

**МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ**

**ФАКУЛЬТЕТ ФІНАНСІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І
СИСТЕМ**

**КВАЛІФІКАЦІЙНА РОБОТА
на тему:**

Система безпеки інформаційного простору в умовах інформаційної війни

Здобувача вищої освіти першого (бакалаврського) рівня,
4 курсу, групи КБ-19-1, спеціальності 122 «Комп'ютерні науки»,
освітня програма «Інформаційні управляючі системи і технології (за галузями)»


(підпис)

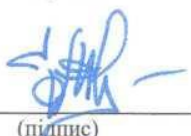
Роженка Нікіти Даниловича
(прізвище, ім'я, по батькові)

Науковий керівник


(підпис)

Філоненко Михайло
Миколайович, к.ф.-м.н.,
доцент
(прізвище, ім'я, по батькові, науковий
ступінь, вчене звання)

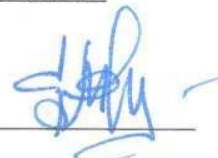
Керівник освітньо-
професійної програми


(підпис)

Федотова - Півень Ірина
Миколаївна, к.т.н, доцент
(прізвище, ім'я, по батькові, науковий
ступінь, вчене звання)

Допущено до захисту за рішенням кафедри
протокол від «26» травня 2023 № 13

Завідувач кафедри


(підпис)

Філоненко Михайло
Миколайович, к.ф.-м.н.,
доцент
(прізвище, ім'я, по батькові,
науковий ступінь, вчене звання)

Реєстрація № 27

06.06.2023

(дата)



(підпис відповідально

Результати перевірки

до захисту

(до захисту, на доопрацювання)

06.06.2023

(дата)

Результат захисту

4 (добре)

(оцінка)

14.06.2023

(дата)



Голова комісії:


(підпис)В.М. Франчук

Члени комісії:


(підпис)М.М. Філоненко
(підпис)О.В. Редич
(підпис)Є.В. Котух

БЛАНК ОЦІНЮВАННЯ ВИПУСКНОЇ РОБОТИ

Об'єкти контролю	Діапазон оцінки в балах	Фактична кількість балів	Примітки	Дата, П.І.Б.: керівника, голови комісії членів комісії, секретаря, (підписи)
ОЦІНЮВАННЯ КВАЛІФІКАЦІЙНОЇ РОБОТИ КОМІСІЄЮ ПО ЗАХИСТУ				
1. Зміст випускної роботи (якість теоретичного матеріалу, його зв'язок з практичним, вміння представляти матеріал в логічній послідовності, наявність висновків та пропозицій)	від 0 до 30	26		14.06.2023 Франчук В.М. Філоненко М.М. Редич О.В. Котух С.В. Суховерхня Л.П.
2. Дотримання вимог щодо оформлення	від 0 до 10	7		
3. Вчасне виконання роботи на всіх етапах у встановлені кафедрою терміни	від 0 до 5	3		
4. Рецензент	від 0 до 5	4		
РАЗОМ БАЛІВ	від 0 до 50	40		

Оцінювання кваліфікаційної роботи науковим керівником - 40 балів.

ПЕРЕВЕДЕННЯ ОЦІНКИ ЗА 100-БАЛЬНОЮ ШКАЛОЮ ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою	Дата	П.І.Б.: голови, членів комісії, секретаря, (підпис)
80	B	4 (добре)	14.06.2023	Франчук В.М. Філоненко М.М. Редич О.В. Котух С.В. Суховерхня Л.П.

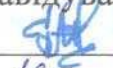
ПРАВИЛА ПЕРЕВЕДЕННЯ ОЦІНОК ДО НАЦІОНАЛЬНОЇ ШКАЛИ ТА ШКАЛИ ЄКТС

Оцінка за 100-бальною шкалою	Оцінка за шкалою ЄКТС	Оцінка за національною шкалою
90-100	A	5 (відмінно)
80-89	B	4 (добре)
70-79	C	
60-69	D	3 (задовільно)
50-59	E	
35-49	FX	2 (незадовільно)

Факультет фінансів та цифрових технологій
 Кафедра комп'ютерних та інформаційних технологій і систем
 Галузь знань: 12 «Інформаційні технології»
 Спеціальність: 122 «Комп'ютерні науки»
 Освітня програма: «Інформаційні управляючі системи і технології (за галузями)»

Затверджую

Завідувач кафедри

 Філоненко М.М.

«16» 11 2022

Завдання на кваліфікаційну роботу

здобувачу вищої освіти

Роженко Нікіта Данилович

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи

Система безпеки інформаційного простору в умовах інформаційної війни.

Затверджена наказом ректора від «15» листопада 2022 № 1205 (зі змінами наказ від «04» квітня 2023 № 361)

2. Строк здачі закінченої роботи «26» травня 2023

3. Цільова установка

Мета роботи аналіз та розрахунок систем безпеки інформаційного простору в умовах інформаційної війни та підвищення ефективності методів ведення бойових дій в інформаційній війні.

Об'єкт дослідження процес втручання в інформаційний простір країн світу.

Предмет дослідження методи захисту інформаційного простору мовою інформаційної війни, методи координації сил при веденні інформаційної війни, методи координації сил при веденні інформаційної війни.

База дослідження середовища MATLAB.

4. Вихідні дані до роботи проаналізувати технології, методи втручання в інформаційний простір й основних елементів організації безпеки інформаційного простору; визначити вимоги до механізмів захисту інформаційного простору; розробити метод вирішення інформаційного конфлікту шляхом переваги над ворогом; провести розрахунок розробленого методу.

5. Перелік графічного матеріалу кваліфікаційна робота містить 48 сторінок основного тексту, 2 рисунка, 1 таблицю.

6. Зміст випускної кваліфікаційної роботи (перелік питань за кожним розділом)

1.1 Інформаційна війна та її сутність

1.2 Особливості безпеки на сучасному етапі розвитку інформаційних технологій

1.3 Інформаційна війна проти України

- 2.1 Ризики та вразливості в інформаційній сфері в умовах інформаційної війни
 2.2 Інструменти інформаційної війни
 2.3 Несанкціоновані учасники та порушники
 3.1 Протидія інформаційній війні
 3.2 Засоби посилення безпеки інформаційного простору в умовах інформаційної війни
 3.3 Інструменти виявлення втручання в інформаційному полі

7. Календарний план виконання роботи

№ п/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	
		За планом	Фактично
1	2	3	
1	Вибір теми, підбір літературних джерел, формування структури кваліфікаційної роботи	15.11.2022	15.11.2022
2	I розділ (розкрити сутність і стан дослідження наукової проблематики роботи, після чого навести її загальну характеристику; огляд літератури за темою і вибір конкретних напрямів досліджень)	01.02.2023	01.02.2023
3	II розділ (аналіз експериментальної частини про методики досліджень)	03.04.2023	04.04.2023
4	III розділ (проведені теоретичні і (або) експериментальні дослідження та проектні рішення)	10.05.2023	09.05.2023
5	Висновки	15.05.2023	15.05.2023
6	Доопрацювання роботи з урахуванням зауважень наукового керівника	26.05.2023	26.05.2023
7	Отримання відгуку керівника	06.06.2023	06.06.2023
8	Отримання зовнішньої рецензії	08.06.2023	08.06.2023

8. Дата видачі завдання «16» листопада 2022

9. Керівник випускної кваліфікаційної роботи


(підпис)

Філоненко
(прізвище, іні

10. Керівник освітньо-професійної програми


(підпис)

Федотова
І.М.
(прізвище, іні

11. Завдання до виконання отримав здобувач вищої освіти


(підпис)

Роженко
(прізвище, іні

АНОТАЦІЯ

Система безпеки інформаційного простору в умовах інформаційної війни

Метою даного дослідження є аналіз та розрахунків систем безпеки інформаційного простору в умовах інформаційної війни та підвищення ефективності методів ведення бойових дій в інформаційній війні.

Завдання роботи включає:

- аналіз способів втручання в інформаційний простір;
- випробування моделей завад в інформаційному просторі;
- провести математичні розрахунки в середовищі MATLAB щодо інформаційної безпеки в умовах інформаційної війни.

Предметом дослідження є методи захисту інформаційного простору в мовою інформаційної війни, методи координації сил при веденні інформаційної війни, методи координації сил при веденні інформаційної війни.

Об'єктом дослідження є процес втручання в інформаційний простір країн світу.

Базою дослідження є середовища MATLAB.

За результатами дослідження розроблено математичну модель аналізу сил конфліктуючих сторін в рамках інформаційної війни втручання в інформаційний простір що дозволило провести аналіз переваг над ворогом.

Кваліфікаційна робота містить 57 сторінок, 1 таблиця, 4 рисунки, список використаних джерел 27 найменувань.

Ключові слова: інформаційна безпека, інформаційна система, інформаційні технології, інформаційна війна.

Рік виконання кваліфікаційної роботи: 2023 р.

Рік захисту роботи: 2023 р.

ANNOTATION

Security system of the information space in the conditions of information war

The method of this study is the analysis and calculation of the security system of the information space in the conditions of information war and increasing the effectiveness of the methods of conducting combat operations in the information war.

The task of work includes:

- analysis of methods of intervention in the information space;
- testing of interference models in the information space;
- perform mathematical calculations in the MATLAB environment regarding information security in the conditions of information warfare.

The subject of research is the methods of protecting the information space in the information war, the methods of coordinating the forces of the information war, the methods of coordinating the forces of the information war.

The object of the study is the process of intervention in the information space of the countries of the world.

The basis of the study is the MATLAB environment.

According to the results of the research, a mathematical model of the analysis of the forces of the conflicting pages as part of the information war of interference in the information space was developed, which made it possible to analyze the advantages over the enemy.

The qualification work contains 57 pages, 1 table, 4 images, a list of 27 references.

Keywords: information security, information system, information technology, information war.

Year of qualification work: 2023.

Year of job protection: 2023.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	9
ВСТУП	10
Розділ 1. Теоретичні основи інформаційної війни	12
1.1. Інформаційна війна та її сутність	12
1.2. Особливості безпеки на сучасному етапі розвитку інформаційних технологій	15
1.3. Інформаційна війна проти України	19
Розділ 2. Вплив інформаційної війни на національну безпеку	23
2.1. Ризики та вразливості в інформаційній сфері в умовах інформаційної війни	23
2.2. Інструменти інформаційної війни	31
2.3. Несанкціоновані учасники та порушники	33
РОЗДІЛ 3. Удосконалення систем безпеки в інформаційному просторі	36
3.1. Протидія інформаційній війні	36
3.2. Засоби посилення безпеки інформаційного простору в умовах інформаційної війни	40
3.3. Інструменти виявлення втручання в інформаційному полі	52
ВИСНОВОК	57
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	58

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІБ – Інформаційна безпека.

ІС – Інформаційна система.

ІТ– Інформаційні технології.

ІВ – Інформаційна війна.

СВА – Система виявлення атак.

СВВ – Система виявлення вторгнень.

ВСТУП

Актуальність. Поява та інтенсифікація загроз в інформаційній сфері, зокрема загроз, пов'язаних з веденням інформаційних війн, значно підвищила значення і роль інформаційної безпеки в системі національної безпеки України та розширила її зміст.

Особливу увагу слід приділити соціальним і культурним наслідкам інформаційної пропаганди, інформаційних операцій та інформаційної війни: На основі вивчення історії та еволюції ІТ, підбурювання, пропаганди та інформаційної війни слід оцінити ризики в інформаційних системах та проаналізувати загрози.

Метою інформаційної війни є ослаблення сил ворога або опонентів і посилення можливостей власних сил. Вона також включає в себе контрпропагандистські заходи для впливу на людську свідомість. Цей вид війни не призводить безпосередньо до кровопролиття або руйнувань, немає жертв і ніхто не втрачає даху над головою. Основною метою інформаційної війни є маніпулювання масами. Цілями цієї маніпуляції майже завжди є впровадження у свідомість суспільства та окремих людей ворожих і шкідливих ідей та думок; заплутування та дезінформація громадськості; послаблення певних переконань; залякування власного народу образом ворога; залякування ворога власною могутністю; забезпечення ринку збуту для економіки; залякування ворога. У цьому випадку інформаційна війна є елементом конкуренції.

Метою даного дослідження є аналіз та розрахунок систем безпеки інформаційного простору в умовах інформаційної війни та підвищення ефективності методів ведення бойових дій в інформаційній війні.

Для досягнення поставленої мети вирішуються наступні завдання:

- аналіз способів втручання в інформаційний простір;
- випробування моделей завад в інформаційному просторі;

- провести математичні розрахунки в середовищі MATLAB щодо інформаційної безпеки в умовах інформаційної війни.

Об'єктом дослідження є процес втручання в інформаційний простір країн світу.

Предметом дослідження є методи захисту інформаційного простору в мовою інформаційної війни, методи координації сил при веденні інформаційної війни, методи координації сил при веденні інформаційної війни.

