УДК 321

**М. А. Томчук**
**Т. М. Закусило**
**Р. О. Білий**

# ЕФЕКТИВНА ПРОТИДІЯ ІНФОРМАЦІЙНІЙ ВІЙНІ

Вінницький національний технічний університет

***Анотація***

*Проаналізовано роль інформаційних війн у політико-комунікативному просторі. Охарактеризовано види і особливості сучасних інформаційних війн. Інформаційно-комп'ютерна революція відкриває широкі можливості для впливу на суспільство, маніпулювання свідомістю та поведінкою людей навіть на відстані. Тому можна припустити, що інформаційні види агресії будуть пріоритетними у майбутньому.*

**Ключові слова:** інформаційна війна, політична комунікація, засоби масової комунікації, інформаційний агресор.

***Abstract***

*The role of mformation war in the political-communicative space. The characteristic features of spedes i modern mformation wars. Information and computer revolution opens the wide opportumties to mfluence sodety, mampulation consdousness and the behavwr of people even at a distance. We can therefore assume that kind of aggressrnn will Informational The priority III the future.*

**Keywords**: Information War, Potitical komunikatsiya, mass communication, mformation aggressor.

**Вступ**

Впровадження інформаційно-комунікаційних технологій в різні сфери життя суттєво підвищило залежність суспільства, кожної людини від надійності та особливостей функціонування інформаційної інфраструктури, достовірності отриманої інформації, її захищеності від несанкціонованої модифікації, а також протиправного доступу до неї. Сучасна людина стає дедалі більш залежною від масової комунікації. Інформаційні технології як реальний ресурс стали активно використовуватись для маніпулювання свідомістю. Набули поширення нові методи інформаційного управління людьми. Нині засоби масової комунікації фактично створили в суспільстві своєрідну «суб'єктивну реальність», що робить людину відкритою і беззахисною перед маніпулювальними технологіями [1, с. 70]. Отже, бурхливий розвиток інформаційно-комунікаційних технологій приносить не лише нові можливості, але й низку загроз, серед яких вирізняється інформаційна війна.

Інформаційна війна останнім часом стає предметом дослідження як зарубіжних, так і вітчизняних вчених. Серед них найбільш відомими є С. Гриняєв, С. Денисюк, О. Дубас, О. Калиновський, В. Корнієнко, А. Крутських, М. Павлютенкова, А. Федоров, І. Шаравов та ін. Характер і особливості інформаційної війни були докладно представлені у працях Д. Волкогонова.

Виходячи з вищезазначеного, метою дослідження є аналіз інформаційної війни як дієвої технології і складової політичної комунікації.

Очевидно, що намагання дати визначення інформаційної війни на сьогоднішній день передчасні. Можна згодитись, що інформаційна війна – це особливо інтелектуальна війна. Мортін Лібікі із Університету національної оборони з намагань дати визначення інформаційної війни вимовив: "Намагання в повній мірі усвідомити всі грані поняття інформаційної війни нагадує зусилля сліпих, які намагаються зрозуміти природу слона: той, що общупує його ногу, називає її деревом, той, що общупує хвіст, називає його канатом ... . Чи можливо таким чином одержати правильне уявлення? Можливо слона і немає, а є тільки дерева та канати. Деякі підводять під це визначення дуже багато, другі практикують тільки один аспект інформаційної війни як визначення в цілому ...". Приведена думка говорить, що остаточне формулювання давати ще рано. Але ми зробимо спробу визначити поняття інформаційної війни. На наш погляд, інформаційна війна не може бути випадковою або відокремленою від інформаційного простору. Вона припускає злагоджену діяльність по використанню інформаційної зброї для ведення "бойових дій" в економічній, політичній, соціальній, ідеологічній,

військовій та інших сферах. Якість захисту інформації можна оцінити або характеризувати показниками інформаційної безпеки. Інформаційна безпека є захищеність інформації і підтримуючої інфраструктури від випадкових та навмисних впливів природного та штучного характеру, в результаті яких наносяться збитки володарям або користувачам інформації і інфраструктурі, що їх підтримує. Інформаційна безпека забезпечується за рахунок захисту інформації [6].

Слушною є думка американського дослідника М. Маклуена стосовно того, що «істинно тотальною війною є війна за допомогою інформації». Власне засоби масової комунікації є новими «природними ресурсами», які збільшують багатства суспільства. Тобто боротьба за капітал, простори збуту та інше відходять на другий план, а головним постає доступ до інформаційних ресурсів, знань, що призводить до того, що війни ведуться переважно в інформаційному просторі та за допомогою інформаційного озброєння. Відомо, що великомасштабні інформаційні технології, які дістали назву «інформаційних війн», мають тисячолітню історію [2, с. 44].

