МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально–науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
доктор економічних наук, доцент	доктор економічних наук, доцент
_____ С.В.Легомінова	_____ С.В.Легомінова
«___»_____20__ р.	«___»_____20__ р.

ДИПЛОМНА РОБОТА

на тему:

СОЦІАЛЬНІ МЕРЕЖІ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

СТУДЕНТ**:** Стародубець Владислав Олександрович _____
(підпис)

НАУКОВИЙ КЕРІВНИК: к.т.н. Рабчун Дмитро Ігорович _____
(підпис)

НОРМОКОНТРОЛЕР: к.т.н., с.н.с. Щебланін Юрій Миколайович _____
(підпис)

Київ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально–науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Освітньо–кваліфікаційних рівень – бакалавр

Спеціальність «Кібербезпека»

Спеціалізація «Управління інформаційною безпекою»

«ЗАТВЕРДЖУЮ»

Завідувач кафедри УІКБ

_____ С.В.Легомінова

(підпис)

«___» _____ 2020 р.

ЗАВДАННЯ

на дипломну роботу

студенту Стародубцю Владиславу Олександровичу

1. Тема роботи «Соціальні мережі як інструмент інформаційних операцій», затверджена наказом по університету від «16» березня 2020 р. № 81.

2. Термін здачі студентом оформленої роботи «5» червня 2020 р.

3. Об'єкт дослідження: система інформаційної безпеки держави.

4. Предмет дослідження: методи проведення інформаційних операцій через системи масових комунікацій.

5. Мета дослідження: визначити шляхи вдосконалення процесів протистояння інформаційним операціям в соціальних мережах.

6. Перелік питань, які мають бути розроблені:

1. Вивчення історії розвитку досліджень політичних комунікацій як інструменту інформаційних операцій.
2. Дослідити соціальні мережі в системі інформаційних операцій.
3. Визначити шляхи щодо виявлення потенційно небезпечних повідомлень в соціальних мережах.

7. Дата видачі завдання «24» березня 2020 р.

КАЛЕНДАРНИЙ ПЛАН
виконання дипломної роботи
студентом Стародубцем Владиславом Олександровичем

Дата видачі завдання: «24» березня 2020 р.

№ з/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	09.03.2020	
2.	Збір та аналіз літератури.	30.03.2020	
3.	Вивчення історії розвитку досліджень політичних комунікацій як інструменту інформаційних операцій.	16.04.2020	
4.	Дослідження соціальних мереж в системі інформаційних операцій.	30.04.2020	
5.	Визначення шляхів щодо виявлення потенційно небезпечних повідомлень в соціальних мережах.	15.05.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	22.05.2020	
7.	Оформлення роботи.	29.05.2020	
8.	Оформлення презентації.	05.06.2020	
9.	Отримання рецензії на роботу.	08.06.2020	
10.	Захист в ДЕК.	10.06.2020	

Студент: Стародубець Владислав Олександрович

_____
(підпис)

Науковий керівник: Рабчун Дмитро Ігорович

_____
(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню особливостей соціальних мереж як інструменту інформаційних операцій. Робота складається зі вступу, трьох розділів, що містять 5 рисунків та 1 таблицю, висновків до кожного розділу, загальних висновків, списку використаних джерел із 44 найменувань. Загальний обсяг роботи становить 89 аркушів, з яких 4 аркуші займає список використаних джерел.

Об’єкт дослідження – система інформаційної безпеки держави.

Предмет дослідження – методи проведення інформаційних операцій через системи масових комунікацій.

Мета дослідження – визначити шляхи вдосконалення процесів протистояння інформаційним операціям в соціальних мережах.

У дипломній роботі на основі вивчення та аналізу відповідних джерел визначимо основні особливості соціальних мереж, дослідимо засоби та методи інформаційних операцій в соціальних мережах в різних країнах світу та запропонуємо основні засоби захисту для збереження персональних даних в соціальних мережах, як одного з інструментів сучасних інформаційних операцій.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою держави у контексті протидії загрозам, пов’язаним із веденням інформаційної війни в соціальних мережах.

Ключові слова: СОЦІАЛЬНІ МЕРЕЖІ,СПАМ, ІНФОРМАЦІЙНА ОПЕРАЦІЯ, ІНФОРМАЦІЙНА ВІЙНА, ІНФОРМАЦІЙНІ ОПЕРАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ.

ЗМІСТ

ВСТУП

Актуальність теми. Актуальність і своєчасність звернення до даного питання обумовлена тим, що, по-перше, на сьогодні Інтернет, як форма подання і поширення інформації використовується переважною більшістю населення різного віку і соціального стану; по-друге, інформація, поширювана в Інтернеті, як правило доходить до цільової аудиторії без необхідної «фільтрації» з боку державних органів, що дозволяє її розповсюджувачам практично безконтрольно реалізовувати відомості протиправного характеру; по-третє, вітчизняна правова система ще не виробила завершений правовий механізм, який регулює правовідносини у віртуальному просторі.

Зворотною стороною стрімкого розвитку соціальних мереж є те, що вони неминуче стають об'єктами та засобами інформаційного управління, а також ареною інформаційного протиборства. Соціальні мережі сьогодні – один з ключових і найбільш ефективних інструментів інформаційного впливу, в тому числі засіб для маніпулювання особистістю, соціальними групами та суспільством в цілому. Не дивно, що вони все частіше використовуються в якості майданчику для ведення інформаційних війн.

Що таке Інтернет для сучасного суспільства? Соціальні мережі – повноцінне спілкування і його невід'ємні атрибути: дружба, сварки, віртуальна любов, загрози. Мережа – клуб за інтересами, «круглий стіл» для обговорення питань, починаючи від варіантів підгузників для дитини і закінчуючи політичними дебатами.

Інтернет – потужний маніпулятор людської свідомості. Нічого не варто "загуглити" в мережі інформацію про супротивників або прихильників будь-якої партії, угруповання. Чи не замислювалися ви про те, що всі ваші дані зберігаються в системі, яку можуть розкрити в будь-яку хвилину?

