

2. Микроэкономика : учебник для бакалавров / А. С. Булатов, С. А. Бартечев, О. В. Соколова, В.Б. Супян ; под ред. А. С. Булатова. – М. : Издательство Юрайт, 2016. – 439 с.
3. Lange, Glenn-Marie, Quentin Wodon, and Kevin Carey, eds. 2018. *The Changing Wealth of Nations 2018: Building a Sustainable Future*. Washington, DC: World Bank. doi:10.1596/978-1-4648-1046-6.
4. Шумська, С. С. Національне багатство України у вимірі показників СНР [Текст] / С. С. Шумська // *Фінанси України*. – 2012. – № 4. – С. 27-40
5. Чечель О. М. Базові критерії добробуту населення / О. М. Чечель // *Інвестиції: практика та досвід*. – 2011. – № 1. – С. 82-85. – Режим доступу: http://nbuv.gov.ua/UJRN/ipd_2011_1_23.
6. Куклин В., Сиренькая А. Богатство и социальное развитие наций / В. Куклин, А. Сиренькая // *Український соціологічний журнал*. – 2016. – № 1–2. – С. 42-57.
7. Бобух І. М. Національне багатство як основа для фінансового розвитку України / І. М. Бобух // *Модернізація публічного сектору в Україні: можливості, виклики та обмеження фіскальної децентралізації* : зб. матеріалів Міжнар. наук.-практ. семінару, Київ, 11-14 квіт. 2016 р. / ДВНЗ «Київ. нац. екон. ун-т ім. Вадима Гетьмана», каф. фінансів ; редкол.: В. Федосов (голова) [та ін.]. – Київ : Аграр Медіа, 2016. – С. 43–47. – Текст парал. англ.
8. Шутаєва О.О. Структура та основні підходи к оцінки людського капіталу / О.О. Шутаєва // *Культура народів Причорноморья*. – 2014. – № 278, Т. 2. – С. 31-34.

References

1. Fedorenko, V., Didenko, O., Ruzhens'kii, M., and O. Itkin. *Political economy*, Alerta, 2008.
2. Bulatov, A., Bartenev, S., Sokolova, O., and V. Supian. *Microeconomics*, Yurait, 2016.
3. Lange, Glenn-Marie, Quentin, Wodon, and Kevin Carey, eds. *The Changing Wealth of Nations 2018: Building a Sustainable Future*, World Bank, 2018. doi: 10.1596/978-1-4648-1046-6.
4. Shums'ka, S. "Ukrainian national wealth in measure of SNA indicators." *Finances of Ukraine*, no.4, 2012, pp 27-40.
5. Chechel, O. "Basic criteria of the population's welfare." *Investments: practice and experience*, no.1, 2011, pp. 82-85. Vernadsky national library of Ukraine, nbuv.gov.ua/UJRN/ipd_2011_1_23. Accessed 1 Mar. 2018.
6. Kuklin, V., and A. Sirenkaia. "Wealth and social development of the nation." *Ukrainian sociological journal*, no.1–2, 2016, pp. 42-57.
7. Bobuh, I. "National wealth as the basis for Ukraine's financial development." *International scientific conference "Modernization of the Ukrainian public sector: opportunities, challenges and restrictions of the fiscal decentralization"*, 2016, pp. 43-47.
8. Shutaieva, O. "Structure and main approaches to human capital assessment." *Culture of the Black Sea people*, vol. 2, no. 278, 2014, pp. 31-34.

Рецензенти:

Ткачук І.Г. (головний редактор) – доктор економічних наук, професор, завідувач кафедри фінансів ДВНЗ "Прикарпатський національний університет імені Василя Стефаника",

Кропельницька С.О. – кандидат економічних наук, доцент кафедри фінансів ДВНЗ "Прикарпатський національний університет імені Василя Стефаника".

УДК 338.2+355.40

ББК 32.973

Король В.С.