Практична цінність даного дослідження полягає в аналізі моделей захисту інформаційного простору в умовах інформаційної війни, а також у проведенні математичних розрахунках для визначення переваг та недоліків. Недоліки протиборчих сторін.

Розділ 1. Теоретичні основи інформаційної війни

1.1. Інформаційна війна та її сутність

Позитивне інформаційне розгортання як основа сучасного суспільства сприяє швидкій глобалізації, стираючи межі між державами, регіонами та кордонами. Інформація, разом з політикою та економікою стає важливим фактором розвитку держав, а також та засобом ведення війни в геополітичних відносинах і може сформувати новий тип війни, а саме - інформаційну війну.

На сьогоднішній день науковці виділяють п'ять підходів до визначення цього поняття. Представники першого підходу визначають інформаційну війну як серію політичних воєн. Інформаційна війна - це сукупність політичних, економічних, соціальних дипломатичних і технологічних методів, прийомів і засобів для досягнення інформаційна війна - це сукупність політичних, економічних, дипломатичних і технологічних методів, прийомів і засобів для досягнення вигідного ефекту в інформаційній сфері, якщо вона спрямована на об'єкта агресії та захисту власних інтересів. Прихильники другого напрямку називають його найбільш гострою формою боротьби в інформаційному просторі, в основі якої лежить протистояння між агресивними сторонами з різних позицій.

Згідно з третім підходом, інформаційна війна трактується як форму ведення війни з використанням електронних інформаційних засобів. Як зазначає Уін Швартов, "інформаційна війна - це електронний конфлікт. Інформація є стратегічним активом, що підлягає захопленню або знищенню" [1, с.99]. Представники четвертого підходу трактують інформаційну війну як Протистояння сучасним технологічним системам.

Сучасний нестримний розвиток суспільства і світу вимагає іншого підходу до трактування цього поняття. Життя людини базується на впливі інформаційної війни та прихованої інформації [1, с.99]. Як і інші явища, інформаційна війна має відмінні риси від звичайної війни:

- відсутність видимих фізичних ушкоджень може затримати оборонну реакцію країни;

- інструменти інформаційної війни є майже непередбачуваними і постійно змінюються відповідно до оперативної обстановки, що робить варіанти протидії, які повинні базуватися на аналітичній спроможності та високому інтелектуальному потенціалі і залучати посадових осіб на всіх рівнях влади, надзвичайно складними в сучасних умовах;

- в інформаційній війні не завжди відбувається фізичне захоплення персоналу, але досягається контроль над свідомістю;

- вибірковість базується на принципі максимізації ефективності. Іншими словами, інформаційна війна є ефективною, коли вона має реальний вплив на осіб, які приймають рішення в країні, що атакується;

- короткострокова інформаційна війна є неефективною, коли інформаційна інфраструктура впливової країни є слабкою;

- розуміння істини сплющується, аргументи стають абсурдними, а здоровий глузд порушується;

- впливати на думки противника так, щоб він приймав рішення на користь нападника;

- перетворіть перевагу опонента на недолік;

- гра з емоціями та відволікання від непотрібного [3, с.27].

Тому інформаційна війна передбачає послаблення матеріальних і моральних сил противника, а також посилення власних можливостей ведення інформаційної війни. У процесі інформаційної війни використовуються засоби пропаганди для впливу на свідомість людини шляхом ідеологічного та емоційного впливу. Відповідно до методів ведення інформаційної війни та засобів впливу на об'єкт, сучасні науковці розрізняють різні види інформаційної війни, одним з теоретиків інформаційної війни є М. Лібікі, який проаналізував характеристики інформаційної війни у своїй книзі "Що таке інформаційна війна?" виокремлює сім типів інформаційних конфліктів:

- "Командно-адміністративні", спрямовані на порушення каналів комунікації між командою та практиком;
- "Розвідка" включає в себе збір і захист конфіденційної особистої інформації;
- "Психологічні" особливості включають пропаганду, обробку суспільної інформації, деморалізацію та дезінформацію;
- "Злом" здійснюється шляхом створення спеціальних програм і саботажу або нападу на ворога;
- "Економіка" втілюється в інформаційних блокадах та інформаційному імперіалізмі;
- "Електроніка" зосереджується на електронних засобах зв'язку, таких як радіо, радары та комп'ютерні мережі.

Крім того, науковці розрізняють такі види війни: психологічна війна, кібернетична війна, мережева війна (мережевий інформаційний простір, основні стратегічні операції (як розвідувальні, так і військові), а також її інформаційне забезпечення, дипломатичне, економічне та технологічне забезпечення. У свою чергу, багато науковців науковці пропонують іншу класифікацію видів інформаційних війн: політичні, економічні, психологічні та електронні. економічну, психологічну та електронну, які можуть сформувати оптимальні інструменти для подолання глобальних загроз [1, 100].

Таким чином, процес розвитку інформаційного суспільства супроводжується модернізацією всіх аспектів суспільного життя, існує чимало загроз домінування, зомбування особистості, маніпулювання масовою свідомістю, поширення чуток, соціальна нестабільність, втрати від терористичних актів, широкі можливості для інформаційної війни та багато інших. В інформаційній війні основними об'єктами впливу та захисту є населення, військові, опозиційні політичні еліти та системи, що формують маси. Обізнаність і думка Інформаційна війна не призводить безпосередньо до кровопролиття, ні руйнувань, ні жертв, ні голоду. Однак ці війни ведуться для подолання свідомості.

1.2. Особливості безпеки на сучасному етапі розвитку інформаційних технологій

На сучасному етапі розвитку цивілізації інформація відіграє важливу роль у функціонуванні суспільних і державних інститутів та в житті кожної людини. На наших очах процес інформатизації розвивається дуже швидко і часто непередбачувано, і це лише початок шляху до усвідомлення його соціальних, суспільно-політичних, економічних, військових та інших можливих наслідків. Глобальна інформатизація веде до створення єдиного світового інформаційного простору, в якому інформація накопичується, обробляється, зберігається та обмінюється між суб'єктами цього простору (людьми, організаціями та державами). Швидкий обмін політичною, економічною, науково-технічною, спеціалізованою та іншою інформацією, використання нових інформаційних технологій у всіх сферах суспільного життя, особливо у виробництві та управлінні, безсумнівно, буде корисним для людства. Однак, подібно до того, як швидкий промисловий розвиток ставить під загрозу екологію планети, а досягнення ядерної фізики створюють небезпеку ядерної війни, інформаційні технології можуть спричинити багато серйозних проблем у глобальному масштабі.

Поняття "зв'язки з громадськістю" є багатогранним і має багато інтерпретацій. У книзі Чумикова "Зв'язки з громадськістю" воно визначається наступним чином: «...забезпечення того, щоб керівництво організації було поінформоване про громадську думку, своєчасно реагувало на неї, було готове до змін і використовувало їх найбільш ефективно. Визначення та підкреслення основної місії суспільства, яка полягає в служінні суспільним інтересам...» і так далі [4].

Вплив знань на колективну свідомість присутній завжди шамани та жреці також використовували його як техніку і намагалися будувати. Термін "інформаційна війна" має багато визначень. У цьому контексті доцільно взяти

до уваги найбільш популярні з них, виокремивши ознака, притаманна всім тлумаченням цього явища.

Таблиця 1.1 - Складові психологічної операції по Г.Г.Почепцова.

	Компоненти психологічної операції					Остаточна мета
публік рілейшнз	оцінка ситуації	планування операції			виконання	Поведінкові зміни у цільовій аудиторії
Інформаційні війни	Збір розвідувальної інформації	Аналіз цільової аудиторії	Розробка продукту	Відбір каналів поширення	виробництво медіа поширення	

Інформаційно-психологічна війна – це:

- вплив поширення певної інформації на цивільне населення та військовослужбовців в інших країнах. Термін "інформаційно-психологічна війна" запозичений з військового лексикону США. В перекладі на англійську мову цей термін ("інформаційно-психологічна війна") може перекладатися як "інформаційна війна" або "інформаційно-психологічна війна", залежно від контексту конкретного офіційного документа чи наукової публікації;
- дії, спрямовані на досягнення інформаційного домінування шляхом завдання шкоди інформації, інформаційним процесам та інформаційним системам противника і захисту власної інформації, інформаційних процесів та інформаційних систем противника [10];
- командування і контроль, загальна стратегія, заснована на зростаючій важливості та цінності інформації в політиці, економіці та соціальному житті;

- нова форма боротьби між сторонами з використанням спеціалізованих оборонних методів і засобів для впливу на інформаційне середовище противника та досягнення стратегічних цілей війни [5].

Основним завданням інформаційної війни є маніпулювання громадською думкою. Цілями такої маніпуляції є, в більшості випадків, впровадження у свідомість громадськості та окремих осіб ворожих і шкідливих ідей та думок; заплутування та дезінформація громадськості; послаблення певних переконань; залякування власного народу образом ворога; залякування ворога власною силою; забезпечення ринків збуту для своєї економіки. У цьому випадку інформаційна війна є елементом конкуренції [13].

Аналіз визначення дозволяє виявити особливості, які характеризують ведення інформаційної війни:

- Вплив на різні соціальні групи, такі як військово-службовці, робітники, інтелігенція тощо.
- Різноманітність передаваної інформації.
- Агресивний характер стратегії застосування інформаційних засобів.
- Мета інформаційної війни полягає в зміні способу мислення у впливовому напрямку і зайнятті більш вигідної позиції.
- Захист власного простору від нападу.

Існує також інша класифікація складових інформаційної війни:

- Психологічні операції - використання інформації для впливу на дестабілізацію солдатів противника.
- Радіоелектронна боротьба - використання різних засобів для запобігання отримання противником точної інформації.
- Дезінформація - надання ворогові неправдивої інформації про свої потужності.

- Фізичне знищення - може бути частиною інформаційної війни, але тільки тоді, коли вона спрямована на вплив на елементи інформаційної системи.

- Заходи безпеки - прагнення уникнути того, щоб противник дізнався про наші можливості.

Вплив інформації на противника має свої особливості, що відрізняються від інших форм боротьби і спілкування в області обміну інформацією. Зокрема, в інформаційній війні об'єктом впливу є масова свідомість противника, а не окрему, що вони спотворюють факти, викликають неадекватну поведінку противника або змушують його займати не вигідну позицію.

Ще однією особливістю інформаційної війни є те, що вона може мати дуже довготривалий ефект. Інформаційні війни можуть бути спрямовані на зміну світогляду, політичних поглядів, поведінки і навіть культурних традицій інших країн. Ці процеси можуть тривати десятиліттями і мати глибокий вплив на країну і її громадян.

Отже, інформаційна війна є складним процесом, який вимагає детального аналізу і вивчення складових частин. Вона може мати серйозні наслідки для країн і людей, на яких спрямована. Тому важливо бути уважним та обережним щодо інформації, яку ми сприймаємо і розповсюджуємо, а також уважно вивчати і аналізувати її джерела та інформаційні стратегії.

Серед методів маніпуляції масовою свідомістю можна виділити такі:

- Використання навіювання;
- Перенесення приватного факту в загальну сферу;
- Використання чуток, домислів, тлумачень в складній соціальній або політичній ситуації;
- Метод «потрібні трупи»;
- Метод «страховиська»;
- Замовчування деяких фактів і випікання інших;
- Метод фрагментації;

- «Метод Геббельса» (повторення брехні);
- Метод чергування на конвеєрі «правда, правда, правда, неправда, правда»;
- Створення неправдивих подій та містифікація [14].

Підтипом інформаційної війни є кібервійна, що означає протистояння в кіберпросторі за допомогою методів інформаційних технологій. Німецькі експерти виділили такі методи кібервійни:

- Шпигунство - проникнення в комп'ютерні системи противника з метою отримання інформації;
- Атака на збій системи - група комп'ютерів одночасно атакує комп'ютерну систему противника, викликаючи збій у роботі цієї системи через великий потік інформації.

Іншим підтипом інформаційної війни є гібридна війна, яка об'єднує в собі різні види воєнних дій, включаючи інформаційні та кібернетичні. Головною метою гібридної війни є не тільки перемога військами на полі бою, але й підірвання довіри громадськості до влади і демонстрація недостатньої ефективності державних структур в роботі з населенням.

Існує також інформаційна конкуренція, що полягає у змаганні між різними суб'єктами за право контролювати інформаційні потоки в суспільстві. Це можуть бути державні органи, політичні партії, релігійні організації, мас-медіа, комерційні структури тощо. У такій конкуренції важливо мати засоби інформаційного впливу на громадськість, зокрема, володіти навичками ефективної комунікації та знати принципи побудови різних типів дискурсу.