Зокрема, у Біблії згадується Гедеон, який під час війн часто вдавався до залякування ворогів. Одного разу залякування супротивника привело до того, що він розгубився і вдарив по своїх військах. Іншими словами, прикладів інформаційного впливу на моральну стійкість супротивника можна знайти чимало і у давньому Римі, і в епоху феодалізму, і в пізніші часи. Звичайно, особливого значення інформаційні війни набули у XX-XXI ст., коли ЗМІ охопили масову аудиторію. Уже у 20-х роках XX ст. США спрямовували інформаційні потоки на регіони своїх «традиційних інтересів» — країни Латинської Америки, Великобританія — на свої колонії. Німеччина, яка домагалася перегляду умов Версальського миру — на німців Померанії і Верхньої Сілезії у Польщі, Судетів — у Чехії. Тоді ж, у 30-х роках, інформаційні війни перестають бути додатком до збройних і перетворюються у самостійне явище — як от: німецько-австрійська радіовійна 1933-34 рр. з приводу приєднання Австрії до рейху. Саме тоді й з'явилося поняття — «інформаційний агресор» [3].

На сьогодні за допомогою інформаційної зброї протиборчі сторони здатні вирішувати стратегічні завдання, зокрема: завдавати серйозної шкоди національним інтересам, підривати основи державності; дискредитувати органи влади й ускладнювати прийняття ними важливих рішень, паралізувати управління країною в кризових ситуаціях; створювати атмосферу напруженості в суспільстві, провокувати соціальні, політичні, національні і релігійні безладдя, ініціювати страйки, масові заворушення й інші акції економічного протесту; створювати атмосферу бездуховності й аморальності, негативного ставлення до культурного спадку; дезорганізовувати техносферу, економіку, систему комунікацій; підривати міжнародний авторитет держави, перешкоджати її співробітництву з іншими країнами.

У науковій літературі існують різні класифікації інформаційних війн. Зокрема, є стратегічна інформаційна війна першого і другого покоління. Стратегічна інформаційна війна першого покоління включає основні методи інформаційної війни, які нині США реалізують на державному та військовому рівнях. Стосовно інформаційної війни другого покоління, то її скоординовані операції у перспективі можуть привести до відмови від використання військової сили.

Прикладом інформаційних війн можуть бути російсько-грузинський конфлікт 2008 р., теперішній російсько-український конфлікт та багато інших. Ще з часів проголошення незалежності України Російська Федерація веде постійну інформаційну війну проти України. Від початку агресії Російської Федерації (лютий 2014 р.) російська пропаганда набула форм габбельсівської пропаганди часів Другої світової війни. Сьогодні в Російській Федерації на всіх рівнях суспільства розгорнута пропаганда [4, с. 98]. Уряд Росії фінансує досить багато видань за кордоном, які реалізують політику В. Путіна і підривають авторитет України в очах світової спільноти.

Звичайно, у політичній комунікації це явище пов'язане з прагненням дискредитації реального стану в певній державі для того, щоб показати світовій громадськості обмеженість історичної можливості подолати існуючу небезпеку для політичної системи держави.

В економіці робиться все, щоб послабити економіку в країні, на яку спрямований вплив, викликати різного роду труднощі за допомогою дискримінаційних заходів у торгівлі, економічних зв'язках, блокуванні обмінів і контактів.

У духовному світі використовується неправда, наклеп, агітація людей, спрямована на зміну політичного ладу, вплив на сферу як теоретичної (ідеологію, політичні концепції, певні соціальні принципи), так і на сферу повсякденної свідомості.

Цілеспрямований інформаційний вплив на населення передбачає пануюче становище суб'єкта інформаційної війни у всіх сферах життєдіяльності іншої держави: економічній, політичній,

психологічній, релігійній, науково-технічній, мистецькій, а також міжнаціональних і міжнародних зв'язків. Зростання ефективності заходів безпосереднього підриву, зокрема ІВ, досягається за рахунок встановлення контролю над Інформаційним простором іноземної країни, точності та цілеспрямованості таких акцій з урахуванням необхідного обсягу та рівня достовірності інформації, що доводиться, ступеня диференціації населення за системами матеріальних і духовних цінностей, здатності адекватно сприймати відомості та реагувати на них, а також політичної, економічної, етнорелігійної та іншої ситуації в державі й регіоні.