Таким чином, на основі вивчення та аналізу відповідних джерел визначимо основні особливості соціальних мереж, дослідимо засоби та методи інформаційних операцій в соціальних мережах в різних країнах світу та

запропонуємо основні засоби захисту для збереження персональних даних в соціальних мережах, як одного з інструментів сучасних інформаційних операцій.

Мета і завдання дослідження. **Мета роботи** визначити шляхи вдосконалення процесів протистояння інформаційним операціям в соціальних мережах.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Вивчення історії розвитку досліджень політичних комунікацій як інструменту інформаційних операцій.
2. Дослідити соціальні мережі в системі інформаційних операцій.
3. Визначити шляхи щодо виявлення потенційно небезпечних повідомлень в соціальних мережах.

Об'єкт дослідження – система інформаційної безпеки держави**.**

Предмет дослідження – методи проведення інформаційних операцій через системи масових комунікацій.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи теоретичного аналізу літератури, методи аналізу, синтезу та порівняння, соціологічні методи.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації комплексу заходів з захисту персональних даних в соціальних мережах.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу захистити користувачів та їх дані в системах масових комунікацій та дати для користувачів розуміння важливості всіх даних залишених в віртуальному просторі.

РОЗДІЛ 1. ІСТОРІЯ РОЗВИТКУ ДОСЛІДЖЕНЬ ПОЛІТИЧНИХ КОМУНІКАЦІЙ ЯК ІНСТРУМЕНТУ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

1.1.Особливості політичного впливу в умовах інформаційної війни

Ще за п'ять століть до н.е. китайський стратег Сунь Цзи визначав інформацію, як основу війни.

Сьогодні, в епоху глобалізації, в світі створено єдиний глобальний інформаційний простір всієї планети, в якому розгорнулося геостратегічне інформаційне протиборство між провідними країнами світу за досягнення переваги в світовому інформаційному просторі.

У такій ситуації людина щодня піддається інформаційним атакам відкритим або замаскованим.

Вчені впевнені, що "інформаційний вплив на громадян, що реалізується через засоби масової інформації та комунікації, потенційно здатний створити атмосферу напруженості та політичної нестабільності в суспільстві, спровокувати соціальні, національні, релігійні конфлікти, масові заворушення, привести до руйнівних наслідків для політичного розвитку країни». Їхня думка не раз підтверджувалась історичними прикладами. Часом інформаційні атаки надають набагато більш руйнівний ефект, аніж силові.

Вважається, що вперше в історії воєн психологічну операцію як частину єдиного плану бойових дій здійснив в 1779 році А.В. Суворов. Він наказував своїм військам «при ударах робити великий шум і міцно бити в барабани».

Сьогодні ж ми все частіше чуємо термін «інформаційна війна». І зараз це куди більш складна система технологій і методів інформаційного протиборства, яка дуже швидко розвивається, ніж за часів великого полководця.

Ще в минулому столітті в ході ведення звичайної війни використовували деякі приймання інформаційного протиборства: радіоелектронну боротьбу, вогневе придушення елементів інфраструктури супротивника, перехоплення інформаційних повідомлень противника, поширення дезінформації та ін.

Сьогодні, в епоху інформаційних технологій використовуються більш мудрі підходи:

- створення атмосфери бездуховності й аморальності, негативного ставлення до культурної спадщини супротивника;
- маніпулювання суспільною свідомістю і політичною орієнтацією соціальних груп населення країни з метою створення політичної напруженості та хаосу;
- дестабілізація політичних відносин між партіями, об'єднаннями та рухами з метою провокації конфліктів, розпалювання недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції, провокація взаємознищення;
- зниження рівня інформаційного забезпечення органів влади та управління, інспірування помилкових управлінських рішень;
- дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління;
- провокування соціальних, політичних національних і релігійних зіткнень;
- ініціювання страйків, масових заворушень та інших акцій економічного протесту;
- ускладнення прийняття органами управління важливих рішень;
- підрив міжнародного авторитету держави, його співпраці з іншими країнами;
- нанесення шкоди життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах.

Сучасний етап розвитку інформаційного протиборства почався з появи персональних комп'ютерів і відкритих телекомунікаційних мереж (ВІТМ – відкрита інформаційно-телекомунікаційна мережа.)

Основним носієм інформації стали виступати комп'ютери, а найважливішим засобом доведення інформації - телекомунікаційні мережі.

Сьогодні «Інформаційні війни» розглядають як самостійне явище політичного життя суспільства, яке не обов'язково супроводжується відкритими збройними зіткненнями. У цій частині розділу розглянемо що ж мають на увазі вчені, вживаючи термін «інформаційна війна», ознайомимося з основними принципами й технологіями її ведення.

Інформаційна війна з'явилася як форма інформаційного протиборства, і в цьому відношенні вона є продуктом розвитку суспільства, який зібрав весь досвід, котрий накопичило людство в ході даного протиборства.

Сучасному поняттю «інформаційна війна» (ІВ) існує безліч визначень.

А.В. Манойло у своїй монографії пропонує розділити це різноманіття на три групи.

Автори першої групи зводять поняття ІВ до окремих інформаційних заходів та операцій, інформаційних способів і засобів корпоративної конкуренції або ведення міждержавного протиборства або збройної боротьби. Найбільш відомим прихильником цієї групи він називає Г.Г. Почепцова. Наводить автор із визначення С.П. Расторгуєва: «відкриті й приховані цілеспрямовані інформаційні впливи інформаційних систем один на одного з метою отримання певного виграшу в матеріальній сфері».

Автори другої групи – в основному, представники військових відомств, як закордонних, так і українських, - відносять ІВ до сфери військового протиборства. ІВ розглядається ними як особливий вид військових дій, що носять маніпулятивний або руйнівний характер.

Автори третьої групи визначень вважають, що вона є таким собі несиловим засобом вирішення зовнішньополітичних завдань, в той час, як видимих силових дій сторонами не робиться.

До вчених цієї групи дослідник відносить таких дослідників, як Г.В. Ємельянов і А.А. Стрільців, які стверджують: «Під інформаційною війною розуміється особливий вид відносин між державами, при якому для вирішення, що існує міждержавне сперечання використовуються методи, засоби й технології силового впливу на інформаційну сферу цих держав».

