УДК 004.056.5+001.102:355.01 https://doi.org/10.31713/ve3202212
JEL: M10

Маланчук Л. О. [1; ORCID ID: 0000-0002-6341-5639],
к.е.н., доцент,
Савчук Р. В. [1; ORCID ID: 0000-0003-0218-6438],
здобувач вищої освіти другого (магістерського) рівня,
Кохан О. С. [1; ORCID ID: 0000-0002-1294-8849],
здобувач вищої освіти другого (магістерського) рівня

[1]*Національний університет водного господарства та природокористування, м. Рівне*

ІНФОРМАЦІЙНА БЕЗПЕКА СУСПІЛЬСТВА В ПЕРІОД ВІЙНИ

У статті досліджено інформаційне суспільство та його специфіку. Розглянуто Інтернет, який чинить сильний вплив на динаміку соціальних змін та свідомість сучасної молоді, соціалізація якої в інформаційному суспільстві здійснюється під потужним впливом ЗМІ в цілому та мережі Інтернет зокрема. Зазначено, що мережеве спілкування має певні переваги, які змушують забути про його недоліки, як і в ситуації інформаційного доступу, що робить легкодоступною як корисну інформацію, але також й інформацію негативного змісту. Розглянуто інформаційну безпеку суспільства і відмічено, що інформаційно-технічний прогрес сприяє появі нових видів небезпек, до найбільш значних із них належать: інформаційну зброю, соціальні злочини в IT-сфері, а також застосування інформаційних технологій у політичній боротьбі. Прагнення до інформаційного суспільства породжує нові види небезпек та загроз. Саме суспільство змушене реагувати на виклики міжнародної, національної, громадської та особистої безпеки. Наведено способи боротьби з інформаційною війною та методи захисту інформаційного простору суспільства.

Ключові слова: інформаційне суспільство; інформаційна безпека; інформаційна війна; інформація; інформаційні технології.

Вступ

Інформаційне суспільство – це один із типів суспільства, що склався в результаті розвитку соціального прогресу. У соціальних просторах інформація стає матеріалізованим результатом спілкування, заснованого на знаннях. Інформаційні дані, або інформація, яку ми передаємо, є частиною подальшого курсу дій у суспільстві, і її значення є унікальним. Варто зазначити, що безпека стала важливим фактором у кожному суспільстві. Деякі автори пропонують замінити терміни «мир» і «війна» категоріями «безпека» і «загроза». У певному сенсі взаємозамінність цих термінів також зумовлена соціокультурними змінами. Сучасні соціологічні теорії

також пояснюють і пояснюють безпекові процеси, що відбуваються протягом останніх кількох років. Вони базуються на різних моделях соціальної реальності, показуючи, що фактори, які забезпечують безпеку на мікро- та макрорівнях відрізняються між собою.

Сучасні дослідження розглядають вплив і значення глобальної інформаційної системи на інформаційну безпеку суспільства як найважливішу складову національної безпеки – це визначає ефективність заходів національної безпеки проти зовнішніх і внутрішніх загроз країни.

Аналіз останніх досліджень

Розгляду інформаційного суспільства та інформаційної безпеки присвятили багато праць як зарубіжні, так і вітчизняні вчені, а саме: З. М. Бржевська, В. Л. Бурячко, Г. І. Гайдур, М. В. Гуцалюк, Н. М. Довженко, Р. В. Киричок, О. С. Щербіна та інших. Проблеми впливу інформаційних війн на суспільну свідомість досліджували В. А. Богуш, О. Г. Корченко, Б. Я. Корнієнко, А. П. Шевчук, О. К. Юдін та інші вчені.

Мета та завдання дослідження

Метою даного дослідження є аналіз управління інформаційною безпекою суспільства в період війни. Завданням дослідження є розгляд інформаційного суспільство та його специфіки, пріоритетним завданням є розкриття сутності інформаційної безпеки суспільства, як одного з головних чинників національної безпеки країни, а також розкриття способів боротьби з інформаційною війною та методи захисту інформаційного простору суспільства.