Загрозливим в умовах інформаційних війн є руйнування ціннісних орієнтирів суспільства, національного менталітету, суспільних ідеалів [5, с. 170]. Чим більш розвинутим є суспільство, тим більше воно покладається на інформацію та засоби її доставки. Сюди відноситься також Інтернет, який є лише вершиною цієї інформаційної конструкції. Будь-яка розвинена країна має телефонну, банківську та безліч інших мереж, що керуються комп'ютерами, отже, мають слабкі місця [6].

Було проведено соціологічного дослідження "Вивчення рівня інформованості населення України про можливу загрозу тероризму / екстремізму і правилах поведінки в екстремальних умовах".

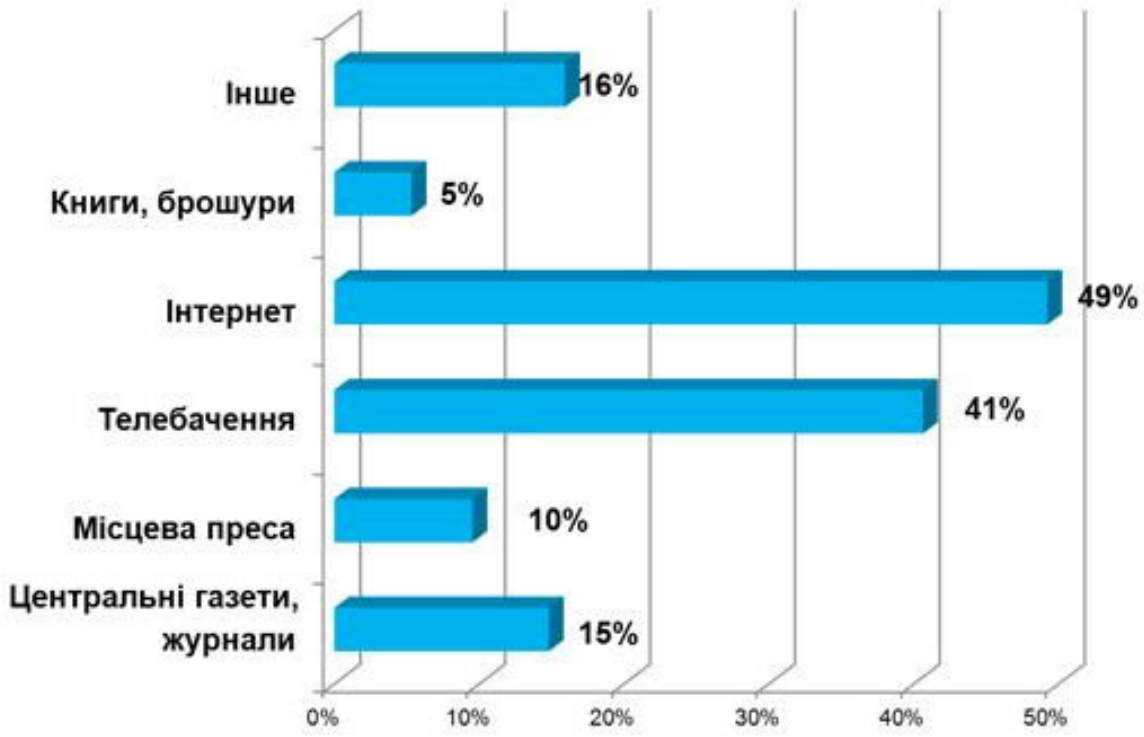


Рис. 1. Джерела інформації за рівнем довіри

Інформаційно-комп'ютерна революція відкриває широкі можливості для впливу на народи та владу, маніпулювання свідомістю та поведінкою людей навіть на віддалених просторах. Беручи до уваги процес глобалізації телекомунікаційних мереж, що відбувається у світі, можна припустити, що саме інформаційним видам агресії буде наданий пріоритет у майбутньому. Потрібна серйозна увага фахівців різного профілю до цього питання, щоб уникнути найнегативніших наслідків цієї війни для всього людства.

Інформаційну війну, що є інформаційним забезпеченням агресії Російської Федерації проти України, відомий російський політик Борис Нємцов охарактеризував як війну нацистському режиму проти демократичної держави: «Виграти війну можуть нацисти із Геббельсом на чолі. Те, що Україна програла інформаційну війну — це факт. Але те, що ви не повинні з цього приводу дуже переживати — це теж факт. Ви ж не нацистська держава», — сказав російський опозиціонер.