У сучасному світі інформаційна війна стає все більш актуальною, оскільки інформаційні технології стають все потужнішими та доступнішими. Тому важливо розуміти, які методи маніпуляції масовою свідомістю використовуються в таких конфліктах, як підвищувати свою інформаційну грамотність та критичне мислення, і як узгоджувати дії в інформаційному просторі для досягнення мирної співпраці та взаєморозуміння між націями та державами.

1.3. Інформаційна війна проти України

Як свідчить аналіз досліджень, проведених науковцями, інформаційна зброя, створена у вигляді програмно-технічних комплексів та засобів, є не тільки економічною, легко маскується під засоби оборони та здатна діяти анонімно без оголошення війни, але й має такі характеристики: універсальність, багатовимірність структури, застосування та екстремальність дії (в сенсі нанесення максимальної шкоди) та інші особливості. Наразі Україна є неофіційно відкритою, оскільки підключена до глобальної інформаційної інфраструктури - Інтернету. Тому наша країна є особливо вразливою для інформаційної зброї. У цій ситуації жодна держава, в тому числі і наша, не може бути спокійною, оскільки наші громадяни можуть бути піддані інформаційним атакам в будь-який момент.

Вперше в історії наша країна зіткнулася з однією з найнебезпечніших форм війни - інформаційною. Головним ворогом у тривалому інформаційному конфлікті стала Російська Федерація. Інформаційний тиск здійснюється і з боку Заходу.

Росія застосовує передові форми гібридної війни в Україні з початку 2014 року. Росія прагне максимального невтручання Заходу в події в Україні, щоб виграти час для встановлення і розширення свого військового втручання в конфлікт. Росії також вдалося посіяти насіння розбрату в НАТО і ЄС і створити напруженість між їхніми урядами, особливо через антиросійські санкції.

Таким чином, головною метою Російської Федерації у цій війні є створення викривленого бачення подій серед громадян України та Росії. Це, в свою чергу, деморалізує український народ і українських солдатів та заохочує до зради і дезертирства.

У своїх розвідувальних наступальних діях проти України Росія використовує різноманітні методи і прийоми, залежно від того, на які групи

спрямовані розвідувальні атаки. Основними методами розвідувальних атак проти України є наступні:

- 1) дезінформація та маніпуляції
- 2) пропаганда
- 3) Диверсифікація громадської думки
- 4) психологічний та психотропний тиск
- 5) поширення чуток [8].

Основні наслідки та уроки інформаційно-пропагандистської війни Росії проти України як важливої складової "гібридної війни" є безпрецедентними за своїм змістом, масштабами та спрямованістю:

По-перше, інформаційна війна розпочалася задовго до військового вторгнення Росії в Україну і продовжує супроводжувати його на кожному етапі, попередньо адаптуючи до поточних цілей і завдань;

По-друге, проект пропаганди та дезінформації

Це операції та заходи, спрямовані на всі сегменти російської та західної громадської думки, а також на всі регіони України, кожен з яких має свою мету та завдання;

По-третє, метою інформаційної війни в Україні є знищення української держави. У Росії - здобути громадську підтримку для легітимізації дій російського керівництва. Для західних країн - дискредитація дій українського керівництва та збройних сил [1].

Ця війна є викликом для міжнародної спільноти в цілому і становить зростаючу розвідувальну загрозу для світового порядку. Слід зазначити, що Україна не готова до такого масштабного військового та розвідувального наступу.

Указом Президента України законодавчо забезпечено національну безпеку в інформаційній сфері шляхом введення в дію Рішення Комітету з питань національної безпеки і оборони України від 2014-4-28 "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки в Україні":

- Визначення механізмів протидії негативним інформаційно-психологічним впливам;
- підготовка проекту стратегії розвитку інформаційного простору України, зокрема, визначення мети, завдань, структури та режиму функціонування державної системи забезпечення інформаційної безпеки та проекту кібернетичної стратегії безпеки України;
- підготовка Закону України "Про кібербезпеку України". Для того, щоб запобігти дезінформації та психологічному впливу, необхідно дотримуватися певних правил.
- Критично ставитися до пропаганди іноземних ЗМІ та більше довіряти інформації з офіційних джерел і публікацій.
- Не давати різких оцінок ситуації навколо або всередині інформаційного простору.
- Будьте уважні до ворожої пропаганди та протидійте їй. Завдання цієї пропаганди - створити у свідомості бажаний образ поточної ситуації [9].

Таким чином, можна зробити висновок, що метою інформаційної війни є ослаблення матеріальних і моральних сил противника і посилення самого противника. Перемагає в інформаційній війні та сторона, яка зможе змодельовати поведінку противника в різних ситуаціях, визначити власні алгоритми поведінки і, зрештою, реалізувати їх. Ретельне моделювання поведінки противника означає збір, зберігання та обробку інформації про нього. Знання та розуміння історії, культури та способу життя противника.

Розділ 2. Вплив інформаційної війни на національну безпеку

2.1. Ризики та вразливості в інформаційній сфері в умовах інформаційної війни

Інформаційні ризики можна поділити на три категорії залежно від їхнього джерела:

- Ризики, пов'язані з втратою інформації (витік, знищення або зникнення). Вони є особливо небезпечними, коли існує ризик втрати інформації, яка є критично важливою або з обмеженим доступом для організації, наприклад, банківської або комерційної таємниці.

- Ризики, пов'язані зі складом джерел інформації (неповнота, використання недостовірної інформації, відсутність необхідної інформації, дезінформація);

- Ризики, пов'язані з впливом інформації на діяльність підприємства (поширення неправдивої або негативної інформації, інформаційно-психологічний вплив на працівників, клієнтів та акціонерів, інформаційний тероризм);

Враховуючи, що в ринковій економіці ризик є однією з характеристик господарської діяльності, а у випадку підприємницької діяльності ризик є однією з її складових, виключити ризик з інформаційних відносин суб'єктів господарювання, або навіть з будь-яких відносин, неможливо.

Конкуренція та наявність вищезазначених ризиків створюють певні загрози для інформації, що використовується підприємством. Водночас, діяльність останнього передбачає безперервний процес планування та прийняття рішень, що потребує підтримки достовірної інформації. Водночас, участь людей в економічному житті породжує потребу в об'єктивній та всебічній інформації про діяльність бізнес-організацій.

На жаль, у процесі конкурентної боротьби інформація завжди несе загрозу впливу на споживачів товарів і послуг, який не завжди є об'єктивним, оскільки не тільки неправомірно порушує інформацію конкуруючих

організацій, але й сприяє формуванню правильних уявлень про товари, послуги та організації, що їх виробляють і надають. Послуги та організації, що їх виробляють і надають

Таким чином, в інформаційних відносинах бізнес-організацій можливі загрози, пов'язані з вторгненням в інформаційні ресурси (особливо ті частини, доступ до яких обмежений), загрози, що виникають у процесі формування середовища та умов діяльності таких організацій. У першому випадку інформація є об'єктом загрози, у другому - інструментом реалізації загрози.

Як показує досвід, основними методами реалізації таких загроз є

- Маніпулювання інформацією (дезінформація, викривлення інформації, подання в інформаційне середовище неповної або неправдивої інформації).
- Порушення встановленого порядку обміну інформацією, несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів, незаконне збирання та використання інформації;
- знищення та незаконне використання інформаційних ресурсів, що належать іншим особам; та
- інформаційний тероризм (наприклад, поширення комп'ютерних "вірусів", встановлення програмних або апаратних пристроїв для імплантації, встановлення електронних пристроїв для перехоплення інформації, неправомірне використання або знищення інформаційно-комунікаційних систем, нав'язування неправдивої інформації, розголошення небезпечної інформації).

Найпоширеніші загрози для інформації організації включають розголошення, крадіжку, зміну або знищення конфіденційної або чутливої інформації, неправомірне використання інформації, що становить ринковий інтерес, включаючи інтелектуальну власність організації, а також доступ до захищеної інформації несанкціонованими особами.

Розголошення інформації - будь-яка протиправна, навмисна або необережна дія державного службовця або іншої особи, що призводить до оприлюднення (передачі) несанкціонованої інформації та встановлює

відповідні процедури розголошення, які не потребують залучення державних службовців. Це може бути зроблено шляхом повідомлення, передачі, передачі, опублікування, втрати або іншого розголошення відповідної інформації.

Викрадення інформації - це отримання таємниці з метою подальшого використання або передача носіїв інформації (документів, електронних носіїв, відео- та аудіозаписів) іншою особою цієї особи.

Фальсифікація інформації - це зміна змісту інформації, що міститься на певному носії, або самого носія (комп'ютерної програми) таким чином, що використання цієї інформації стає повністю неможливим або вимагає значного уточнення чи аналізу цієї інформації.

Несанкціоноване використання інформації - це використання певних даних, інформації та технологій, що належать конкретній юридичній або фізичній особі, у службовій чи іншій діяльності без її згоди або особами, яким ця інформація відома.



Рис 2.1. Структура інформаційної війни

Структура інформаційної війни доволі велика, але можна виділити основні інструменти введення інформаційної війни, а саме :

- Взлом комп'ютера;
- «Denial-of-service» атака;

- Комп'ютерні віруси, хробаки, логічні бомби;
- Електронна зброя;
- Інформаційні блокади;
- «Trojan horse» програми;
- «Спуфінг» мережі або електронної адреси;
- Соціальна інженерія;
- Підробка електронної пошти;
- Підробка даних;
- Управління сприйняттям;
- Вербування агентів;
- Open source intelligence;
- Злом пароля;
- Підслуховування;
- Мережеві сніфери.

Несанкціонований доступ, який порушує встановлені правила доступу до інформації, також є несанкціонованим доступом.

Основні загрози в інформаційній війні.

- Комп'ютерні програми (віруси, хробаки, троянські коні, логічні бомби, недоліки в програмах і системах комп'ютерної безпеки (випадкові або навмисні);

- Комп'ютерне обладнання (мікроскопічні машини та мікроорганізми, високоенергетичні випромінювачі та електромагнітні імпульси, що порушують роботу електронних схем).

- Спеціальні та вбудовані функції чіпа також можуть бути реалізовані в інтегральних схемах (мікросхемах). Сценарії активації таких функцій варіюються від певного набору програмного коду до спеціальних радіосигналів на певній радіочастоті.

- Наномашини - мікроскопічні роботи, які можуть проникати в комп'ютери і пошкоджувати електронні схеми та обладнання.

Ці загрози є загальними і однаково стосуються всіх видів інформації, включаючи документи, електронні пристрої та інформацію. Звичайно, кожен вид інформації має додаткові та специфічні характеристики, які є унікальними для певних типів інформаційних загроз. Розглядати кожну з цих ситуацій окремо було б недоцільно, оскільки заходи щодо захисту та протидії цим типам загроз можуть забезпечити безпечну інформаційну ситуацію з підвищеною гарантією. Водночас, враховуючи тісний зв'язок сучасного бізнесу з комп'ютерними інформаційними технологіями, необхідно надати деяку характеристику загроз цим технологіям, особливо з огляду на перспективи подальшої інформатизації та розвитку суспільства.

У реалізації загроз бізнес-організаціям важливе місце займають канали витоку інформації, до яких відносяться візуально-оптичні, акустичні та акустичної обробки, електромагнітні (в тому числі магнітні та електричні), матеріально-речові (магнітні носії, папір, фотографії і т. д.).

Візуальні оптичні канали створюються як світлові шляхи від об'єкта інформації до приймача. Для цього потрібні енергетичні, часові та просторові умови і відповідні технічні засоби. Створенню таких каналів сприяють відповідні характеристики, такі як склад, поведінка та активність об'єкта інформації. Особлива цінність інформації, отриманої за допомогою таких каналів, полягає в тому, що вони є найбільш достовірними, ефективними і служать підтвердженням отриманої інформації.

Джерелами акустичних каналів є об'єкти і механізми, що викликають вібрації і коливання, такі як голосові зв'язки людини, мобільні телефони, системи звукопідсилення, гучномовці та пристрої звукозапису і відновлення звуку.

Звукові хвилі, вироблені людським голосом або іншими вібруючими звуками, поширюються в просторі і взаємодіють з відповідними перешкодами (дверима, вікнами, стінами, підлогою і різними пристроями), змінюючи тиск і перетворюючи його в вібрацію. При впливі на спеціальні пристрої (мікрофони)

звукові коливання створюють відповідні електромагнітні хвилі. Інформація, вироблена звуковими коливаннями, передається на певну відстань.

