МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 20__ р.

На правах рукопису
УДК 004.62

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система безпеки інформаційного простору в умовах інформаційної війни

Виконавець: Д. А. Татарчук
Керівник: к.т.н.,доцент А. Б. Петренко
Нормоконтролер: к.т.н.,доцент А. Б. Петренко

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«___» _____ 20__ р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Татарчука Дмитра Андрійовича

1. Тема: *Система безпеки інформаційного простру в умовах інформаційної війни* затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.
2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.
3. Вихідні дані: 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.
4. Зміст пояснювальної записки: аналіз втручань в інформаційний простір; дослідження та візуалізація моделі Річардсона.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	19.04.2021	*Виконано*
2.	Аналіз літературних джерел	20.04.2021-22.04.2021	*Виконано*
3.	Обґрунтування вибору рішення	23.04.2021	*Виконано*
4.	Збір інформації	24.04.2021-01.05.2021	*Виконано*
5.	Аналіз втручань в інформаційний простір	02.05.2021-09.05.2021	*Виконано*
6.	Аналіз базових механізмів безпеки інформаційного простору	10.05.2021-12.05.2021	*Виконано*
7.	Дослідження моделі Річардсона	13.05.2021-24.05.2021	*Виконано*
8.	Оформлення і друк пояснювальної записки	25.05.2021-01.06.2021	*Виконано*
9.	Оформлення презентації	02.06.2021	*Виконано*
10.	Перевірка на антиплагіат	03.06.2021-07.06.2021	*Виконано*
11.	Отримання рецензій від рецензента	08.06.2021	*Виконано*

Здобувач вищої освіти _____ Д. А. Татарчук
(підпис, дата)

Керівник дипломної роботи _____ А. Б. Петренко
(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, і має 63 сторінки основного тексту, 5 рисунків, 1 таблицю. Список використаних джерел містить 17 найменуваннь.

Метою роботи є розрахунок системи безпеки інформаційного простору в умовах інформаційної війни, підвищення ефективності способів боротьби при інформаційній війні.

В роботі обґрунтовано необхідність забезпечення додаткової безпеки інфрмаційного простору країни шляхом аналізу інформаційних потужностей. Розглянуто принципи функціонування та механізми захисту інформаційного простору.

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

Ключові слова: інформаційний простір, інформаційний ресурс, інформаційна війна, конфіденційність, модель Річардсона.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 6
ВСТУП 7
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ СФЕРИ ІНФОРМАЦІЙНИХ ВІЙН 9
1.1 Інформаційна війна та її сутність 9
1.2. Особливості інформаційної безпеки на сучасному етапі розвитку суспільства 12
1.3 Інформаційна війна проти України 17
1.4 Висновки до розділу 1 20
РОЗДІЛ 2. ВПЛИВ ІНФОРМАЦІЙНОЇ ВІЙНИ НА НАЦІОНАЛЬНУ БЕЗПЕКУ 21
2.1. Ризики та вразливості інформаційного простору в умовах інформаційної війни 21
2.2. Засоби інформаційної війни 31
2.3 Зловмисники та порушники 33
2.4 Висновки до розділу 2 34
РОЗДІЛ 3. Вдосконалення система безпеки інформаційного простору в умовах інформаційної війни 35
3.1 Методи протидії інформаційній війні 35
3.2 Засоби посилення безпеки інформаційного простору в умовах інформаційної війни 40
3.3 Інструменти виявлення втручань в інформаційних простір 55
3.4 Висновки до розділу 3 60
ВИСНОВКИ 61
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 62

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. Виникнення та посилення загроз в інформаційному секторі, зокрема загроз внаслідок інформаційних воєн, суттєво підвищує значенн та роль інформаційної безпеки для національної безпеки України а розширює її зміст.

Особливу увагу приділено соціальним і культурним наслідкам інформаційної пропаганди, інформаційних операцій і бойових дій. Грунтуючись на дослідженні історії та еволюції ІТ, агітації, пропаганди й інформаційної війни, необхідно оцінитиризики та проаналізувати загрози в інформаційних системах.

Мета інформаційної війни – послабити сили супротивника або конкурента, посилити власні. Вона передбачає заходипропагандистського впливу на свідомість людини. Такі війни не призводять безпосередньо до кровопролиття, руйнувань, при їх веденні немає жертв, ніхто непозбавляється даху над головою. Головне завдання інформаційних війнполягає у маніпулюванні масами. Мета такої маніпуляції найчастіше полягає у внесеннів суспільну та індивідуальну свідомість ворожих, шкідливих ідей та поглядів;дезорієнтації й дезінформації мас; послабленні певних переконань; залякуванні свогонароду образом ворога; залякуванні супротивника своєю могутністю; забезпеченняринку збуту для своєї економіки. У цьому випадку інформаційна війна є складовоюконкурентної боротьби.

Метою роботи є аналіз та розрахунок системи безпеки інформаційного простору в умовах інформаційної війни, підващення ефективності способів боротьби при інформаційній війні.

Для досягнення поставленої мети вирішуються такі задачі:

- провести аналіз методів втручань в інформаційний простір;
- протестувати модель втручання в інформаційний простір;
- провести математичний розрахунок у “MATLAB” інформаційної

безпеки в умовах інформаційної війни.

Об’єктом дослідження є процеси втручання в інформаційний простір країни.

Предмем дослідження є методи захисту інформаційного простору у мовах інформаційної війни, методи корегування сил при ведені інформаційної війни.

Практична цінність полягає у тому, що здійснено аналіз моделі захису інформаційного простору в умовах інформаційної війни, а також її математичний розрахунок, за рахунок чого ми можемо визначити переваги та недоліки конфліктуючих сторін.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ СФЕРИ ІНФОРМАЦІЙНИХ ВІЙН

1.1. Інформаційна війна та її сутність

Активний інформаційний розвиток, на якому базується сучасне суспільство, сприяє швидкій глобалізації і затемнює міждержавні та прикордонні кордони. Інформація, поряд з політичними та економічними чинниками, стає важливим чинником розвитку держави, служить інструментом і засобом війни в геополітичних відносинах і може формувати новий тип війни, тобто інформаційну.

На сьогоднішній день вчені виділили 5 підходів до визначення поняття інформаційної війни.Представники першого підходу розкривають інформаційну війну як сукупність політичних, економічних, соціальних, дипломатичних і технічних методів, прийомів і засобів, з метою досягнення поставленої мети вони роблять благотворний вплив на інформаційну сферу об'єкта агресії і захищають власні інтереси. Прихильники другого напрямку називають його найгострішою формою боротьби в інформаційному просторі, передумовою якої є протистояння агресивних сторін різних напрямків.Відповідно до третього підходу, інформаційна війна трактується як форма бойових дій з використанням електронних інформаційних засобів. Як пише Уін Швартов:" інформаційна війна-це електронний конфлікт, а інформація-це стратегічний актив, який необхідно захопити або знищити " [1, с.99]. Представники 4-го підходу трактують інформаційну війну як протистояння сучасних технологічних систем.Оскільки розвиток суспільства і світу не зупинився, сьогодні починається інший підхід до трактування поняття інформаційної війни.Життя людини з використанням впливу явної та прихованої інформації [1, с.99]. Як і будь-яке інше явище, інформаційна війна має свої особливості, що відрізняються від звичайної війни.До них відносяться:

- Відсутність видимих фізичних руйнувань може затримати оборонну відповідь країни.

- Оскільки засоби ведення інформаційної війни практично непередбачувані і постійно змінюються в умовах операцій, варіанти боротьби з такими засобами повинні ґрунтуватися на аналітичних навичках, високому інтелектуальному потенціалі, в тому числі на всіх рівнях управління, що дуже складно в сучасних умовах.

- Під час інформаційної війни людські ресурси не завжди фізично захоплюються, але контроль над їх свідомістю встановлюється

- Вибірковість, заснована на принципі досягнення максимального ефекту;тобто інформаційна війна ефективна, коли вона досягає реального ефекту в своєму впливі на осіб, які приймають рішення в країні, що піддається нападу.

- Короткострокова інформаційна війна неефективна, коли інформаційна інфраструктура впливової країни тендітна.

- Нівелюється розуміння істини, аргументи стають абсурдними, порушується здоровий глузд;

- Впливати на хід мислення противника, щоб останній прийняв рішення на користь нападника;

- Перетворіть перевагу противника в недолік.

- Гратися в емоціях і відволікатися від марного[3, с.27].

Таким чином, інформаційна війна передбачає ослаблення моральних і матеріальних сил противника, а також посилення власних інформаційних сил. В ході інформаційної війни використовуються пропагандистські засоби, що впливають на свідомість людини ідеологічного та емоційного характеру. Залежно від методів інформаційної війни і засобів впливу на об'єкти сучасні вчені виділяють різні види інформаційної війни. М. Лібікі є одним з провідних теоретиків інформаційної війни і вивчає особливості інформаційної війни у своїй роботі "Що таке інформаційна війна? "Перерахував 7 типів інформаційних конфліктів:

- "Командування і управління", спрямоване на руйнування каналу зв'язку між командою і виконавцем.

- "Розвідка" включає в себе збір і захист важливої особистої інформації.

- "психологічний" характеризується пропагандою, інформаційною обробкою населення, втратою морального духу, дезінформацією.

- "Злом" здійснюється шляхом диверсій і атак на ворогів шляхом створення спеціальних програм.

- "Економіка" втілюється в інформаційній блокаді та інформаційному імперіалізмі.

- "Електроніка" спрямована на електронні засоби зв'язку: радіо, радіолокацію, комп'ютерні мережі.

Крім цього, вчені виділяють наступні види воєн: психологічна війна, кібервійна, мережева війна (мережевий інформаційний простір, основні стратегічні операції - як розвідувальні, так і військові), а також їх медійне, дипломатичне, економічне і технічне забезпечення. У свою чергу, низка науковців, пропонує інший поділ різновидів інформаційної війни: політичний, економічний, психологічний та електронний, що дозволить сформувати найбільш оптимальний інструментарій подолання всесвітньої загрози. [1, с. 100].

Таким чином, в процесі розвитку інформаційного суспільства, поряд з модернізацією всього суспільного життя, існує безліч загроз: повне домінування, зомбування ідентичності, маніпулювання суспільною свідомістю, поширення чуток, дестабілізація суспільства, втрати через терористичні акти, широкі можливості і т.д. до інформаційної війни і так далі.

В ході інформаційної війни основними об'єктами впливу і захисту є населення, військові, політична еліта опозиції, система формування масової свідомості, думок. Інформаційні війни безпосередньо не призводять до кровопролиття або руйнувань, жертв немає, їжу не віднімають. Але ці війни ведуться для того, щоб побороти свідомість.

1.2. Особливості інформаційної безпеки на сучасному етапі розвитку суспільства

На сучасному етапі розвитку цивілізації інформація відіграє важливу роль у функціонуванні громадських і державних інститутів і в житті кожної людини.На наших очах процес інформатизації розвивається настільки стрімко і часто непередбачувано, що це тільки початок шляху сприйняття його соціальних, соціальних, політичних, економічних, військових та інших можливих наслідків.Глобальна інформатизація призводить до створення єдиного світового інформаційного простору, в якому здійснюється накопичення, обробка, зберігання та обмін інформацією між суб'єктами цього простору (людьми, організаціями, державами).Зрозуміло, що можливість швидкого обміну політичною, економічною, науково-технічною, спеціальною та іншою інформацією, можливість використання нових інформаційних технологій у всіх сферах суспільного життя, особливо у виробництві та управлінні, є безсумнівною вигодою.Людство.Однак точно так само, як швидке промислове зростання поставило під загрозу екосистему Землі, а досягнення в галузі ядерної фізики створили небезпеку ядерної війни, інформатизація може викликати безліч серйозних проблем у глобальному масштабі.