Пропаганда є терміном, який вже з часів першої світової викликає негативні асоціації, тому частина країн до сьогодні його уникає. Під пропагандою ми будемо розуміти інтенсивні комунікативні

процеси, що мають на меті зміну поведінки аудиторії, на яку вони налаштовані. Витоки пропаганди можна побачити в будь-якій людській цивілізації.

Суттєвим для поглядів на пропаганду є намагання відокремити її від інших варіантів комунікативного впливу, таких як реклама чи виборчі технології. В історії та теорії визначено два можливі варіанти впливу, що мають назву маніпулятивна та підсилювальна теорії. Як приклад можливостей маніпулятивної теорії наводять фашистську Німеччину, яка під керівництвом Геббельса досягла в цьому нечуваних успіхів. Згідно з цією теорією комунікація може змінити ставлення населення в будь-який бік. Сьогоднішнім прикладом такої активної ролі може слугувати теорія, що розглядає пресу як таку, що задає порядок денний для суспільства. Ми обговорюємо лише те, що записано в цьому переліку. Факти, які до нього не потрапили, залишаються невідомими суспільству. У межах підсилювальної теорії вважається, що досить важко переконати людей у протилежному, якщо вони вже мають власну думку про той чи інший об'єкт чи подію. Пропаганда в її старому розумінні скоріше стосується першого підходу. Реклама вже є представником другого, вона ближча підсилювальної теорії [3].

Ще одним підходом до розрізнення цих процесів є намагання акцентувати увагу на двох варіантах цілей комунікації: з одного боку, це може бути породження повідомлень, з іншого – породження позитивних контекстів того чи іншого майбутнього рішення. Паблік рилейшнз (а з ним і пропаганда) може стосуватися породження позитивних контекстів. Реклама – породжує повідомлення. Сучасна іміджева реклама спрямована на породження контекстів. Виходячи з того, що пропаганду розрізнюють за тим, наскільки в ній утаємничений пропагандист, пошук правильного визначення може йти і в цьому напрямі. Пропаганда є "білою", коли джерело відоме, "чорною" – коли ні, або джерело є перекрученим. "Сіра" пропаганда може мати і відоме, й невідоме джерело. Джерело є прихованим, якщо пропагандист не хоче асоціювати цілі повідомлення із собою. Цей акцент на прихованості, що дає змогу навіть класифікувати пропагандистські повідомлення, говорить про суттєві зміни в поведінці, які хоче викликати пропагандист і про невідповідність цілей нормам аудиторії. З іншого боку, найефективніші листівки, що спонукають до дезертирства, ніколи не приховують, що йдуть від противника [2].

Інформаційні війни давно зайняли належне місце у військовій парадигмі. Існує інфраструктура відповідної підготовки спеціалістів та їх місце у військовій ієрархії. Все це трапилося на наших очах, коли прийшло нове бачення війни, що було підказане новим інструментарієм – інформаційним. Це також співпало зі зміною парадигми війни в цілому, що реалізувалася в переході військових і до нелегальних видів зброї, і до більш складної роботи з населенням. Інформаційні війни є інформаційними технологіями, що впливають на інформаційні системи, маючи на меті введення в оману масової чи індивідуальної свідомості, виведення з ладу або десинхронізацію процесів управління суспільством та його складовими, передовсім військовими. Причому сьогодні чітко стало зрозумілим, що важливим компонентом для виграшу є не лише населення ворожої сторони, а й власне населення, бо війни можуть вигравати на полі боя, а програватися в свідомості людей [2].

Сьогодні Україна стала відкритою в інформаційному відношенні державою, уже сьогодні вона підключилась до Глобальної інформаційної інфраструктури (системи Інтернет, Глобалстар, GSM та інші), володіє замкнутими інформаційними системами низького рівня. Вказане робить Україну особливо вразливою інформаційною зброєю. Тому створення та безперервне вдосконалення систем та засобів захисту інформаційної інфраструктури України, створення оборонної інформаційної інфраструктури, є першочерговою задачею, вирішення якої забезпечить національну безпеку України.

Аналіз показує, що інформаційна зброя, створена в вигляді програмних або програмно-апаратних систем та засобів, може бути економічною, легко замаскованою під засоби захисту, може діяти анонімно без оголошення війни, володіючи в той же час такими властивостями як універсальність застосування, багатоваріантність побудови та використання, скритність та радикальність дії (у розумінні заподіяння максимальної шкоди).

