МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет права, публічного управління та національної безпеки
Кафедра економічної теорії, інтелектуальної власності та публічного управління

Кваліфікаційна робота
на правах рукопису

БУРЯЧЕК РУСЛАН ОЛЕКСАНДРОВИЧ
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК: 329.09.5
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА

НАПРЯМИ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ДЕРЖАВИ В КОНТЕКСТІ ВОЄННОЇ АГРЕСІЇ

(тема роботи)

281 «Публічне управління та адміністрування»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Р. О. БУРЯЧЕК
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи:
ДАЦІЙ Надія Василівна
(прізвище, ім'я, по батькові)

доктор наук з державного управління , професор
(науковий ступінь, вчене звання)

Житомир – 2022

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління
за результатами попереднього захисту: **БУРЯЧЕК Руслан Олександрович** допущений до захисту

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № ____ від «____» грудня 2022 р.

Завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління
к.е.н., професор _____ Валентина ЯКОБЧУК
(науковий ступінь, вчене звання) (підпис) (власне ім'я та прізвище)

«___» грудня 2022 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти **БУРЯЧЕК Руслан Олександрович** захистив
(прізвище ,ім'я, по батькові)

кваліфікаційну роботу з оцінкою:
сума балів за 100-бальною шкалою _____
за шкалою ECTS _____
за національною шкалою _____

Секретар ЕК
_____-_____ _____ Настасія ПУГАЧОВА
(науковий ступінь, вчене звання) (підпис) (власне ім'я та прізвище)

АНОТАЦІЯ

БУРЯЧЕК Р. О. Напрями сучасної інформаційної політики держави в контексті воєнної агресії. – Кваліфікаційна робота на правах рукопису. Кваліфікаційна робота на здобуття освітнього ступеня магістра за спеціальністю 281 «Публічне управління та адміністрування». – Поліський національний університет, Житомир, 2022.

Метою роботи є дослідження та аналіз інформаційної політики держави в контексті військової агресії. В роботі обґрунтовано необхідність забезпечення додаткової безпеки інформаційного простору країни шляхом аналізу інформаційних потужностей. Розглянуто принципи функціонування та механізми захисту інформаційного простору.

В роботі представлено метод та його візуалізація для проведення аналіз своїх сил при ведені інформаційної війни для того щоб у подальшому їх можна було б збільшити. Розроблений метод відносяться до галузі інформаційної безпеки і може бути використаний для підвищення рівня захищеності.

Ключові слова: інформаційний простір, інформаційна безпека, інформаційна війна, інформаційна агресія, воєнна агресія.

SUMMARY

BURYACHEK R. A. directions of modern information policy of the state in the context of military aggression. – Qualification work on the rights of the manuscript. Qualification work for obtaining a master's degree in specialty 281 «Public Administration and administration». – Polessky National University, Zhytomyr, 2022.

The aim of the work is to study and analyze the information policy of the state in the context of military aggression. The paper substantiates the need to ensure additional security of the country's information space by analyzing information capacities. The principles of functioning and mechanisms of information space protection are considered.

The paper presents a method and its visualization for analyzing their forces in the conduct of information warfare in order to increase them in the future. The developed method belongs to the field of information security and can be used to increase the level of security.

Keywords: information space, information security, information warfare, information aggression, military aggression.

ЗМІСТ

ВСТУП

Сучасна інформаційна політики держави в контексті воєнної агресії передбачає значні загрози в інформаційній сфері, особливо тих, що пов’язані з інформаційними війнами, значно підвищили значення та роль інформаційної безпеки для національної безпеки України та розширили її зміст.

Особливу увагу приділено соціальним та культурним наслідкам інформаційних кампаній, інформаційних операцій, військових дій. Виходячи з досліджень історії та еволюції інформаційних технологій, агітації, пропаганди та інформаційних воєн, існує потреба в оцінці ризиків та аналізі загроз в інформаційних системах.

Інформаційна війна має на меті послабити сили супротивника чи конкурента та посилення власної сили. Це міра впливу пропаганди на людську свідомість. Такі війни безпосередньо не призводять до кровопролиття і руйнувань, ведуться без жертв і нікого не позбавляють притулку. Головне завдання інформаційної війни – маніпулювання масами. Цілі такого маніпулювання часто включають впровадження ворожих, шкідливих ідей і поглядів у суспільну та приватну свідомість; дезорієнтацію та дезінформацію серед мас; послаблення певних переконань; залякування свого народу в образі ворога; залякування іншого; забезпечення його економічного ринку. У цьому випадку інформаційна війна є невід'ємною частиною конкурентної боротьби.

Наразі питання дослідження напрямів сучасної інформаційної політики держави в контексті воєнної агресії розглянуті в праці таких авторів як: А.М. Бабенко, А.Б. Блага, Б.М. Головкін, В.К. Грищук, С.Ф. Денисов, О.М. Джужа, А.П. Закалюк, Д.П. Калаянов, М.В. Карчевський, І.М. Копотун, В. О. Меркулова, М.І. Панов, Н.А. Орловська, О.П. Рябчинська, В.Я. Тацій, В.О. Туляков, С.І. Халимон, В. В. Шаблистий, Н. С. Юзікова, О. Н. Ярмиш.

Об’єкт дослідження – процес реалізації та захист інформаційного простору в контексті військової агресії.

Предмет дослідження – загальна характеристика інформаційної політики держави в контексті військової агресії.

Метою даної роботи є дослідження та аналіз інформаційної політики держави в контексті військової агресії. Для досягнення мети досить важливим слід вирішити наступні завдання:

- дослідити поняття та інформаційної війни;
- дослідити інформаційну агресію, яка ведеться проти України;
- висвітлити проблемні аспекти та вразливість інформаційного простору,
- охарактеризувати методи ведення інформаційної війни;
- дослідити засоби протидії інформаційної агресії.

Структура роботи дослідження. Робота побудована відповідно до мети та завдань проведеного дослідження. Вона складається із вступу, трьох розділів, вісім підрозділів, висновків і списку використаних джерел. Загальний обсяг роботи становить 32 сторінок. Список використаних джерел складається з 20 найменувань.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ЗАСАДИ В СФЕРІ ІНФОРМАЦІЙНІЙ ПОЛІТИЦІ ДЕРЖАВИ В КОНТЕКСТІ ВОЄННОЇ АГРЕСІЇ

1.1. Поняття та значення інформаційної війни

Динамічний розвиток інформації, від якої залежить сучасне суспільство, сприяв швидкій глобалізації та розмиванню міждержавних і прикордонних кордонів. Разом із політичними та економічними факторами інформація стала важливим чинником національного розвитку, а в геополітичних відносинах стала знаряддям і засобом ведення війни, що може сформувати новий тип війни, тобто інформаційну.