ІНФОРМАЦІЙНА БЕЗПЕКА: АНАЛІЗ ОСНОВНИХ ЗАГРОЗ ДЛЯ УКРАЇНИ

Тернопільський національний економічний університет,
Міністерства освіти і науки України,
Кафедра менеджменту і маркетингу,
вул. Дністровська, 32, м. Івано-Франківськ,
76000, Україна,
тел.: 77-30-90,
e-mail: king_stat@i.ua

Анотація. У сучасних умовах XXI ст. інформаційна безпека набуває все вагомішої ролі, а питання її забезпечення стають дедалі гострішими. Стрімке впровадження інформаційних технологій у всі сфери життєдіяльності суспільства та розвиток в умовах глобалізаційних процесів актуалізує проблему визначення обґрунтованих та ефективних шляхів забезпечення інформаційної безпеки.

Досліджено проблему інформаційної безпеки України та захисту національного інформаційного простору від негативних впливів. Проаналізовано теоретичні підходи до визначення сутності поняття інформаційна безпека; всебічно досліджено види реальних і потенційних інформаційних загроз для України. Визначено практичні рекомендації щодо вдосконалення державної інформаційної політики та створення ефективної системи інформаційної безпеки України

Ключові слова: інформаційна безпека України, національний інформаційний простір; інформаційні загрози.

Korol' V.S.

INFORMATION SECURITY: ANALYSIS OF THE MAIN THREATS TO UKRAINE

Ternopil National Economic University,
Ministry of Education and Science of Ukraine,
Department of Management and Marketing,
Dnistrovs'ka str., 32, Ivano-Frankivsk,
76000, Ukraine,
tel.: 77-30-90,
e-mail: king_stat@i.ua

Abstract. In modern conditions of the XXI century. information security is becoming more and more important, and the issue of its provision is becoming more acute. The rapid introduction of information technology in all spheres of society and development in the context of globalization processes, actualizes the problem of determining reasonable and effective ways of ensuring information security.

The problem of information security of Ukraine and protection of the national information space from negative influences was investigated. The theoretical approaches to the definition of the essence of the notion of information security are analyzed; the types of real and potential informational threats for Ukraine are thoroughly investigated. The practical recommendations for improving the state information policy and creation of an effective information security system of Ukraine are defined.

Key words: information security of Ukraine, national information space; information threats

Вступ. На початку XXI ст. поява і швидке зростання соціальної значущості глобальної комп'ютерної мережі Інтернет детермінував безліч соціальних проблем і суперечливих ситуацій, які не мають однозначного рішення в рамках існуючої соціальної і культурної системи. Нова ера глобальних інформаційно-комп'ютерних технологій не тільки сприяє генезису глобального світопорядку, а й ставить під сумнів багато традиційних атрибутів та інституційних особливостей. Наприклад, мова йде про державний суверенітет, який піддається загрозам і викликам з боку нового глобального інформаційного світопорядку. В даний час стає очевидним, що негативний вплив на країну, її громадян може бути надано за допомогою, в тому числі, інформаційно-комунікаційного впливу (інформаційні війни, інформаційний тероризм і т.д.). Крім того, глобальна комп'ютерна мережа Інтернет сприяє стиранню просторово-часових (в тому числі і національних) меж, що негативно позначається на патріотизмі громадян, їх відношенню до власної країни.

Інформаційну безпеку, проблеми захисту національного інформаційного простору досліджували багато науковців. Зокрема, проблему відображено у працях А. Марущака, В. Петрика, В. Ліпкана, Б. Кормича, В. Почепцова та інших фахівців. Проблемні

питання забезпечення кібернетичної безпеки досліджували Р. Лук'янчук, В. Бурячок, А. Бабенко, В. Гавловський, Д. Дубов, В. Номоконов, М. Погорецький, В. Шеломенцев та інші науковці. Однак у працях вищезазначених фахівців інформаційна безпека досліджувалась, радше, як складова національної безпеки, її невід'ємний компонент. Поза увагою науковців залишились проблеми чіткого окреслення інформаційних загроз, вивчення їхніх джерел, всебічне дослідження технологій ведення інформаційної війни.