Виклад основного матеріалу

У результаті інформаційної революції створюється принципово новий тип суспільства, зі своїми законами та принципами функціонування, а також ризиками та загрозами. Цей тип суспільства, що отримав назву «інформаційне суспільство», характеризується порушенням лінійності, наступності, стабільності та передбачуваності у суспільному розвиткові, що принципово відрізняє його від усіх попередніх типів суспільства, що існували в історії нашої цивілізації. Дане суспільство, створене пануванням інформації та її тотальним впливом на свідомість та поведінку індивідів, має найвищий потенціал наукового та технологічного розвитку, але водночас містить у собі такий самий високий потенціал загрози для безпеки суспільства.

Специфіка інформаційного суспільства полягає в тому, що інформація та знання в ньому набувають особливого статусу, перетворюючись на основний стратегічний ресурс розвитку суспільства та держави. Тому за доступ до цього ресурсу

розгортається конкурентна боротьба у різних сферах суспільства (політиці, економіці, культурі тощо) та на різних рівнях (міжнародному, державному, громадському). Проникаючи дедалі глибше у різні сфери життя, сучасні інформаційні технології не тільки впливають на свідомість і поведінку індивідів, а й визначають загалом життєвий стиль особистості та суспільства, характер відносин і взаємодій, і навіть тенденції у сфері розвитку, політики, культури, освіти тощо.

У цьому ключі зростає інтерес вчених до такого феномену, як Інтернет, який чинить сильний вплив на динаміку соціальних змін та свідомість сучасної молоді, соціалізація якої в інформаційному суспільстві здійснюється під потужним впливом ЗМІ в цілому та мережі Інтернет зокрема, що формує ціннісні установки, стильові зразки, пріоритетні моделі поведінки та інші аспекти того, що складає молодіжний світ чи світ молодіжної культури.

Безумовно, Інтернет має безліч привабливих не тільки для молодого, але й для старшого покоління властивостей, серед яких особливої значущості набуває доступність інформації найрізноманітнішого характеру і воістину безмірні можливості комунікації, що долає кордони, стереотипи, мовні та етнічні перепони тощо. Одним словом, мережеве спілкування має певні переваги, які змушують забути про його недоліки, як, втім, і в ситуації інформаційного доступу, що робить легкодоступною як корисну інформацію, але й також інформацію негативного змісту (сатаністського, екстремістського, фашистського тощо).

Інформаційні загрози походять також від сучасного телебачення, яке містить у своїх сюжетах, інформаційних, аналітичних та публіцистичних повідомленнях безліч негативних емоцій, нав'язуючи глядачам стан страху та тривоги, а також передач відверто агресивного та жорстокого характеру.

У світі інформація стала грати принципово іншу роль: вона перетворилася на ідола сучасного людства, з допомогою якого відбувається виправдання його дій і вчинків. Інформація, по суті, перетворилася на комунікацію, яка множиться та прискорюється. Більше того, інформаційні ресурси активно використовуються для здійснення маніпулятивних дій у різних сферах, формування певної громадської думки шляхом нав'язування «порядку денного» та інтерпретації подій у заданому напрямку, що подаються в «потрібному» світлі. У цьому контексті інформаційний простір постає як сфера виробництва та відтворення інформаційних ризиків.

Прикладом може вважатися Інтернет, у якому не створюються знання, але створюється можливість різноманітних комунікацій,

імітацій, створення символів тощо, тобто всього того, що стає основою інформаційно-комунікативного поля та створюваної в його просторі масової інформації, під впливом якої формується масова культура і, як наслідок, масове суспільство, або суспільство мас, яке зовсім позбавлене індивідуальності, почуття смаку, критичного мислення та мотивації для креативної діяльності. Звичайно ж, цей висновок має узагальнений характер і не означає, що впровадження інформаційних та комунікативних технологій несе в собі лише негативний заряд. Безумовно, з розвитком інформаційних технологій людство не просто зробило крок уперед, а буквально перестрибнуло через прірву, яка тепер поділяє доінформаційне суспільство та постінформаційне, якщо можна так висловитися, маючи на увазі те суспільство, яке вже немислимо без інформаційно-комунікативних технологій. Однак слід розуміти, що будь-які інновації, у тому числі революційного характеру, до яких належить поява та розвиток інформаційних та мережевих технологій, можна використовувати як з користю для розвитку людства, так і на шкоду йому.