На сьогодні науковці визначили певні способи визначення поняття інформаційної війни. Представники першого підходу виявили, що інформаційна війна – це сукупність політичних, економічних, соціальних, дипломатичних і технічних засобів, прийомів і засобів для досягнення поставленої мети та сприятливого впливу на інформаційне поле об’єкта інформаційної війни. Агресія і захист власних інтересів. Прихильники другого напряму називають його найгострішою формою боротьби в інформаційному просторі, яка передбачає протистояння агресорів з різних напрямків. Відповідно до третього підходу інформаційна війна трактується як форма ведення війни з використанням електронних засобів інформації. Як писав Він Швартов: «Інформаційна війна – це електронний конфлікт, а інформація — це стратегічний актив, який необхідно захопити або знищити.» Представники Четвертого руху трактують інформаційну війну як протистояння сучасних технологічних систем. Оскільки розвиток суспільства і світу не зупиняється, сьогодні починаються різні способи трактування поняття інформаційної війни. Відкрита та прихована інформація, яка впливає на життя людини [1, с. 74].

Досить значною слід виділити думку Я. Малик, який відмічає, що інформаційна війна є формою ведення інформаційного протистояння між різними суб’єктами (державами, неурядовими, економічними та іншими

структурами), яка передбачає проведення комплексу з нанесення шкоди інформаційній сфері конкуруючої сторони і захисту власної інформаційної сфери, конкуруючої сторони і захисту власної інформаційної безпеки [2].

Не менш важливим слід відмітити думку С. Шпилик, яка зазначає, що інформаційною війною є послаблення моральної та матеріальної сили супротивника або конкурента й посилити власні. Вона передбачає заходи пропагандистського впливу на свідомість людини. Такі війни не призводять безпосередньо до кровопролиття, руйнувань. При їх веденні немає жертв, ніхто не позбавляється даху над головою [3, с. 182].

Розглядаючи чинне законодавство слід відмітити, що згідно ст 17 Конституції України, передбачено, що захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [4].

Також досить значною слід відмітити Указ Президента України від 25 лютого 2017 року № 47/2017 «Про Доктрину інформаційної безпеки України», який відмічає, що національними інтересами в інформаційній війні є забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів; забезпечення вільного обігу інформації, крім випадків, передбачених законом; розвиток та захист національної інформаційної інфраструктури; забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України; захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом.

Наведене дозволяє зрозуміти, що інформаційна агресія стала нашим повсякденням жодна людина не почуває себе в безпеці в цьому відношенні, не потребує доведення. Саме тому всі громадяни держави, а особливо ті, які перебувають на «передовій» інформаційних протистоянь (маємо на увазі журналістів, редакторів), повинні усвідомлювати можливі ризики, бути здатними протистояти інформаційним загрозам і впливам, а отже – глибоко

розбиратися у витоках, причинах, методах ведення війн такого типу. Шкідливо думати, що інформаційні війни менш руйнівні, порівняно з тими, в яких застосовуються танки чи бомбардувальники. Руйнування суспільної психології та психології особи, «перекроювання» інтелектуальних і ціннісних орієнтирів представників того чи іншого народу завдають не менше шкоди, ніж полум'я силових конфліктів, а наслідки усуваються десятиліттями, а то й сотнями років.

1.2. Інформаційна безпека в сьогоденні

В сьогоденні розвиток цивілізації інформація відіграє важливу роль у функціонуванні громадських і державних інститутів, у житті кожної людини. Як почати сприймати його соціальні, соціальні, політичні, економічні, військові та інші можливі наслідки. Глобальна інформатизація призводить до створення єдиного світового інформаційного простору, в якому інформація накопичується, обробляється, зберігається та обмінюється між суб'єктами цього простору (людьми, організаціями, країнами). Очевидно, стає можливим швидкий обмін політичною, економічною, технологічною та спеціальною інформацією, а застосування нових інформаційних технологій у різних сферах суспільного життя, особливо у виробництві та управлінні, безсумнівно вигідно людству. Однак так само, як швидкий промисловий розвиток загрожує екосистемі Землі, а досягнення ядерної фізики створюють небезпеку ядерної війни, так само інформатизація спричинить багато серйозних проблем у глобальному масштабі.

Інформаційний вплив на супротивника має багато характеристик, які відрізняються від інших форм боротьби та комунікації у сфері обміну інформацією. Розглянемо основні частини цих функцій. На відміну від маніпулювання міжособистісною свідомістю, інформаційна війна впливає на масову свідомість супротивника, враховуючи колективні характеристики великих груп, на які спрямована акція, а також певні особливості людської свідомості. Обмежений і негативний вплив інформації на окрему людину або

невелику кількість людей не є інформаційною війною. На відміну від звичайного впливу на інформацію, в процесі інформаційної війни об'єкту впливу нав'язуються різні цілі та бажання, в результаті чого їх реалізація завдає шкоди йому самому [5, с. 114].

Це приносить користь іншій стороні, спотворюючи факти або викладаючи факти в спотвореному вигляді, змушуючи іншу сторону поводитися неналежним чином або змушуючи іншу сторону емоційно усвідомлювати факти.

Необхідність забезпечення інформаційної безпеки визначається, по-перше, необхідністю забезпечення загальної національної безпеки України, по-друге, наявністю в інформаційній сфері країни загроз, які можуть завдати істотної шкоди загальним інтересам країни, по-третє, врахуванням враховуйте той факт, що за допомогою інформації можна здійснити зміни у свідомості та поведінці людей. Завданням інформаційної безпеки є створення системи реагування на інформаційні загрози для захисту національного інформаційного простору, інформаційної інфраструктури та національних інформаційних ресурсів. У ситуаціях загострення кризи і конфлікту інформаційна боротьба може трансформуватися в інформаційну війну, яка ведеться за допомогою інформаційної зброї. Індикатори включають, серед іншого, мету, масштаб і складність дій.

Деякі засоби, які зараз вважаються інформаційною зброєю, наприклад, спеціальні психологічні операції, існують і активно використовуються вже давно, інші, особливо специфічні засоби комп’ютерної війни, з’явилися лише кілька років тому. Але всі вони мають одну спільну рису – усі вони засновані на ідеї непрямого впливу на фізичний світ.