Фахівці МЗС України під інформаційною війною розуміють «протиборство між державами в інформаційному просторі з метою нанесення збитку інформаційним системам, процесам і ресурсам, критично важливим структурам, підриву політичної, економічної й соціальної систем, а також масованої психологічної обробки населення з метою дестабілізації суспільства і держави».

Засобами, методами й способами ІВ в українських авторів є або інформація, або інформаційні впливи, які інформаційні технології. В.А. Лисичкін і Л.А. Шелепін вважають, що інформаційна війна – це війна «якісно нового типу, де зброєю базується на інформації, а боротьба ведеться за цілеспрямовану зміну суспільної свідомості». При цьому Г.В. Ємельянов, А.А. Стрільців, В.Ф. Прокоф'єв, В.В. Серебряніков, І. Цибульський, А. Крутских, А. Федоров і фахівці МЗС України абсолютно вірно вказують на насильницький характер дій в ході ІВ, який є необхідним обов'язковою ознакою війни в період відсутності відкритого збройного конфлікту.

Цілями ІВ називаються досить близькі положення:

- нав'язування необхідного для впливу рішення;
- нав'язування противнику своїх духовно-моральних і культурологічних цінностей в заміну військових дій;
- встановлення контролю над діями супротивника і напрям його діяльності у вигідному річищі;
- цілеспрямований вплив на супротивника через свою і його інформаційну інфраструктуру;
- гуманітарне поневолення;
- нав'язування протиборчої сторони своєї політичної волі.

Психологічна війна між політичними противниками властива не тільки для зовнішньополітичної сфери, а й активно використовується у внутрішньополітичній діяльності.

І.М. Панарін визначає інформаційну боротьбу, як «форму боротьби сторін, що становить собою використання спеціальних методів, способів і засобів для впливу на інформаційне середовище протилежної сторони й захисту власної в інтересах досягнення поставлених цілей». Воно, на наш погляд, є найбільш загальним.

Слідом за цим дослідником виділимо три складові частини інформаційної боротьби в політичній сфері:

- Стратегічний політичний аналіз.
- Інформаційний вплив.
- Інформаційна протидія.

Боротьба ведеться на трьох рівнях: стратегічному, оперативному, тактичному.

Однією з головних передумов ведення ефективної інформаційно-психологічної війни є розробка державної інформаційної політики.

Мабуть, усвідомлення цього факту і призвело до того, що на різних рівнях все частіше піднімається питання розробки ідеології.

Схематично модель інформаційної війни повинна базуватися на наступних складових:

1. Багатоцільовий об'єкт для подальшого комунікативного резонансу: в якому порушені інтереси великого числа різнорідних соціальних груп, що в результаті створює можливість для їх об'єднання.

2. В якості «динаміки» для масової свідомості використовується однорідна група населення, яка не має чіткої залежності від теперішньої влади, наприклад, студенти, шахтарі, пенсіонери.

3. Опосередкованість мети: як правило, вал критики не йде на владу прямо, а тільки побічно, з цієї причини влада не може не підтримати народне волевиявлення, яке в результаті направляється на іншу мету.

4. Усний канал: через блокування в ряді випадків офіційних каналів комунікації поширення інформації йде за усними каналами.

5. Стимуляція обговорення: завданням стає також підбір таких ключових повідомлень, які б стимулювали обговорення ситуації в цільових групах населення. Можливий і варіант анекдоту або слуху, який сам виходить на подальше поширення. При цьому обговорення є вигідним для комунікатора феноменом, оскільки в результаті відбувається явище групової поляризації.

6. Багатоканальний вплив: аудиторія отримує повідомлення одного типу по безлічі каналів.

7. Опора на вже наявній: однорідна група (студентство, шахтарі, пенсіонери) цікава також тим, що вона має готові соціальні та інформаційні мережі, куди входять її представники.

Бо об'єктом впливу в інформаційній війні є людська психіка, психологія груп і цілих товариств, а основним засобом впливу – інформація, саме цьому феномен іноді має іншу назву – інформаційно-психологічна війна.

Отже, основний метод «атаки» – інформаційно-психологічний вплив.

Тепер розшифруємо наведені поняття. Вплив – дія, спрямована на кого-небудь з метою домогтися чого-небудь, вселити що-небудь.

Інформаційно-психологічний вплив являє собою «цілеспрямоване виробництво і розповсюдження спеціальної інформації, яка надає безпосередній вплив на функціонування і розвиток інформаційно-психологічного середовища суспільства, психіку і поведінку політичної еліти й населення держави».

Об'єктами впливу можуть бути: психіка людей, інформаційно-технічні системи різного масштабу і призначення, система формування, поширення і використання інформаційних ресурсів, система формування суспільної свідомості (за допомогою пропаганди й ЗМІ), система формування і функціонування громадської думки, система прийняття рішень.

У тому випадку, якщо об'єктом атаки є психіка людини – відбувається інформаційно психологічна боротьба, якщо інформаційно-технічні та інформаційно-аналітичні системи – інформаційно-технічна боротьба.Далі у роботі автор буде досліджувати це.

«Основною формою здійснення акцій ІВ є таємні інформаційно-психологічні операції ... Вони здійснюються шляхом надання інформаційного впливу на індивідуальне, групове і масову свідомість, почуття, волю громадян іншого боку, дезінформування суб'єктів прийняття політичних, економічних та інших рішень, в здійсненні підриву інформаційної інфраструктури іншого боку. Інформаційно-психологічні операції орієнтовані на формування умов для прийняття вигідних для інших держав та їхніх ділових кіл рішень у військовій, політичній, економічній та інших сферах в країнах-мішенях, що є об'єктами інформаційно-психологічного впливу ».

Основним засобом інформаційної війни є інформаційна зброя (ІС).

А.В. Манойло визначає його як «сукупність засобів, методів, способів і технологій інформаційно-психологічного впливу, спеціально створених для таємного управління інформаційною сферою супротивника, процесами й системами, що функціонують на основі інформації, а також – для нанесення їм шкоди.