Інформаційно-технічний прогрес сприяє появі нових видів небезпек. До найбільш значних із них належать: інформаційна зброя, соціальні злочини в IT-сфері, а також застосування інформаційних технологій у політичній боротьбі.

Перший вид небезпек здатний завдати найбільшої шкоди. Застосовуючи таку зброю у мирний час, можна спровокувати кризу в іншій країні або викликати протестні настрої суспільства щодо чинного політичного режиму. Отже, інформаційна зброя впливає не тільки на свідомість та психіку людей, але при цьому вона здатна змінити інформаційно-технічну складову суспільства. Прикладом інформаційної зброї можуть бути комп'ютерні віруси, які здатні вивести з ладу системи управління, фальсифікацію інформації, логічні бомби тощо.

Соціальні злочини в інформаційній сфері є не менш значущим видом небезпек, оскільки можуть бути спрямовані проти особи, суспільства та держави. Прикладами цього виду злочинів можуть бути: шахрайські маніпуляції з електронними грошима, комп'ютерне хуліганство. На даний момент запобігання подібним видам злочинів проти суспільства та держави є одним із ключових завдань національної безпекової політики. Це більшою мірою пов'язане з активним розвитком кібертероризму та міжнародної комп'ютерної злочинності.

Третій вид небезпек є найменш агресивним, але не варто недооцінювати його значення. Насамперед посилення впливу інформаційних технологій у політичній боротьбі зумовлене

ослабленням державного тиску. Ключову роль відіграє інформація, а вміння правильно розпорядитися інформаційними ресурсами забезпечує перемогу на політичній арені здебільшого.

Виходячи з вищевикладеної думки, постає цілком логічною та необхідною інформаційна безпека суспільства.

Прагнення до інформаційного суспільства породжує нові види небезпек та загроз. Саме суспільство змушене реагувати на виклики міжнародної, національної, громадської та особистої безпеки.

Соціальний розвиток суспільства та його національна безпека визначаються багато в чому тим, яким змістом наповнено інформаційний простір, у якому здійснюють свою діяльність окремі індивіди, соціальні групи, організації та держави. Надзвичайно важливе значення набуває ціннісного і культурного змісту інформаційного простору, а також процес трансляції його цінностей і норм підростаючому поколінню як найактивнішому споживачеві інформаційних послуг, що генерує у своїй практиці не лише нові можливості та продукцію інформаційного суспільства, а й загрози, що виходять від нього.

Відповідно до ст. 13 Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»: «інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [2].

З початком війни в Україні, Російська Федерація веде активну інформаційну війну, метою якої є розповсюдження дезінформації, для висвітлення якої використовуються не лише ЗМІ, або публічні статті, ай спеціальні «боти», які активно працюють в соціальних мережах, створюючи фейкові сторінки, акаунти, на яких розповсюджують інформація, яка часто не відповідає дійсності для дестабілізації ситуації в суспільстві.

В інформаційній війні є три основні цілі: контроль над інформаційним простором і забезпечення захисту власної інформації від ворожих дій, використання контролю над інформаційним простором для проведення інформаційних атак на супротивника, підвищення загальної ефективності інформаційна функція зброї.

Під інформаційною безпекою під час війни слід розуміти такий стан суспільства (соціальної системи), у якому воно здатне протистояти дестабілізуючому впливу негативних інформаційних

чинників, і навіть систему заходів, вкладених у досягнення зазначеного стану.

Методи досягнення інформаційної безпеки пов'язані з уникненням і попередженням деяких негативних інформаційних ситуацій, зазначених на рисунку.