Стратегічна інформаційна протидія – це самостійний, принципово новий вид протидії, який дозволяє вирішувати конфлікти без використання збройних сил у традиційному розумінні. Для вивчення закону інформаційного протистояння та аналізу його кількісних характеристик необхідно формалізувати не лише поняття рівня національної інформаційної оснащеності, а й механізм еволюції конкретного національного ресурсного потенціалу та

його впливу. зовнішнє середовище. В даному випадку за основу аналізу було обрано інформаційний стан України [6, с. 51].

Можна зробити наступні висновки: кожна країна, яка є частиною глобального інформаційного простору, має розробити власний комплекс заходів для сталого інформаційного розвитку в умовах жорсткої конкуренції з урахуванням факторів інформаційної безпеки. Для цього потрібно:

- розуміти інформаційні атаки та реагувати на них

- розробка програмного забезпечення проти інформаційних атак;

- аналіз індикаторів інформаційних загроз для вдосконалення механізмів прийняття рішень національної системи управління;

- забезпечують максимальний захист від зовнішніх впливів;

- аналіз ситуації та технічний огляд усіх засобів зв'язку;

- консолідація діяльності органів державної влади та ЗМІ у сфері суспільно-політичного інформування для усунення негативних психологічних ефектів в умовах кризи та конфлікту.

В Україні всі види інформаційних технологій та засоби їх виробництва та доставки становлять особливу сферу діяльності, розвиток якої визначається Державною інформаційною політикою та Державною програмою інформатизації. Визначення завдань національного плану інформатизації, пріоритетних напрямів розвитку інформатизації, обсягів, джерел та черговості формування бюджетних коштів визначаються Кабінетом Міністрів України та щорічно затверджуються Верховною Радою України.

Національну безпеку України в інформаційній сфері слід розглядати як сукупність чотирьох складових – особистої, громадської (суспільства), комерційної (підприємства) та національної безпеки. Тому при визначенні характеру ризику слід враховувати наступні елементи:

- концептуальні основи, принципи, стандарти та правила політичної безпеки, що відповідають чинному законодавству та принципам забезпечення безперервності персональних, соціальних, комерційних (компанійних) структур і національних систем інформаційної безпеки;

- визначення об'єктів і завдань;

- визначити прийнятні структури з точки зору забезпечення інтересів усіх сторін, що встановлюють контроль над об'єктом безпеки, а також оцінки та управління ризиками;

- визначення статусних функціональних ролей, очікувань і рівнів відповідальності відповідних сторін, включаючи повідомлення про інциденти, які становлять потенційну загрозу [7, с. 86].

Державна політика щодо забезпечення національної інформаційної безпеки визначає основний напрямок діяльності органів державної влади у цій сфері. Ці напрями визначаються змістом національних інтересів держави, суспільства та особи. Насправді це так, оскільки завдання заходів інформаційної безпеки полягає в тому, щоб мінімізувати збитки внаслідок неповної, несвоєчасної або недостовірної інформації, або негативних інформаційних наслідків внаслідок роботи інформаційних технологій та несанкціонованого поширення інформації. Тому інформаційна безпека потребує наявності певних державних інституцій та умов для існування суб’єктів, які регулюються міжнародним та внутрішнім законодавством [8, с. 131].

Отже, спрямованість державної інформаційної політики має ґрунтуватися на забезпеченні права на достовірну, повну та своєчасну інформацію, свободи слова та інформаційної діяльності, змісту та внутрішньої організації, що не допускають втручання в обробку інформації, крім випадків, передбачених законодавством відповідно до Конституції України, збереження та вдосконалення вітчизняної державної Інформаційних продуктів і технологій, забезпечення інформаційної та національної культурної самобутності України у світовому інформаційному просторі, забезпечення державної підтримки та розвитку науково-технічної продукції та інформаційних ресурсів.

1.3. Інформаційна агресія, яка ведеться проти України

Аналіз досліджень, проведених вченими, показує, що інформаційна зброя, створена у вигляді програмних або мікропрограмних систем і засобів, є економічною, легко маскується під засіб захисту, може діяти анонімно без оголошення війни, а також є універсальною тощо. Характеристики, багатовимірність структура Використання, агресивна поведінка (у сенсі заподіяння максимальної шкоди). Сьогодні Україна неофіційно відкрита, тому що підключена до Інтернету, глобальної інформаційної інфраструктури. Це робить нашу націю особливо вразливою до інформаційної зброї. У такій ситуації жодна країна, в тому числі і наша, не може почуватися в безпеці, оскільки громадяни в будь-який час піддаються інформаційним атакам.

Вперше в нашій історії наша країна зіткнулася з інформаційною війною, однією з найнебезпечніших форм війни. Головним опонентом у багаторічному інформаційному протистоянні стала Російська Федерація. Інформаційний тиск також йде із Заходу.

Росія використовує в Україні передові форми гібридної війни з початку 2014 року. Росія прагне максимального невтручання Заходу в події в Україні та виграє час, щоб нарощувати та розширювати свою військову участь у конфлікті. Росія також зуміла посіяти розбрат в НАТО та ЄС, створивши напругу в урядах цих країн, особливо через антиросійські санкції. Можна підкреслити, що головне завдання РФ у цій війні – створити викривлене уявлення про події серед громадян України та Росії. Це знижує моральний дух українського народу та вояків української армії та спонукає їх до зради та переходу на інший бік. Росія використовувала різноманітні методи та техніки для проведення розвідувальних атак на Україну, націлюючись на групи, на які здійснювалися розвідувальні атаки.

Основними методами інформаційної агресії проти України є:

1) дезінформування та маніпулювання;

2) пропаганда;

3) диверсифікація громадської думки;

4) психологічний та психотропний тиск;

5) поширення чуток [9, с. 93].

Вищевикладене дозволяє зрозуміти, насамперед, що інформаційна війна почалася задовго до російського військового вторгнення в Україну і супроводжувала його на кожному етапі, заздалегідь адаптуючись до сучасних цілей і завдань.

По-друге, інформаційні кампанії та проекти, операції та заходи з дезінформації, спрямовані на всі верстви населення Росії та західних країн, а також усіх регіонів України – у кожного регіону різні цілі та завдання;

По-третє, метою української інформаційної війни є ліквідація української держави. У Росії громадська підтримка використовується для виправдання дій російського керівництва. Для Заходу – це дискредитація на діях українського керівництва та його збройних сил.