Поняття" зв'язки з громадськістю " багатогранно і має безліч тлумачень. У книзі Чумикова "Зв'язки з громадськістю" вона визначається наступним чином : забезпечити, щоб керівництво організації було поінформовано про громадську думку, своєчасно реагувало на нього, готувалося до змін і дозволяло їх найбільш ефективно використовувати.Визначити головне завдання суспільства-служити суспільним інтересам - і особливо підкреслити її..."І так далі. [4].

Вплив інформації на колективну свідомість присутній завжди. Шамани і жерці також використовували його як технологію, намагаючись"побудувати майбутнє"в якомусь напрямку.

Існує безліч визначень поняття "інформаційна війна". У зв'язку з цим рекомендується розглянути найбільш популярні з них і підкреслити особливості, властиві всім трактуванням цього явища.

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

<table>
<tr><td></td><td colspan="6">Компоненти психологічної операції</td><td>Остаточна мета</td></tr>
<tr><td>паблік рілейшнз</td><td>оцінка ситуації</td><td colspan="3">планування операції</td><td colspan="2">виконання</td><td rowspan="2">Поведінкові зміни у цільової аудиторії</td></tr>
<tr><td>Інформаційні війни</td><td>Збір розвідувальної інформації</td><td>Аналіз цільової аудиторії</td><td>Розробка продукту</td><td>Відбір каналів поширення</td><td>виробництво медіа</td><td>поширення</td></tr>
</table>

Інформаційна війна – це:

- вплив поширення певної інформації на цивільне населення та / або військовий персонал в інших державах. Термін "розвідка і психологічна війна" був запозичений зі словника американських військовослужбовців. Якщо перекласти цей термін ("інформаційно-психологічна війна") на англійську мову, він може звучати як" інформаційна війна", так і" інформаційно-психологічна війна", залежно від контексту конкретного офіційного документа або наукової публіка;
- дія, ініційована для досягнення інформаційної переваги шляхом нанесення шкоди інформації, інформаційним процесам та інформаційним системам противника при одночасному захисті власної інформації, інформаційних процесів та інформаційних систем противника. [10];

- цілісна стратегія, заснована на зростаючій важливості та цінності інформації в командуванні, управлінні, політиці, економіці та суспільному житті.
- нова форма боротьби між сторонами, яка впливає на інформаційне середовище противника і використовує спеціальні методи і засоби захисту для досягнення стратегічних цілей війни. [5].

Головне завдання інформаційних воєн полягає у маніпулюванні масами. Мета такої маніпуляції найчастіше полягає у: внесенні в суспільну та індивідуальну свідомість ворожих, шкідливих ідей та поглядів; дезорієнтації та дезінформації мас;послабленні певних переконань; залякуванні свого народу образом ворога; залякуванні супротивника своєю могутністю; забезпечення ринку збуту для своєї економіки. У цьому випадку інформаційна війна є складовою конкурентної боротьби [13].

Аналіз визначення дозволяє виявити особливості, які завжди присутні при веденні інформаційної війни.:

1. Вплив на будь-яку соціальну групу (військово службовців, робітників, інтелігенцію тощо).
2. Інформація, передана цій аудиторії.
3. Стратегія застосування інформаційних засобів носить виключно агресивний характер.
4. Мета інформаційної війни - змінити спосіб мислення у впливовому напрямку і зайняти більш вигідну позицію.
5. Захист власного простору від нападу.

Існують й інші класифікації складових інформаційної війни :

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

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

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

Вплив інформації на противника має ряд особливостей, що відрізняються від інших форм боротьби і спілкування в області обміну інформацією. Розглянемо основні з цих особливостей. На відміну від маніпуляції міжособистісною свідомістю, об'єктом впливу в інформаційній війні є масова свідомість противника, яке враховує колективні особливості великих груп, що є об'єктами впливу, а також певні особливості людської свідомості. Обмежений і негативний вплив інформації на окремих осіб або невелике число людей не є інформаційною війною. На відміну від звичайного впливу на інформацію, в ході інформаційної війни об'єкту впливу нав'язуються окремі від нього цілі, прагнення, в результаті чого його досягнення завдає шкоди самому собі.

Це приносить користь іншій стороні, спотворюючи або представляючи факти таким чином, що вони спотворюють факти, викликають неадекватну поведінку противника або змушують його емоційно усвідомлювати факти.

Ознаки прихованої маніпуляції включають емоції, сенсаційність і терміновість, повторення, фрагментацію всієї картини фактів, видалення з контексту,"тоталітаризм"("надійне джерело"), джерело повідомлення, плутанину інформації і думок, приховування авторитету, стереотипи.

До методів маніпуляції масовою свідомістю відносять такі [14]:

- використання навіювання;
- перенесення приватного факту в сферу загального, в систему;
- використання чуток, домислів, тлумачень у незрозумілій політичній або соціальній ситуації;
- метод під назвою «потрібні трупи»;
- метод «страховиськ»;
- замовчування одних фактів і вип'ячування інших;

- метод фрагментації;
- «Метод Геббельса» (багаторазові повтори);
- метод чергування на конвеєрі «правда, правда, правда, неправда, правда»;
- створення неправдивих подій, містифікація.

Підтипом інформаційної війни є так звана кібервійна, тобто протистояння в кіберпросторі за допомогою методів інформаційних технологій. Німецькі експерти згадали 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 комп'ютерної системи противника через великий потік інформації.

В основі "мережевої війни" лежить щось далеке від загальноприйнятих концепцій війни і миру. У цій моделі тіло противника більше не є об'єктом фізичного нападу, що призводить до того, що завоювання інформаційного панування безпосередньо змінює його волю, і в кінцевому підсумку всі форми ідеологічного або політичного протистояння оцінюються як війна.

1.3. Інформаційна війна проти України

Аналіз досліджень, проведених вченими, показує, що інформаційна зброя, створена у вигляді програмних або мікропрограмних систем і засобів, є економічним, може бути легко замасковано під засіб захисту, може діяти анонімно без оголошення війни, але також володіє такими характеристиками, як універсальність, багатовимірна структура.використання, радикальна поведінка (в сенсі заподіяння максимальної шкоди). Сьогодні Україна знаходиться в неформально відкритому стані, тому що вона підключена до Інтернету, який є глобальною інформаційною інфраструктурою. Це робить нашу державу особливо вразливою для інформаційної зброї. У цій ситуації

жодна держава не може відчувати себе в безпеці, в тому числі і ми, тому що громадяни в будь-який момент можуть піддатися інформаційним атакам.

Нашій країні вперше за весь час свого існування довелося зіткнутися з інформаційною війною-однією з найнебезпечніших форм війни. Головним противником інформаційного протистояння, яке триває вже дуже давно, стала Російська Федерація. Інформаційний тиск також йшов із Заходу.

Росія використовує передові форми гібридної війни в Україні з початку 2014 року. Росія домагається від Заходу найбільшого невтручання в події на Україні і заробляє час для встановлення і розширення своєї військової участі в конфлікті. Росії також вдалося посіяти розбрат в НАТО і ЄС, викликавши напруженість всередині урядів цих країн, особливо в питанні антиросійських санкцій.

Як бачите, основними завданнями Російської Федерації в цій війні є: формування спотвореного бачення подій у громадян України і Росії. Це знижує моральний дух українського населення, солдатів української армії і спонукає їх зраджувати і переходити на інший бік.

Росія використовувала безліч методів і прийомів, що використовуються в розвідувальних атаках проти України, націлюючись на групи, які були об'єктом розвідувальних атак.

Основними методами інформаційної агресії проти України є: [8]:

1) дезінформування та маніпулювання;

2) пропаганда;

3) диверсифікація громадської думки;

4) психологічний та психотропний тиск;

5) поширення чуток.

Головний висновок і урок інформаційно-пропагандистської війни Росії проти України як ключового компонента "гібридної війни" полягає в тому, що вона має безпрецедентний характер за своїм змістом, масштабом і спрямованістю. [1]:

по-перше, інформаційна війна почалася задовго до військового вторгнення Росії проти України і продовжує супроводжувати її на кожному етапі, заздалегідь адаптуючись до поточних цілей і завдань.;

по-друге, інформаційно-пропагандистські та дезінформаційні проекти, операції та заходи, спрямовані на всі верстви населення Росії і західних країн, а також всіх регіонів України-кожен з різними цілями і завданнями;

по-третє, метою інформаційної війни в Україні є ліквідація української держави. У Росії-отримати громадську підтримку, щоб виправдати дії російського лідера. Для Заходу-дискредитація дій керівництва України та її збройних сил.

Ця війна є викликом всьому міжнародному співтовариству і супроводжується збільшеною інформаційною загрозою світовому порядку. Слід зазначити, що Україна не була готова до такого масштабного військового нападу і розвідувальних атак.

Указом Президента України введено в дію рішення Комісії національної безпеки і оборони України від 2014-4-28 років "Про заходи щодо вдосконалення формування та реалізації державної політики в галузі інформаційної безпеки України" та правового забезпечення національної безпеки в інформаційній сфері. [9]:

– визначення механізму реакції на негативний інформаційно-психологічний вплив;

– підготовка проекту Стратегії розвитку інформаційного простору України, зокрема, для визначення цілей, завдань, структури та режиму функціонування державної системи інформаційної безпеки держави, а також проекту кіберстратегії забезпечення безпеки України;

– підготовка проекту Закону України"про кібербезпеку в Україні". Щоб запобігти неправдиву інформацію і психологічні наслідки, необхідно дотримуватися деяких правил.:

– критикуйте пропаганду іноземних засобів масової інформації та більше довіряйте інформації з офіційних джерел та публікацій.;

– не висловлюйте різко ситуацію навколо або всередині інформаційного середовища.;

– будьте пильні і чиніть опір ворожій пропаганді. Завдання його пропаганди - створити в голові бажане уявлення про поточну ситуацію.

Таким чином, можна зробити висновок, що метою інформаційної війни є ослаблення моральних і матеріальних сил противника і посилення самого противника. Переможцем в інформаційній війні стає Та сторона, яка може змоделювати дії противника в різних ситуаціях, визначити власний алгоритм дій і, нарешті, реалізувати його. Найбільш повне моделювання поведінки противника означає збір, зберігання та обробку інформації про супротивника. Знати і розуміти його історію, культуру і життя.

1.4. Висновки до розділу 1

Конфлікт між інформацією та технологіями є важливим аспектом сучасної інформаційної політики. У сучасних умовах стрімко розвиваються не тільки засоби масової інформації та комунікації, а й комп'ютери, системи автоматичного управління, електронні засоби масової інформації, особливо Інтернет, міжнародна глобальна інформаційна мережа, з'являються принципово нові технології та методи представлення інформації.