Утворюються акустичні канали:

- поширенням акустичних (механічних) коливань у вільному просторі (відкриті простори, приміщення з відкритими вікнами, квартири, двері, витік через вентиляційні канали);

- внаслідок впливу акустичних коливань на будівельні елементи та конструкції (стіни, стелі, підлоги, вікна, двері, системи вентиляції, водопроводи, системи опалення та кондиціонування);

Через особливості фізичних характеристик та особливостей використання технічних засобів, що застосовуються для забезпечення виробничої діяльності, електромагнітні канали є найнебезпечнішими та найпоширенішими для отримання інформації. Такі канали створюються завдяки наявності технічних засобів, що використовуються для генерування небезпечних джерел сигналів. Першим з таких джерел сигналу є процесор. Це пристрій, який перетворює зміни однієї фізичної величини у зміни іншої фізичної величини. В електронній термінології процесор визначається як пристрій, що перетворює неелектричну величину в електронний сигнал і навпаки. Хороше розуміння функції процесора дозволяє ідентифікувати неконтрольовані характеристики фізичного поля, яке формує електромагнітний канал витоку (передачі) інформації. Водночас, враховуючи ідентичність технічних і конструкторських рішень, електронних схем процесорів обробки інформації та забезпечення виробничої діяльності компаній і банків, всі вони потенційно можуть мати електромагнітні канали витоку (передачі) інформації. Тому в будь-якому випадку використання технічних засобів обробки та передачі інформації призводить до загрози її неконтрольованого витоку (передачі).

Матеріальні канали отримання інформації утворюють відходи виробництва (зіпсована продукція або її фрагменти, чернетки різних нотаток, записів, листів тощо), крадіжки, несанкціоноване ознайомлення, копії

документів тощо, фотографії, відеозаписи, зразки планів, результати апаратних і програмних досліджень.

Ще однією дуже небезпечною загрозою для сучасного бізнесу в ІТ-секторі є всім відомий кібертероризм. Кібер-тероризм особливо небезпечний тим, що загрожує інформаційним ресурсам компанії, а також її іміджу та суспільній репутації її діяльності. Експерти також вважають, що в останні роки кібератаки стали дуже різноманітними, включаючи кібершпигунство, хактивізм і кібервимагання. Багато з них пов'язані з бізнесом. Це нафтова промисловість, телекомунікації, авіація, суднобудування та розробники високих технологій. Найпоширенішою загрозою тут є поширення вірусів та різноманітних шкідливих програм, які не лише пошкоджують програмне забезпечення, а й перешкоджають його відновленню. Кібератакам зазвичай передують збір інформації про передбачувану ціль атаки. Слід зазначити, що кібератаки поширюються як на стаціонарні комп'ютери, так і на мобільні пристрої, підключені до комп'ютерних мереж: За даними 2013 року, Україна входить до трійки лідерів за кількістю інфікованих мобільних пристроїв. За ризиком зараження через Інтернет наша країна посідає 45,6 місце серед країн високого ризику (9% користувачів). Це означає, що ІТ-інфраструктура сучасних компаній є дуже вразливою і потребує ефективного захисту. Слід також звернути увагу на так звані офісні загрози бізнес-інформації, тобто інформації, що міститься в документах, а також інформації, яку зберігають і використовують офісні працівники в процесі своєї роботи. Якщо дати відповідь на питання, що таке офісна діяльність, то вона буде такою: це сукупність дій персоналу організації, організованих у часі та просторі, спрямованих на забезпечення управління діяльністю організації. Іншими словами, офісна діяльність є частиною процесу управління. І якщо існують певні загрози такій діяльності, то вони впливатимуть на процес управління, в даному випадку на діяльність організації. Оскільки управління значною мірою пов'язане з інформаційними технологіями, офісна діяльність спрямована на виконання різноманітних завдань, завдань, процедур та операцій, пов'язаних з

інформаційним забезпеченням процесу управління. Структура, методологія та зміст цієї підтримки називається технологією діловодства. Останні являють собою відповідні джерела інформації, які обробляються, інтерпретуються та використовуються для підтримки управлінської діяльності. Таким чином, можна побачити, що діловодство ґрунтується на роботі з інформацією організації, а робота в управлінській ланці визначає особливу важливість такої діяльності. Основними складовими офісної діяльності є знання офісних працівників та відповідна документація. За таких обставин зусилля підприємства, спрямовані на заволодіння інформацією організації або на підірив суспільної репутації діяльності організації, будуть сконцентровані на персоналі та документації.

Реалізація схеми отримання доступу до офісної інформації через працівника може становити реальну загрозу як для працівника, так і для бізнесу. Загрози тут можуть включати залучення таких працівників або третіх осіб, або залякування офісних працівників з метою отримання доступу до офісних інформаційних ресурсів. Спонування працівників до неправомірного використання або розголошення офісних технологій чи інформації. В останньому випадку підбурювання може відбуватися в самому офісі або в середовищі, де офісні працівники задовольняють власні потреби та інтереси. Незадоволеність умовами, що впливають на реалізацію цих потреб та інтересів, провокує поведінку, яка може становити загрозу для інформації в офісі. Працівник не обов'язково раніше був зловмисним або нелояльним до компанії чи банку. Такі риси можуть бути спровоковані атмосферою в офісі, стилем взаємовідносин і способом роботи; це явище є загрозою саме по собі і в кінцевому підсумку може становити серйозну загрозу для інформації, що знаходиться в офісі. Більше того, такі загрози зазвичай не мають матеріальної цінності, і люди не відчувають провини за те, що інформація була скомпрометована не з їхньої вини. Необхідно документувати діяльність організації, яка створює додаткові ризики для інформації.

Тут можуть бути присутніми наступні загрози для службової інформації

- Втрата або неналежне знищення документів
- ігнорування запитів співробітників офісу щодо створення, виконання, обліку, передачі та зберігання документів;
- маніпуляції з документами з обмеженим доступом у присутності осіб, які не мають до них доступу; несанкціонована передача таких документів стороннім особам;
- використання інформації з обмеженим доступом у неопублікованих документах, публікаціях та особистих записах;
- Внесення до документів з обмеженим доступом зайвої інформації;
- Копіювання офіційних, конфіденційних та секретних документів в обсязі, що перевищує необхідний для виконання службових обов'язків; - Копіювання документів під час спілкування (в тому числі засобів зв'язку);
- Переклад документів у повідомленнях (у тому числі засобами листування), цитування тексту документів у повідомленнях або пересилання електронною поштою.

2.2. Інструменти інформаційної війни

Інформаційна війна розглядає інформацію як окремий об'єкт, потенційну зброю та об'єкт інтересів. Її також можна вважати якісно новим видом війни. Інформаційна війна - це атака на інформаційну функцію, будь-якими засобами.

Причому характер деструктивного впливу на інформаційну сферу, тобто процеси отримання, обробки, зберігання і передачі інформації всіх видів, визначає три форми інформаційної війни:

- Вплив на формати повідомлень, механізми передачі, зберігання, обробки даних тощо
- Перешкоджання передачі повідомлень;
- Вплив на зміст повідомлень [15].

Національний інститут стратегічних досліджень США та деякі західні експерти і науковці виділяють сім елементів інформаційної війни:

1. стратегія і тактика нейтралізації інститутів управління противника (командна війна);
2. розвідувальна війна;
3. радіоелектронна боротьба;
4. психологічна війна;
5. комп'ютерна війна;
6. інтелектуальна власність в економічній сфері;
7. інформаційний тероризм [15].

Інформаційно-комп'ютерна революція відкриває широкі можливості впливу на людей та уряди, маніпулювання їхньою свідомістю та поведінкою, навіть на відстані. Враховуючи процес глобалізації комунікаційних мереж у світі, можна припустити, що такі інформаційні атаки триватимуть і надалі. Для того, щоб уникнути найбільш негативних наслідків цієї війни для всього людства, фахівцям різних професій необхідно серйозно поставитися до цього питання.

Піар часто визначають як маніпуляцію та обман споживачів. Наприклад. Так, стверджується, що "зв'язки з громадськістю, реклама, інформаційна війна..." як засіб вирішення конфліктів між домінуючими групами. Однак, порівнюючи поняття "паблік рілейшнз" та "інформаційна війна", можна розмежувати, по-перше, ситуацію, а по-друге, самі ці поняття.

Ототожнення зв'язків з громадськістю з "брудними" технологіями впливу на громадську думку, ймовірно, пов'язане з тим, що вони використовують дуже схожі засоби для досягнення своїх цілей. На це також може вплинути той факт, що деякі компанії недобросовісно використовують можливості зв'язків з громадськістю.

Однак не варто забувати, що цілі цих дисциплін різні. Діяльність фахівців зі зв'язків з громадськістю є інформативною, тоді як діяльність фахівців з інформаційної війни є агресивною та маніпулятивною.

Ще однією характеристикою є якість наданої інформації. Якщо зв'язки з громадськістю надають достовірну інформацію, то інформаційна війна широко використовує не лише приховування фактів, але й фальсифікацію.

Інформаційна війна та зв'язки з громадськістю схожі лише в досягненні своїх цілей, але самі цілі принципово відрізняються.

ЗМІ не обов'язково повинні бути ініціатором або інструментом зміни свідомості окремих осіб або соціальних груп. Вони можуть бути як інструментом руйнування, так і інструментом творення і прогресу. Їх позитивна чи негативна роль залежить від того, які соціальні сили і з якою метою їх використовують.

2.3. Несанкціоновані учасники та порушники

Аналіз динаміки інформаційного законодавства за останні роки показує, що основний інститут інформаційного законодавства сконцентрований у напрямку інформаційної безпеки. Це пов'язано із загостренням негативних наслідків інформаційних та пов'язаних з ними загроз національній безпеці в інформаційній сфері Російської Федерації. Тому чинне національне законодавство доповнюється низкою законів, які, за словами їх авторів, спрямовані на створення системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного переміщення інформації, створення розвиненого національного інформаційного простору та визначення інноваційного підходу до захисту інформаційного суверенітету.

Ці дії були негативно оцінені не лише засобами масової інформації, але й експертами в галузі права (практиками та науковцями) та інших сферах, пов'язаних із законодавчим забезпеченням в інформаційній сфері.

Аналізуючи відповідність Указу та рішення РНБО про заборону доступу інтернет-провайдерів до ресурсів/послуг користувачам Інтернету закону, Конституції та міжнародно-правовим зобов'язанням України, дотримання законності в процесі застосування санкцій та стан їх виконання, допустимість, законність та доцільність обмежувальних заходів та їх вплив на реалізацію

конституційних прав і свобод людини, автор доходить висновку, що вони не відповідають критеріям законності і це є обґрунтованим.

Так, санкції, передбачені Указом Президента України "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)", які забороняють інтернет-провайдерам надавати інтернет-користувачам доступ до ресурсів/сервісів, не тільки не відповідають критеріям законності в частині обмеження свободи інформації, але й не відповідають технічним можливостям.

Наприклад, доступ до популярних сервісів російської компанії "Яндекс" було відновлено через два дні після технічних заходів, вжитих місцевим провайдером, але не тому, що оператор припинив блокування. Причиною стала організація низки блокувальних заходів у вигляді технічних операцій та контрзаходів, тобто додатки "Яндекса" були перенесені в іншу хмару і тепер живуть там (перехід зі статичних на динамічні IP-адреси). Єдиний спосіб розібратися з цією ситуацією і виконати вимоги Закону - постійно моніторити ситуацію, що технічно неможливо. Але динамічні адреси принаймні можна часто змінювати. Експерти Інтернет Асоціації (IAU) зазначають, що вже через рік всі IP-адреси в Європі будуть заблоковані. Відключати інтернет від країн стане простіше. У всьому світі йде таке полювання на тих, хто прийшов захопити цей бізнес, і на тих, хто безсистемно намагається його впорядкувати. І хоча закрити його системно на 100% неможливо, потрібно купувати дороге обладнання, щоб зробити його більш-менш ефективним" [3].

Те саме стосується і соціальних мереж, таких як "ВКонтакте" та "Однокласники" [4].

Слід зазначити, що блокування інформаційних ресурсів (серверів та веб-сайтів) в Україні легалізовано за рішенням суду відповідно до Кодексу про інтелектуальну власність лише у випадках порушення авторських прав, що не є поширеним явищем.

Однак слід визнати, що багато провайдерів виконують (або принаймні намагаються виконувати) рішення РНБО в таких випадках, щоб уникнути

незручних ситуацій. Однак для того, щоб дійсно заборонити доступ до іноземних сайтів, необхідно масово закупити обладнання для моніторингу трафіку. Інакше доступ через проксі-сервери стане звичним явищем. Ситуація простіша для звичайних користувачів Інтернету, які не підпадають під санкції закону і не потребують нагляду, поки не вчинять ІТ-правопорушення. Існує низка технологій або спеціалізованих сервісів, які дозволяють користувачам підключатися до інших веб-сайтів, які в іншому випадку можуть бути заборонені або заблоковані. Це означає, що користувачі можуть бачити потрібні їм веб-сайти через веб-сайти-посередники, а не безпосередньо. Звичайно, такі ресурси можна приховати, але це перетворює їх на неадекватні засоби "кібервійни".