Ця війна є викликом усьому міжнародному співтовариству та супроводжується зростанням інформаційних загроз світовому порядку. Зазначимо, що Україна не готова до такого масштабного військового удару та розвідувальної атаки [10, с. 62].

Звідси можна зробити висновок, що метою інформаційної війни є послаблення моральної та матеріальної сили противника та посилення самого противника. Перемагає в інформаційній війні та сторона, яка зможе змоделювати дії противника в різних ситуаціях, визначити власні алгоритми дій і врешті-решт їх реалізувати. Найбільш повне моделювання поведінки супротивника означає збір, зберігання та обробку інформації про супротивника.

РОЗДІЛ 2.
РЕАЛІЇ СЬОГОДЕННЯ ЩОДО ІНФОРМАЦІЙНОЇ ВІЙНИ, ЯКА ВЛИВАЄ НА БЕЗПЕКУ ДЕРЖАВИ ТА СУСПІЛЬСТВО

2.1. Найбільш проблемні аспекти та вразливість інформаційного простору

Проблеми в інформаційному просторі за походженням поділяються на три категорії:

- Стосовно втрати інформації (витік, знищення, знищення). Це особливо небезпечно, коли існує ризик втрати важливої для організації інформації, наприклад банківської чи комерційної таємниці, або іншої інформації з обмеженим доступом.

- пов'язані з формуванням інформаційних ресурсів (неповнота, використання недостовірної інформації, відсутність необхідної інформації, неправильна інформація);

- пов'язані з впливом інформації на діяльність суб'єкта (поширення неправдивої та негативної інформації, інформаційно-психологічний вплив на працівників, клієнтів та акціонерів, інформаційний тероризм).

Враховуючи те, що ризик є характеристикою господарської діяльності в ринковій економіці та однією з її складових у випадку підприємницької діяльності, не можна виключати ризик як з інформаційних відносин суб’єктів господарювання, так і з будь-яких відносин загалом [11, с. 149].

Існування конкуренції та наявність вищезазначених ризиків становить певну загрозу для інформації, яка використовується підприємствами, водночас діяльність останніх супроводжується безперервним процесом планування та прийняття рішень, що вимагає достовірної інформації. підтримка. Водночас участь людей в економічному житті створює попит на об'єктивну та всебічну інформацію про підприємницьку діяльність.

На жаль, у процесі конкуренції інформація завжди впливає на споживачів товарів і послуг, які не тільки незаконно узурпують інформацію конкуруючих

суб’єктів, але й сприяють формуванню правильних уявлень про товари, які не завжди є об’єктивними. послуги та організації, які їх надають.

Таким чином, в інформаційних відносинах суб'єктів господарювання можуть існувати загрози, пов'язані з проникненням на інформаційні ресурси (переважно в частині з обмеженим доступом), загрози, що виникають під час формування середовища та стану цих суб'єктів. У першому випадку інформація є предметом загрози, а в другому інформація є інструментом реалізації загрози.

Досвід показує, що основні способи реалізації таких погроз:

- Маніпулювання інформацією (неправдива інформація, спотворення інформації, подача в інформаційне середовище неповної або неправдивої інформації);

- порушення встановленого порядку обміну інформацією, несанкціонований доступ або неправомірне обмеження доступу до інформаційних ресурсів, незаконний збір і використання інформації;

- Знищення та незаконне використання чужих інформаційних ресурсів;

- Інформаційний тероризм (розповсюдження комп'ютерних "вірусів", встановлення програмно-апаратних вбудованих пристроїв, впровадження радіоелектронних засобів для перехоплення інформації, незаконне використання або порушення роботи інформаційно-телекомунікаційних систем, нав'язування неправдивої інформації, публікація інформації, що перебуває під загрозою зникнення, тощо).

Найпоширенішими загрозами організаційній інформації є розкриття, крадіжка, зміна або знищення чутливої та конфіденційної інформації, несанкціоноване використання інформації (включаючи інтелектуальну власність організації на користь ринку) і доступ до захищеної інформації неавторизованим персоналом.

Розголошенням інформації є протиправна, умисна або необережна дія посадової чи іншої особи, внаслідок якої здійснюється оприлюднення (розповсюдження) несанкціонованої інформації без участі посадової особи [12, с. 78].

Це може бути зроблено шляхом сповіщення, передачі, передачі, публікації, втрати чи іншого розголошення такої інформації. Крадіжка інформації — це викрадення секретів для подальшого використання іншими особами або передача носіїв інформації (документів, електронних носіїв, відео- та аудіозаписів) іншим особам. Зміна інформації означає зміни змісту інформації, що міститься на конкретному носії, або самого носія (комп'ютерної програми), так що використання цієї інформації стає повністю неможливим, або така інформація потребує важливого уточнення та аналізу.

Незаконне використання інформації стосується поведінки конкретної юридичної чи фізичної особи, яка використовує певні дані, знання та технології, що належать конкретній юридичній чи фізичній особі, без їхньої згоди чи відома, або іншу поведінку.

Основні загрози при веденні інформаційної війни:

- комп'ютерні програми (віруси, "хробаки", "троянські коні", логічні бомби, прорахунки (випадкові чи навмисні) у програмах і системах комп'ютерної безпеки;

- комп'ютерна техніка (мікромашини та мікроорганізми, що руйнують електронні схеми, випромінювачі високої енергії, електромагнітні імпульси).

- спеціальні функції мікросхем, функції можуть бути вбудовані в інтегральні схеми (мікросхеми). Сценарії активації таких функцій: від певного набору програмних кодів до спеціальних радіосигналів на заданій радіочастоті [13, с. 105].

Ці загрози мають універсальний характер і однаково стосуються всіх типів інформації, включаючи документи, електроніку та знання. Звичайно, кожен вид інформації має додаткові та специфічні характеристики, які притаманні лише окремим видам інформаційних загроз.

Серед основних загроз можна виділити наступні, а саме:

1) втрачені або неналежним чином знищені документи;

2) нехтування вимогами адміністративного персоналу щодо оформлення, оформлення, обліку, передачі та зберігання документів;

3) маніпулювати файлами з обмеженим доступом (за наявності)

4) несанкціонована передача таких документів визначеним особам особами, які не мають до них доступу;

5) використання інформації з обмеженим доступом у неопублікованих документах, публікаціях та особистих справах;

6) розмістити зайву інформацію та обмежити доступ до документів;

7) фотокопії офіційних документів, конфіденційних документів та конфіденційних документів, кількість яких перевищує кількість, необхідну для виконання службових обов'язків;

8) Усний переклад документа в повідомленні (включаючи засоби зв'язку), уривок тексту документа в повідомленні або передача електронною поштою.