Інформаційна зброя, на його думку, використовується в поєднанні із засобами й способами його доставляння (ЗМІ, ВІТМ, сучасними засобами зв'язку), технологіями впровадження інформаційної зброї й технологіями забезпечення умов його використання.

Інформаційна зброя нерозривно пов'язана з інформацією. Вона в разі ІВ є й об'єктом нападу, і зброєю нападу, і засобом захисту.

Л.В. Воронцова пропонує наступне визначення ІВ: "інформаційна зброя – це сукупність засобів, методів і способів, спеціально створених для нанесення шкоди інформаційній сфері, а також процесів і систем, що функціонують на основі інформації".

Інформаційну зброю І.М.Панарін визначає, як «пристрої й засоби, призначені для нанесення протиборчої сторони максимальної шкоди в ході інформаційної боротьби (шляхом небезпечних інформаційних впливів)».

Однак в інформаційній боротьбі важливо не тільки «атакувати», а й «тримати оборону». Коли в ході інформаційного протистояння противник

робить інформаційний випад, реагувати на небажану інформацію потрібно якомога швидше.

Звідси, згідно С.П.Расторгуєву, слідують і основні напрямки організації захисту:

- зменшення розміру мішені;
- захист мішені; регулярне знищення «інформаційних бур'янів»;
- установка власного жорсткого контролю за власною системою управління.

Г.Г. Почепцов виділяє наступні приймання відповіді на інформаційну атаку:

1. Описати дану дію іншим способом, який носить більш сприятливий характер.
2. Перевести акцент на деякі інші дії.
3. Акцентувати негатив супротивника.

У будь-якому випадку ми «знищуємо» вихідну інформацію шляхом введення її сурогатних замінників. При цьому саме їх ми тепер вважаємо більш правдивими.

А.В. Манойло виділяє шість складових інформаційно-психологічного впливу:

1. Маніпулювання.

Об'єктом маніпулювання є як окремі люди, так і групи людей, точніше сфера їх підсвідомості.Об'єктивна сторона маніпулювання полягає у виборі ефективних технологій психологічного впливу на об'єкт і надання цього впливу на підсвідомому для об'єкта рівні.

2. Дезінформування.

Дезінформування – процес доведення до іншої сторони умисно спотворений або сфабрикованої інформації.

3. Лобіювання.

Створення ситуації, яка може спонукати об'єкт до реалізації інтересів суб'єкта.

4. Пропаганда.

Формування у свідомості людей установки на прийняття пропагандистської інформації.

5. Управління кризами.

Підбір та застосування спеціальних кризових технологій, які дають можливість створення кризових ситуацій і управління ними в потрібному для суб'єкта напрямі.

6. Шантаж.

Умисні дії, спрямовані на надання впливу на об'єкт в потрібному для суб'єкта напрямі.

Далі розглянемо погляди вчених на політичні дії.

1.2. Технології та засоби політичного впливу як об'єкт дослідження в ході проведення інформаційних операцій

Технології та засоби політичного впливу широко розглядаються у вітчизняній науці. Розглянемо погляди кількох вчених, що працюють в різних напрямках.

С.Г.Кара-Мурза у своїй книзі «Влада маніпуляції» докладно розглядає маніпуляцію як засіб політичного впливу.

Дослідник відзначає, що мова і мислення – великі складні системи, на які можна впливати з метою програмування людини. Він пише: «Людина володіє складною психікою й уявою, живе у двох вимірах: реальному й уявному. Другий світ визначає поведінку людини, але він хиткий і на нього можна впливати. Людина живе не тільки в фізичному світі, але і в ноосфері (світі культури).» С.Г. Кара-Мурза не розкриває механічних методів впливу (електрошок, вживлення чіпів і ін.), бо вважає їх незаконними. Його предмет вивчення – «маніпуляція свідомістю за допомогою законних засобів». Людина не може сховатися від маніпуляції, але може виробити механізми захисту, розпізнаючи її. Слово «маніпуляція» має негативне забарвлення. Дослідник

визначає його як «спритне поводження з людьми як з речами, об'єктами». Він виділяє дві її ознаки: спритність і скритність.

На його думку, у створенні «фальшивої» дійсності беруть участь ЗМІ. Вони транслюють авторитетні думки, які засвоюються людьми й сприймаються як власні.

Вчений цитує Е.Фромма: «Насправді людям здається, що вони приймають рішення, що це вони хочуть чогось, в той час як насправді вони піддаються тиску зовнішніх сил, внутрішнім або зовнішнім умовностям і «хочуть» саме того, що їм доводиться робити ».

Приховування інформації – обов'язкова ознака маніпуляції, хоча як приймання маніпулятори використовують і гру в щирість.

Виділяє С.Г.Кара-Мурза і ще одна ознака: маніпуляція вимагає вміння, майстерності та знань від комунікатора.

Дослідник відзначає і ще одну особливість маніпуляції, як психологічного впливу, цитуючи Г.Франке: «Вона не тільки спонукає людину, що знаходиться під таким впливом, робити те, чого бажають інші, але і змушує її хотіти це робити».

С.Г.Кара-Мурза ділить методи маніпуляції на дві групи в залежності від мішені: знакові системи та духовні процеси.

До знакових систем вчений відносить Логосфера (світ слів). Це і засоби спілкування і «вербальне мислення».

Мова – головний засіб підпорядкування, вважає він. Причому, особлива роль відведена дієсловам (заборона, спонукання).

Цитує С.Московічі «Наука про маси»: «Звертатися з ними (словами) слід не як з частинками мови, а як з зародками образів, як із зернами спогадів, майже як з живими істотами».

Слово втратило свою святість, разом зі свободою слова прийшла безвідповідальність за наслідки сказаного, вважає вчений.

Він цитує слова французького філософа І. Ілліча: «... слова стали на ринку одним з найголовніших товарів, що визначають валовий національний продукт.

Саме гроші визначають, що буде сказано, хто це скаже, і тип людей, яким це буде сказано ... »

«Правильні» слова штучної мови відрізняють здається «науковість», тому будь-яка сказана думка ніби підкріплюється авторитетом науки. Політичну мову С.Г. Кара-Мурза також вважає штучною.