Очевидно, що основними об’єктами інформаційної війни, по суті мішенню інформаційної зброї є і будуть національна інформаційна інфраструктура та глобальна інформаційна інфраструктура. В цілому об’єктами застосування інформаційної зброї можуть бути виробництво, силові відомства, зв’язок, транспорт та енергетика, фінанси, наука та освіта, засоби масової інформації та інше. Але в першу чергу інформаційна зброя буде націлюватись на розв’язання суперечок в економічній, політичній та ідеологічній областях, ця зброя буде націлюватись на збройні сили, підприємства оборонного комплексу, силові структури, відповідальні за безпеку держави. При цьому імовірніше

всього, що найбільший розвиток та використання інформаційна зброя знайде в економічній області – шпигунство через електронні системи, знищення та підробка інформації, введення в оману та інше – реалії сьогоднішнього дня. В таких складних умовах вижити може тільки держава, яка створить і буде повсякчасно покращувати якість національної оборонної інформаційної інфраструктури.

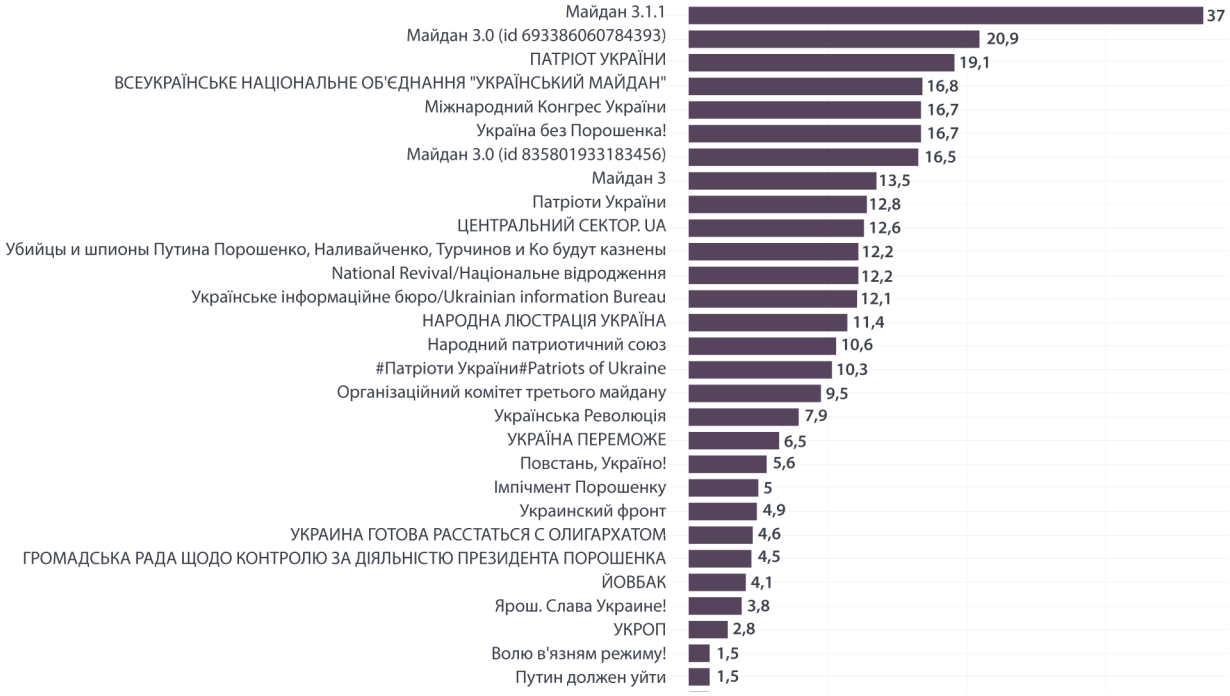


Рис. 2. Діаграма відсоткового показника кількості атак на українські сайти, сторінки за 2016 рік

Світове співтовариство зустрілося з новою глобальною загрозою безпеці країн — інформаційною зброєю. Проблеми розробки, використання і захисту від інформаційної зброї на сьогодні стали вищими пріоритетами політики національної безпеки США та інших західних країн, орієнтованої на XXI ст.

Інформаційна зброя принципова відрізняється від інших засобів ведення війни тим, що з її допомогою ведуться неоголошені і, найчастіше, невидимі війни, та що об’єктами впливу є, насамперед, громадські інститути суспільства і держави. Крім того, військова стратегія використання інформаційної зброї виявилася тісно пов’язаною із цивільним сектором і стала багато в чому від нього залежати [7, с. 188].