Таким чином, інформаційна зброя виступає ефективним засобом знищення, зміни або розкрадання інформаційних масивів, отримання з них необхідної інформації після подолання систем безпеки, обмеження або заборони доступу до законних користувачів, втручання в роботу технічних засобів, відключення мереж зв'язку та комп'ютерів. Мережа, все високотехнологічне забезпечення суспільства, а також функції державної структури.

Якщо ми належним чином обізнані про деталі інформаційного співтовариства в контексті загострення глобальних проблем, то сьогодні ми повинні діяти таким чином, щоб нейтралізувати страшний потенціал

інформаційної війни і страшний потенціал катастрофи цивілізації, яка виникає і накопичується в цьому процесі.

РОЗДІЛ 2. ВПЛИВ ІНФОРМАЦІЙНОЇ ВІЙНИ НА НАЦІОНАЛЬНУ БЕЗПЕКУ

2.1. Ризики та вразливості інформаційного простору в умовах інформаційної війни

Інформаційні ризики за своїм походженням поділяються на три категорії:

- ризик, пов'язаний з втратою інформації (витік, знищення, знищення). Це особливо небезпечно, коли існує ризик втрати важливої для організації інформації, такої як банківська або комерційна таємниця, або іншої інформації з обмеженим доступом.
- ризики, пов'язані з формуванням інформаційних ресурсів (неповнота, використання недостовірної інформації, відсутність необхідної інформації, дезінформація);
- ризики, пов'язані з інформаційним впливом на діяльність суб'єкта (поширення неправдивої і негативної інформації, інформаційно-психологічний вплив на співробітників, клієнтів і акціонерів, інформаційний тероризм);

Враховуючи, що в ринковій економіці ризик-це 1 з характеристик економічної діяльності, а в разі підприємницької діяльності ризик-1 з її складових, неможливо виключити ризик з інформаційних відносин господарюючих суб'єктів, та й взагалі-з будь-яких відносин.

Наявність конкуренції та наявність вищевказаних ризиків становлять певну загрозу для інформації, що використовується підприємством.У той же час діяльність останніх супроводжується безперервним процесом планування

і прийняття рішень, що вимагає надійної інформаційної підтримки.У той же час участь людей в економічному житті створює потребу в об'єктивній і всебічній інформації про діяльність підприємницького органу.

На жаль, під час конкуренції існує загроза того, що інформація завжди буде впливати на споживачів товарів і послуг, що не тільки незаконно зазіхає на інформацію конкуруючих суб'єктів, а й сприяє формуванню правильних уявлень про продукт, не завжди об'єктивних. Послуги та організації, які їх виробляють або надають.

Тому в інформаційних відносинах господарюючого суб'єкта можуть існувати загрози, пов'язані з вторгненням в інформаційні ресурси (в першу чергу в ті частини, доступ до яких обмежений), загрози, що виникають в процесі формування середовища, і умови для таких суб'єктів. У першому випадку інформація є предметом загроз, а в другому-інструментом їх реалізації.

Як свідчить досвід, основними способами реалізації таких загроз є:

- маніпулювання інформацією (дезінформація, викривлення інформації, подання в інформаційне середовище неповної або неправдивої інформації);
- порушення встановленого порядку інформаційного обміну, несанкціонований доступ або необґрунтоване обмеження доступу до інформаційних ресурсів, протиправне збирання і використання інформації;
- руйнування та використання з протиправною метою чужих інформаційних ресурсів;
- інформаційний тероризм (поширення комп’ютерних «вірусів», установлення програмних та апаратних закладних пристроїв, упровадження радіоелектронних приладів перехвату інформації, незаконне використання чи порушення роботи інформаційних і телекомунікаційних систем, нав’язування фальшивої інформації, оприлюднення компрометуючої інформації та ін.).

Найбільш поширеними загрозами інформації організації є розкриття конфіденційної та конфіденційної інформації, її крадіжка, зміна або

знищення, несанкціоноване використання інформації, зокрема інтелектуальної власності організації, яка приносить користь ринку, і доступ до інформації, захищеної неуповноваженими особами.

Під розголошенням інформації розуміється незаконне, умисне або недбале дію державної посадової особи або іншої особи, в результаті якого публікується (поширюється) несанкціонована інформація і встановлюються відповідні процедури її розголошення без необхідності участі посадової особи. Це може бути зроблено шляхом повідомлення, передачі, передачі, публікації, втрати або іншого розкриття такої інформації.

Крадіжка інформації - це вилучення секретів для подальшого використання або передачі носія інформації (документів, електронних носіїв, відео-та аудіозаписів) іншими особами таким особам.

Зміна інформації - це внесення змін до змісту інформації, що міститься в конкретному носії, або в сам носій (комп'ютерні програми), в результаті чого використання цієї інформації стає повністю неможливим, або така інформація вимагає значного уточнення та аналізу.

Незаконне використання інформації відноситься до використання певних даних, знань і технологій, що належать конкретній юридичній або фізичній особі, без її згоди або особою, якій відома така інформація, Службова чи інша діяльність.

Рис 2.1. Структура інформаційної війни

Структура інформоційної 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 данних;
- Управління сприйняттям;
- Вербування агентів;
- Open source intelligence;
- Злом пароля;

- Підслуховування;
- Мережеві сніфери.

Несанкціонованим буде також доступ до інформації з порушенням встановлених правил доступу до неї.

Основні загрози при ведені інформаційної війни:

- Компютерні програми (віруси, «хробаки», «троянські коні», логічні бомби, прорахунки в програмах, і системах компютерної безпеки(випадкові або навмисні);
- Апаратна частина комютерів (мікроскопічні машини і мікроби, які знищують електронні схеми, високоенергетичні випромінювачі, електромагнітні імпульси).
- Спеціальні функції чіпів, вмонтуванн функцій може здійснюватися і в інтегральні схеми (мікрочіпи). Сценарії активізації таких функцій від певного набору програмних кодів до спеціального радіосигналу на заданій радіочастоті.
- Наномашини – мікроскопічних розмірів роботи, які можуть проникати всередину компютера і спричиняти електронні замикання і псувати обладнання.

Ці загрози є загальними за своєю природою і однаково застосовні до всіх видів інформації, включаючи документацію, електроніку та знання.Звичайно, кожен тип інформації має додаткові і специфічні особливості, властиві тільки певним типам інформаційних загроз.Ймовірно, нереалістично розглядати кожен з цих випадків, оскільки вжиття заходів щодо захисту та протидії цим типам загроз забезпечує безпечний стан інформації з розширеними гарантіями.У той же час, враховуючи, що сучасний бізнес тісно пов'язаний з комп'ютерними інформаційними технологіями, необхідно навести деякі особливості загрози таким технологіям, особливо враховуючи перспективи подальшої інформатизації суспільства та його розвитку.

В реалізації загроз суб’єктів підприємництва важливе місце займають канали її витоку, до яких можна віднести: візуально-оптичні, акустичні та акустоперероблювальні, електромагнітні (в тому числі і магнітні та електричні), матеріально-речові (магнітні носії, папір, фотографії і т. д.).

Візуальний оптичний канал створюється як оптичний шлях від об'єкта інформації до одержувача. Для цього потрібні енергетичні, тимчасові, просторові умови і відповідні технічні засоби. Створенню таких каналів сприяють відповідні характеристики інформаційного об'єкта, такі як конфігурація, поведінка і активність. Особлива цінність інформації, отриманої по таких каналах, полягає в тому, що вона є найбільш достовірною, ефективною і виступає в якості письмового підтвердження отриманої інформації.

Джерелом акустичного каналу є тіло і механізми, які викликають вібрації або коливання, такі як голосові зв'язки людини, мобільні машини, телефони, системи посилення голосу, динаміки, засоби запису і відновлення голосу і т. д.

Звукові хвилі від людського голосу та інших звуків вібрації створюють звукові хвилі, поширюються в просторі і взаємодіють з відповідними перешкодами (двері, вікна, стіни, підлоги, різні пристрої), щоб змінити тиск і перевести його в режим вібрації. При впливі на спеціальні пристрої (мікрофони) звукові коливання створюють відповідні їм електромагнітні хвилі.Він несе інформацію, яка передається на відстань і генерується звуковими коливаннями.

Акустичні канали створюються:

- поширення акустичних (механічних) коливань у вільному просторі (у відкритих просторах, в приміщеннях з відкритими вікнами, витоку з квартир, дверей, вентиляційних каналів);
- через вплив акустичної вібрації на елементи і конструкції будівлі (стіни, стелі ,підлоги, вікна, двері, системи вентиляції, водопровідні труби, Системи опалення, кондиціонування повітря);

В силу особливостей експлуатації фізичних властивостей і технічних засобів, що забезпечують виробничу діяльність, електромагнітні канали є найбільш небезпечними і досить поширеними для отримання інформації.Такі канали створюються за рахунок наявності технічних засобів, які використовуються для генерації небезпечних джерел сигналу.Перш за все, до таких джерел відносяться Процесори.Тобто пристрій, який перетворює зміну однієї фізичної величини в зміну іншої.В електронному плані процесор визначається як пристрій, що перетворює неелектричну величину в електронний сигнал або навпаки.Достатнє знання функцій процесора дозволяє ідентифікувати неконтрольовані ознаки фізичного поля, яке створює електромагнітний канал для витоку (передачі) інформації.При цьому, враховуючи ідентичність технічних і конструкторських рішень, електронних схем технічних засобів обробки інформації та забезпечення виробничої діяльності підприємств і банків, всі вони можуть мати електромагнітні канали витоку (передачі) інформації. Тому в будь-якому випадку використання технічних засобів обробки і передачі інформації створює неконтрольовану загрозу витоку (передачі).

Матеріальні канали створюються для отримання інформації шляхом розслідування відходів виробництва (зіпсованих документів або їх фрагментів, чернеток різних заміток, записів, листів і т.д.), крадіжок, несанкціонованих знайомств, копій, фотографій, відеозаписів документів і т. д., зразків планів, апаратного або програмного забезпечення.

Ще однією загрозою, яка дуже небезпечна для сучасного підприємництва в інформаційному секторі, є вже відомий кібертероризм.Особлива небезпека кібертероризму полягає в тому, що він становить загрозу інформаційним ресурсам підприємства і в той же час загрозу суспільній оцінці іміджу та діяльності підприємства.Також, на думку експертів, в останні роки кібератаки стали досить різноманітними, включаючи кібершпіонаж, хактивізм і кібер-рекет.Багато з них відносяться до бізнесу.Йдеться про нафтову промисловість, телекомунікаційну галузь,

аерокосмічні компанії, суднобудівні компанії та розробники високих технологій. Найбільш поширеною загрозою тут є поширення вірусів і різних шкідливих програм, які не тільки руйнують програмне забезпечення, але і перешкоджають відновленню.Кібератаки зазвичай передують збору інформації про так звану мету атаки.Шпигунське ПЗ.Слід зазначити, що кібератаки поширюються як на настільні комп'ютери, так і на мобільні пристрої, підключені до комп'ютерних мереж.Україна, за даними 2013 року, увійшла в топ-3 країн за кількістю заражених мобільних пристроїв.За рівнем ризику зараження вірусом через Інтернет наша країна займає 45,6 місце серед країн з високим ризиком (9% користувачів).Тобто ІТ-інфраструктура сучасного підприємництва дуже крихка і вимагає ефективного захисту.