Постановка завдання. Саме тому необхідно зосередити увагу на негативних аспектах зростання соціального впливу Інтернету та інформаційно-комп'ютерних технологій. Україна покликана боротися з виникаючими загрозами, бо в іншому випадку може виявитися під питанням і подальша доля нашої країни, як незалежної держави в умовах глобального постіндустріального світу початку XXI ст.

Результати. Стосовно функціонування глобальної комп'ютерної мережі Інтернет необхідно зосередити увагу на соціологічному аналізі її небезпечних інформаційних впливів на свідомість аудиторії. Такого роду дії зазвичай поділяють на два види. Перший пов'язаний з втратою цінної інформації, що, або знижує ефективність власної діяльності, або підвищує ефективність діяльності противника, конкурента. Якщо об'єктом такого впливу є свідомість людей, то мова йде про розголошення державних таємниць, вербування агентів, спеціальні заходи і засоби для підслуховування, використання детекторів брехні, медикаментозних, хімічних та інших впливах на психіку людини. Безпека від інформаційного впливу даного виду забезпечують органи цензури, контррозвідки та інші суб'єкти інформаційної безпеки.

Другий вид інформаційного впливу пов'язаний з впровадженням негативної інформації, що може не тільки привести до небезпечних помилкових рішень, а й змусити діяти на шкоду, навіть підвести суспільство до катастрофи. Інформаційну безпеку цього виду повинні забезпечувати спеціальні структури інформаційно-технічної боротьби. Вони нейтралізують акції дезінформації, припиняють маніпулювання громадською думкою, ліквідують наслідки комп'ютерних атак.

Істотні загрози можуть виникати і в аспекті так званого інтелектуального суверенітету держави. Ситуація ускладнюється і тою обставиною, що спочатку Інтернет був військовою розробкою, альтернативної інформаційно-комунікаційною мережею на випадок виникнення ядерної війни. Як свідчать публікації дослідників, на початку 1990-х років в Європейському центрі ядерних випробувань в Женеві Т. Бернерс-Лі розробив сучасний вигляд технології "Всесвітньої павутини" (World Wide Web = WWW). У другій половині 1990-х років почався стрімкий розвиток мережі Інтернет і пов'язаних з ним комунікаційних технологій. В кінці XX століття в глобальній мережі налічувалося понад 300 млн. постійно підключених до нього серверів.

З огляду на вищевикладене, необхідно усвідомлювати, що, не беручи участь в розробках новітніх глобальних інформаційно-комунікаційних брендів, інтегруючись в глобальне комп'ютерне середовище, можна просто не усвідомлювати глибини можливостей «архітекторів» нового інформаційного порядку. Тим часом, саме зараз необхідний детальний моніторинговий аналіз потенціалу Інтернету, його модифікацій в аспекті їх впливу на українське суспільство, його соціальні інститути і підсистеми, основні соціальні явища і процеси.

Новий рівень розвитку соціальної системи приносить і цілком зримі тривоги – як для вчених, так і для представників соціального управління. Йдеться про зміну характеру і спрямованості загроз інформаційній безпеці з боку Інтернету. В постіндустріальному, інформаційному суспільстві все менше використовується "фізична зброя" і все частіше домінує зброя інформаційна. Зараз не обов'язково

завойовувати країни фізично, досить їх завоювати ідеологічно, так як в сучасних умовах інформаційна індустрія є одним з головних джерел розвитку суспільства. Цілеспрямована зміна життєвого стилю, принципів, стандартів, моделей споживання і поведінки населення, особливо молоді, за допомогою інформаційних технологій направлено на стратегічне використання інформації, підрив держави зсередини, що не завжди і не відразу сприймається як інформаційна агресія - саме цим вона небезпечна для країни, проти якої направлена. Разом з тим, як і у випадках з іншими проявами науково-технічного прогресу, вплив інформаційно-комп'ютерних технологій виявило і свою "зворотний бік", що складається у використанні їх потенціалу в деструктивних цілях. Це проявилось у виникненні комплексу нових і трансформації традиційних загроз безпеки.