Нині є величезна кількість різноманітних технологій здійснення негативного впливу на духовно-ідеологічну сферу життєдіяльності суспільства. їх можуть застосовувати спецслужби іноземних держав, терористичні організації, політизовані радикальні угруповання, кримінальні структури, транснаціональні корпорації та інші формальні й неформальні учасники сучасних міжнародно-правових відносин. Принаймні можливість такого використання видається досить реальною [8].

Таким чином, інформаційна зброя може служити ефективним засобом знищення, зміни або розкрадання інформаційних масивів, здобування з них необхідної інформації після подолання систем захисту, обмеження або заборони доступу до них законних користувачів, дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних мереж, усього високотехнологічного забезпечення життєдіяльності суспільства і функціонування державних структур.

Отже, інформаційна війна є ефективною технологією і складовою політичної комунікації. Інформаційна війна передує озброєному конфлікту, готує «громадську думку» до прийняття певних рішень, потрібних політикам. Як правило, при цьому використовуються різні засоби масової комунікації та адресні групи.

**Висновки**

Під час виконання даної роботи було охарактеризовано види і особливості інформаційних війн, наведено різноманітні приклади та думки експертів. А також проаналізовано роль інформаційних війн у політико-комунікативному просторі сучасності. Інформаційно-комп'ютерний прогрес надав широкі можливості для впливу на суспільство, маніпулювання свідомістю та поведінкою людей, можливістю створення різноманітних тисків та примусів. Тому дана тематика є надзвичайно актуальною і у майбутньому тільки розвиватиметься.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Дубас О. Інформаційна війна: нові можливості політичного протиборства [Текст] / О. Дубас // Освіта регіону. – 2010. – № 1. – С. 69-72.
2. Веймер Д. Л. Аналіз політики: концепції і практика [Текст] / Веймер Девід Л., Вайнінг, Ейден Р.; пер. з англ. І. Дзюб. – К. : Основи., 2000. – 656 с.
3. Политика безрассудства или как руководители Украины «о народе думают» [Электронный ресурс]. – Режим доступа : http://www.dnepr.com/forum/cat-novostiukrainyiimira/topic-14169.html.
4. Денисюк С. Г. Імідж України у внутрішньо і геополітичних контекстах сучасності [Текст] / С. Г. Денисюк, В. О. Корнієнко // – Житомир-Київ-Краків : ФОП Євенюк О. О., 2014. – Вип. 4. - С. 93-100.
5. Денисюк С. Г. Ідеали в структурі політичної комунікації [Текст] / С. Г. Денисюк // Нова парадигма : журнал наукових праць [голов. ред. В. П. Бех]. – К. : Вид-во НПУ імені М. П. Драгоманова, 2011. – Вип. 102. – С. 164-172.
6. Диявол криється в деталях. Інформаційна війна в світлі російської військової доктрини [Электронный ресурс]. – Режим доступа: http://www.osw.waw.pl/en/publikacje/point-view/2015-05-19/ devil-details-nformation-warfare-light-russias-military-doctrine
7. Денисюк С. Г. Інтернет як інструмент ефективності політичної комунікації [Текст] / С. Г. Денисюк // Політологічний вісник : збірник наукових праць. – К. : ІНТАС, 2012. – Вип. 62. – С. 183-190.
8. Анатомія Російської інформаційної війни [Электронный ресурс]. – Режим доступа : http://www.osw.waw.pl/n/puЬlikacje/pomt-view/2014-05-22/anatomy-mssian-шformation-warfare-crimean -operation-a-case-study.



***Томчук Микола Антонович*** – к.т.н., доцент кафедри безпеки життєдіяльності та педагогіки безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: tomchuk@vntu.edu.ua

***Закусило Тарас Миколайович*** – магістр комп'ютерних наук, Вінницький національний технічний університет, e-mail: tapac.zakusylo@gmail.com

***Білий Роман Олександрович*** – студент другого курсу, групи УБ-16, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, email: *wintervinnitsa@gmail.com*

***Nikolay A. Tomchuk*** – docent of life safeness and pedagogic of security, Vinnytsia National Technical University. Vinnitsa, e-mail: tomchuk@vntu.edu.ua

***Zakusylo Taras M.*** – computer science teacher, Vinnytsia National Technical University. e-mail:tapac.zakusylo@gmail.com

***Bilyi Roman O.*** – student of another course, group UB-16, Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: *wintervinnitsa@gmail.com*