Не можна не звернути уваги і на т. з. офісні загрози інформації суб’єктів підприємництва, а саме загрози інформації, що міститься в документах та інформації, якою володіють і використовують у процесі роботи офісні працівники. Якщо дати відповідь на зміст поняття офісна діяльність, то вона може бути такою: це відповідним чином організована у просторі та часі сукупність дій персоналу певного суб’єкта, спрямована на забезпечення управління його діяльністю. Тобто, офісна діяльність – це частина управлінського процесу. І у разі, коли у такій діяльності існують певні загрози, то це все буде відбиватись на процесі управління, у даному випадку діяльністю суб’єкта підприємництва. Оскільки управління значним чином пов’язане з інформаційними технологіями, то офісна діяльність спрямована на виконання різного роду завдань, робіт, процедур та операцій інформаційного забезпечення процесу управління. Структура, методика та зміст такого забезпечення формує т. з. офісну технологію. Об’єктом останньої є відповідний інформаційний ресурс, що оброблюється, інтерпретується та використовується для забезпечення управлінської діяльності. Звідси можна бачити, що в основі офісної діяльності є робота з інформацією суб’єкта підприємництва, причому робота в ланці управління, що визначає особливу важливість такої діяльності. Основними

компонентами в офісній діяльності виступають знання працівників офісу і документи, які її супроводжують. За таких умов, зусилля суб’єктів, які прагнуть заволодіти інформацією суб’єктів підприємництва або нанести шкоди суспільній оцінці його діяльності будуть зосереджені саме навколо персоналу та документів.

Реалізація плану отримання офісної інформації через ваших співробітників може становити реальну загрозу як для ваших співробітників, так і для вашого бізнесу.Найбільш поширеними загрозами тут можуть бути: залучення таких співробітників і третіх осіб; шантаж офісних працівників з метою отримання доступу до інформаційних ресурсів офісу.Неправомірне використання або розголошення офісних технологій або інформації шляхом підбурювання до ініціативи співробітників.В останньому випадку провокації можуть формуватися в самому офісі або в середовищі, де офісні працівники забезпечують потреби та інтереси.Незадоволеність цими потребами та умовами, що впливають на надання пільг, викликає дії, які можуть становити загрозу для інформації в офісі.І тут не обов'язково, щоб співробітник раніше був зловмисним або не лояльним до компанії або банку. Такі характеристики можуть бути викликані атмосферою офісу, стилем взаємин, способом роботи, що саме по собі є загрозливим явищем, яке в кінцевому підсумку може становити серйозну загрозу для інформації суб'єкта. Крім того, такі загрози зазвичай не мають нічого спільного з матеріальними цінностями, і люди не завжди відчувають себе винними в тому, що інформація була розкрита з їхньої вини. Необхідно документувати діяльність господарюючих суб'єктів, що створює додаткові ризики щодо інформації.

Тут можуть існувати наступні загрози для офісної інформації:

- втрата чи неправильне знищення документів;
- ігнорування вимог адміністративного персоналу до розробки, впровадження, обліку, передачі та зберігання документів;
- маніпулювання документами з обмеженим доступом, коли є люди, які не мають до них доступу, несанкціонована передача таких

документів призначеній особі;

- використання інформації обмеженого доступу в неопублікованих документах, публікаціях та особистих записах;
- розміщення надлишкової інформації з обмеженим доступом до документів;
- копії офіційних документів, конфіденційних документів та конфіденційних документів, що перевищують суму, необхідну для виконання службових обов'язків;
- усний переклад документа в повідомленні (включаючи засоби зв'язку), витяги з тексту документа в повідомленні або передача по електронній пошті.
-

2.2. Засоби інформаційної війни

В інформаційній війні ви розглядаєте інформацію як окремий об'єкт або як потенційну зброю і вигідну мету. Його також можна вважати якісно новим видом бою. Інформаційна війна-це атака на інформаційні функції, незалежно від засобів.

Крім того, характер деструктивного впливу на інформаційний простір, тобто процес отримання, обробки, зберігання і поширення всіх видів інформації, визначає 3 форми інформаційної війни. [15]:

- вплив на формат повідомлень, механізм передачі, зберігання, обробку даних і т. д.;
- блокування передавання повідомлень;
- вплив на зміст повідомлень.

Національний інститут стратегічних досліджень США і деякі західні експерти і вчені виділили 7 елементів інформаційної війни. [15]:

1. Стратегія і тактика нейтралізації органів управління противника (командна війна).
2. Розвідувальна війна.

3. Електронна війна.
4. Психологічна війна.
5. Комп'ютерна війна.
6. ІВ в економічній сфері.
7. Інформаційний тероризм.

Інформаційна та комп'ютерна революція відкриває широкий спектр можливостей для впливу на людей і владу, маніпулювання свідомістю і поведінкою людей, навіть у віддалених районах. Враховуючи процес глобалізації комунікаційних мереж, що відбувається в світі, можна припустити, що в майбутньому тип інформаційної атаки переважатиме. Серйозна увага фахівців різних профілів до цього питання необхідно для того, щоб ця війна уникла самих негативних наслідків для всього людства.

Визначення зв'язків з громадськістю часто визначається як маніпулювання та обман споживачів. Наприклад,"...отже, PR, реклама, інформаційна війна як засіб вирішення спорів між правлячими групами...". Однак, порівнюючи поняття"зв'язки з громадськістю"і" інформаційна війна", можна, по-перше, описати ситуацію, а по-друге, розрізнити ці поняття.

Ототожнення зв'язків з громадськістю з «брудними» технологіями впливу на громадську думку викликано, швидше за все, тим, що вони використовують дуже схожі засоби реалізації своїх цілей. Ймовірно, ще один факт, що вплинув на це – несумлінне використання можливостей зв'язків з громадськістю деякими компаніями.

Однак необхідно мати на увазі, що цілі діяльності цих сфер різні. Якщо діяльність спеціаліста зі зв'язків з громадськістю носить інформаційний характер, то фахівця з інфовійни – наступальний і маніпулює.

Так само відмінною рисою є якість наданої інформації. Якщо у зв'язках з громадськістю використовується правдива інформація, то для ведення інформаційної війни широко застосовується не тільки замовчування окремих фактів, але навіть їх фальсифікація.

Інформаційна війна і зв'язок з громадськістю схожі тільки на етапі реалізації цілей, проте самі цілі принципово різні.

Засоби масової інформації не обов'язково є ініціатором або суб'єктом змін у свідомості окремої людини або соціальної групи. Вони самі по собі не можуть бути ні засобом руйнування, ні засобом творення і прогресу. Їх позитивна чи негативна роль залежить від того, які соціальні сили використовуються з якою метою.

2.3. Зловмисники та порушники

Аналіз динаміки інформаційного законодавства останніх років свідчить про його активізацію в напрямку інформаційної безпеки, як провідної інституції інформаційного права. Обумовлено це загостренням негативного інформаційного впливу та відповідних загроз національній безпеці країни в інформаційному секторі з боку РФ. Саме тому чинне національне законодавство було поповнено низкою правових актів спрямованих, по задуму їх авторів, на визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації, створення розвиненого національного інформаційного простору і захист її інформаційного суверенітету.

Зазначені акти визвали певну негативну рефлексію не лише засобів масової інформації, а й фахівців (практиків та науковців), як в галузі права, так й в інших напрямах пов’язаних з законотворчим забезпеченням інформаційної сфери.

Аналізуючи Указ і рішення РНБО в частині запровадження заборони Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів з метою оцінки їх відповідності законам і Конституції, а також міжнародно-правовим зобов’язанням України, стану дотримання законності при запровадженні санкцій і введенні їх в дію, допустимості, правомірність і адекватність обмежувальних заходів, їх впливу на реалізацію

конституційних прав і свобод людини, вчений доходе висновку про їх невідповідність критеріям законності, обґрунтованості і пропорційності при обмеженні свободи інформації та необхідність їх скасування.

Так, передбачені Указом Президента «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» санкції в частині запровадження заборони Інтернет-провайдерам надання послуг з доступу користувачам мережі Інтернет до ресурсів/сервісів е відповідають не лише критеріям законності при обмеженні свободи інформації, а й технологічним можливостям.

Наприклад, доступ до популярних сервісів російського "Яндексу", відновився вже через два дні після технологічних заходів вітчизняних провайдерів, але не з того, що оператори перестали його блокувати. Це було пов’язано із технологічними маніпуляціями, організацією ряду антиблокувальних заходів у формі контр діянь – додатки Яндексу переїхали на іншу хмару і тепер живуть там (переходом із статичної на динамічну форму IP-адреси). Єдиним засобом протидії цьому і виконання вимог Закону є постійний моніторинг ситуації, що технологічно не можливо, але ж динамічна адреса міняти хоч кожний час. Фахівці Інтернет-асоціації (ИнАУ) відмічають, що "... просто через рік заблокуємо всі IP-адреси в Європі. Простіше вже відрізати Інтернет від країни. Ці догонялкі існують в усьому світі в усіх, хто підходить уводити, увести до ладу цій роботі безсистемно. Системно це теж неможливо заблокувати на 100%, але щоб воно було більш-менш ефективно, потрібно закуповувати дороге устаткування" [3].

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

Зауважимо, що блокування інформаційних ресурсів (серверів та сайтів) в Україні легалізація за рішенням суду можлива лише згідно законодавства про інтелектуальну власність у справах про порушення авторських прав, а не як ні загалом.

Але, треба визнати, що в цій ситуації багато провайдерів виконали (або як мінімум спробували виконати) припис РНБО, щоб не потрапити в опалу. Але, для того, щоб реальне заборонити доступ до іноземним сайтів, потрібне придбання устаткування для пакетного інспектування трафіку. Інакше елементарно залишається доступ через прокси-сервер.

Щодо пересічного споживача Інтернету, який не яким чином підпадає під санкції закону, та якого немає смислу контролювати до моменту скоєння ним інформаційного правопорушення, то справа простіше. Існує безліч технологій – спеціальних сервісів, через які можна підключатися до інших сайтів, що можуть бути заборонені й заблоковані. Тобто, ви можете переглядати будь-який потрібний вам сайт через сайт-посередник, не напряму. Звичайно, такі ресурси теж можна прикрити, але тоді це вже переросте в елементи неадекватної "кибервійни".

Наприклад, одним із самих популярних плагинов для більшості браузерів є Hola чи плагин Zenmate. Цей плагин безкоштовний, і дозволяє вибрати замість українського російський IP, а отже одержати доступ до будьяких російських сайтів. Програма Tor, яка є анонімною віртуальною мережею, гарантує не тільки повну анонімність, але й доступ до санкційних ресурсів. У браузері Opera вбудований "турбо-режим", який також може дати доступ до "заборонених" сайтів. А одним з найпростіших розв’язків може бути використання перекладача Google. Якщо в запиті на переклад тексту вставити потрібний сайт, то відкриється шукана сторінка, пропущена через сервер у США.

Але, не зважаючи на різного плану петиції сумлінної громади та технологічну можливість, треба визнати, що обмеження кількості їх користувачів соцмереж і глядачів "ворожих" TV-каналів обумовлене не рішеннями РНБО України та, навіть, не особистим прикладом президента країни [7], а приватним рішенням користувача – свідомого громадянина, людини з певним рівнем правової та інформаційної культури, в державі, яка прагне стати демократичною.