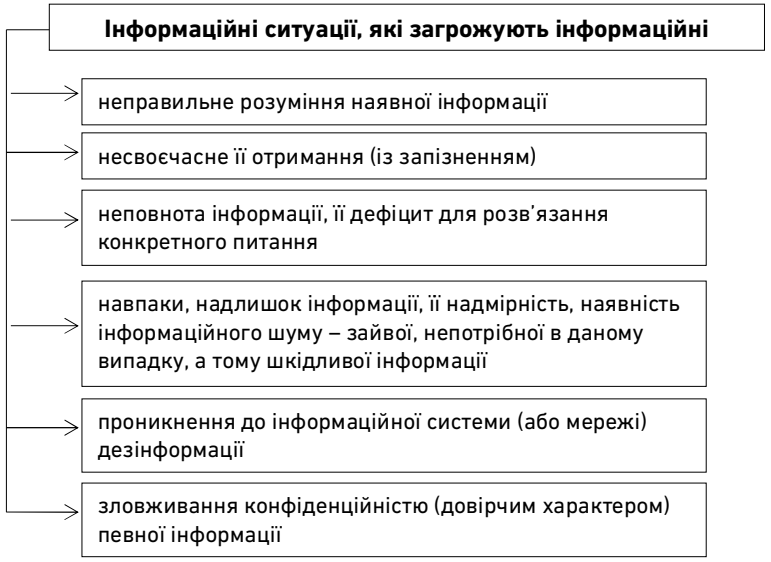

Рисунок. Інформаційні ситуації, які загрожують інформаційній безпеці [3, С. 313]

Досягнення інформаційної безпеки передбачає захист особи, суспільства та держави від злому шляхом розвитку інформаційних, технологічних, інтелектуальних, соціально-політичних та етичних систем. Цей процес запобігає суттєвому пошкодженню зовнішньої інформації кожною системою.

Можна виділити наступні способи боротьби з інформаційною війною та методи захисту інформаційного простору суспільства:

– пряме спростування;

– встановлення та знешкодження потенційних каналів просочування інформації;

– непряме спростування (наприклад, вказати джерело інформації як підозріле; зробити твердження абсурдним; пов'язати джерело інформації з будь-якою негативною подією; представити інший негативний факт, який легко спростувати);

– відволікання уваги. Варіантами відволікання можуть бути: перенаправлення ресурсу ворога на інший об'єкт шляхом перенаправлення його на іншу діяльність (наприклад, відбиття інформаційної атаки на нього), введення в інформаційний простір нової сенсаційної інформації та переключення уваги аудиторії на нове відчуття; переключити увагу аудиторії на незначний факт в межах поточного питання (концентрація уваги аудиторії на неважливих для вас моментах в межах питання);

– мінімізація впливу (наприклад, підкреслення того факту, що в повідомленні вказана якась реальна подія);

– дискредитація інформації (навмисна поведінка, спрямована на підрив авторитету, іміджу та довіри до джерела негативної інформації). Варіаціями можуть бути: публікація секретних матеріалів; публікація віртуальних компрометуючих матеріалів; негативна похвала (ця дія означає публічну похвалу ненадійного об'єкта, зокрема, як і кого похвалили, якщо похвала походить від негативного погляду аудиторії на об'єкт, то це також матиме негативний характер); невмотивовані освистування (масове висловлювання негативних суджень про повідомлення чи його джерело); публічне обурення (метод, який наближається до невмотивованих освистувань, але викликає інші соціальні емоції у аудиторії);

– розмивання негативу (генерує нейтральну або позитивну інформацію про об'єкт, яка перевищує кількість негативної інформації);

– доводити ворожу інформацію до абсурду (метод, заснований на вихованні в аудиторії імунітету до негативу про об'єкт) [1, С. 92].

Враховуючи надзвичайно високу небезпеку, яку становить предмет інформаційної війни для всіх держав, особливо для органів державної влади, державних структур і міжнародних організацій, необхідно розробити відповідну нормативно-правову базу з урахуванням усіх можливостей сучасних мереж. Інформаційно-телекомунікаційні технології; зосередитися на виробництві та розвитку інформаційно-телекомунікаційних технологій у сфері державного управління, покращити здатність державних органів та органів місцевого самоврядування використовувати ефективні технології управління та організовувати конструктивну взаємодію з громадськістю; звернути увагу на рівень підготовки талантів у сфері створення та використання інформаційно-телекомунікаційних технологій, сформулювати низку заходів для покращення рівня захисту.