Почавши говорити «словами без кореня» людина стала вразливою, бо втратила свою опору. Створення таких слів стало найважливішим способом атомізації суспільства. Введення слів-амеб в тексти ЗМІ змушує аудиторію сприймати повідомлення відсторонено, через те, що воно не зачіпає глибинних основ нашого розуму. Ці слова підривають логічне мислення людини.

Кара-Мурза вказує характеристику привабливості слів-амеб для людини: помітність (дзвінкі приголосні, подвоєні, змішання стилів, поєднання слів з несумісними стилями). Розглядає маніпулятивну семантику (метод побудови фрази, підбору слів). Виділяє два напрямки створення штучної мови: підбір схожого за змістом слова-замінника та облік асоціацій, які викликає слово. Так, політики уникають слів, сенс яких устоявся в суспільній свідомості. Найважливіший інструмент впливу політичної мови – навішування ярликів. Поширюється маніпуляція і на мову чисел. Число має авторитет точності та неупередженості. Якщо людина прийняла абсурдне твердження мовою чисел, переконати її раціональними доводами практично неможливо. Числа додають ваги тексту, для маніпуляції часто використовуються відсотки. Мішенню маніпуляторів є і мова образів. С.Г. Кара-Мурза цитує Ле Бона: «Могутність слів знаходиться в тісному зв'язку з викликаними ними образами та абсолютно не залежить від їх реального сенсу». Маніпулятор посилає приховане повідомлення, сподіваючись, що воно розбудить у свідомості людини потрібні образи. Текст в поєднанні з образом включає два види сприйняття: семантичне й естетичне. А поєднання образу, тексту і чисел дає неймовірно високий відсоток ефективності. Саме завдяки ефективності взаємодії образу і тексту широку популярність придбали комікси, як вид впливу. Звідси ж і пропагандистська роль кіно, яку ми знаємо з історії.

Для маніпуляції використовуються і звуки. Вони впливають в основному на почуття людини. Відзначається, що музика посилює ефект маніпуляції, тому що не дає людині можливості спокійно ясно обміркувати отриману інформацію і змушує поспішно приймати її.

Перейдемо до другої групи мішеней маніпуляції: духовні процеси.

Перша мішень тут – логічне мислення. Воно добре вивчено, тому в нього не так важко вдертися і спотворити: викликати «збій програми». Якщо внести хаос в логічний ланцюжок, то людина плутається і шукає «поводиря», в якості якого йому надають «лідера думок» з уже готовою відповіддю. Вчений зазначає, що розум, вільний від догм, легше піддається впливу. Тому захист від цього типу впливу – в традиціях, приміщенні в історичну та етичну систему координат. В якості мішені розглядається та аутистична свідомість людини.

Цей тип мислення виникає, коли людина занадто захоплена фантастичними образами у своїй уяві й втрачає зв'язок з реальністю, занадто сконцентрована на внутрішніх розумових процесах. Людина у владі аутистичної свідомості уникає дій, переконання., чим і користуються маніпулятори. Але для цього потрібно добре знати бажання аудиторії й вміло апелювати до них. Долучать комунікатори та асоціативне мислення, зокрема, використовуючи метафори.

Дослідник відзначає, що хороша метафора зачаровує і заганяє мислення в вузький коридор, вихід із якого є тільки через умовивід, передбачене маніпулятором.

Маніпулюють і категоріями. Особливо популярно поняття «свобода». Вчений підкреслює, що найефективніше впливати словами, які трактуються неоднозначно. Дослідник припускає наступні моменти маніпуляції:

1. впровадження у свідомість під виглядом об'єктивної інформації неявного, але бажаного для певних груп змісту;
2. впливати на больові точки суспільної свідомості, що збуджують страх, тривогу, ненависть та інше;

3. реалізацію якихось задумів і приховуваних цілей, досягнення яких комунікант пов'язує з підтримкою громадською думкою своєї позиції ».

Споживач інформації буквально «губиться» в достатку фактів, думок, оцінок, що розширює можливості для маніпулювання людьми. Автор наводить термін «багатошарової людини»: «У такої людини виникає повна мішанина понять і немає ніякого взаємозв'язку подій, єдина система, в яку вона здатна підставляти окремі факти, – це система стереотипів, що вже склалися у неї в голові».

Окремим параграфом А.М.Цуладзе розглядає мову жестів, як засіб маніпулювання.

«Політик може досягти своїх цілей, впливаючи на аудиторію за допомогою слів, жестів, різних хитрощів, іншими словами – всього того арсеналу засобів, яким користуються професійні тележурналісти, актори, коментатори. При цьому політик повинен переконати виборця в суспільну значущість своїх слів ».

Він цитує А.Піза: «невербальні сигнали несуть у 5 разів більше інформації, ніж вербальні, і в разі, якщо сигнали неконгруентності (Конгруентність – відповідність слів і супутніх їх жестів.), люди покладаються на невербальну інформацію, віддаючи перевагу її словесної».Особлива значущість жестів в тому, що ми вже звикли не довіряти словам. Для нас очевидно, що оратор говорить одне, має на увазі інше, а думає третє.

Але за допомогою жестів політик може як обдурити аудиторію, так і видати себе. Цитує А.Піза: «навіть досвідчені фахівці можуть імітувати потрібні рухи тільки протягом короткого періоду часу, оскільки незабаром організм мимоволі передасть сигнали, що суперечать його свідомим діям».

Серед найбільш примітних жестів дослідник виділяє:

1. Відкриті долоні.

Відкрита долоня вважається ознакою чесності, доброзичливості, щирості.

2. Кулак.

Кулак свідчить про агресивність говорить, вказує на бажання його господаря розв'язувати всі проблеми разом, «одним ударом сімох». У промові такого політика переважають заклики до силового, радикального розв'язання проблем.

3. Два зустрічних кулаки – «зіштовхнути лобами, посварити».

Окремо дослідник розглядає маніпулятивний потенціал ЗМІ. На його думку, у громадськості є всі підстави дорікати ЗМІ в маніпуляції. Він цитує М. Паренти: «ЗМІ відбирають більшу частину інформації і дезінформації, якими ми користуємося для оцінки соціально-політичної дійсності. Наше ставлення до проблем і явищ, навіть сам підхід до того, що вважати проблемою або явищем, багато в чому зумовлені тими, хто контролює світ комунікацій ».