2.2. Методи ведення інформаційної війни

У контексті військової агресії інформаційна політика країни розглядає інформацію як окремий об'єкт або як потенційно озброєний і прибутковий об'єкт. Інформаційну війну можна розглядати як якісно новий вид війни, який є активною протидією в інформаційному просторі. Незалежно від використовуваних засобів, інформаційна війна є нападом на інформаційну функцію. Певна зброя використовується для ведення стратегічної інформаційної війни. Ця зброя не завдає фізичної шкоди, але веде до справжньої війни.

Завдяки поширенню масової інформації процес уряду або відповідальної особи формує необхідні точки зору, громадську думку, взаємодоповнюючі процеси логічного мислення та повну систему точок зору щодо певних питань у суспільстві чи групі людей для користь організаторів інформаційної пропаганди. У результаті маніпулятор бачить певні факти чи події в необхідному світлі, формуючи необхідні погляди чи життєві позиції з питань, які раніше містили протиріччя чи непорозуміння. За відсутності протиріч і існуючих стійких систем думок завдання інформаційної війни полягає в тому, щоб породити сумніви, посіяти протиріччя і домисли в існуючих переконаннях.

Розвиток людини влаштований таким чином, що людина завжди шукає відповіді на хвилюючі її питання, спірні питання, і це є невід'ємною частиною постійного пізнавального процесу [14].

Слід відмітити, що Провокація є важливою частиною прийомів і засобів політичної інформаційної війни. Провокація – це особливий вид інформаційного маніпулювання, який змушує супротивника використовувати невдалі стратегії та лінії поведінки. Дратувати опонента означає, що він використовує стратегію проти себе за рахунок цілеспрямованого впливу інформації. Також очевидно, що необхідно заздалегідь знати і прораховувати численні невдалі стратегії конкурентів. Дезінформація – це форма інформаційного впливу, яка вводить суб’єктів в оману щодо справжніх намірів суб’єкта.

Зрозуміло, що інформаційна війна частіше використовується на міжнародному рівні. Україна і Росія роками ведуть таку війну. Росія продовжує провокувати українську владу гучними заявами та у своїх інформаційних матеріалах просто зневажає українців, ображає їх як народ і бажає намалювати Україну терористичною державою [15].

Інформаційну зброю можна охарактеризувати за такими показниками: призначення, вибірковість, розсіювання, сфера впливу, масштаб, швидкість передачі, складність впливу на людей, технічні засоби і системи. Притаманні такі характеристики: скритність – здатність досягати цілей без явної підготовки та оголошення війни; масштаб – потенціал завдати непоправної шкоди без визначення національних кордонів і суверенітету; універсальність – потенціал атакуючої держави для багаторазового використання військовими та цивільними структурами проти військових і цивільних об’єктів атакованої держави; економічна ефективність — співвідношення витрат, необхідних для розробки засобів впливу, і отриманих ефектів порівняно з очікуваною катастрофою атакованої держави, що є вигідним для атакуючого.

Якість наданої інформації також є відмінною рисою. Якщо в паблік рилейшнз використовується реальна інформація, то для ведення інформаційної

війни широко використовується не тільки замовчування певних фактів, але навіть їх фальсифікація.

Інформаційна війна та спілкування з громадськістю схожі лише на етапі досягнення мети, але самі цілі принципово різні. ЗМІ не обов'язково є ініціатором чи суб'єктом змін у свідомості окремих людей чи соціальних груп. Самі по собі вони не можуть бути засобом ні руйнування, ні творення та прогресу. Їхні позитивні чи негативні наслідки залежать від того, які соціальні сили з якою метою використовуються.

РОЗДІЛ 3.
МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВОЄННОЇ АГРЕСІЇ

3.1. Процес виявлення втручання в інформаційний простір

Тестування інтервенцій існує на інформаційному та соціологічному рівнях. Моніторинг ЗМІ – це найшвидший і найдешевший спосіб вивчення громадської думки та відстеження її поширення. Шляхом регулярного аналізу матеріалів ЗМІ спеціалізованими структурними підрозділами чи залученням сторонніх експертів можна виявити певні тенденції в ретроспективі та вперед. Це дозволяє передбачити майбутні наслідки певних дій сьогодні або визначити причинно-наслідкові тенденції, які призводять до певних ситуацій чи фактів, які відбуваються зараз. Цю роботу можна розглядати як первинний аналіз із матеріалом, який дає змогу зрозуміти певні процеси в цілому та визначити певні загрози чи позитивні тенденції.

Контрольовані репродукції – повні репродукції друкованих видань, друкованих фрагментів інформаційних стрічок, матеріалів для інтернет-видань, теле- та радіосюжетів. Крім того, на кожній роздруківці міститься посилання на публікацію, дата, номер, номер сторінки чи Інтернет-адреса, звідки взято матеріал.

Контент-аналіз матеріалів ЗМІ. За даними моніторингу не рідше одного разу на тиждень та не рідше одного разу на місяць проводиться змістовний аналіз зібраних даних з метою перетворення якісних показників та характеристик у кількісні показники та характеристики.

Способи проведення швидких опитувань у соціальних мережах За допомогою соціальних мереж онлайн можна проводити типові соціологічні дослідження і, головне, опитування. Порівняно з класичними соціологічними дослідженнями результати опитувань у соціальних мережах мають більш значні статистичні похибки. Це пов’язано з нестабільністю на місцях (дослідження іноді відмовляються або не дозволяють групувати, згруповані

вибірки не завжди репрезентативні тощо). Проте отримані результати дуже чітко відображають загальні тенденції в контексті географічних сегментів або конкретних цільових груп [16, с. 137].

Для проведення опитування думок представників цільової групи можна скористатися відповідними власними сервісами провідних соціальних мереж або міжмережевими сервісами.

У переважній більшості фірмових сервісів анкета налаштовується в блоці шаблону, який використовується для створення поста.

Схема створення анкети проста і автоматично генерується. Розробникам потрібно лише надати тему та основне запитання з кількома відповідями.

При розробці блоку опитування бажано додати візуальну підтримку – картинку чи відео, що допоможе швидше зрозуміти суть опитування та привернути до нього увагу.

Для полегшення підготовки та проведення опитувань у соціальних мережах існують програми сервісів (зокрема, Facebook, Instagram, Telegram тощо).

