyber-security-awareness-month>. (2018, вересень, 26).
[5] Cyber Security Awareness Month. *Government of Canada.* <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/csm-en.aspx>. (2018, липень, 31).
[6] *National cyber security strategy 2018* (Her Majesty the Queen in Right of Canada). *Government of Canada.* <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf>.
[7] Depow, J. Poor personal cyber hygiene is putting your fellow Canadians at risk. *iPOLITICS* <https://ipolitics.ca/article/poor-personal-cyber-hygiene-is-putting-your-fellow-canadians-at-risk>. (2018, вересень, 28).
[8] *National cyber security strategy 2018* (Her Majesty the Queen in Right of Canada). *Government of Canada.* <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf>. (2018, червень, 12).
[9] *National cyber security strategy 2018* (Her Majesty the Queen in Right of Canada). *Government of Canada.* <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf>. (2018, червень, 12).
[10] *National cyber security strategy 2018* (Her Majesty the Queen in Right of Canada). *Government of Canada.* <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf>. (2018, червень, 12).

поширення обізнаності у сфері кібербезпеки. Зусилля, вжиті в рамках Стратегії кібербезпеки 2010 року, покращили спроможність правоохоронних органів боротися з кіберзлочинністю[1]. За сприяння Канадської ініціативи щодо доброчесності виборів Facebook розробив гід з цифрової гігієни з метою інформування політичних діячів та політичних партій Канади щодо забезпечення захищеності їх сторінок та акаунтів у даній соціальній мережі[2].

Що стосується політики Росії у напрямі впровадження правил цифрової гігієни та забезпечення кібербезпеки держави та її громадян, то, у порівнянні з Канадою, тут спостерігається певне відставання. 5 грудня 2016 року Президент РФ підписав оновлену Доктрину інформаційної безпеки Російської Федерації[3], основні положення якої суттєво не змінилися у порівнянні з редакцією 2000 року. Одними з ключових положень даної доктрини є забезпечення та захист прав і свобод громадян у частині отримання та використання інформації, недоторканість особистого життя, збереження духовно-моральних цінностей, а також сприяння міжнародній інформаційній безпеці[4].

Занепокоєння уряду Російської Федерації викликає, зокрема, той факт, що Інтернет та різноманітні соціальні мережі використовуються терористичними та екстремістськими організаціями для здійснення інформаційного впливу на свідомість окремих індивідів, соціальних груп та суспільства загалом з метою розпалення соціальної та міжнаціональної ворожнечі, етнічної та релігійної ненависті, пропаганди, поповнення рядів терористичних та екстремістських груп та організацій[5]. Більше всього даному впливу піддаються діти та підлітки, які користуються соціальними мережами. Відповідно до досліджень організації «Крибрум» на початок 2019 року близько 5 млн. (35%) аканунтів російських підлітків були залученими до деструктивних течій у соціальних мережах, і їх кількість постійно зростає[6].

Доктрина інформаційної безпеки Російської Федерації визначає зростання комп'ютерної злочинності у фінансовій сфері, а також злочинів, пов'язаних з порушенням конституційних прав і свобод громадян, зокрема прав щодо недоторканості особистого життя та обробки персональних даних за допомогою використання інформаційних технологій[7]. Саме тому, держава ставить на меті створення конкурентоспроможних інформаційних технологій для протидії кіберзагрозам в економічній сфері.

Оскільки РФ є активною учасницею сучасних «гібридних війн» (зокрема – проти України), які ведуться головно за допомогою засобів Інтернету, то значна увага у її безпекових документах відводиться використанню інформаційних технологій спецслужбами інших держав для здійснення інформаційно-психологічного впливу на населення держави з метою дестабілізації внутрішньополітичної та соціальної ситуації у різних регіонах світу, а також у військово-політичних цілях з метою підриву суверенітету та порушення територіальної цілісності інших держав[8].

---

[1] *National cyber security strategy 2018* (Her Majesty the Queen in Right of Canada). *Government of Canada.* <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf>. (2018, червень, 12).

[2] Facebook Cyber Hygiene Guide for Politicians and Political Parties. *Facebook Canadian Election Integrity Initiative* <http://facebookcanadianelectionintegrityinitiative.com/pdfs/cyber-hygiene-en.pdf>. (2017, жовтень, 20).

[3] *Доктрина информационной безопасности Российской Федерации 2016* (Президент Российской Федерации). *Официальный интернет-портал правовой информации.* <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017>.

[4] *Доктрина информационной безопасности Российской Федерации 2016* (Президент Российской Федерации). *Официальный интернет-портал правовой информации.* <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017>.