2.4. Висновки до розділу 2

Організовуючи інформаційну безпеку слід мати на увазі, що переважна частина загроз формується саме через його працівників, незалежно від того, чи це інформація у вигляді знань працівників, чи це інформація, що міститься в документах. Звідси важливо знати основні фактори, що обумовлюють поведінку працівників за якої вони можуть вдатись до розголошення офісної інформації. Такими факторами можна вважати об'єктивні умови за яких працівники є основним джерелом інформації. Об'єктивним є і непередбаченість, малокерованість поведінки працівників в різних ситуаціях. До того ж, прогноз це лише ймовірність, сподівання на те, що вчинки, реакції людини можуть бути саме такими як ми передбачаємо. Факторами також виступають недоліки виховання працівників, особливості їх характеру, що у свою чергу може стати мотивацією працівників до невідповідної поведінки та вчинків. Недоліки професійної підготовки працівників, особливо щодо роботи з документами та інформацією обмеженого доступу, а також такі якості, як безвідповідальність, недисциплінованість та інші негативні вади теж можуть обумовлювати розголошення інформації офісними працівниками. Як випливає із наведених особливостей офісної роботи та умов, за яких можуть виникати загрози інформації, останні обумовлюються причинами як об'єктивного так і суб'єктивного характеру. Тому побудова системи інформаційної безпеки будь-якого офісу має включати заходи спрямовані на формування безпечних умов функціонування інформації в офісі, а також заходи, що виключають або суттєво обмежують можливості неправомірної поведінки персоналу.

РОЗДІЛ 3. ВДОСКОНАЛЕННЯ СИСТЕМА БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ

3.1. Методи протидії інформаційній війні

Розгляд питань інформаційної безпеки дозволяє виділити чотири групи інформаційно-технологічних небезпек для суспільства і держави, зумовлених досягненнями науково-технічного прогресу. Першу групу пов'язують зі стрімким розвитком нової зброї інформаційного характеру, що здатна результативно впливати на людську психіку і інформаційнотехнологічні державні структури. Аналіз досліджень сьогодення в цій галузі дає змогу говорити про ефективні результати програмування, спрямованого на поведінку окремих особин, що піддаються впливу, на комп'ютерну систему банків даних

знань і інформаційні ресурси. Другою групою передбачається наявність нового вигляду правопорушень соціального спрямування, що базуються на досягненнях новітнього інформаційнотехнологічного забезпечення: махінації з операціями банку; хуліганство у комп'ютерній сфері; протизаконне копіювання технологічних рішень тощо. Як вважають провідні дослідники цієї галузі, комп'ютерні технології стають провідними знаряддями злочинів. Третьою групою є електронний контроль життя, настроїв, планів населення та організацій політичного характеру, тотальний комп'ютерний контроль за суспільством держави. Інформаційними технологіями дозволяється накопичення, зберігання і використання величезних масивів інформації про здоров’я, активність соціального плану, політичні настрої, відносини, фінансове забезпечення громадян. Четвертою групою є використання інформаційних технологічних засобів у політичній боротьбі. Підвищення впливу ЗМІ на політичні процеси, роботи владного механізму – одна з головних тенденцій розвитку суспільства у наш час.

Розвитком науково-практичної бази, що має інформаційна безпека, зумовлюються: розроблення стратегії забезпечення інформаційної безпеки держави; обґрунтовування державної політики за умови глобалізаційних інформаційних явищ, створення інформаційних мереж світового значення, бажання певних країн мати найкращий розвиток і застосовувати світовий інформаційний простір; розроблення науково-практичної бази створення і провадження державної політики у такій сфері, як інформаційна безпека; обґрунтовування пріоритетних завдань нацбезпеки, що містять довгостроковий інтерес, відповідний суспільному розвиткові.

Одна з головних передумов, що сприяє національній безпеці держави – наявність її економічного потенціалу, тобто комплекс потужностей матеріального і духовного спрямування громадськості та здатність держави задіяти ці потужності, щоб забезпечити свою безпеку. В свій час, інформацією охоплюються усі сфери функціонування людини і підвищується рівень економічного потенціалу держави, сприяючи зростанню матеріального і

духовного суспільного потенціалу, створювати передумови координації та мобілізації. Окрім цього, вона формує матеріальний і інтелектуальний ресурс країни для того, щоб забезпечити ефективний захист від агресивних в інформаційному плані країн.

З вищесказаного очевидно, що державна політика в сфері формування інформаційних ресурсів і інформатизації повинна бути спрямована на створення умов для ефективного і якісного інформаційного забезпечення рішення задач соціально-економічного розвитку країни. Серед основних напрямків державної політики в сфері інформатизації виділяють: забезпечення умов для розвитку і захисту всіх форм власності на інформаційні ресурси; формування і захист державних інформаційних ресурсів; створення і розвиток федеральних і регіональних інформаційних систем і мереж, забезпечення їхньої сумісності і взаємодії в єдиному інформаційному просторі; створення умов для якісного й ефективного інформаційного забезпечення громадян, органів державної влади, організацій і суспільних об'єднань на основі державних інформаційних ресурсів; забезпечення національної безпеки в сфері інформатизації, а також забезпечення реалізації прав громадян, організацій в умовах інформатизації; сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій, засобів їхнього забезпечення; формування і здійснення єдиної науково-технічної і промислової політики в сфері інформатизації з обліком сучасного світового рівня розвитку інформаційних технологій; підтримка проектів і програм інформатизації; створення й удосконалювання системи залучення інвестицій і механізму стимулювання розробки і реалізації проектів інформатизації; розвиток законодавства в сфері інформаційних процесів, інформатизації і захисту інформації.

Існує багато різних засобів несанкціонованого доступу до інформації. Під захистом інформації від несанкціонованого доступу розуміють діяльність із запобігання одержання інформації, яка захищається, зацікавленим суб'єктом з порушенням установлених правовими документами чи власником інформації

прав чи правил доступу до інформації, що захищається. Під системою захисту інформації зазвичай розуміють сукупність органів і виконавців, техніку захисту інформації, а також об'єкти захисту, організовані і функціонуючі за правилами, установленими відповідними правовими, організаційно-розпорядницькими і нормативними документами про захист інформації.

Вітчизняні дослідники Бондаренко В.О. та Литвиненко О.В. у загальній системі захисту інформації вирізняють такі напрями: законодавчонормативне забезпечення, яке передбачає розробку відповідних законодавчих актів, нагляд за виконанням законодавства з боку правоохоронних органів, судовий захист; організаційно-технічне забезпечення, що розкриває систему заходів, спрямованих на недопущення реалізації загроз безпеці інформаційного ресурсу; страхування інформаційних ризиків, що прийнятне лише для недержавних установ.

Якщо людина свідома, та має критичне мислення – ні одна інформаційна маніпуляція її не задіне. Тож якщо людина бачить явну маніпуляцію то вона вже не є об’єктом маніпуляції.

Проаналізуємо процес обробки інформації свідомою людиною.

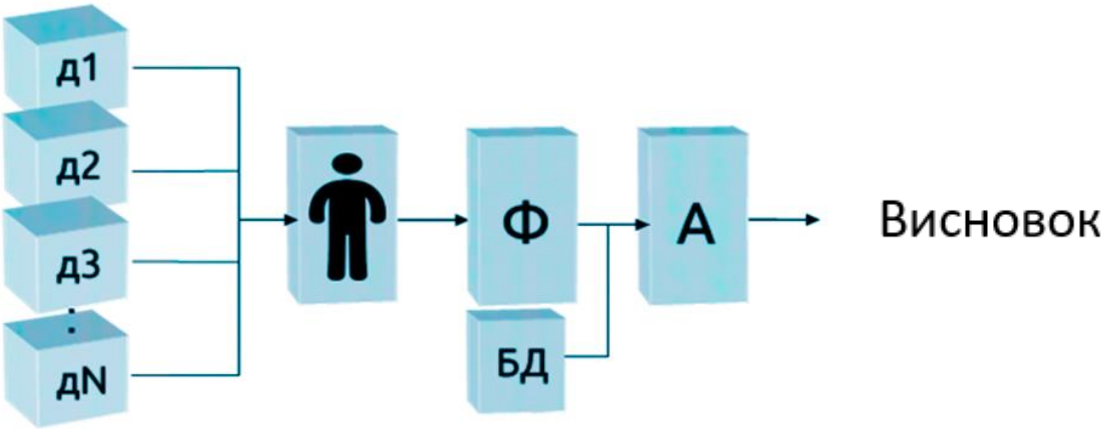

Рис. 3.1. Процес обробки інформації свідомою людиною.

де д1,д2,д3,д4 – джерела інформації;

ф – фільтр (оцінка достовірності інформації);

А – 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 тд. Однією з головних завдань є протидія цим факторам. Якщо суспільство не робить спроб до протидії, то процес обробки інформації зводиться до звичайного підсумування отриманої інформації.

Слід зразу зазначити, що ніякі окремо взяті засоби захисту не мають змоги стати запорукою адекватної безпеки. Наявність надійного захисту, що можливий тільки за умов створення механізмів комплексного забезпечення безпеки. Як правило, виділяють три головні складники такої комплексної діяльності: нормативно-правовий; технічний; засоби організації.

Нормативно-правовий інструментарій захисту визначають державні законодавчі акти, що врегульовують правила застосування, оброблення та передавання інформаційних даних, що мають обмежений доступ та визначають рівень відповідальності за їх порушування. Ст. 34 Конституції України розглядає право українських громадян на інформацію, забезпечування процесів інформаційного характеру. Ця та решта статей Конституції повинні виступати як основа розвитку законодавства інформаційної сфери. Невідповідний характер діючого законодавства України вимогам, що ставить інформаційний прогрес одна з головних проблем про захист інформації, що за наявних в державі потужних науковотехнічних ресурсів може спричинити особливо тяжкі наслідки.

Увесь комплекс технічних засобів поділяють на фізичні та апаратнопрограмні, що включають прилади електричного, механічного, електромеханічного та електронного типу. Фізичним засобам притаманне втілення як автономних пристроїв та систем, що здійснюють функції загального захисту об’єктів, які обробляють на них інформацію. Розміщення апаратних технічних засобів відбувається власне в обчислювальної техніки, в

телекомунікаційних апаратах чи в приладах, що зв’язуються з такою апаратурою стандартним інтерфейсом. Програмним засобам співвідносне поняття програмного забезпечення, що забезпечує функції захисту інформаційних даних.

Організаційні засоби захисту поділяють на ті, що мають організаційнотехнічний характер та ті, що мають організаційно-правовий, який використовують при створенні та функціонуванні будь-яких структур. Іншими словами, лише на нормативно-правовій базі та за наявністю апаратно-програмного забезпечення можливо ефективно керувати за широкого впроваджування новітніх інформаційного технологічного забезпечення. Ці питання часто недооцінюють керівники різноманітних організацій.

Розвиток законодавчих основ забезпечення інформаційної безпеки передбачає окреслення почерговості розроблення актів законодавчого і нормативно-правового характеру та механізмів практичного втілення чинної законодавчої системи.