Сучасні технології соціальних мереж вимагають постійного вдосконалення методів моніторингу та оцінки ефективності соціальної комунікації. Це означає, що автор інформативного повідомлення має розуміти не лише кількість «лайків» і зміст коментарів, а й загальну тенденцію уподобань цільової групи та прогнозувати характер їх подальшого розвитку. Зазначену проблему можна вирішити за допомогою підходу до синтезу профілю – складного застосування якісних і кількісних характеристик шляхом моніторингу, аналізу контенту та систематизації даних профілю за допомогою окремих інструментів.

Методологічною основою дослідження є методика інформаційної діагностики, яка діагностує ефективність процесу просування діяльності організації в мережі Інтернет.

методика роботи. Комплексне моніторингове дослідження було проведено на основі архівної бази даних, що репрезентує цільову групу респондентів в Інтернеті. Програма виконується у формі моніторингового

дослідження на трьох рівнях. Загальна процедура роботи включає підготовчий етап і чотири послідовні робочі етапи.

На підготовчому етапі формується база даних на мережевих ресурсах профілю, відповідного цільовій групі об'єкта в Інтернеті. які можуть бути:

Соціальна мережа, де можна розміщувати матеріали або згадувати події закладу.

ЗМІ, включаючи веб-сайти газет, журнали, інтернет-видання, телеканали, радіостанції.

Веб-сайти, організовані спеціально в галузі навчання.

Інформаційно-довідковий портал, заснований на огляді діяльності об'єкта або на суміжні теми.

Портал центральних та місцевих органів державної влади та самоврядування.

Фірмові сайти громадських організацій, що працюють у предметній сфері діяльності, а також профільні проекти за Міжнародною програмою.

Сайти політичних об'єднань і громадських рухів, які мають певний вплив на загальну суспільно-політичну ситуацію в країні.

Персональні веб-сторінки публічних діячів (політиків, громадських діячів, чиновників), прямо чи опосередковано пов’язаних з предметом діяльності суб’єкта.

3.2. Засоби протидії інформаційної агресії

Розглядаючи питання інформаційної безпеки, можна виділити чотири групи інформаційно-технологічних загроз суспільству та державі, спричинених досягненнями науково-технічного прогресу. Перша група пов'язана зі стрімким розвитком нової інформаційної зброї, здатної ефективно впливати на психологію людини та інформаційно-технологічні державні структури. Аналіз сучасних досліджень у цій галузі дозволяє говорити про ефективні результати програмування поведінки індивідів під впливом комп’ютерних систем баз даних знань та інформаційних ресурсів. Друга група передбачає існування нових видів злочинів соціального характеру, заснованих на досягненнях, підкріплених новітніми інформаційними технологіями: банківське шахрайство; хуліганство в комп'ютерній сфері; незаконне відтворення технологічних рішень тощо. За словами провідних дослідників у цій галузі, комп’ютерні технології стають основним знаряддям для злочинів. Третя група — електронний контроль життя, настроїв, планування населення та організації політичного характеру, тотальний комп’ютеризований контроль національного суспільства. Інформаційні технології дозволяють накопичувати, зберігати і використовувати величезні обсяги інформації про здоров'я, діяльність соціального планування, політичні погляди, стосунки та економічну підтримку громадян. Четверта група — використання засобів інформаційних технологій у політичній боротьбі. Посилення впливу ЗМІ на політичні процеси та роботу владних механізмів є однією з головних тенденцій суспільного розвитку сучасності.

Можна підкреслити, що національна політика у сфері формування інформаційних ресурсів та інформатизації має бути спрямована на створення умов для ефективного та якісного інформаційного забезпечення вирішення завдань економічного та соціального розвитку країни. Основними напрямками державної політики у сфері інформатизації є: забезпечення умов для розвитку та захисту різних форм власності на інформаційні ресурси; формування та захист державних інформаційних ресурсів; створення та розвиток федеральних і регіональних інформаційних систем і мереж, забезпечення що вони

знаходяться в єдиному інформаційному просторі сумісність та взаємодія на місцях; на основі національних інформаційних ресурсів створюють умови для якісного та ефективного інформаційного забезпечення громадянами, державними органами, організаціями та соціальними групами; забезпечують національну безпеку у сфері інформатизації та забезпечення користування громадянами та організаціями інформацією в умовах інформатизації реалізації прав; сприяти формуванню ринків інформаційних ресурсів, послуг, інформаційних систем, технологій та засобів їх підтримки; формувати та здійснювати єдину науково-технічну та промислову політику у сфері інформатизації з урахуванням рівня розвитку інформаційних технологій у сучасному світі; підтримувати проекти та плани інформатизації, створення надійної системи заохочення інвестицій та механізму стимулювання розробки та реалізації проектів інформатизації, формування законодавства у сферах обробки інформації, інформатизації та захисту інформації [17, с. 221].

Наведене дозволяє зрозуміти, що основними засоби протидії інформаційної агресії :

1. Координує діяльність волонтерів з моніторингу ЗМІ на наявність матеріалів шкідливого інформаційного впливу та здійснення такої діяльності працівниками Центру. Наприклад, це може бути сталкерський матеріал, який містить заклики до порушення територіальної цілісності, насильницького повалення конституційних інститутів тощо. За результатами моніторингу своєчасно повідомляти відповідну інформацію до правоохоронних органів.

2. Заохочуйте громадськість створювати ресурси для викриття дезінформації та робити результати доступними для громадськості в легкодоступній формі.

3. Внести до органів законодавчої та виконавчої влади актуальні законодавчі пропозиції щодо вдосконалення національної системи інформаційної безпеки.

4. Надати громадянам країни фактичну інформацію, яка має шкідливий інформаційний вплив, та створити умови для критичного аналізу громадянами країни інформації з відповідних ЗМІ.

5. Адаптувати сучасні методи інформаційної боротьби до вітчизняних реалій та надати відповідним державним відомствам рекомендації щодо їх застосування.

3.3. Вдосконалення інформаційної безпеки в умовах воєнної агресії

Національна інформаційна політика має відображати актуальні проблеми, що виникають на міжнародній арені та в таких сферах, як інформаційна безпека. Необхідно забезпечити законодавчий захист прав та інтересів усіх суб'єктів інформаційної діяльності. Найскладнішими тут є завдання, що передбачають координацію забезпечення національної, індивідуальної та соціальної інформаційної безпеки з одночасним визначенням нагальних пріоритетів, серед яких має бути створення/відновлення основних осередків захисту системи національної безпеки у сфері інформації, практична реалізація згаданого вище створення ефективної національної інформаційної безпеки. Систематичний план перегляду переліку нових інформаційних загроз, усунення існуючих загроз та визначення масштабів і тяжкості можливих наслідків.