[5] *Доктрина информационной безопасности Российской Федерации 2016* (Президент Российской Федерации). *Официальный интернет-портал правовой информации.* <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017>.

[6] Касперская, Н., Ашманов, И. (2019) Методическое пособие по выявлению признаков риска поведения в социальных медиа. *Цифровая гигиена. Молодежь в сети. (г. Москва, 28 марта 2019 г.).* Москва.

[7] *Доктрина информационной безопасности Российской Федерации 2016* (Президент Российской Федерации). *Официальный интернет-портал правовой информации.* <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017>.

[8] *Доктрина информационной безопасности Российской Федерации 2016* (Президент Российской Федерации). *Официальный интернет-портал правовой информации.* <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017>.

Як наслідок, Російська Федерація у свої Доктрині інформаційної безпеки визначає основні напрямки забезпечення державної та суспільної кібербезпеки , до яких відносить:

– протидію використанню інформаційних технології для поширення пропаганди ідей екстремістських та терористичних організацій, порушення державної цілісності, суверенітету, політичної та соціальної стабільності, ідей націоналізму та ін., припинення діяльності, яка створює загрози національній безпеці Російської Федерації;

– підвищення захищеності об'єктів критичної, інформаційної та військової інфраструктури в інформаційній сфері;

– нейтралізацію негативного впливу, спрямованого на розмивання духовно-маральних традицій держави;

– розвиток кадрового потенціалу у галузі забезпечення кібербезпеки та використання інформаційних технологій;

– забезпечення захисту громадян від інформаційних загроз, зокрема за рахунок формування культури особистої інформаційної безпеки[1].

Одним з кроків впровадження цифрової гігієни та боротьби з кіберзагрозами в Росії стала спроба блокування у квітні 2018 року мобільного додатку для передачі повідомлень Telegram через відмову розробників програми надати уряду держави ключі шифрування для можливості відслідковувати повідомлення користувачів. З метою протидії кіберзагрозам Російська Федерація вже в 2019 році має намір впровадити ізоляцію російського сегменту мережі Інтернет. З цією метою 16 квітня 2019 року Президент Російської Федерації підписав відповідний Закон[2], відповідно до якого уряд Росії має право контролювати точки інтернет-з'єднання країни з іншими державами світу, а також самостійно, без залучення провайдера, блокувати небезпечні сайти, портали та інтернет-з'єднання (закон набуде чинності з 1 листопада 2019 року).

Висновки.

Проаналізувавши можливі ризики та загрози, пов'язані з використанням кіберпростору, збільшення впливу інформаційних технологій як на життя окремої людини, так і всього суспільства, а також підходи двох держав до впровадження політик кібербезпеки та цифрової гігієни, слід зазначити, що кожна держава світу має розробити власну ефективну та комплексну стратегію забезпечення кібербезпеки громадян, державних та приватних структур. Ключовими аспектами при розробці стратегії є:

– визначення основних термінів та понять, пов'язаних з забезпеченням кібербезпеки держави та її громадян[3];

– співпраця з приватним сектором, бізнес-структурами та звичайними громадянами для виявлення ключових проблем та загроз безпеці у кіберпросторі;

– підвищення рівня обізнаності громадян, співробітників державних та бізнес-структур щодо основних загроз кіберпростору, засобів боротьби з ними та правил цифрової гігієни для ефективного забезпечення безпеки особистих даних та конфіденційності інформації при роботі в мережі Інтернет;

– створення спеціальних органів для виявлення загроз інформаційній безпеці держави та її громадян та боротьби з кіберзлочинністю, а також підвищення кваліфікації кадрів існуючих структур;

– впровадження законів та нормативно-правових актів, які забезпечують ефективне забезпечення кібербезпеки та регулюють функціонування державних та бізнес-структур у кіберпросторі, а також адаптувати інші нормативно-правові акти з урахуванням нових реалій;

---

[1] *Доктрина информационной безопасности Российской Федерации 2016* (Президент Российской Федерации). *Официальный интернет-портал правовой информации.* <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017>.

[2] *Федеральный закон о внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» 2019* (Государственная Дума Российской Федерации). *Официальный интернет-портал правовой информации. <http://publication.pravo.gov.ru/Document/View/0001201905010025>*. (2019, травень, 01).

[3] Шаповал, О., Лозова, І., Гнатюк, С. (2016). Рекомендації щодо розробки стратегії забезпечення кібербезпеки України. *Захист інформації, 18, 1,* 57-65.