Розроблення нормативно-правового і організаційно-методичного переліку документів містить створення документації, що регламентує: роботу в галузі інформаційної безпеки державних владних структур; взаємовідносини суб'єктів інформаційної діяльності для забезпечування інформаційної безпеки; врегулювання державними органами процесів роботи і розвитку, що здійснює ринок засобів інформації, розвиток інформаційних продуктів і послуг; інформаційних відносин в соціумі і на державному рівні, зважаючи на ринкову економіку та ін.

Правовий статус для суб'єктів інформаційної безпеки потребує забезпечення такого статусу для користувачів інформаційного і телекомунікаційного напрямку; вимагає визначити їхню відповідальність за забезпечування процедури втілення законодавчих норм і актів до суб'єктів, на які поширюється інформаційна безпека, які вчинили злочин, працюючи із закритими даними, та злочин, що передбачає застосування незахищеного засобу інформації; розробити склад злочинів, враховуючи специфіку

відповідальності карного, цивільного, адміністративного, дисциплінарного характеру.

3.2. Засоби посилення безпеки інформаційного простору в умовах інформаційної війни

Покращення організації, спрямованої на форми і методи уникнення і усунення загроз інформаційній безпеці включає: розроблення нормативноправових основ життєдіяльності системи інформаційної безпеки, розрізнення повноважень державних владних структур, що повинні забезпечувати інформаційну безпеку; розроблення моніторингової системи, що аналізує інформаційну безпеку на предмет її стану; розроблення ідей по створенню позитивних факторів, щоб подолати критичний стан промислових сфер України, у галузі, що поширюється на інформатизацію і захист інформації; аналізування техніко-економічного показника українського і іноземного програмно-технічного забезпечення, спрямованого на інформаційну безпеку і обрання ефективних напрямів розвитку українського технічного забезпечення; розроблення системи даних економічного і статистичного характеру, що показують результативність роботи, проробленої системою забезпечування такої галузі, як інформаційна безпека; досліджування критеріїв і методології оцінювання результативності інформаційної безпеки та ін.

Розвиток новітніх методів інформаційної безпеки це розробка форм і інструментів, що сприяють цивілізованому впливові держав на формування колективної свідомості суспільства і практичних рекомендацій із реалізації у практичному застосуванні; розроблення методології комплексних досліджень роботи працівників інформаційної системи, разом з тим і методів підвищування мотиваційного рівня, морально-психологічної стабільності і соціального захисту осіб, що провадять роботу із секретними і конфіденційними даними; розробка практичних рекомендацій зі збереженням і зміцненням суспільної

політичної рівноваги; забезпечення прав і свобод населення; зміцнення таких понять як законність і правопорядок методологією, що має інформаційна безпека; створення шляхів і інструментів для забезпечування органів державної влади, фірм і осіб достовірними, повними і своєчасними даними; розроблення головних діяльнісних напрямів по запобіганню негативного інформаційного впливу на настрої індивідуальної, групової і суспільної свідомості; розроблення цивілізованої, демократичної форми і методології впливу на ЗМІ; розроблення механізмів розвитку, що мають інформаційні відносини у підприємницькій сфері і зарахування інформаційних ресурсів до господарських відносин; досліджування головних методів зниження криміногенних обставин, зменшення кількості злочинів комп'ютерного характеру, насамперед, у межах кредитно-фінансової сфери; розроблення методології і практичної рекомендації із контролем над експортними операціями щодо вітчизняного наукомісткого технологічного забезпечення; обґрунтовування напрямів протистояння засобам, що вважаються інформаційною зброєю; вдосконалення видів контролювання персоналу у рамках захищених систем інформаційної сфери.

Розглянемо модель вирішеняня конфлікту двох країн (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:

$$\boldsymbol{N_1} = M_1(L_1 - N_1)[1 - \exp(-p_1(k_1\boldsymbol{N_2} - a_1N_1 + g_1))]$$

$$\boldsymbol{N_2} = M_2(L_2 - N_2)[1 - \exp(-p_2(k_2\boldsymbol{N_1} - a_2N_2 + g_2))] \qquad (3.1)$$

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;

$M_{1,}M_2$ – вартіть 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 визначать координати положень рівноваги :

а) $N_1^p = N_1^*; N_2^p = N_2^*$ б) $N_1^p = N_1^*; N_2^p = L_2$

в) $N_1^p = L_1\,; N_2^p = N_2^*$ г) $N_1^p = N_2^*; N_2^p = L_2$ (3.2)

де $\mathrm{N}_1^*, \mathrm{N}_2^*$ - 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 u1,u2 система має вигляд :

$$\boldsymbol{x_1} = M_1(\delta_1 - x_1)\big[1 - \exp\big(p_1(a_1x_1 - k_1x_2)\big)\big] + r_1^0(x_1 - x_2)$$
$$\boldsymbol{x_2} = M_2(\delta_2 - x_2)\big[1 - \exp\big(p_2(a_2x_2 - k_2x_1)\big)\big] + r_2^0(x_2 - x_1) \qquad (3.3)$$

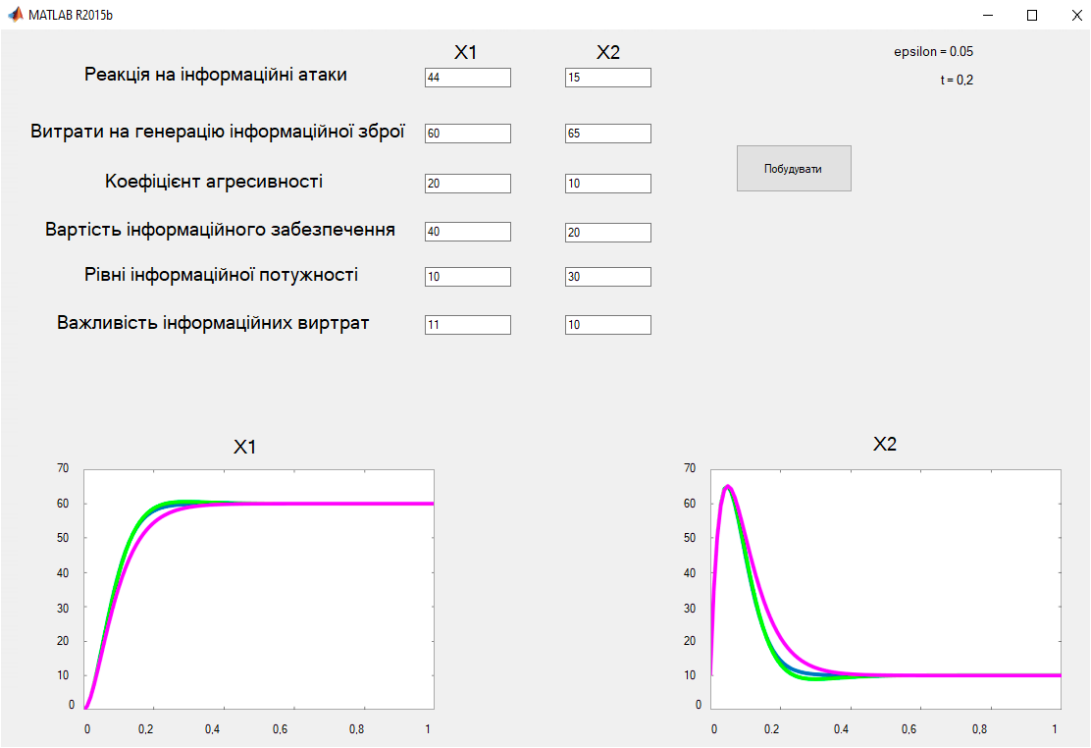

Рис. 3.2. Візуалізація моделі Річардсона.

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, слід 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 IT-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 BigData на базі штучного інтелекту.

Більш широке обгрунтування проблемних питань, пов’язаних із застосуванням BigData-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 BigData-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 [16, 7];
- проблеми забезпечення інформаційної безпеки в умовах поширення BigData-технологій (використання хакерами BigData-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).

Крім того, зауважимо, що якщо раніше компанії здійснювали управління майном, грошима, інтелектуальною власністю, то сьогодні з’явився новий актив дані, які не лише використовуються для прийняття управлінських рішень, в інтересах отримання додаткового прибутку, зокрема шляхом таргетингової реклами, але і самі стали товаром.

У той час, як розвивалася інформатизація та технології обробки значних масивів даних, роль джерел інформації перейшла смартфонам, ноутбукам, соцмережам, інтернет-покупкам, квитанціям із маркетів, банкоматам, смарт-телевізорам та ін., які надають детальні відомості щодо поглядів та поведінки їхніх власників. Тисячі складових, що становлять таку

«інформаційну мозаїку», кожного дня збираються до єдиного профілю користувача, «віртуальної» скриньки, де містяться взаємопов'язані інформаційні бази, який без відома їх власника використовують для одержання прибутків треті особи.

Якщо раніше загроза порушення права особи на недоторканність приватного життя внаслідок використання BigData-технологій розглядалась виключно у контексті дотримання норм моралі та етики, сьогодні, як засвідчили результати останніх виборів Президента США, це вже питання національної безпеки. Так, під час слухань комітету з розвідки американського сенату щодо ролі соціальних мереж при втручанні Росії у вибори 2016 року, Google, Facebook і Twitter визнали, що стали інструментом для маніпуляцій з боку спецслужб РФ [14].

В той же час, дані соціальних мереж, які використовуються BigDataалгоритмами, не такі точні, як дані з месенджерів мобільних телефонів, оскільки телефоном люди частіше говорять те, що думають та передають відомості про свої реальні дії, не усвідомлюючи цього. Як відомо, мобільні оператори, що функціонують на території України, розвивають власні месенджери (наприклад, Veon від «Київстар»), завдяки яким отримають необмежений доступ до персональних даних українських користувачів [19].

Отже, через динамічний розвиток BigData-технологій для спецслужб інших держав стануть доступними дані українських користувачів мобільними послугами, а отже й нові важелі інформаційного впливу, що є цілком реальною загрозою для вітчизняної національної безпеки. Якщо колись із цією метою використовувалися засоби масової інформації та соціальні медіа, то зараз користуються соціально-орієнтованими сервісами мобільних засобів зв'язку. Через антидержавну політику у сфері телекомунікації та зв'язку, яка велася упродовж десятиліть, нині було фактично втрачено один із елементів українського суверенітету, а Україна все ще вкрай вразлива до нових викликів в інформаційному сегменті: тими, хто розпоряджається персональними даними у

соціальних мережах є американські компанії, а даними сервісів мобільного зв'язку володіють оператори, яких контролює російська влада.

Множинність інструментів протидії інформаційним загрозам та різноманіття їх комбінацій, відповідно до особливостей цих загроз, дають змогу для того, щоб вести мову у множині щодо механізмів протидії інформаційним загрозам для національної безпеки.