Форми та методи організаційного вдосконалення, спрямовані на уникнення та усунення загроз інформаційній безпеці, у тому числі: розробка нормативно-правових засад важливих напрямків діяльності системи інформаційної безпеки, відмежування силової безпеки від структури державної влади, яка повинна забезпечувати інформаційну безпеку, розробка систем моніторингу, що аналіз стану інформаційної безпеки; ідеї розвитку, створення позитивних чинників, подолання критичного стану української промисловості у сфері інформатизації та захисту інформації; аналіз техніко-економічних показників українського та іноземного програмно-технічного забезпечення інформаційної безпеки та вибір ефективні напрямки розвитку української технічної підтримки; Розробляти системи економічних та статистичних даних для демонстрації ефективності системи в забезпеченні інформаційної безпеки

та інших сферах, досліджувати стандарти та методи оцінки ефективності інформаційної безпеки тощо [18, с. 319].

Розробка новітніх методів забезпечення інформаційної безпеки — це розробка форм і засобів, що сприяють цивілізаційному впливу держави на формування колективної свідомості суспільства, а також практичних рекомендацій щодо їх впровадження в практичне застосування; методика комплексного вивчення роботи працівників інформаційних систем, підвищення рівня мотивації, морально-психологічної стійкості та підходів до соціального захисту осіб, які працюють з секретними та секретними даними, розробити практичні рекомендації щодо збереження та зміцнення соціально- політичний баланс, забезпечення прав і свобод людей, використання підходів з інформаційною безпекою Зміцнення таких понять, як законність і правопорядок; створювати методи та інструменти для надання державним органам влади, компаніям та громадянам достовірних, повних та своєчасних даних; розвивати ключові напрями діяльності для запобігання впливу негативної інформації на емоції окремих осіб, груп та суспільну свідомість; розвивати цивілізовані, демократичні форми вплив і методи медіа розробити механізми розвитку інформаційних відносин у комерційній сфері та інтеграції інформаційних ресурсів в економічні відносини вивчити основні методи зниження криміногенної ситуації та зменшення кількості комп'ютерних злочинів, переважно у сфері кредитування і фінанси, сформулювати контроль вітчизняної наукової Методології та практичних порад щодо інтенсивного технологічного забезпечення експортних операцій, обґрунтовані вказівки проти засобів, що вважаються інформаційною зброєю; удосконалення видів контролю персоналу в рамках захищених систем в інформаційній сфері.

Механізми протидії інформаційним загрозам із зовнішніх джерел нагально потребують організації багаторівневого та різноспрямованого комплексного підходу, насамперед із врахуванням конкретних обставин зовнішніх факторів (геополітична та регіональна конфігурація ситуації, структурно-функціональна роль тощо). державного та транснаціонального організованого впливу злочинних груп).

Тому особливу увагу слід приділяти моніторингу характеру, специфіки, масштабу та подальшому прогнозуванню небезпек. Прогнозування є важливим самостійним елементом, який належить до заходів із запобігання зовнішнім джерелам інформаційної небезпеки та забезпечення національної безпеки. Основний метод моделювання прогнозування, основними принципами якого є мета побудови моделі; виявлення обмеженої кількості основних факторів, що зазнають істотних змін у досліджуваній системі; визначення характеру взаємозв'язків між цими факторами; принципи для встановлення множинних зв’язків між факторами, а також для виділення суттєвих зв’язків, які визначають прогрес системи та характер її змін.

Система стратегічних знань, отримана шляхом прогнозування результатів, може проілюструвати модель прогресу дослідницького середовища та підтвердити специфіку змісту його структурних компонентів. Будь-яке середовище із зовнішніми джерелами, здатними генерувати та відтворювати загрози особистій, громадській та національній інформаційній безпеці, підходить для моніторингу, прогнозування та запобігання небезпекам. Необхідно враховувати застарілість загальноприйнятих технологій і механізмів протидії зовнішнім загрозам національній безпеці, а також появу нових підходів, які сприяють розгортанню загроз і мінімізують пов’язані з цим ризики. Це зумовлено стрімким розвитком українського суспільства, його інформаційною природою, що також сприяє вдосконаленню методів ведення інформаційної війни [19, с. 175].

Розрізняють наступні групи підходів до протидії зовнішнім інформаційним загрозам

Такі джерела, як:

- набір профілактичних або превентивних методів, які мають запобігти даній загрозі та її розвитку або запобігти подальшим ризикам на початковій стадії;

- комплекс оперативних методів протидії агресії, поширенню загрози зовнішніх джерел інформації, пов'язаних з його розробкою та реалізацією.

Механізми протидії загрозам інформаційного характеру, в основному засновані на принципах управління ризиками, здатні запобігати деструктивним елементам, атрибутам, процесам, які є деструктивними для інформаційної безпеки та систем національної безпеки, а також стимулювати конструктивні можливості, елементи, атрибути, вдосконалення їх функцій і процес розвитку [20, с. 52].

Підсумовуючи, можна зробити висновок, що достатній рівень інформаційної безпеки може забезпечити комплекс політичних, економічних та організаційних заходів, які дозволяють реалізувати інформаційні права та інтереси країни та її суб'єктів.

Дослідження проблем національної інформаційної безпеки дозволяють стверджувати, що забезпечення інформаційної безпеки базується на національній організації інформації. Організація має забезпечувати гарантії інформаційної безпеки країни та її суб'єктів в умовах зростання загроз, таких як процес глобалізації та міжнародний тероризм. На жаль, в Україні існує багато факторів, які перешкоджають створенню такої інформаційної організації, не останньою з яких є відсутність координації між органами державної влади у забезпеченні інформаційної безпеки.

ВИСНОВКИ

Підсумовуючи, інформаційна зброя – це ефективні засоби знищення, зміни або викрадення інформаційних масивів, отримання необхідної інформації після зламу систем безпеки, обмеження або заборони доступу законних користувачів, втручання в роботу технічного обладнання, відключення тощо. Мережі зв'язку та комп'ютерні мережі, все, що забезпечує суспільство високими технологіями, і функції державних структур.

Якщо ми правильно розуміємо деталі інформаційної спільноти в контексті загострення глобальних проблем, ми повинні діяти сьогодні так, щоб протистояти жахливому потенціалу інформаційної війни та катастроф цивілізації, які виникають і відбуваються. накопичених у цьому процесі.