Можливості ЗМІ в маніпуляції широкі: навмисне спотворення реального стану речей шляхом замовчування одних фактів і випинання інших, публікації помилкових повідомлень, пробудження в аудиторії негативних емоцій за допомогою візуальних засобів або словесних образів і т.д. Всі ці приймання створюють необхідний емоційний настрій і психологічні установки в аудиторії.

Згідно з політичною моделлю ЗМІ, «будь-які новини є продуктом діяльності людей, що мають певні ідеологічні погляди, а також, створюються під тиском політичного оточення, в якому знаходиться організація, що робить новини».

Отже, приймання маніпуляції в ЗМІ дослідник розглядає в залежності від його типу.

На телебаченні, існує ряд факторів, які дозволяють журналістам маніпулювати політиком або його висловлюваннями. Адже багато в чому саме від них залежить, як політик буде виглядати в очах виборців.

Має значення ситуація, в якій береться інтерв'ю.

У прямому ефірі політик гарантований від того, що його висловлювання можуть бути перекручені, в записі ж його слова можуть бути перекручені. Атмосфера задає тон дискусії.Вона може бути формальна – неформальна, довірча – ворожа.

Предметом політичної пропаганди є ідеології, система цінностей, стратегія певних політичних сил. Пропагандистська комунікація відрізняється односпрямованим характером, активним, агресивним, що нав'язує типом впливу.

Політична реклама – це форма політичної комунікації в умовах вибору, адресний вплив на електоральні групи, що має на меті «піднести в доступній, емоційній, лаконічній, оригінальній формі, легко запам'ятовується суть політичної платформи певних політичних сил; налаштувати на їх підтримку, сформувати й впровадити в масову свідомість певне уявлення про їхній характер, створити бажану психологічну установку, що зумовлює напрямок почуттів, симпатій, а потім і дій людини ».

Предметами політичної реклами виступають кандидат, партія і їх програми, а також політична акція, рух підтримки або протесту та ін.

Об'єкти – учасники політичного процесу, що роблять той чи інший вибір, що визначають для себе ту або іншу політичну орієнтацію, в кожному конкретному випадку конкретну цільову групу;

в ситуації виборчої кампанії – електоральні сегменти.

Методи рекламної діяльності лежать в площині комунікативних методів, орієнтованих на управлінні масовою поведінкою за допомогою впливу на їх свідомість. Реклама воліє ірраціональні методи, через те, що емоційно подана інформація засвоюється швидше.

Директ-маркетинг ґрунтується на встановленні прямих зв'язків між виробником і споживачем. Цей інструмент замінює особистий діалог.

Фахівці в сфері технологій директ-маркетингу виділяють кілька його різновидів, в політичних кампаніях активно використовуються такі:

- Поштова розсилка
- Телефонний маркетинг
- Електронний маркетинг.

Однак директ-маркетинг є улюбленим інструментом антимаркетингу. У практиці виборчих кампаній директ-маркетинг застосовується для дискредитації конкурента.

Особисті продажі – це персональна групова та міжособистісна комунікація в процесі зустрічей з виборцями, на мітингах, в кампанії «від дверей до дверей».

Стимулювання збуту (sales promotion) – короткочасні спонукальні заходи заохочення купівлі або продажу товару або послуги. Основні особливості стимулювання збуту полягають в тому, що цей вплив розрахований на тимчасове короткострокове підвищення інтересу до предмета (кандидату) за допомогою пропозиції будь-яких особливих пільг, що мають на увазі активну співпрацю, засновану на персоналізованої мотивації. Ця комунікаційна стратегія активно використовується у виборчих кампаніях.

У другому розділі дипломної роботи ми розглянемо як всі перераховані приймання та засоби впливу «працюють» в соціальних мережах. Але спочатку поговоримо про феномен інтернету і соціальних мереж і їх місце в системі масових комунікацій.

1.3. Визначення статусу Інтернету і місця соціальних мереж в системі масових комунікацій

Перш ніж розглядати місце мережі Інтернет та соціальних мереж в системі СМК(система масових комунікацій), визначимося з поняттям «масова комунікація». У сучасних підручниках з теорії комунікації цей термін трактується, як «процес виробництва і передачі повідомлень великим масам людей за допомогою спеціальних технічних засобів». У документах Міжнародного симпозіуму з прав людини і масової комунікації (Зальцбург, 1968 г.) зазначено: «масова комунікація виникає тоді, коли публічне сповіщення передається одночасно чисельно великий і розосереджених

аудиторії. До засобів масової комунікації заведено відносити книги, кіно, пресу, телебачення і радіо.

Тут варто відзначити: вчені розходяться в думці, чи варто вважати поняття ЗМІ та СМК тотожними.

За роз'ясненням звернемося до одного з законів про ЗМІ: «під засобом масової інформації розуміється періодичне друковане видання, радіо-, теле-, відео програма, кінохронікальна програма, інша форма періодичного поширення масової інформації». Виходячи із закону, бачимо, що ЗМІ має на увазі періодичність. Однак не всі матеріали масової комунікації мають цю ознаку. Таким чином, бачимо, що поняття СМК ширше поняття ЗМІ.

Сьогодні як такої полеміки з приводу того, чи є Інтернет засобом МК, не спостерігається. Вчені все частіше одностайно дають ствердну відповідь. Якщо в підручниках початку нульових років, Інтернет згадується лише побіжно, то у 2006 році входить в ряд СМК і підкреслюється, що персональний комп'ютер відіграє вагому роль в житті людини, а розвиток мережі інтернет сприяє розвитку інформаційного суспільства та посиленню важливості інформації в суспільному житті. А в другому десятилітті 21 століття статей про віртуальну реальність вже присвячені окремі розділи в збірниках робіт науково-практичних конференцій. Вчені визнають, що «Міжнародна комп'ютерна мережа стала загальнодоступним засобом масової комунікації, майданчиком економічних і політичних операцій, засобом соціалізації, інформаційним ресурсом, місцем проведення дозвілля і навіть релігійних дій».