Як зазначає Р. Р. Марутян, найсуттєвішою загрозою національній безпеці України в інформаційній сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій. Це відбувається через систематичне поширення тенденційної, неповної або упередженої інформації про Україну та політичні процеси, що відбуваються на її теренах. Усе це впливає на зовнішню та внутрішню політику нашої держави, знижує її міжнародний імідж, має політичне та економічне підґрунтя. Метою таких інформаційних операцій є забезпечення власних національних інтересів інших держав [6]

Як зазначено у Законі України "Про основи національної безпеки" однією з основних загроз інформаційній безпеці є "намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації" [8]. У Доктрині інформаційної безпеки України, визначено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ, а також мережу Інтернет; деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками [3]

Отже, національний інформаційний простір України, на жаль, зазнає суттєвих загроз, викликів, які становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури.

Для істотного підвищення ефективності побудови системи інформаційної безпеки в сучасних умовах державі необхідна політична воля, а також усвідомлення і перегляд ролі політики і політичних відносин в системі інформаційної безпеки. В першу чергу мова йде про такі політичні фактори, «впливовість» яких обумовлена специфікою соціальної трансформації, визначає внутрішній вигляд і характер інформаційної безпеки, її систему в умовах соціального реформування, спрямованість її подальшого розвитку. До політичних факторів даного роду відносяться політична ідеологія, політична культура, політична соціалізація, політико-інституціональна сфера держави і громадянського суспільства, політичні відносини і процеси трансформаційної спрямованості. Саме ці чинники безпосередньо пов'язані з інформатизацією, суміжна з нею є сфера соціалізації, цілісно характеризують політичну сферу суспільного життя, що розвивається в умовах соціальної трансформації сучасної України.

Висновки. Таким чином, в завершенні вважаємо за необхідне зробити ряд висновків і узагальнень. Зокрема, основна проблема суспільства початку ХХІ ст., на наш погляд, полягає в невідповідності темпів техніко-технологічних і соціальних змін.

Перші демонструють високу швидкість і досить швидкими темпами змінюють життя соціуму. Однак поява Інтернету, електронних інформаційних технологій повинно супроводжуватися відповідними соціальними і соціокультурними змінами, які поки не спостерігаються в достатній мірі для досягнення соціальної стабільності. Саме тому в суспільстві виникають ефекти, подібні віртуалізації соціального простору. У міру розвитку віртуальної реальності все активніше продукуються і відповідні загрози і ризики, пов'язані з відсутністю достовірних знань, а відповідно, і апробованих управлінських технологій та ефективних рішень. Внаслідок вищевикладеного в останні роки наша країна стикається зі зростаючими загрозами інформаційній безпеці, пов'язані з інтернет-середовищем. Активність кіберзлочинності, агресивних комунікаторів часто має масу негативних наслідків і практично не карається державою. Дана проблема може значно загостритися в найближчі роки, так як технологічний розвиток прискорюється, а суспільство просто не встигає адекватно реагувати на зміни, що відбуваються.

Особливу клопотаність у даний час викликають:

- відсутність дієвих, ефективних механізмів соціального контролю і управління в Інтернеті;
- можливості анонімних дій, маскуванню своєї діяльності і, як наслідок, виникнення відчуття безкарності;
- транснаціональний характер інтернет-середовища, стирання просторово-часових меж, загроза державному суверенітету.

Варто зазначити, що з метою захисту національного інформаційного простору, створення ефективної системи забезпечення інформаційної безпеки, з боку української влади здійснюються певні заходи. Зокрема, 14 січня 2015 року Кабінет Міністрів України ухвалив Постанову, згідно з якою створено Міністерство інформаційної політики України, пріоритетними завданнями якого є протидія інформаційній агресії з боку Російської федерації; розроблення ефективної стратегії інформаційної політики держави та Концепції інформаційної безпеки України; узгодженість та координація функціонування і діяльності органів державної влади і інформаційній сфері.