Наприклад, одним з найпопулярніших плагінів для більшості браузерів є плагін Hola або Zenmate. Цей плагін є безкоштовним і дозволяє вибрати російську IP-адресу замість української, що дає змогу отримати доступ до будь-якого російського веб-сайту. Програма Tor, анонімна віртуальна мережа, гарантує не тільки повну анонімність, але й доступ до авторизованих ресурсів; браузер Opera має вбудований "турборежим", який дозволяє отримати доступ до "заборонених" сайтів. Одним з найпростіших рішень є використання Google Translate. Додайте потрібний сайт до запиту на переклад тексту, і сторінка, яку ви шукаєте, відкриється, але вона пройде через сервер у США.

Однак, незважаючи на різноманітні петиції свідомих спільнот та технічні можливості, кількість користувачів соціальних мереж та глядачів "ворожих" телеканалів не буде обмежена рішенням Ради національної безпеки і оборони України чи особистим прикладом Президента країни, слід визнати, що це пов'язано з приватними рішеннями користувачів, які в державі, що прагне до демократії, є свідомими громадянами з певною правовою та інформаційною культурою [7].

РОЗДІЛ 3. Удосконалення систем безпеки в інформаційному просторі

3.1. Протидія інформаційній війні

Розглядаючи питання інформаційної безпеки, можна класифікувати інформаційно-технологічні загрози суспільству і державі, що виникають у зв'язку з науково-технічним прогресом, на чотири групи. Перша група пов'язана зі стрімким розвитком нових видів інформаційної зброї, здатних ефективно впливати на психіку людини та інформаційно-технологічні структури держави. Аналізуючи існуючі дослідження в цій сфері, можна говорити про ефективні результати програмування, спрямованого на вплив на поведінку окремих осіб, комп'ютерні системи інформаційних банків та інформаційні ресурси. Друга група прогнозує появу нових видів соціальних злочинів на основі результатів новітнього інформаційно-технічного забезпечення. Шахрайство в банківській сфері, хуліганство в комп'ютерній сфері, піратство технологічних рішень і т.д. На думку провідних дослідників у цій галузі, комп'ютерні технології стають важливим інструментом злочинності. Третя група - електронний контроль за життям, настроями і планами громадян і політичних організацій, повний комп'ютерний контроль суспільства з боку держави. Інформаційні технології дозволяють накопичувати, зберігати і використовувати великі обсяги інформації про здоров'я громадян, їхню соціальну активність, політичні настрої, людські стосунки та економічну безпеку. Четверта група - використання інструментів інформаційних технологій у політичній боротьбі. Зростання впливу засобів масової інформації на політичні процеси та функціонування владних структур є однією з основних тенденцій розвитку сучасних суспільств. Розвиток науково-практичних основ інформаційної безпеки, розробка стратегій забезпечення національної інформаційної безпеки, глобалізація інформаційного феномену, створення глобально значущих інформаційних мереж, обґрунтування державної політики в контексті прагнення окремих країн до оптимального освоєння та використання

глобального інформаційного простору, науково-практичне підґрунтя для формування та реалізації національної політики в таких сферах, як інформаційна безпека та обґрунтування пріоритетів національної безпеки (в тому числі в сфері електронної реєстрації та е-реєстрації). Однією з головних передумов забезпечення національної безпеки є наявність економічного потенціалу держави, тобто матеріальних і розумових здібностей її громадян, а також здатність держави використовувати цей потенціал для забезпечення національної безпеки. При цьому інформація охоплює всі сфери життєдіяльності людини, підвищує рівень економічного потенціалу держави, сприяє зростанню її матеріального і духовного суспільного потенціалу, створює передумови для координації та мобілізації. Крім того, знання формують матеріальні та інтелектуальні ресурси країни для забезпечення ефективної оборони від агресивної держави. З огляду на вищезазначене, очевидно, що державна політика у сфері інформаційних ресурсів та інформації має бути спрямована на створення умов для ефективного та якісного інформаційного забезпечення вирішення завдань соціально-економічного розвитку країни. Основними напрямками державної політики в інформаційній сфері є: створення умов для розвитку і захисту всіх форм власності на інформаційні ресурси; створення і захист національних інформаційних ресурсів; створення і розвиток федеральних і регіональних інформаційних систем і мереж, забезпечення їх сумісності та взаємодії в єдиному інформаційному просторі; створення умов для якісного та ефективного інформаційного забезпечення громадян, органів державної влади, організацій і державних установ на основі національних інформаційних ресурсів. Існують різні способи несанкціонованого доступу до інформації. Захист інформації від несанкціонованого доступу - це діяльність, спрямована на запобігання отриманню зацікавленими особами захищеної інформації з порушенням правових документів або прав доступу до захищеної інформації чи правил, встановлених власником інформації. Під системою захисту інформації прийнято розуміти сукупність суб'єктів і виконавців, технологій захисту інформації та об'єктів захисту, організованих і

функціонуючих згідно з правилами, встановленими відповідними документами законодавства, організаційними та нормативними актами з питань захисту інформації. Вітчизняні дослідники Бондаренко В.О. та Литвиненко О.В. виділяють такі напрями в загальній системі захисту інформації Нормативно-правове забезпечення: формування відповідних нормативно-правових актів, нагляд за виконанням законів правоохоронними органами, судовий захист; Організаційно-технічне забезпечення: визначення системи заходів щодо запобігання реалізації загроз безпеці інформаційних ресурсів; Страхування інформаційних ризиків: приймається тільки неурядовими організаціями. Якщо людина обізнана і має критичне мислення, інформаційні маніпуляції на неї не впливають. Тому, якщо людина бачить явну інформаційну маніпуляцію, вона вже не піддається на неї. Тепер проаналізуємо, як свідомою людиною обробляється інформація.

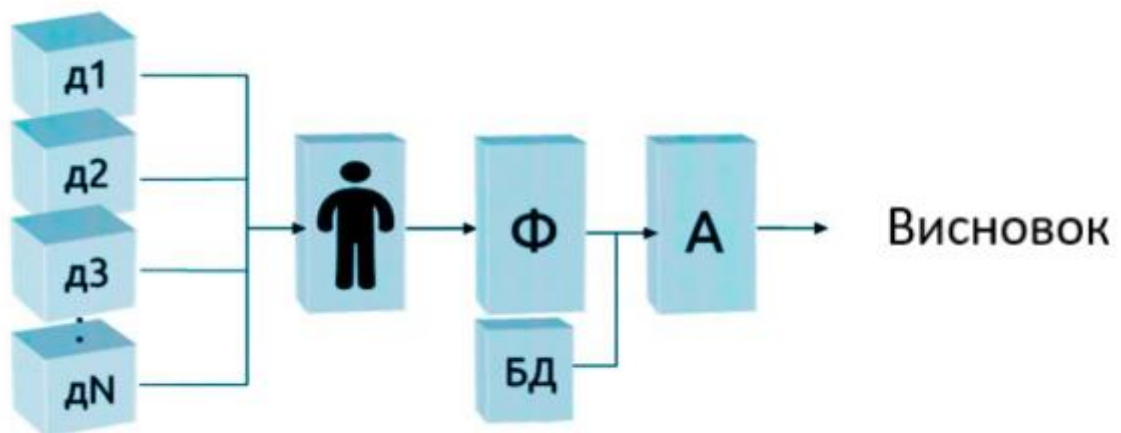


Рис. 3.1. Процес обробки інформації свідомою людиною.

де d_1, d_2, d_3, d_4 – джерела інформації;

ϕ – фільтр (оцінка достовірності інформації);

A – аналізатор інформації (аналіз вироблення висновків);

БД – база даних (знання, якими володіє людина).

Процес, описаний на Рис. 3.1. ідеалізовано. Через низку властивих інформаційній війні дій: руйнування світогляду (філософії, методології); порушення хронології (історії, хронології всіх галузей і знань) і т. д.

Одним з головних викликів є протидія цим факторам. Якщо суспільство не намагається усунути ці фактори, то процес обробки інформації стає лише узагальненням отриманої інформації. Одразу слід зазначити, що жоден захід захисту не може гарантувати адекватну безпеку. Надійний захист можливий лише за наявності комплексних механізмів безпеки. В принципі, такі комплексні заходи мають три основні складові: нормативно-правові засоби, технічні засоби та організаційні засоби. Нормативно-правові засоби захисту визначаються національними законодавчими актами, які встановлюють правила використання, обробки та передачі інформаційних даних з обмеженим доступом та визначають міру відповідальності за їх порушення. Стаття 34 Конституції України передбачає право громадян України на отримання та обробку інформації. Ця та інші статті Конституції мають слугувати основою для розвитку законодавства в інформаційній сфері. Невідповідність чинного законодавства України вимогам інформаційного прогресу є однією з основних проблем захисту інформації і може мати особливо серйозні наслідки, враховуючи наявні в державі потужні науково-технічні ресурси.

Усі технічні засоби можна поділити на фізичні засоби, до яких належать електричне, механічне, електромеханічне та електронне обладнання, а також апаратні та програмні засоби. Фізичним засобам притаманна форма автономних пристроїв і систем, які виконують загальну функцію захисту об'єктів, що обробляють інформацію. Апаратні засоби представлені комп'ютерами, телекомунікаційним обладнанням або пристроями, які взаємодіють з таким обладнанням через стандартизовані інтерфейси. Програмні засоби відповідають поняттю програмного забезпечення, що виконує функції захисту інформаційних даних. Організаційні засоби захисту поділяються на засоби організаційно-технічного характеру, які використовуються при створенні та функціонуванні будь-якої структури, та засоби організаційно-правового характеру. Іншими словами, ефективне управління широким використанням сучасних засобів інформаційних технологій можливе лише на основі

нормативно-правової бази та наявності апаратно-програмного забезпечення. Ці питання часто недооцінюються керівниками різних організацій.

Розвиток нормативно-правової бази інформаційної безпеки вимагає визначення пріоритетності розробки нормативно-правових актів та механізмів практичної реалізації існуючого законодавства. Підготовка переліку нормативно-правових та організаційно-методичних документів включає підготовку документів, що регулюють: роботу державних органів у сфері інформаційної безпеки; відносини між суб'єктами інформаційної діяльності щодо забезпечення інформаційної безпеки; регулювання державними органами процесів роботи та розвитку, що здійснюються на ринку засобів масової інформації, розвитку інформаційних продуктів та послуг; інформаційні відносини на суспільному та державному рівні з урахуванням ринкової економіки. Правовий статус суб'єктів забезпечення інформаційної безпеки вимагає гарантування їх статусу користувачам інформації та телекомунікацій, визначення їх відповідальності за гарантування правових норм і правозастосовних процедур щодо суб'єктів забезпечення інформаційної безпеки, які вчиняють правопорушення, пов'язані з обробкою конфіденційних даних та використанням незахищених носіїв інформації; склад правопорушення повинен встановлюватися з урахуванням видів кримінальних, цивільних, адміністративних, дисциплінарних та кримінально-процесуальних правопорушень, до яких необхідно готуватись.

3.2. Засоби посилення безпеки інформаційного простору в умовах інформаційної війни

Удосконалення організації форм і методів запобігання та усунення загроз інформаційній безпеці, розробка нормативно-правової бази підтримки системи інформаційної безпеки, розмежування повноважень органів державної влади, які повинні забезпечувати інформаційну безпеку, розробка системи моніторингу для аналізу стану інформаційної безпеки відповідної держави,

розробка інформаційної системи та розробка ідей, які створять позитивні чинники для подолання критичного стану промислової сфери України в галузі захисту інформації. Розробка сучасних методів забезпечення інформаційної безпеки, розробка форм і засобів, що сприяють цивілізаційному впливу держави на формування колективної свідомості суспільства та розробка практичних рекомендацій у практичному застосуванні, розробка методик комплексного дослідження роботи працівників інформаційних систем та мотивації тих, хто обробляє конфіденційні та секретні дані на рівні засобів, розробка методик та розробка практичних рекомендацій щодо підвищення морально-психологічної стійкості та соціального захисту фінансовій сфері, розробка методик та практичних рекомендацій щодо регулювання експорту вітчизняного високотехнологічного обладнання, створення напрямів протидії засобам, що розглядаються як інформаційна зброя, а також удосконалення управління персоналом в системі захисту інформаційного простору. Розглянемо модель двостороннього врегулювання конфліктів (модель Річардсона).

В основі моделі покладено:

- У процесі інформаційного втручання кожна з країн прагне забезпечити зростання ефективності своєї інформаційної зброї, так, щоб вона дорівнювала рівню суперника;
- Держави збільшують рівень інформаційних сил, керуючись власними прагненнями.