– визначення відповідальності за всі можливі види кіберзлочинів та правопорушень[1];

– підвищення рівня технологічного розвитку держави для використання більш ефективних засобів боротьби з кіберзагрозами;

– вихід держави за межі власних кордонів та співпраця з міжнародними партнерами з метою залучення їх досвіду для збільшення ефективності захисту особистих даних та протидії злочинності у кіберпросторі, а також формування законодавчої бази держави з врахуванням досвіду інших держав.

References:

1. Cerf, V.G. (2000). Statement to the United States Congress Joint Economic Committee. <https://www.jec.senate.gov/archive/Documents/Hearings/cerf22300.htm> [in English].
2. Cyber Security Awareness Month. *Government of Canada.* <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/csm-en.aspx> (2018, July, 31). [in English].
3. Depow, J. Poor personal cyber hygiene is putting your fellow Canadians at risk. *iPOLITICS* <https://ipolitics.ca/article/poor-personal-cyber-hygiene-is-putting-your-fellow-canadians-at-risk> [in English]. (2018, September, 28).
4. *Doktrina informacionnoj bezopasnosti Rossijskoj Federacii 2016* (Prezident Rossijskoj Federacii) [Doctrine of Information Security of the Russian Federation (The President of Russian Federation)]. *Oficial'nyj internet-portal pravovoj informacii* [Official Internet portal of legal information]. <http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017> [in Russian].
5. Facebook Cyber Hygiene Guide for Politicians and Political Parties. *Facebook Canadian Election Integrity Initiative.* <http://facebookcanadianelectionintegrityinitiative.com/pdfs/cyber-hygiene-en.pdf > [in English].
6. *Federal'nyj zakon o vnesenii izmenenij v Federal'nyj zakon «O svjazi» i Federal'nyj zakon «Ob informacii, informacionnyh tehnologijah i o zashhite informacii» 2019* (Gosudarstvennaja Duma Rossijskoj Federacii). [Federal Law No. 90-ФЗ "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection" 2019 (The State Duma of Russian Federation)]. *Oficial'nyj internet-portal pravovoj informacii* [Official Internet portal of legal information]. <http://publication.pravo.gov.ru/Document/View/0001201905010025>. (2019, May, 01) [in Russian].
7. Global Digital 2019 reports. *We Are Social.* <https://wearesocial.com/global-digital-report-2019> (2019, January, 30). [in English].
8. Kasperskaja, N., Ashmanov, I. (2019). Metodicheskoe posobie po vyjavleniju priznakov riska povedenija v social'nyh media [Methodological guide for identifying signs of risk behavior in social media]. *Cifrovaja gigiena. Molodezh' v seti. (g. Moskva, 28 marta 2019 g.)* [Digital hygiene. Youth online (Moscow, March 28, 2019)]. [in Russian].
9. Maslow, A.H. (1970). *Motivation and Personality (2nd ed.).* New York: Harper & Row [in English].
10. National Cybersecurity Awareness Month. *Official website of the Department of Homeland Security* <https://www.dhs.gov/national-cyber-security-awareness-month> (2018, September, 26). [in English].
11. National cyber security strategy 2018 (Her Majesty the Queen in Right of Canada). *Government of Canada*. <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf>. (2018, June, 12). [in English].
12. Ovchinnikov, S.A., Rusakova, N.A. (2013). Demokraticheskie problemy obespechenija informacionnoj bezopasnosti [Democratic problems of information security]. *Informacionnaja bezopasnost' regionov* [Regional Information Security], *no 1(12),* 5-12. [in Russian].
13. Shapoval, O., Lozova, I., Gnatjuk, S. (2016). Rekomendacii shhodo rozrobky strategii zabezpechennja kiberbezpeky Ukrainy [Recommendations for cybersecurity strategy of Ukraine development]. *Zahyst informacii* [Ukrainian Information Security Research Journa], *vol.18, no. 1,* 57-65. [in Ukrainian].
14. Vojskunskij, A. (2010). Informacionnaja bezopasnost': psihologicheskie aspekty [Information security: psychological aspects]. *Nacional'nyj psihologicheskij zhurnal* [National psychological journal], *no. 1(3),* 48-53. [in Russian].
15. What is cyber hygiene? *CyberSecurity Forum*. <https://cybersecurityforum.com/cybersecurity-faq/what-is-cyber-hygiene.html>. (2019, March, 04). [in English].

[1] Шаповал О., Лозова І., Гнатюк С. (2016) Рекомендації щодо розробки стратегії забезпечення кібербезпеки України. *Захист інформації, Т.18, 1, 57-65*