В умовах нових інформаційних викликів Україна має бути готова до забезпечення своєї інформаційної безпеки, при цьому нашій державі необхідно розробити всеосяжну і чітку стратегію інформаційного захисту, що має сприяти досягненню поставлених цілей, а не перешкоджати їх досягненню. В майбутньому цю систему необхідно розвивати, враховуючи правові, технологічні, матеріально-фінансові, та інші аспекти. Адже сьогодні, коли ресурсні можливості держави обмежені. Необхідний пошук нових шляхів і напрямів забезпечення інформаційної безпеки України в умовах зростання інформаційних і військових викликів та загроз. Нині, інформаційна безпека може бути реалізована за умови створення відповідної ієрархічної організаційної структури і орієнтування на вітчизняну наукову та виробничу інфраструктуру.

1. Богуш В. Інформаційна безпека держави [Текст] / В. Богуш, О. Юдін; [гол. ред. Ю.О. Шпак]. – К. : МК-Прес, 2005. – 432 с.
2. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення [Електронний ресурс] / Ю.О. Горбань. – Режим доступу: <http://www.visnyk.academy.gov.ua/wpcontent/uploads/2015/04/20.pdf>
3. Доктрина інформаційної безпеки України [Електронний ресурс]. – Режим доступу: <http://www.zakon3.rada.gov.ua/laws/show/514/2009>
4. Захист інформаційної безпеки як функція держави [Електронний ресурс]. – Режим доступу: <http://www.mego.info/матеріал/23-захист-інформаційної-безпеки-як-функція-держави>
5. Концепція національної безпеки України [Електронний ресурс]. – Режим доступу: http://www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1

6. Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України [Електронний ресурс] / Р. Р. Марутян. – режим доступу: http://www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk;
7. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. – К. : Вид. дім “Києво-Могилянська академія”, 2015. – 497 с.
8. “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. [Електронний ресурс]. – Режим доступу: <http://www.zakon5.rada.gov.ua/laws/show/n0004525-14>.

References

1. Bohush, V. *State Information security*, МК-Pres, 2005.
2. Horban, Yu.O. “Information war against Ukraine and means of its conduct.” <http://www.visnyk.academy.gov.ua/wp-content/uploads/2015/04/20.pdf> Accessed 12 Mar. 2018.
3. “Doctrine of Information Security of Ukraine.” The Verkhovna Rada of Ukraine, www.zakon3.rada.gov.ua/laws/show/514/2009. Accessed 11 Mar. 2018.
4. “Protection of information security as a function of the state.” Mego.info, www.mego.info/material/23-zakhystinformatsiinoi-bezpeky-iak-funktsiia-derzhavy. Accessed 1 Mar. 2018.
5. “The Concept of National Security of Ukraine.” The Verkhovna Rada of Ukraine, www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1. Accessed 11 Mar. 2018.
6. Marutian, R. R. “Recommendations for improving the policy of ensuring information security of Ukraine.” DSaua.org, www.dsaua.org/index.php?option=com_content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk. Accessed 12 Mar. 2018.
7. Pochepstov, H. *Modern information wars*, Vyd.dim “Kyievo-Mohylianska akademiia”, 2015.
8. “On measures to improve the formation and implementation of state policy in the field of information security of Ukraine. Decision of the National Security and Defense Council of Ukraine from 28.04.2014.” The Verkhovna Rada of Ukraine, www.zakon5.rada.gov.ua/laws/show/n0004525-14. Accessed 12 Mar. 2018.

Рецензенти:

Ткач О.В. – д.е.н., професор ДВНЗ “Прикарпатський національний університет імені Василя Стефаника”;

Стефінін В.В. – к.е.н., доцент ДВНЗ “Прикарпатський національний університет імені Василя Стефаника”