Приведемо позначення $N(t)$ рівні інформаційні потужності кожної з країн конфлікту, де t – час. Тепер, наші умови дії моделі можуть бути спроектовані у вигляді системи двох диференціальних рівнянь:

$$\begin{aligned} N_1 &= M_1(L_1 - N_1)[1 - \exp(-p_1(k_1N_2 - a_1N_1 + g_1))] \\ N_2 &= M_2(L_2 - N_2)[1 - \exp(-p_2(k_2N_1 - a_2N_2 + g_2))] \end{aligned} \quad (3.1)$$

де N_1, N_2 - інформаційні потужності кожної з сторін конфлікту;

k_1, k_2 – коефіцієнти реакції на інформаційні атаки;

a_1, a_2 – показники витрат на генерації інформаційної зброї;
 g_1, g_2 – коефіцієнти агресивності, якщо вони позитивні;
 M_1, M_2 – вартість наявного інформаційного забезпечення;
 L_1, L_2 – граничні значення рівнів інформаційних потужностей;
 p_1, p_2 – коефіцієнти ступеня важливості інформаційних витрат.

Модель допускає існування особливих розв'язків, що визначають координати положень рівноваги :

$$\begin{array}{ll}
 \text{а) } N_1^p = N_1^*; N_2^p = N_2^* & \text{б) } N_1^p = N_1^*; N_2^p = L_2 \\
 \text{в) } N_1^p = L_1; N_2^p = N_2^* & \text{г) } N_1^p = N_2^*; N_2^p = L_2
 \end{array} \quad (3.2)$$

де N_1^*, N_2^* - рішення системи лінійних алгебраїчних рівнянь.

Нехай функції $u_1 = r_1^0 (x_1 - x_2)$ і $u_2 = r_2^0 (x_2 - x_1)$ характеризують політику кожної країни в сфері інформаційного протистояння, де змінні $x_1 = N_1 - N_1^*$; $x_2 = N_2 - N_2^*$ мають значення відхилень від рівноважних рівнів

інформаційної потужності. Тут r_1^0, r_2^0 – стаціонарні параметри управління. З врахуванням вигляду функції u_1, u_2 система має вигляд :

$$\begin{array}{l}
 x_1 = M_1(\delta_1 - x_1)[1 - \exp(p_1(a_1x_1 - k_1x_2))] + r_1^0(x_1 - x_2) \\
 x_2 = M_2(\delta_2 - x_2)[1 - \exp(p_2(a_2x_2 - k_2x_1))] + r_2^0(x_2 - x_1)
 \end{array} \quad (3.3)$$

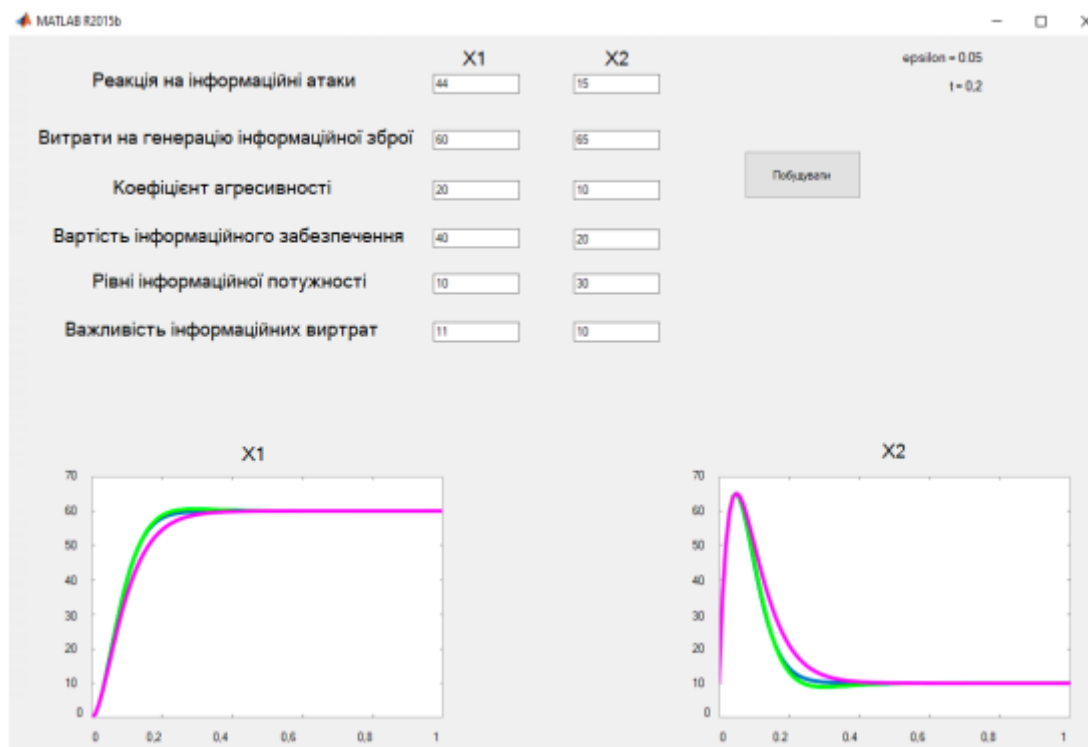


Рис. 3.2. Візуалізація моделі Річардсона

Як ми можемо бачити, сили та інформаційні потужності об'єкта X1 мають перевагу над супротивником X2.

З огляду на те, що один з головних пріоритетів політики української національної безпеки найближчих років – це захист інформаційної сфери, лід зауважити, що разом із тенденцією до втілення відомих раніше загроз інформаційній безпеці (фейки, спрямоване на суспільну свідомість маніпулювання за допомогою ЗМІ та соціальних медіа, залучання хакерів до вирішення політичних завдань, здійснення кібератак на критичну інфраструктуру та ін.), спецслужби іноземних країн намагаються «озброїтися» сучасними ІТ-рішеннями, щоб отримати переваги в межах міждержавного протистояння, вивчаючи методи, покликані здійснювати цілеспрямований інформаційний вплив на користувачів мобільних послуг, використовуючи їхні персональні дані та технології обробки Big Data на базі штучного інтелекту.

Більш широке обґрунтування проблемних питань, пов'язаних із застосуванням Big Data-технологій наведено у наукових працях зарубіжних дослідників:

- загрози «прайвесі», незаконна дискримінація (висунення підозр про здійснення терористичної діяльності, відмова у видачі кредитів тільки на підставі висновків Big Data-алгоритмів), створення бірж приватних даних (торгівля персональними даними без відома їх власників), компрометація особи, маніпулювання особистістю та суспільною думкою через рекламу, стратифікація суспільства за ознакою доступу до інтернету, що призводить до збільшення розриву між багатими та бідними [7, 16];

- проблеми забезпечення інформаційної безпеки в умовах поширення Big Data-технологій (використання хакерами Big Data-технологій у злочинних цілях, багатогранність проблем цілісності та конфіденційності через необхідність об'єднання та співставлення даних з різних джерел та платформ, отримання доступу до інформації з обмеженим доступом та раніше невідомої інформації шляхом аналізу зв'язків між елементами загальнодоступних даних) [14];

- загрози національній безпеці (отримання даних про об'єкти критичної інфраструктури, здобування критично важливої інформації шляхом аналізу публічних даних).

Важливо також зазначити, що якщо раніше компанії управляли майном, грошима та інтелектуальною власністю, то сьогодні з'явився новий актив - дані, які не тільки використовуються для прийняття бізнес-рішень і отримання додаткового прибутку, особливо в таргетованій рекламі, але й самі стали товаром. З розвитком обчислювальної техніки та технологій обробки великих обсягів даних роль джерел інформації перейшла до смартфонів, ноутбуків, соціальних мереж, онлайн-покупок, продуктових чеків, банкоматів та смарт-телевізорів, які надають детальну інформацію про думки та поведінку своїх власників. Щодня тисячі компонентів, з яких складається ця "інформаційна мозаїка", збираються в єдиному профілі користувача, у "віртуальній" скриньці, що містить взаємопов'язані бази даних, які використовуються третіми особами для отримання прибутку, а їхні власники про це не знають. Якщо раніше загроза порушення прав на приватність особи через використання технологій

Big Data оцінювалася лише в контексті дотримання морально-етичних норм, то сьогодні вона стала питанням національної безпеки, що засвідчили результати останніх президентських виборів у США. Наприклад, на слуханнях у Комітеті з питань розвідки Сенату США, присвячених ролі соціальних мереж у втручанні Росії у вибори 2016 року, було визнано, що Google, Facebook і Twitter стали інструментами маніпуляцій з боку російських спецслужб [14].

Водночас дані з соціальних мереж, які використовуються алгоритмами Big Data, не настільки точні, як дані з програм обміну повідомленнями в мобільних телефонах. Це пов'язано з тим, що люди часто говорять те, що думають, і мимоволі передають інформацію про свою реальну поведінку. Мобільні оператори, що працюють в Україні, розробили власні месенджери (наприклад, Veon від "Київстар"), які, як відомо, надають необмежений доступ до персональних даних українських користувачів [19].

Таким чином, динамічний розвиток технології Big Data дозволить спецслужбам інших країн отримати доступ до даних українських користувачів мобільного зв'язку та захопити нові гілки інформаційного впливу, які становлять цілком реальну загрозу національній безпеці. Якщо раніше для цього використовувалися засоби масової інформації та соціальні мережі, то сьогодні - високосоціальні послуги мобільного зв'язку. Десятиліття антидержавної політики у сфері телекомунікацій та зв'язку фактично усунули один з елементів суверенітету України, і країна залишається надзвичайно вразливою до нових викликів в інформаційній сфері. Персональні дані в соціальних мережах контролюються американськими компаніями, а мобільні дані належать операторам, підконтрольним російській владі. Про механізми протидії інформаційним загрозам національній безпеці можна говорити у множині, оскільки існує широкий спектр способів протидії інформаційним загрозам, а їх комбінації змінюються залежно від характеру загрози.

Залежно від місця розташування джерела загрози всі загрози національній безпеці, в тому числі й інформаційні, умовно поділяються на дві групи: зовнішні та внутрішні. Внутрішні загрози інформаційній безпеці

конкретного об'єкта - це загрози, "що виникають безпосередньо від об'єкта і викликають взаємодію між елементами та суб'єктами об'єкта", тоді як зовнішні загрози - це загрози, "що виникають внаслідок взаємодії із зовнішніми об'єктами" [9, с.18].

Слід зазначити, що Стратегія розрізняє прояви інформаційно-психологічної війни (п. 3.1), кібернетичну безпеку та загрози безпеці інформаційних ресурсів (п. 3.7) і загрози власне інформаційній безпеці (п. 3.6), що не є доцільним. Національна доктрина інформаційної безпеки та Стратегія кібербезпеки України визначають низку загроз національним інтересам і національній безпеці України в інформаційному просторі. Сучасний стан впливу на суспільну свідомість за допомогою інформаційних операцій необхідно враховувати при формуванні стратегій національної безпеки. Національні розвідки та контррозвідки використовують методи дезінформації та пропаганди в розвідувальних конфліктах з метою отримання секретної інформації або введення противника в оману через дезінформацію [1]. Сучасна інформаційна війна в основному спрямована на два типи цілей: по-перше, на технологічні засоби противника (комп'ютерні мережі та інше обладнання) і, по-друге, на людські ресурси. Атаки на інформаційні системи противника мають на меті вивести з ладу життєво важливі сектори держави, такі як енергетика, оборона та управління, тоді як другий тип атак спрямований на психологічну "обробку". Інформаційна агресія зазвичай будується в три етапи формування "ядра" (великої кількості людей, незадоволених статус-кво), формування середовища (альтернативного інформаційного простору) та формування атмосфери (зміна громадської думки за допомогою "точкових атак") [10, с. 51-52, 21]. Інформаційне насильство, що застосовується в інформаційних конфліктах, характеризується як завуальоване, приховане і не завжди розпізнаване. При цьому завданням держави в таких конфліктах є захист інформаційних систем, суспільної свідомості від дій противника та недопущення доступу противника до даних, які можуть підірвати обороноздатність держави. Сьогодні глобальна мережа Інтернет слугує

основною ареною протистояння різних сил і засобів, які потребують сучасного захисту національної безпеки від інформаційних загроз різного роду. Водночас, наявність інформаційної агресії, що поширюється в кіберпросторі, має значний вплив на діяльність усіх національних та міжнародних антитерористичних та контр-екстремістських організацій. Тому основною метою системи превентивних заходів, що реалізуються національними компетентними органами в інформаційному просторі, має бути підвищення стійкості колективної свідомості населення до деструктивного впливу ідей. Реалізація зовнішніх загроз призводить до пошуку слабких місць в інформаційній структурі з метою отримання доступу до ключових вузлів інформаційної інфраструктури, сховищ інформації, організаційних мереж, носіїв секретної інформації тощо. Інструментами реалізації зовнішніх інформаційних загроз є різноманітна "інформаційна зброя" (наприклад, віруси, хробаки, "троянські коні" та інші засоби зараження шкідливим програмним забезпеченням або впливу на інформацію).