До недавнього часу комп'ютери були персональним засобом збору, обробки та аналізу інформації. У 1973 році з'явилася концепція нової всесвітньої мережі та з'явився термін «Internet» (скорочення від Interconnected Network – «з'єднані мережі»).

У науковому світі усвідомлюється важливість вивчення Інтернету. У своїй дисертації «Інтернет як засіб масової комунікації: соціологічний аналіз» кандидат соціологічних наук А.Н. Шеремет, зазначає: «Інтернет сьогодні є, з

одного боку, найбільш динамічно розвивається, а з іншого – найменш вивченої формою масової комунікації».

Він пише, що можливості мережі стають предметом інтересу соціологів, політологів, філософів, юристів, економістів.

Вітчизняними дослідниками розглядаються деякі приватні питання використання Інтернету в різних сферах соціокультурної діяльності, його роль у розвитку освіти та місце в політичній сфері й т.д..

У своїй роботі він розглядає значущість інтернету і його вплив на життя суспільства. Він пише: «Сформована субкультура сучасної української Інтернет-спільноти є основою для формування нової інформаційної культури соціуму і містить відповідні норми та цінності, а саме: повага свободи слова та плюралізму думок, наявність стійкої власної думки, сформованої на базі зібраної інформації з безлічі різноманітних джерел, висока швидкість масових комунікацій, висока вибірковість і активність учасників масово-комунікаційного процесу, діалогові форми масової комунікації, раціональність, незалежність, оптимізм ».

За ступенем впливу Інтернет як засіб масової комунікації він зіставляє з традиційними пресою, радіо і телебаченням.

Інтернет, він називає основним фактором симбіозу і конвергенції «традиційних» і «нових» засобів масової комунікації, які не витісняє інші форми і типи мас-медіа, а трансформує їх і навіть допомагає здобувати аудиторію.

О.Г. Філатова у своїй статті «Інтернет як мас-медіа» розглядає його як ЗМІ: «Інтернет є багатостороннім ЗМІ, який створює безліч різних форм комунікації». Слідом за М. Морріс вона ділить їх на 4 категорії:

1. Асинхронна комунікація «сам на сам» (електронні листи)
2. Асинхронна комунікація «багатьох з багатьма» (наприклад, мережа юзернет: листи розсилок, де потрібна згода на розсилки або пароль, для входу в програму, в якій повідомлення стосуються певних тем)

3. Синхронна комунікація «сам на сам», «один і кілька», «один з декількома» будуються навколо будь-якої конкретної теми, наприклад, рольові ігри, чати

4. Асинхронна комунікація, де зазвичай користувач намагається розшукати сайт для отримання певної інформації та тут можна зустріти комунікацію «багато та один», «сам на сам», «один і багато» (веб-сайти, гороскопи).

Вона виділяє ряд переваг Інтернету в порівнянні з традиційними ЗМІ: можливість використання мультимедіа, персоналізація (можливість надання індивідуальної інформації, розсилки на особисту пошту), інтерактивність, відсутність посередників.

Кордон між мережевими ЗМІ й традиційної преси, що приходить в мережу, останнім часом все більше стирається, вважає дослідник. «Конвергенція Інтернету і ЗМІ створює передумови інтегрованих мультиканального маркетингових комунікацій, що поєднують в часі та просторі можливості локального охоплення аудиторій друкованих та радіомовних ЗМІ й глобального охоплення Інтернет-аудиторії».

О.Г. Філатова аналізує і вплив мережі на мислення людини: «Інтернет змінює весь спосіб життя людей, стиль мислення людини, трансформує особистість, розширює її межі. Підвищується соціальна мобільність, створюються нові моделі поведінки, технології впливу на масову свідомість стають більш ефективними. Розвиток нових інформаційно-комунікативних технологій сприяють інтернаціоналізації ринків праці та посилення їх взаємозалежності, індивідуалізації та плюралізації стилів життя ».

А.С. Біккулов у своїй дисертації «Інтернет як засіб масової комунікації», відзначаючи важливість «всесвітньої павутини», пише, що «Інтернет стає засобом не просто масовою, але глобальної комунікації, переступають через національні кордони та об'єднує світові інформаційні ресурси в єдину систему».

Він зауважує, що Інтернет не є просто набором комп'ютерів і проводів з якимсь безліччю сайтів. Це впорядковане середовище, в якому активно йдуть процеси організації та самоорганізації.

Ю.П.Зінченко в статті «Віртуалізація реальності: від психологічного інструментарію до нової субкультури» розглядає феномен віртуальної реальності. Він пише: «глибина проникнення віртуальності в соціальне та індивідуальне життя дозволяє говорити про віртуалізацію суспільства». З одного боку, комп'ютерні мережі розширюють інформаційний простір людини, а з іншого, сприяють існуванню людини у двох реальностях, і, в разі, якщо віртуальне «я» стане домінувати над реальною особистістю людини, то може бути завдано шкоди. Тому потрібно суворо дотримуватися балансу існування у двох реаліях

Таким чином, можемо зробити висновок, що людина, яка звикла до «легкого спілкування», буде або прагнути ввести подібну модель спілкування в реальне життя, або зводити до мінімуму свою присутність в реальному житті та йти в віртуальну реальність.

Відзначають вчені й інші небезпечні сторони інтернет-комунікації. Однак, якщо А.Н.Шермет вважає, що їх не більше, ніж в традиційних ЗМК, а «Видання і канали, які орієнтуються на аудиторію як пасивного приймача масової інформації, матеріал для маніпуляцій, навряд чи мають шанси на успіх», то Філатова справедливо зауважує, що «Масова комунікація стає не тільки "магічним вікном", через яке ми дивимося на світ, а й "дверима", через які ідеї проникають в нашу свідомість. Це відноситься до всіх засобів масової комунікації, і, перш за все, до всесвітньої комп'ютерної мережі Інтернет ».

Слідом за комунікацією в інтернеті, звернемося до теми соціальних мереж. «Соціальна мережа – являє собою соціальну структуру, яка складається з групи вузлів. Ці вузли є соціальними об'єктами (організації або люди) і зв'язками між ними (соціальні взаємини) ».