Залежно від місцезнаходження джерела можливої загрози, всі загрози національній безпеці, у тому числі – інформаційні, – традиційно поділяються на дві групи: зовнішні й внутрішні. Для інформаційної безпеки того чи іншого об'єкта внутрішніми вважаються ті загрози, що «виникають безпосередньо на об'єкті та зумовлюють взаємодію між його елементами або суб'єктами», тоді як зовнішніми – ті загрози, що «виникають внаслідок його взаємодії із зовнішніми об'єктами» [9, с. 18]

Чинна Стратегія національної безпеки України серед основних загроз національній безпеці, які мають безпосереднє відношення до інформаційної сфери, визначає агресивні дії Росії, що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території, у тому числі інформаційно-психологічна війна, приниження української мови і культури, фальшування української історії, формування російськими засобами масової комунікації альтернативної до дійсності викривленої інформаційної картини світу, а також ведення інформаційної війни проти України, відсутність цілісної комунікативної політики держави, недостатній рівень медіакультури суспільства, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [1]. Необхідно зауважити, що у Стратегії відмежовуються прояви інформаційно-психологічної війни (п. 3.1), загрози кібербезпеці і безпеці інформаційних ресурсів (п. 3.7) від суто загроз інформаційній безпеці (п. 3.6), що не є доцільним.

Доктринами інформаційної безпеки держави, як і Стратегією кібербезпеки України, визначається цілий комплекс небезпек для національних інтересів та національної безпеки України у галузі інформації.

При розробці стратегій забезпечення національної безпеки також обов'язково враховується сучасний рівень впливу на суспільну свідомість за допомогою інформаційних маніпуляцій. Розвідки й контррозвідки держав використовують в інформаційному протиборстві методи дезінформації й пропаганди, намагаючись добувати секретну інформацію та дезорієнтувати супротивника хибною інформацією. Сучасні інформаційні війни спрямовуються передусім на «мішені» двох класів: по-перше, це технічні засоби супротивника (комп'ютерні мережі, інше устаткування) і, по-друге, це людські ресурси. Якщо метою атак на інформаційні системи супротивника є виведення з ладу критичних секторів життєзабезпечення держави енергетичного, оборонного, управлінського тощо, то метою другого типу атак є психологічна «обробка». Зазвичай інформаційна агресія вибудовується у три етапи: створення «ядра» (акумулювання великої кількості людей, незадоволених поточним станом речей); створення середовища (альтернативного інформаційного простору); створення атмосфери (зміна суспільної думки «точковими ударами») [10, с. 51-52; 21]. Інформаційне насильство, яке використовується в інформаційному протиборстві, характеризується як латентне, приховане, не завжди розпізнаване. В такому разі завдання держави у цих протистояннях захищати власну інформацію, свої інформаційні системи, свідомість громадськості від дій, здійснюваних супротивником та закривання доступу супротивників до даних, розкриття яких може погіршити обороноздатність держави.

Глобальній мережі Інтернет у наш час належить роль основного поля протиставлення різних сил та засобів, що вимагають новітнього забезпечення національної безпеки від загроз різного плану, що характеризуються інформаційним опосередкуванням. Разом з тим, наявність інформаційної агресивності, що транслює віртуальний простір, має суттєвий вплив на

діяльність усіх національних та міжнародних структур антитерористичного і антиекстремістського характеру. Через це система профілактичних заходів, що проводиться компетентними органами державної влади інформаційної сфери, має спрямовуватися в першу чергу на стійкість колективної свідомості громадськості перед ідеями, що чинять деструктивний вплив. Втілення зовнішніх небезпек зумовлює пошук вразливості в інформаційній структурі для доступу до головних вузлів інформаційної інфраструктури, інформаційних сховищ, організаційної мережі, осіб, що є секретоносіями та ін. До інструментів втілення зовнішніх інформаційних загроз зараховують різну «інформаційну зброю» (зараження вірусами, «хробаками», «троянами» та інші форми програмного забезпечення, яке може завдати шкоди, решта знарядь, що здійснюють інформаційний вплив).

Протидія загрозам для інформаційної безпеки нашої держави відбувається при тенденції до переформатування сфер впливу на світовий простір під час глобалізаційних процесів, що зазнають політичні, соціальноекономічні та культурні відносини. Виявлення та аналізування загроз може ускладнитися рядом чинників: відчуттям у частини громадськості відсутніх зовнішніх небезпек для країни; невизначеністю чітких потенційних зовнішніх загроз країні у межах Військової доктрини та Доктрини інформаційної безпеки, що веде до відсутньої чіткої класифікації і ранжування небезпек за важливістю й порівняльною динамікою їх збільшення; відсутністю усвідомлення причин і умов появи подібних небезпек та ін.

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:

-мета системи безпеки

-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 самовідтворюватися.

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.

Механізмами протидії інформаційним загрозам зовнішніх джерел передбачається нагальна потреба організації багаторівневого і різноспрямованого комплексу заходів, що враховувати, в першу чергу, специфіку зовнішніх чинників (конфігурація геополітичної, регіональної кон'юнктури, структурна функціональна роль держави та вплив транснаціональних організованих злочинних угрупувань).

Таким чином, особливе значення надається моніторингу характеру, специфіки, масштабу небезпек та їх подальшому прогнозуванню. Прогнозування – важливий і самостійний елемент, який належить до профілактичних мір щодо інформаційних небезпек зовнішніх джерел та забезпечення національної безпеки. Основний метод прогнозування моделювання, головні принципи якого – встановити мету моделі; виділити обмежену кількість головних чинників істотних змін досліджуваної системи; визначити характер взаємних зв'язків між цими чинниками; встановити принцип множинності зв'язків між чинниками і виділити сутнісні зв'язки, що є визначниками характеру прогресу системи та її змін.

Система стратегічних знань, отриманих через результати прогнозування, дає змогу проілюструвати модель прогресу середовища, що досліджується, та обґрунтувати особливості змісту складників їх структури. Для моніторингу, прогнозування і профілактичних заходів щодо небезпек придатне будь-яке

середовище, що має зовнішні джерела, які здатні продукувати та відтворювати загрози для особистісної, суспільної і державної інформаційної безпеки.

Слід взяти до уваги застарілість звичних технологій та механізмів протидії зовнішнім небезпекам для національної безпеки та вихід на перший план нових способів, що сприяють розгортанню загроз та зведенню до мінімуму ризиків, що виникають внаслідок них. Це пов'язано зі стрімким розвитком українського суспільства, що носить інформаційний характер та теж сприяє вдосконаленню способів проведення інформаційної війни.

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: нормативноправових, 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, співдія у межах ОБСЄ, механізми по зміцненню та розвитку у межах інших угрупувань 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.

Очевидною є спроможність механізмів боротьби з інформаційними загрозами до видозмінення, адже конкретні механізми створюють зразу з визначенням наявних загроз і сформульованою стратегічною метою по їх усуненню. Варто зважати і на те, що умови сьогодення зумовлюють умовність розподілу інформаційних небезпек на небезпеки внутрішнього й зовнішнього типу. Комплексність інформаційних загроз зумовлює те, що замахи на зовнішню систему безпеки держави спричиняють формування загроз для

внутрішньої безпеки, а це викликає внутрішню дестабілізацію та, врешті, веде до зовнішньої вразливості країни.

Слід також враховувати, що загрози, передусім зовнішні, належать до сторонніх щодо системи забезпечення безпеки факторів, а відтак, неможливо не лише досягти стану їх абсолютної відсутності, але і скласти вичерпний перелік, адже вони змінюються в умовах мінливого середовища. То ж у сучасному світі відбувається зміщення акцентів із загроз на ризики, оскільки такий підхід дозволяє відходити від розуміння загроз як констант та застосовувати різнопланові підходи для унеможливлення їх розгортання, особливо за умов невизначеності. Відповідно, механізми протидії інформаційним загрозам зовнішніх джерел, які базуються на принципах управління ризиками, і передбачають процес прийняття та виконання управлінських рішень, спрямованих на зниження вірогідності виникнення несприятливих наслідків та мінімізацію можливої шкоди, викликаної реалізацією загроз, за сучасних умов є найбільш перспективними і результативними. Відповідні механізми дозволяють впливати передусім на керовані елементи (ризики), досягаючи значних для забезпечення її прийнятного стану результатів шляхом застосування відносно незначних зусиль, а також успішно поєднувати профілактичні та оперативні методи протидії інформаційним загрозам.

Механізмами протидії інформаційним загрозам вважають комплекс різних форм роботи, що здійснюються органами державного та військового управління, громадськими організаціями, політичними інститутами та ін., види їхньої взаємодії, що дозволяють здійснювати оперативний вплив на загрози для інформаційної безпеки або керувати ризиками, що ними зумовлюються задля локалізаційного впливу на них і їх нейтралізації. Конкретним механізмам протидії інформаційним загрозам притаманне формування з орієнтиром на систему тих загроз, що є реальними, та тих, що є потенційними і, ймовірність їхнього виникнення, враховуючи цикл розвитку системи (процеси зародження, формування, зрілості, трансформації) і її конкретний стан (процеси кризи, депресії, підйому), зважаючи на наявні фінансові, матеріальні, кадрові

можливості держави, на баланс суспільних зацікавлень, державних, групових, та особистісних. Оцінку механізмів провадять опираючись на: інформаційну державну політику, її вплив на характеристики безпеки; виявлення відхилень характеристик для стабільної роботи, що провадиться системою інформаційної безпеки; визначення зовнішніх умов, що сприяють таким відхиленням, як зростання (за несприятливого зовнішньоекономічного середовища) або зменшення (за сприятливого зовнішнього середовища) небезпек. Отже, механізмами протидії загрозам інформаційного характеру, передусім, в основі яких лежать принципи керування ризиками, дають змогу блокувати деструктивні елементи, властивості, процеси, що є руйнівниками системи інформаційної безпеки та національної безпеки загалом, і можливість стимулювання конструктивних елементів, властивостей, процесів, які покращують їх функціонування та розвиток.

Усе це дає змогу підсумувати, що достатній рівень інформаційної безпеки може забезпечити цілий комплекс заходів політичного, економічного, організаційного характеру тощо, що дають змогу реалізувати інформаційні права та інтереси країни і її суб’єктів.

Дослідження питань державної інформаційної безпеки дає змогу говорити, що забезпечення інформаційної безпеки базується на інформаційній організації країни. Ця організація має надавати гарантію інформаційної безпеки держави та її суб’єктів під час глобалізаційних процесів та підвищення такої загрози, як міжнародний тероризм. На жаль, Україна має дуже багато чинників, які стають перешкодами при створенні такої інформаційної організації, тут відіграє не останню роль неузгодження роботи державних владних органів щодо забезпечення інформаційної безпеки.

3.3. Інструменти виявлення втручань в інформаційних простір

Інструменти виявлення втручаль лежать в інформативній та соціалогічній площині. Розглянемо найбільш інформативні з них.

Моніторинг засобів масової інформації найбільш швидкий та найменш затратний засіб вивчення громадської думки та відстеження зворотного зв'язку в рамках комунікаційного процесу. Здійснюючи силами профільного структурного підрозділу або сторонніх фахівців регулярний аналіз мас-медійних матеріалів, можна виявляти певні тенденції ретроспективного та перспективного спрямування. Це дозволяє або передбачати майбутні наслідки певних сьогоднішніх дій, або виявляти причинно-наслідкові тенденції, що призвели до тих, чи інших ситуацій або фактів, які мають місце нині. Цей напрямок роботи можна вважати первинною аналітикою, матеріали якої дають можливість зрозуміти певні процеси в цілому, виявити окремі загрозливі або позитивні тенденції.