У процесі глобалізації, що впливає на політичні, соціально-економічні та культурні відносини і має тенденцію до реорганізації сфер впливу на світовій арені, актуалізуються загрози інформаційній безпеці нашої країни. Ідентифікація та аналіз загроз може бути ускладнена низкою факторів: Суспільна думка про відсутність зовнішніх загроз для країни, невизначеність у воєнній доктрині та доктрині інформаційної безпеки щодо очевидних потенційних зовнішніх загроз для країни і, відповідно, порівняльної динаміки важливості та наростання загроз. Нечітка класифікація та ранжування загроз за такими факторами: недостатня обізнаність щодо причин та умов виникнення загроз.

Забезпечити безпеку при стрімких змінах внутрішнього і зовнішнього характеру можливо за умови, що наявний дієвий механізм, зокрема це механізм протистояння загрозам, що підтримує системну інваріантність. Механізму протидії інформаційним загрозам зовнішніх джерел може надаватися значення інтегрованої цілісної сукупності потрібних, достатньо дієвих і правових

складників, через які суб'єктом формується раціональна система впливу на загрози для інформаційної безпеки та ризики, що вони зумовили, сприяючи у такий спосіб ефективному виконанню завдань і функцій, що покладаються на систему забезпечення інформаційної безпеки та національної безпеки загалом. Механізмами протидії інформаційним загрозам зовнішніх джерел, як частиною загального механізму державної інформаційної безпеки та національної безпеки загалом, може передбачатися:

- збереження цілісної і захищеної інформаційної системи під час її роботи і розвитку;
- рівень безпеки, що розрізняє структурні складники системи, що можуть зіткнутися з потенційними реальними загрозами;
- сфери безпеки, що окреслюють здатність функціонувати й розвиватися для сфери інформації;
- характеристики безпеки, що визначають допустимі відхилення у потенціалі системи інформаційної безпеки, кількість її складників, їх якість, властивості, зв'язки;
- загрози, наслідки їх втілення й запобіжні механізми обумовлюють: внутрішні закономірності системи інформаційної безпеки й вплив на неї зовнішніх чинників, що ведуть до небажаних і незворотних відхилень в її відтворюванні й розвитку; зміни при втіленні загроз (таких, що піддаються компенсації або не піддаються; які є оборотними та необоротними; що впливають або не впливають на функціонування системи); організаційно оформлена сукупність стратегічних і тактичних дій, що забезпечують роботу системи інформаційної безпеки та її змогу само відтворюватися.

Найбільш небезпечними для національної безпеки нашої держави зараз є інформаційні загрози зовнішніх джерел, такі як:

- несанкціонований доступ до інформаційних даних і вплив на інформаційні ресурси, інформаційну інфраструктуру владної виконавчої системи, що реалізує засади зовнішньої та внутрішньої політики держави,

представників України та об'єднань на міжнародній арені та у межах міжнародних організацій.

- недостатність поінформованості населення за кордоном (насамперед, у сусідніх з Україною державах) про ведення зовнішньополітичної та внутрішньополітичної діяльності країни;

- розповсюдження неправдивої інформації про ведення зовнішньої та внутрішньої політики України;

- інформаційний вплив, що чинять іноземні політичні, економічні, військові і інформаційні структури на розроблення і втілення засад зовнішнього та внутрішнього характеру політичного сегменту нашої держави;

- утиски свобод, що зазнають українські громадяни і юридичні особи в інформаційній сфері поза межами держави.

Механізми протидії зовнішнім розвідувальним загрозам визначили нагальну потребу в організації багаторівневих і різнопланових заходів, які враховують, насамперед, специфіку зовнішніх чинників (склад геополітичної та територіальної ситуації, структурно-функціональну роль держави та вплив транснаціональних організованих злочинних угруповань). Тому особлива увага приділяється моніторингу та подальшому прогнозуванню характеру, специфіки та масштабів загрози. Прогнозування є важливим і самостійним елементом превентивних заходів протидії зовнішнім інформаційним загрозам та забезпечення національної безпеки. Основним методом прогнозування є моделювання, основними принципами якого є визначення цілей моделі; виділення обмеженої кількості ключових факторів суттєвих змін у досліджуваній системі; визначення характеру взаємозв'язків між цими факторами; визначення принципу множинності взаємозв'язків між факторами та визначення характеру розвитку і змін у системі виявлення основних взаємозв'язків, що визначають характер розвитку і змін системи. Середовище із зовнішніми джерелами, здатними створювати та відтворювати загрози індивідуальній, суспільній та національній інформаційній безпеці, потребує моніторингу, прогнозування та превентивної протидії загрозам. Слід

враховувати, що традиційні методи та механізми протидії зовнішнім загрозам національній безпеці застарівають і з'являються нові методи, які сприяють поширенню загроз та мінімізації ризиків, що виникають від них. Це пов'язано зі стрімким розвитком інформаційно орієнтованого українського суспільства, що сприяло розвитку методів ведення інформаційних війн. Виділяють такі групи методів протидії інформаційним загрозам зовнішніх джерел, як:

- група профілактичних, або превентивних методів, що мають не допустити відповідні загрози та їх розвиток чи запобігти подальшим ризиками на початкових етапах;

- група оперативних методів, що застосовуються з метою відповісти на агресію, що транслюють зовнішні джерела інформаційних загроз та пов'язуються з їхнім розвитком та втіленням.

Превентивна протидія інформаційним загрозам зовнішніх джерел, передбачає виділення чотирьох основних груп заходів: нормативно-правових, адміністративних, інформаційних та економічних. Оперативна протидія повинна здійснюватися тільки після виявлення достовірної інформації щодо структур, груп або осіб, що є рушійними силами, оцінки ступеня загрози і наявних ресурсів для її нейтралізації. Зокрема, механізм протидії інформаційним загрозам зовнішніх джерел, розгортання яких відбувається у ході гібридної війни, має включати: постійний контроль інформаційного простору (преса, телебачення, радіо, Інтернет); обмеження розмірів простору, об'єктів інформаційної інфраструктури та соціальних груп, що піддаються ураженню інформаційною дією; посилення авторитету своєї влади та уряду, армії серед населення країни, аби перешкодити переходу на бік ворога та підтримці дій, які він нав'язує; ефективна інформаційна політика: стратегічна спрямованість та зворотний зв'язок із суспільством. Крім цього, можуть виокремлюватися механізми політичного, економічного характеру та інші механізми протистояння небезпекам. В тому числі, зважаючи на суть політичних цілей, пов'язаних з політичною метою та єдиною стратегічною

ціллю забезпечити національну безпеку України, можна здійснити виділення деяких політичних механізмів протистояння інформаційним небезпекам:

- механізми розробки й прийняття рішень Радою безпеки ООН, спів дія у межах ОБСЄ, механізми по зміцненню та розвитку у межах інших угруповань міждержавного характеру, що є інструментом, яким послуговується держава щоб забезпечити політичну, економічну і військову євроінтеграцію України;

- механізми, які забезпечує державне і військове управління, політичні партії, адміністративно-правові режими та ін., механізми, що мають тісний зв'язок із керуванням внутрішньополітичною ситуацією та здійснюють прямий вплив на інформаційну безпеку держави;

- механізми, що спрямовані на те, щоб просунути державні інтереси у міжнародній інформаційній сфері, пов'язані з інформаційним забезпеченням, якого потребує державна політика України, що полягає у інформуванні вітчизняного та іноземного населення про ведення державної політики, прогрес інформаційних технологічних засобів, захист інформаційних ресурсів та ін.;

- механізми протидії небезпекам, яким піддається політична, економічна безпека країни та ін.

Зрозуміло, що механізми протидії інформаційним загрозам будуть еволюціонувати, оскільки конкретні механізми створюються одразу після ідентифікації існуючих загроз та розробки стратегічних завдань щодо їх усунення. Слід також зазначити, що сучасні умови вимагають поділу інформаційних загроз на внутрішні та зовнішні. Комплексність інформаційних загроз означає, що атаки на зовнішні системи безпеки держави можуть призвести до загроз внутрішній безпеці, що, в свою чергу, може спричинити внутрішню нестабільність і, зрештою, зовнішню вразливість держави.

Слід також враховувати, що вичерпний перелік загроз, особливо зовнішніх, не може гарантувати їх абсолютної відсутності не тільки тому, що вони знаходяться поза межами системи безпеки, але й тому, що вони змінюються разом зі зміною зовнішнього середовища. Тому акцент у сучасному світі зміщується від загроз до ризиків. Такий підхід дозволяє відійти

від сприйняття загроз як незмінних і застосовувати різні підходи для запобігання розвитку загроз, особливо в умовах високої невизначеності. Отже, механізми протидії зовнішнім інформаційним загрозам ґрунтуються на принципах ризик-менеджменту і включають процеси прийняття та реалізації управлінських рішень, спрямованих на зниження ймовірності настання негативних наслідків та мінімізацію шкоди, яка може бути завдана в результаті реалізації загрози. перспективним та ефективним. Цей механізм впливає насамперед на керовані елементи (ризики), дозволяє досягти значних результатів щодо забезпечення прийнятних умов при відносно невеликих зусиллях, а також забезпечує успішне поєднання превентивних та оперативних методів протидії інформаційним загрозам. Механізми протидії інформаційним загрозам включають в себе різні форми роботи, що здійснюються державними та військовими органами, неурядовими організаціями, політичними організаціями тощо, а також їх різноманітні форми роботи та види взаємодії між ними, а також їх оперативний вплив на загрози інформаційній безпеці та управління ними з метою локалізації та нейтралізації ризиків, що створюються загрозою, у формуванні реальних і потенційних загроз та ймовірності їх виникнення, орієнтуючись на систему, враховуючи цикл її розвитку (процеси зародження, становлення, дозрівання і трансформації) та її конкретний стан (процеси кризи, стагнації та відновлення), наявні фінансові, матеріальні та людські ресурси держави, суспільні інтереси та баланс між колективним та індивідуальним. Оцінка механізмів базується на інформаційній політиці держави, впливі на характеристики безпеки, виявленні відхилень характеристик для стабільного функціонування систем інформаційної безпеки та виявленні зовнішніх умов, що сприяють відхиленням, наприклад, збільшенню (у несприятливому зовнішньому економічному середовищі) або зменшенню (у сприятливому зовнішньому середовищі) небезпек. Отже, механізми протидії інформаційним загрозам, що базуються насамперед на принципах управління ризиками, дають змогу зупинити деструктивні елементи, характеристики та процеси, які руйнують систему інформаційної безпеки та національну безпеку в

цілому, і стимулювати конструктивні елементи, характеристики та процеси, які покращують її функціонування та розвиток, тому ці механізми є також важливими для розвитку системи інформаційної безпеки та національної безпеки в цілому. З усього цього можна зробити висновок, що належний рівень інформаційної безпеки може бути забезпечений, серед іншого, політичними, економічними та організаційними заходами, що гарантують реалізацію інформаційних прав та інтересів держави та її суб'єктів. Розглядаючи питання національної інформаційної безпеки, можна сказати, що в основі забезпечення інформаційної безпеки лежить національна інформаційна організація. Ця організація повинна гарантувати інформаційну безпеку держави та її громадян в умовах зростаючих загроз, таких як процес глобалізації та міжнародний тероризм. На жаль, існує низка факторів, що перешкоджають створенню такої інформаційної організації в Україні, зокрема, відсутність координації роботи державних органів у сфері забезпечення інформаційної безпеки.

3.3. Інструменти виявлення втручання в інформаційному полі

Інструменти виявлення втручання можна знайти на інформаційному та соціальному рівнях. Розглянемо інформаційні. Моніторинг ЗМІ - найшвидший і найдешевший спосіб аналізу громадської думки та відстеження зворотного зв'язку в процесі комунікації. Матеріали ЗМІ можуть регулярно аналізуватися спеціалізованими структурними підрозділами або сторонніми експертами для виявлення певних тенденцій у минулому та майбутньому. У такий спосіб можна спрогнозувати майбутні наслідки певних поточних дій або виявити причинно-наслідкові зв'язки, що призводять до певних ситуацій чи явищ, які відбуваються зараз.

Робота в цій сфері зазвичай розглядається як первинний аналіз, який дозволяє зрозуміти певний процес і виявити конкретні загрози або позитивні тенденції. Моніторингова копія - складається з ксерокопій друкованих матеріалів, роздрукованих фрагментів новинних стрічок, матеріалів з інтернет-

видань, теле- та радіопередач. Кожна друкована копія містить посилання на видання, з якого взято матеріал, дату, номер, сторінку або інтернет-адресу матеріалу. Контент-аналіз матеріалів ЗМІ. На основі матеріалів моніторингу щонайменше раз на тиждень та щонайменше раз на місяць проводиться контент-аналіз зібраного матеріалу з метою переведення якісних показників та характеристик у кількісні.