Висновки

Отже, забезпечення інформаційної безпеки суспільства є першочерговим завданням сучасного суспільства. Це досить складний та багатофункціональний процес, який залежить як від зовнішніх, так і від внутрішніх факторів. Це пояснюється тим, що на сучасному етапі розвитку суспільства інформаційні технології набувають все більшої значущості в житті не лише окремої людини, а й цілої держави. Заходи щодо інформаційної безпеки суспільства повинні бути такі: розробка міжнародно-правових угод, за допомогою яких можливе здійснення контролю за виробництвом та розповсюдженням інформаційної зброї, про координування діяльності у боротьбі з кібертероризмом та міжнародними комп'ютерними злочинами, про захист інтелектуальної власності та авторських прав на матеріали, що розповсюджуються у відкритому доступ. Необхідно розробити способи контролю за розповсюдженням в Інтернеті нецензурної та ображаючої суспільну моральність інформації, недобросовісної реклами, шахрайських операцій та інших матеріалів, які негативно впливають на фізичне, психічне та моральне здоров'я людей.

1. Бржевська З. М., Довженко Н. М., Киричок Р. В., Гайдур Г. І. Інформаційні війни: проблеми, загрози та протидія. *Кібербезпека: освіта, наука, техніка.* 2019. № 3(3). С. 88–96. **2.** Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 01.09.2022). **3.** Щербіна О. С. Інформаційні війни і безпека інформації. *Матеріали наукової конференції професорсько-викладацького складу, наукових працівників і здобувачів наукового ступеня за підсумками науково-дослідної роботи за період 2019–2020 рр.* (квітень–травень 2021 р.). Вінниця : Донецький національний університет імені Василя Стуса, 2021. С. 311–313.

REFERENCES:

1. Brzhevska Z. M., Dovzhenko N. M., Kyrychok R. V., Haidur H. I. Informatsiini viiny: problemy, zahrozy ta protydiia. Kiberbezpeka: osvita, nauka, tekhnika. 2019. № 3(3). S. 88–96. **2.** Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky : Zakon Ukrainy. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (data zvernennia: 01.09.2022). **3.** Shcherbina O. S. Informatsiini viiny i bezpeka informatsii. *Materialy naukovoi konferentsii profesorsko-vykladatskoho skladu, naukovykh pratsivnykiv i zdobuvachiv naukovoho stupenia za pidsumkamy naukovo-doslidnoi roboty za period 2019–2020 rr.* (kviten–traven 2021 r.). Vinnytsia : Donetskyi natsionalnyi universytet imeni Vasylia Stusa, 2021. S. 311–313.

Malanchuk L. O. [1; ORCID ID: 0000-0002-6341-5639],
Candidate of Economics (Ph.D.), Associate Professor,
Savchuk R. V. [1; ORCID ID: 0000-0003-0218-6438],
Master,
Kokhan O. S. [1; ORCID ID: 0000-0002-1294-8849],
Master

[1]*National University of Water and Environmental Engineering, Rivne*

INFORMATION SECURITY OF SOCIETY IN THE PERIOD OF WAR

The article examines the information society and its specifics. The Internet, which exerts a strong influence on the dynamics of social changes and the consciousness of modern youth, whose socialization in the information society is carried out under the powerful influence of mass media in general and the Internet in particular, is considered. It is noted that network communication has certain advantages that make us forget about its disadvantages, as, however, in the situation of information access, which makes both useful information, but also information of negative content, easily available. The information security of society was considered, and it was noted that information and technical progress contributes to the emergence of new types of dangers, the most significant of which include: information weapons, social crimes in the IT sphere, as well as the use of information technologies in political struggle. It should be noted that the security of personal information is closely related to the security of society. Information security of a person is a state of protection of his psyche and health from harmful information that can lead to inadequate perception of reality and/or deterioration of his physical condition. Social information security is the ability of society and its individual members to freely exercise their constitutional rights related to the free acquisition, processing, creation and distribution of information, as well as the degree of protection against harmful informational influence. The drive towards an information society creates new types of dangers and threats. The society itself is forced to respond to the challenges of international, national, public and personal security. Methods of combating the information war and methods of protecting the information space of society are given.

Keywords: information society; information security; information warfare; information; information technology.

Отримано: 02 вересня 2022 р.
Прорецензовано: 07 вересня 2022 р.
Прийнято до друку: 30 вересня 2022 р.