Моніторинг-копія – комплектується зі скопійованих версій друкованих видань, роздрукованих фрагментів інформаційних стрічок, матеріалів інтернет-видань, теле- та радіо сюжетів. При цьому на кожній роздруківці дається посилання на видання, з якого цей матеріал взято, дату, номер, сторінку, або інтернет-адреси зазначених матеріалів.

Контент-аналіз матеріалів ЗМІ. За матеріалами моніторингу, не частіше ніж раз на тиждень, але не рідше ніж раз на місяць, проводиться змістовний аналіз зібраних матеріалів з метою переведення якісних показників та характеристик у кількісні.

Засоби експрес-опитування в соціальних мережах

За допомогою соціальних онлайн мереж можна проводити типові соціологічні дослідження і перш за все опитування громадської думки. Порівняно з класичними соціологічними дослідженнями результати опитування в соціальних мережах мають більш значну статистичну похибку. Це відбувається через те, що поле є нестабільним (опитування іноді видаляють або не дають дозвіл на розміщення в групах, вибірка по групах не завжди репрезентативна та ін.). Втім, отримані результати доволі чітко віддзеркалюють загальні тенденції, в територіальному розрізі або в контексті конкретних цільових груп.

Для проведення дослідження думки представників цільових груп можна скористатися відповідними власними сервісами провідних соціальних мереж або міжмережевими сервісами.

В переважній більшості власних сервісів анкета опитування налаштовується в шаблонному блоці для створення посту.

Схема створення анкети проста і формується автоматично. Від розробника вимагається лише поставити тему та головне питання із варіантами відповіді.

При розробці блока опитування бажано додавати певне візуальне супроводження – картинка або ролик, які допомагають швидше зрозуміти сутність опитування та привертають до нього увагу.

Для полегшення завдання підготовки та проведення опитування у соціальних мережах існують відповідні сервісні програми:

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

Сучасний стан розвитку соціальних мережевих технологій потребує постійного вдосконалення методів моніторингу та оцінки ефективності соціальних комунікацій. А це означає, що автор інформаційного повідомлення обов’язково має отримати інформацію не тільки про кількість «лайків» та зміст коментарів, але й зрозуміти загальні тенденції уподобань його цільових груп та передбачити характер їх подальшого розвитку. Розв’язати зазначене питання може профільна інтегрована методика – комплексне застосування якісних та кількісних характеристик шляхом використання окремих інструментів моніторингу, контент-аналізу та систематизації профільних даних. Такою є методика SMM-аудиту.

Зазначена методика базується на механізмах моніторингу контенту та його змістовного аналізу. При цьому схема реалізації завдань у контексті методики є гнучкою. Збирання матеріалів для дослідження може здійснюватися

або в автоматичному режимі (відповідні інтернет-сервіси) або засобом прямого збирання та сегментації контенту в ручному режимі.

Мета дослідження в рамках SMM-аудиту - виявлення ефективності розповсюдження в певній зоні Інтернет інформації про досліджувану структуру.

Головними завданнями аудиту є:

Розробка базового інструментарію та методології проведення комплексного поглибленого дослідження та систематичного моніторингу інформаційної активності досліджуваного об’єкта в мережі Інтернет;

Формування цільових баз даних щодо поширення інформації про діяльність об’єкта в мережі Інтернет;

Проведення комплексного дослідження щодо ефективності інформаційної політики об’єкта в мережі Інтернет у рамках певного хронологічного заміру (не менше ніж 6 місяців).

Методологічною основою дослідження є технологія інформаційного діагностування ефективності процесів промоції діяльності організації в мережі Інтернет.

Методика проведення роботи. Комплексне моніторингове дослідження проводилося на основі профільних баз даних, що репрезентують цільові групи досліджуваного об’єкта в мережі Інтернет. Процедура здійснюється в форматі трьох рівнів моніторингового дослідження. Загальна процедура роботи передбачала підготовчий та чотири робочі послідовні етапи.

На підготовчому етапі формуються бази даних по профільних веб-ресурсах, що відповідають цільовим групам об’єкта в мережі Internet. Серед них можуть бути:

Соціальні мережі, в яких можуть бути розміщені матеріали або згадування про діяльність об’єкта.

Засоби масової інформації, зокрема сайти газет, журналів, інтернет-видань, телеканалів, радіостанцій.

Сайти профільних організацій у досліджуваній галузі.

Інформаційно-довідкові портали за профілем діяльності об’єкта або близькою тематикою.

Веб-портали центральних та місцевих органів державної влади та самоврядування.

Корпоративні сайти громадських організацій, що працюють у полі діяльності об’єкта, а також профільних проектів за міжнародними програмами.

Веб-сайти політичних об’єднань та громадських рухів, що мають певний вплив на загальну громадсько-політичну ситуацію в країні.

Особисті веб-сторінки публічних осіб (політики, громадські діячі, чиновники), що мають пряме або опосередковане відношення до тематики діяльності об’єкта.

Моніторинг та ідентифікація достовірності контенту в мережі Інтернет та соціальних онлайн мережах

В умовах сучасної інформаційної війни одним з головних завдань у роботі з контентом є його ідентифікація та встановлення походження текстової інформації, відео та графіки.

Як свідчить практика, за умови необхідності підтримки інформаційного потоку високої щільності, не завжди вистачає реального матеріалу. Тому при формуванні контенту атакуюча сторона може залучати чужі відео, графічні та текстові матеріали. Особливо показовою в цьому плані була російська інформаційна агресія проти України, що відбувалася протягом 2014-2015 рр. Російські медіа неодноразово ловили на підробках, розкриваючи фейки, особливо, коли мова йшла про чисельні жертви від артобстрілів серед мирного населення або певні ситуативні події.

Технічно розкрити фальшування не складно. Для цього можна використати певні сервіси пошукових систем, зокрема у Google або Yandex або застосувавши окремні програмні продукти.

Найбільш популярним на сьогодні серед провідних пошукових систем є Google, який пропонує такі методи ідентифікації контенту.

Для перевірки автентичності тексту можна використати такі методи [3]:

Внести пошуковий запит (цитата, ключові слова) у лапки «...» та задати пошук – програма шукатиме сторінки зі вказаною формою слова, без зайвої інформації та реклами.

У разі, коли в цитаті відсутнє слово або кілька слів, необхідно взятии в лапки всю цитату, а відсутню частину замінити на зірочку «*» - програма шукатиме повну версію.

Коли необхідно шукати контент у певному місці, то можна застосувати такі символи:

inurl - для пошуку всередині URL;

intitle - у заголовку;

intext - у тексті;

inanchor - у тексті посилань.

У разі, коли необхідно дізнатися, хто посилався на конкретний матеріал, необхідно використати оператор link. Останній необхідно поставити разом із двокрапкою перед URL, який є пошуковим.

5. Якщо контент, який розшукується, неможливо знайти за прямою адресою, необхідно шукати в кеші. В такому разі необхідно звернутися до http://cachedview.com. Google обов’язково зберігає інформацію про сайт та його зміст на певний момент.

Пошук та ідентифікація фото передбачає дещо складнішу процедуру, втім розвінчання таких фейків дає найбільш значний ефект та максимально сприяє процесам контрпропаганди.

В якості такого прикладу можна навести результати роботи Джулії Девіс із американського видання Examener.com, яка розвінчувала кремлівські фейки, що базувалися на чужих фото. Типовими були ілюстрації з «подій в Донбасі», для яких використовували фото з Боснії, Китаю, Саудівської Аравії, Африки, самої Росії й навіть іноді з художніх фільмів.

3.4. Висновки до розділу 3

Таким чином, науковий аналіз ряду проблемних питань щодо розробки та втілення державної політики в інформаційній сфері, сьогодні має особливе значення, адже їх розв’язання дасть змогу для розвитку суспільства, що має інформаційний характер і, у такий спосіб забезпечить національну та інформаційну безпеку України. Серед загроз інформаційній безпеці виділено наступні: монополізація інформаційної сфери національними та зарубіжними олігархічними структурами; блокування роботи державних ЗМІ щодо поінформування українського і закордонного населення; дефіцит професійних кадрів; неефективність механізмів забезпечення формування і реалізації державної політики інформаційної безпеки; несанкціонований доступ до інформації; негативний вплив на інформаційні ресурси та в цілому на інформаційну інфраструктуру; недостатність поінформованості населення за кордоном про ведення зовнішньополітичної та внутрішньополітичної діяльності країни; поширювання неправдивої інформації про ведення зовнішньої та внутрішньої політики України; вплив інформаційного характеру, що здійснюють 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 межах інформаційної сфери за кордоном.

ВИСНОВКИ

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 конфліктучих 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&sectionid=8&id=129&Itemid=44

2. Пропаганда [Електронний ресурс] / Матеріал з Вікіпедії — вільної енциклопедії. – [Електронний ресурс]: http://uk.wikipedia.org/wiki/Пропаганда

3. Слісаренко, І.Ю. Відмінне і спільне між паблік рилейшнз і пропагандою [Електронний ресурс]. – [Електронний ресурс]: http://www.pravo.vuzlib.su/book_z426_page_5.html

1. 4. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції: Ýнавч. посіб._ / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. Ę К.: КНТ, 2006. Ę 280 с.

2. 5. Про інформацію (Україна), 2 жовтня 1992, № 2657-XII. Актуально на 01.04.2018. [Електронний ресурс]: http://zakon3.rada.gov.ua/laws/show/2657-12.

6. Абанкина, Т.В. PR некоммерческой организации: теоретические основы современных PRтехнологий [Текст] / Т.В. Абанкина // Музей будущего: информационный менеджмент: сб. ст. / сост. А.В. Лебедев. – М.: Прогресс-Традиция, 2001. – С.168–191.

3. 7. 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.

8. ІНФОРМАЦІЙНІ ВІЙНИ [Електронний ресурс] / Режим доступу: http://pidruchniki.com/18000102/ politologiya/informatsiyni_viyni

9. Почепцов, Г.Г. Інформаційно-психологічна війна [Текст] / Г.Г. Почепцов. – М: Сінтег, 2000. – 180 с.

10. Завадський, І.І. Інформаційна війна – що це таке? [Текст] / І.І. Завадський // Захист інформації.

«Конфідент». – № 4, 1996.

11. Горкіна, М. PR на 100%. Як стати хорошим менеджером по PR [Текст] / М. Горкіна, А. Мамонтов, І. Манн. – М: Альпіна Бізнес Букс, 2009. – 248 с.

12. Лисичкин, В.А. Третья мировая информационно-психологическая война [Електронний ресурс] / В. Лисичкин, Л. Шелепин. – М: Академия социальных наук, 1999. – [Електронний ресурс]: http://www.duel.ru/publish/lisichkin/voina.html.

13. Україна у системі міжнародної безпеки: Ўмонографія_ / ЎЯ. Б. Базилюк, 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. Ę К.: Фоліант: Стилос, 2009. Ę 572 с.

14. Остроухов, В.В. Інформаційна безпека [Електронний ресурс].– [Електронний ресурс]: http://westudents.com.ua/glavy/51894-12-nformatsyna-vyna-yak-forma-vedennya-nformatsynogoprotiborstva.html

15. 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.

16. Малик Я. Інформаційна війна і Україна / Я.Малик // Демократичне врядування. 2015. Вип. 15. [Електронний ресурс]: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3.

17. Носов В. Манжай О. Оремі 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.