Інструменти експрес-досліджень у соціальних мережах Соціальні мережі можна використовувати для проведення типових соціологічних досліджень, зокрема опитувань громадської думки. Порівняно з класичними соціологічними дослідженнями, результати опитувань у соціальних мережах мають велику статистичну похибку. Це пов'язано з нестабільністю поля (опитування іноді видаляють або не дозволяють публікувати в групах, вибірка по групах не завжди є репрезентативною тощо), але отримані результати чітко відображають загальні тенденції, чи то в регіональному контексті, чи то в контексті конкретної цільової групи. Для дослідження думок представників цільових груп можна використовувати власні сервіси основних соціальних мереж та інтернет-сервісів. У більшості фірмових сервісів опитувальник встановлюється в шаблонному блоці для створення постів.

Механізм створення опитування простий і генерується автоматично. Єдине, що потрібно задати розробнику - це тему і основні питання з декількома варіантами відповідей.

При оформленні блоку опитування рекомендується додавати візуальну підтримку, наприклад, зображення або відео, щоб допомогти людям швидше зрозуміти суть опитування і привернути увагу до опитування. У соціальних мережах доступні відповідні сервіси/додатки, які полегшують завдання підготовки та проведення опитувань:

- Facebook - My Polls, Polls, Acepolls;
- Twitter - Acepolls;
- SMM-аудит.

Сучасний стан розвитку технологій соціальних мереж вимагає постійного вдосконалення способів моніторингу та оцінки ефективності соціальних комунікацій. Це означає, що автору інформативного повідомлення недостатньо отримати лише "лайки", а крім коментарів необхідно розуміти загальні тенденції вподобань цільової групи та прогнозувати їх подальший розвиток. Вирішити цю проблему можна шляхом комплексного застосування якісних і кількісних характеристик за допомогою спеціальної інтегрованої методології, тобто використання окремих інструментів моніторингу, контент-аналізу та систематизації конкретних даних. Це і є методологія аудиту СРА. Ця методологія базується на механізмах контент-моніторингу та контент-аналізу. Водночас схема виконання завдань в рамках цієї методології є гнучкою. Матеріал для перевірки може бути зібраний автоматично (через відповідні онлайн-сервіси) або вручну шляхом безпосереднього збору та сегментації контенту. Метою SMM-аудиту є перевірка ефективності поширення інформації про досліджувану структуру в певній сфері Інтернету. Основними завданнями аудиту є комплексне поглиблене дослідження та розробка базових інструментів і методик системного моніторингу інформаційної діяльності досліджуваної структури в мережі Інтернет; створення цільової бази даних щодо поширення інформації про діяльність досліджуваної структури в мережі Інтернет; проведення комплексного дослідження ефективності інформаційної політики об'єкта дослідження в мережі Інтернет протягом визначеного періоду (не менше шести місяців). Методологічною основою дослідження є методика інформаційної діагностики ефективності процесу просування діяльності організації в Інтернеті. Методологія дослідження Комплексне моніторингове дослідження проводилося на основі спеціальної бази даних, що репрезентує досліджувану цільову групу в мережі Інтернет. Процедура проводилася у форматі триетапного моніторингового анкетування. Загальна процедура включала підготовчий етап і чотири послідовні робочі фази. Підготовчий етап передбачав створення бази даних релевантних веб-ресурсів в Інтернеті, що відповідають цільовій групі об'єктів. Сюди увійшли: соціальні мережі, де

публікуються матеріали та згадки про діяльність організації. Засоби масової інформації, зокрема газети, журнали, інтернет-видання, сайти телеканалів та радіостанцій. Веб-сайти професійних організацій у досліджуваному секторі. Інформаційно-довідкові портали, присвячені відповідній діяльності та суміжній тематиці. Веб-портали центральних, регіональних та муніципальних органів влади. Корпоративні сайти неурядових організацій, що працюють у сфері діяльності досліджуваної тематики, а також резюме проектів міжнародних програм. Веб-сайти політичних організацій та громадських рухів, які мають певний вплив на загальну суспільно-політичну ситуацію в країні. Персональні веб-сторінки публічних осіб (політиків, громадських діячів, чиновників), які прямо чи опосередковано пов'язані зі сферою діяльності суб'єкта. В умовах сучасної інформаційної війни одним з головних завдань при роботі з контентом є його ідентифікація та визначення джерела текстової інформації, відео та графіки. Як показує практика, одного лише автентичного матеріалу не завжди достатньо при підтримці високої щільності інформаційних потоків. Тому при створенні контенту зломисники можуть використовувати чужі відео-, графічні або текстові матеріали. У цьому контексті особливої уваги заслуговує інформаційний наступ Росії проти України у 2014-2015 роках. Російські ЗМІ неодноразово виявляли та викривали фальсифікації, зокрема, щодо великої кількості жертв серед цивільного населення внаслідок обстрілів та подій за конкретних обставин. Технічно виявити фальсифікацію не складно. Для цього можна скористатися певним сервісом пошукової системи, наприклад, Google або Yandex, або іншим програмним продуктом. Найпопулярнішою пошуковою системою на сьогодні є Google, за допомогою якої можна перевірити контент наступними способами. Перевірити автентичність тексту можна наступним чином [3]: ввести пошуковий запит (цитату, ключові слова) в лапках "." і задати пошук - програма буде шукати сторінки, що містять слова в зазначеному форматі, без зайвої інформації або реклами. Якщо в уривку пропущено одне або кілька слів, слід взяти весь уривок в лапки і замінити пропущену частину зірочкою "*" - програма шукатиме повну версію.

Якщо вам потрібно шукати контент у певному місці, ви можете використовувати такі символи:

inurl - для пошуку всередині URL-адреси;

intitle - всередині заголовка;

intext - всередині тексту;

inanchor - всередині тексту анкера.

Якщо ви хочете дізнатися, хто посилався на певний фрагмент інформації, вам слід використовувати оператор anchor. Останній ставиться через двокрапку перед URL-адресою, за якою здійснюється пошук.⁵ Якщо потрібний вам контент неможливо знайти безпосередньо за адресою, слід шукати його в кеші. У цьому випадку <http://cachedview.com>. Google завжди зберігає інформацію про сайт і його вміст у певний момент часу. Пошук та ідентифікація фотографій передбачає дещо складну процедуру, але відмова від цього виду шахрайства має найбільший вплив і сприяє і робить найбільший внесок у процес контрпропаганди. Прикладом може слугувати робота Джулії Девіс з американського сайту Examiner.com, яка розвінчувала кремлівські фальсифікації на основі чужих фотографій. Використовувалися типові ілюстрації "подій на Донбасі", зокрема фото з Боснії, Китаю, Саудівської Аравії, Африки, самої Росії, а іноді навіть з фільмів.

ВИСНОВОК

Отже, відповідно до поставленої мети вирішені такі завдання:

1. Проведено аналіз технологій, методів втручання в інформаційний простір й основних елементів організації безпеки інформаційного простору та визначити вимоги до механізмів захисту інформаційного простору;
2. Розроблено математичну модель аналізу сил конфліктуючих сторін в рамках інформаційної війни втручання в інформаційний простір що дозволило провести аналіз переваг над ворогом;
3. Проведено математичний розрахунок системи безпеки засобами MATLAB що дозволило визначити переваги та недоліки конфліктуючих сторін інформаційної війни.

Дана система захисту інформаційного простору в умовах інформаційної війни за допомогою метода Річардсона реалізована у вигляді MATLAB візуалізації.

Державою повинна бути встановлена правова рівновага, яка стосуватиметься прав і свобод у інформаційній галузі та інформаційній діяльності і припустимих обмежень у цьому сегменті щодо інтересів обстоювання прав і свобод громадян. Функції державної політики інформаційної безпеки мають бути спрямовані на інформаційне забезпечення державної внутрішньої і зовнішньої політики, напрямів розвитку України.

Для інформаційного забезпечення (інформаційно-пропагандистської роботи) доцільне залучення широкого кола державних діячів, політиків, учених, спеціалістів. Державна влада, яка недооцінює необхідність активного інформаційного забезпечення власної внутрішньої і зовнішньої політики, як правило, майбутнього не має.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Інформаційні війни та майбутнє України [Електронний ресурс] // БЮЛЛЕТЕНЬ СИАЦ. – №100. – Режим доступу: http://siac.com.ua/index.php?option=com_content&task=category§ionid=8&id=129&Itemid=44
2. Пропаганда [Електронний ресурс] / Матеріал з Вікіпедії — вільної енциклопедії. – [Електронний ресурс]: <http://uk.wikipedia.org/wiki/Пропаганда>
3. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. К.: КНТ, 2006. 280 с. 2.
4. Про інформацію (Україна), 2 жовтня 1992, № 2657-XII. Актуально на 01.04.2018. [Електронний ресурс]: <http://zakon3.rada.gov.ua/laws/show/2657-12>.
5. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін,; Гол. ред. Ю. О. Шпак. -К.: "МК-Прес", 2005. -432 с. // Консультант директора. – М.: ИНФРА-М. – №14(290). –2007. – С.11–21.
6. ІНФОРМАЦІЙНІ ВІЙНИ [Електронний ресурс] / Режим доступу: http://pidruchniki.com/18000102/politologiya/informatsiyni_viyini
7. Почепцов, Г.Г. Інформаційно-психологічна війна [Текст] / Г.Г. Почепцов. – М: Сінтег, 2000. – 180 с.
8. Україна у системі міжнародної безпеки: монографія_ / Я. Б. Базиліук, О. С. Бодрук, Д. Ю. Венцковський та ін.; заг. ред. О. С. Власюк; Рада національної безпеки і оборони України, Національний ін-т проблем міжнар. безпеки. К.: Фоліант: Стилос, 2009. 572 с.
9. Остроухов, В.В. Інформаційна безпека [Електронний ресурс].– [Електронний ресурс]: <http://westudents.com.ua/glavy/51894-12-nformatsyna-vyna-yak-forma-vedennya-nformatsynogoprotiborstva.html>
10. Карнаух А. А., Шевчук З. Ю. Інформаційна війна на сучасному етапі розвитку суспільства / А. А. Карнаух, З. Ю. Шевчук // Науковий часопис НПУ імені М. П. Драгоманова. Серія 18 : Економіка і право. 2015. Вип. 29. С. 98-103.

11. Малик Я. Інформаційна війна і Україна / Я. Малик // Демократичне врядування. 2015. Вип.
8. Носов В. Манжай О. Окремі аспекти протидії інформаційної війни в Україні / В. Носов, О. Манжай // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: науково-технічний збірник. – 2015. – Вип. 1. – С. 26 – 32.
9. Богуш, В. Кривуца та А. Кудін, Інформаційна безпека: Термінологічний навчальний довідник. Київ: ООО «Д.В.К.», 2004.
10. О. Маруненко, "«Зовнішні і внутрішні інформаційні війни у медійному просторі України»", Український науковий журнал «Освіта регіону: політологія, психологія, комунікації», № 4, ст. 91-95, 2011.
11. У. Ільницька, "«Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам»", Політичні науки, № 1(2), ст. 27-32, 2016.
12. Костицький В.В. Інформаційна війна проти України – виклик світовому порядку. URL: <http://oksamyt.org/2015/02/02/0202201511> (дата звернення: 20.05.2023)
13. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: навчальний посібник / О. В. Курбан. – Київ: ВІКНУ, 2016. - 286 с.
14. R. Hryshchuk and K. Molodetska-Hrynhchuk, "Methodological Foundation of State's Information Security in Social Networking Services in Conditions of Hybrid War," Information and Security: An International Journal, vol. 41, pp. 55-73, 2018.
15. Li, Y., Huang, G. Q., Wang, C. Z., & Li, Y. C. (2019). Analysis framework of network security situational awareness and comparison of implementation methods. EURASIP Journal on Wireless Communications and Networking, 2019(1), 205.
16. Інформаційна війна проти України та засоби її ведення / Ю. О. Горбань // Вісник Національної академії державного управління при Президентові України. - 2015. - № 1. - С. 136-141.
17. Інформаційна війна / Р. В. Пилипчук // Енциклопедія Сучасної України [Електронний ресурс] / Редкол.: І. М. Дзюба, А. І. Жуковський, М. Г. Железняк

[та ін.]; НАН України, НТШ. – К. : Інститут енциклопедичних досліджень НАН України, 2011.

18. Залєвська І. І., Удренас Г. І. (2022). Інформаційна безпека в Україні в умовах російської військової агресії. Південноукраїнський правничий часопис, (1), 20-26.

19. Литвинюк А. А. (2008). Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування. Вісник ЦВК, (4), 18-21.

20. Про Концепцію Національної програми інформатизації (Закон України). №720-IX (2020). URL: <https://zakon.rada.gov.ua/laws/show/75/98-вр>

21. Нашинець-Наумова А. Ю. (2017). Інформаційна безпека: питання правового регулювання. Київ: Видав. дім «Гельветика».

22. Про Національну програму інформатизації (Закон України). № 2807-IX (2022). URL: <https://zakon.rada.gov.ua/laws/show/74/98-вр>

23. Ніщименко О. А. (2016). Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право, (1), 17–23.