Організовуючи інформаційну безпеку, слід мати на увазі, що більшість загроз формуються саме через її співробітників, будь то інформація у вигляді знань співробітника або міститься в документах. Тому важливо розуміти основні фактори, що визначають поведінку співробітників, які можуть вдатися до розголошення інформації в офісі. Ці фактори можна розглядати як об'єктивні умови для того, щоб працівники були основним джерелом інформації. Непередбачуваність і неконтрольованість поведінки співробітників у різних ситуаціях також існує об'єктивно. Крім того, передбачення - це лише ймовірність, сподіваючись, що дії та реакції людини будуть саме такими, як ми прогнозуємо. Факторами також є недоліки освіти працівників, особливості їхнього характеру, що в свою чергу може бути спонуканням працівників до неадекватної поведінки та дій. Недоліки в професійній підготовці працівників, особливо в роботі з документами та обмежений доступ до інформації, а також такі якості, як безвідповідальність, недисциплінованість та інші негативні недоліки, також можуть визначати розголошення інформації офісними працівниками. Судячи з вищезазначених характеристик діловодства та умов, які можуть породжувати інформаційні загрози, остання визначається як об’єктивними, так і суб’єктивними причинами. Тому побудова будь-якої системи захисту інформації в офісі повинна включати заходи, спрямовані на

створення безпечних умов для роботи з інформацією в офісі, а також заходи, що виключають або істотно обмежують можливість неправомірних дій персоналу.

Тому науковий аналіз окремих питань, пов’язаних з формуванням та реалізацією державної політики у сфері інформатизації, сьогодні є особливо актуальним, оскільки вирішення цих питань сприятиме розвитку інформаційного суспільства і тим самим забезпечуватиме інформаційну безпеку суспільства. країни та України. Серед загроз інформаційній безпеці – монополія інформаційної сфери вітчизняними та іноземними олігархічними структурами, блокування державними ЗМІ інформації для українського та іноземного населення, нестача профільних кадрів, неефективність механізмів забезпечення формування та реалізації національної інформаційної безпеки. політики; несанкціонований доступ до інформації; загальний негативний вплив на інформаційні ресурси та інформаційну інфраструктуру; недостатні знання іноземного населення про внутрішню та зовнішньополітичну діяльність у країні; поширення дезінформації про зовнішню та внутрішню політику України; зовнішньополітичний, економічний, військовий та інформаційного характеру інформаційної структури на розвиток та реалізацію принципів зовнішнього та внутрішнього характеру політичного сектору в нашій державі, утискається свобода громадян України та юридичних осіб у закордонній інформаційній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. К.: КНТ, 2006. 280 с.

2. Малик Я. Інформаційна війна в Україні. Науковий вісник. 2015 року № 15 URL: https://science.lpnu.ua/sites/default/files/journal-paper/2022/feb/26730/malyk.pdf

3. Шпилик С. Інформаційна війна, пропаганда та pr: такі схожі й такі різні. Галицький економічний вісник Тернопіль : ТНТУ, 2014.Том 47. № 4.С. 178-188.

4. Базилюк Я. Б., Бодрук О. С., Венцковський Д. Ю. Україна у системі міжнародної безпеки: монографія. Рада національної безпеки і оборони України, Національний ін-т проблем міжнар. безпеки. К.: Фоліант: Стилос, 2009. 572 с.

5. Почепцов Г.Г. Інформаційно-психологічна війна. М: Сінтег, 2000. 180 с.

6. Богуш В. Інформаційна безпека держави. К.: "МК-Прес", 2005. 432 с.

7. Остроухов В. В., Присяжнюк М. М., Фармагей О. І., Чеховська М. М. Інформаційна безпека. Підручник К.: Видавництво Ліра К, 2021. 412 с

8. Кавун С. В. Інформаційна безпека. Навчальний посібник. Харків: Вид. ХНЕУ, 2008. 352 с.

9. Мужанова Т.М. Інформаційна безпека держави. навч.посіб. Навчально-науковий інститут захисту інформації. К. 2019 131 с.

10. Богуш В. М., Кривуца В. Г., Кудін А. М. «Інформаційна безпека: Термінологічний навчальний довідник». - за ред. Кривуци В. Г. – Київ, 2004. 508 с.

11. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник. – К.: Видавничо-поліграфічний центр “Київський університет”, 2008. – 274 с

12. Іванченко Є.В., Іванченко І.С., Хорошко В.О., Хохлачова Ю.Є.Забезпечення інформаційної безпеки держави. Вид-во Нац. авіац. ун-ту, 2016. 254 с.

13. Яковчук В.С., Малець Б.І. Інформаційні війни в сучасному світі. URl: https://sci.ldubgd.edu.ua/bitstream/123456789/7424/1/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96%20%D0%B2%D1%96%D0%B9%D0%BD%D0%B8%20%D0%B2%20%D1%81%D1%83%D1%87%D0%B0%D1%81%D0%BD%D0%BE%D0%BC%D1%83%20%D1%81%D0%B2%D1%96%D1%82%D1%96.pdf

14. Макаренко Л. П. Еволюція форм та методів ведення інформаційної війни. URl: https://www.researchgate.net/publication/350008570_EVOLUCIA_FORM_TA_METODIV_VEDENNA_INFORMACIJNOI_VIJNI

15. Дудикевич В. Б., Опірський І. Р., Гаранюк П. І., Зачепило В. С., Партика А. І. Забезпечення інформаційної безпеки держави: Навчальний посібник. Львів : Видавництво Львівської політехніки, 2017. 204 с.

16. Климчук О. О. Забезпечення інформаційної безпеки держави : підручник. К. : ДНУ «Книжкова палата України», 2015. 672 с

17. Остроухов В.В., Присяжнюк М.М., Петрик В.М. та ін. Інформаційна безпека (соціально-правові аспекти): Підручник / За ред. Є.Д.Скулиша. – К., 2010. – 776 с.

18. Петрик В.М., Присяжнюк М.М., Мельник Д.С. та ін. Забезпечення інформаційної безпеки держави: підручник ; за заг. ред. О.А. Семченка та В.М. Петрика. - К.: ДНУ «Книжкова палата України», 2015. - 672 с.

19. Пєвцов Г.В., Залкін С.В., Сідченко С.О., Хударковський К.І. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: [монографія]. – Харків : Цифрова друкарня № 1, 2013. – 270 с.