У віртуальній сфері «соціальна мережа – це онлайн сервіс або ж веб-сайт, призначений для створення, організації всебічного спілкування між реальними людьми в інтернеті».

Вважається, що перша в сучасному розумінні соціальна мережа Classmaters.com була створена в 1995 році Ренді Конрадом. Така концепція стала досить популярною і моментально почався бурхливий розвиток в Інтернеті соціальних мереж.

Соціальних мереж, як самостійного об'єкта, вивченого вітчизняними вченими досить мало. Найчастіше їх навіть не виділяють в ряду комунікацій в інтернеті. Однак, в той час як теоретики не поспішають знайомитися з феноменом соціальних мереж в загальному, деякі дослідники вже активно розглядають їх, як інструмент маніпуляції свідомістю. Про це докладніше ми поговоримо в наступному розділі.

Кандидат філософських наук А.М.Лещенко в дисертації «Соціальні мережі як механізм конструювання комунікації в сучасному суспільстві» зазначає, що «соціальні мережі займають все більше місця в житті сучасного суспільства, зростає кількість як самих мереж, так і зареєстрованих в них користувачів. Багатьма людьми складний процес зміни комунікаційних стандартів сприймається як занурення суспільства в простір мозаїчної, хаотично орієнтованої культури, в зв'язку з чим загострюється питання ціннісних орієнтирів особистості в мережі ».

Соціальні мережі він зіставляє із засобами масової комунікації, тому що вони виконують всі функції засобів масових комунікацій. За критерієм періодичності, доступності, фінансового критерію мережеву комунікацію він характеризує, як найбільш ефективну. Він пише: «Традиційні засоби масової комунікації виступають як центри, спочатку акумулюють інформацію, потім її сортують і поширюють. Соціальні мережі характеризуються потенційно нескінченним числом незалежних центрів акумуляції й поширення інформації, що визначає її глобальність, демократичність, але і безконтрольність ». Автор вважає, що соціальні мережі, є вимушеним, компенсаційним механізмом, що

формується в умовах неефективності держави та інших соціальних інститутів. Він зазначає, що останнім часом все частіше соціальні мережі стають об'єктами й засобами інформаційного управління, ареною інформаційного протиборства.

Однією з характерних рис соціальної мережі він називає соціабельність, яку визначає, як почуття легкості та невимушеності в соціальних взаєминах особистості, засноване на володінні ефективними навичками соціальної взаємодії (це питання ми вже підіймали раніше). В основі соціабельності він вказує феномен довіри, його вважає найбільш значущим фактором створення соціальних мереж.

Автор зазначає, що користувач соціальної мережі має сукупність мотивів і потреб (у спілкуванні, в довірі, самопрезентації), тому привабливість мережі в її мультифункціональності, здатності задовольнити всі запити одночасно. Тому людина потрапляє «в соціальну павутину», тому що складається уявлення про повну задоволеності потреб.

«Соціальна мережа дозволяє координувати дії користувачів, використовуючи переваги неформальних каналів поширення інформації». Цікава думка, що в разі, якщо з якої-небудь причини користувач мережі не може особисто поспілкуватися з іншим користувачем, довірчий характер соціальних відносин дозволяє йому отримати надійну інформацію про його діях і репутації від третіх осіб з-поміж членів соціальної мережі.

Таким чином, ми бачимо: специфіка соціальних інтернет-мереж така, що користувач відчуває себе максимально комфортно, відчуваючи себе серед однодумців. Водночас на нього обрушується величезний потік інформації, змушуючи поверхнево переробляти її. Всі ці фактори роблять людину вразливою до маніпуляції свідомістю і впливу на його мислення. Детальніше про це ми поговоримо у другому розділі роботи.

ВИСНОВКИ ДО ПЕРШОГО РОЗДІЛУ

У цій частині розділу автор дав визначення такому терміну як «інформаційна війна», ознайомив з основними принципами й технологіями її ведення.

Розглянув ІВ, як самостійне явище політичного життя суспільства, дослідив як за допомогою інформаційних війн Вами маніпулюють таким чином, що Ви вважаєте це нормою і навіть не помічаєте.

Інформаційна війна – це комплексне спільне застосування сил і засобів інформаційної та збройної боротьби, це дії, спрямовані на досягнення інформаційної переваги, підтримку національної військової стратегії за допомогою впливу на інформацію та інформаційні системи супротивника при одночасному забезпеченні безпеки та захисту власника інформації. Основними формами ведення технічної ІВ є радіоелектронна боротьба, війна з використанням засобів електронної розвідки й наведення, нанесення віддалених точкових ударів з повітря, психотропна війна, боротьба з хакерами, кібернетична війна.

Інформаційна війна – це цілеспрямовані дії, вжиті для досягнення інформаційної переваги шляхом завдання шкоди інформації, інформаційних процесів та інформаційних систем противника при одночасному захисті власної інформації, інформаційних процесів і інформаційних систем.

Також автор розкрив деякі методи маніпуляцій, які використовують політики з усього світу.

Було розглянуто історію розвитку досліджень політичних комунікацій як інструмента інформаційних операцій та наукову полеміку щодо статусу Інтернету і місце соціальних мереж в системі масових комунікацій.

РОЗДІЛ 2. СОЦІАЛЬНІ МЕРЕЖІ В СИСТЕМІ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

2.1. Дослідження видів аудиторії та характеристика українських соціальних мереж

Соціальні мережі займають все більш міцне місце в житті людини. Дослідники відзначають: 95% постійних і 77% періодичних користувачів Інтернету користуються і соц. мережами. Багато хто навіть 5-ма одночасно.

Кількість інтернет-користувачів у світі зросла до 4,54 мільярда, що на 7% більше торішнього значення (+ 298 мільйонів нових користувачів у порівнянні з даними на січень 2019 року).

У січні 2020 року у світі налічувалося 3,80 мільярда користувачів соціальних мереж, аудиторія соцмедіа виросла на 9% в порівнянні з 2019 роком

Сьогодні більше ніж 5,19 мільярда осіб користуються мобільними телефонами – приріст на 124 мільйони (2,4%) за останній рік.

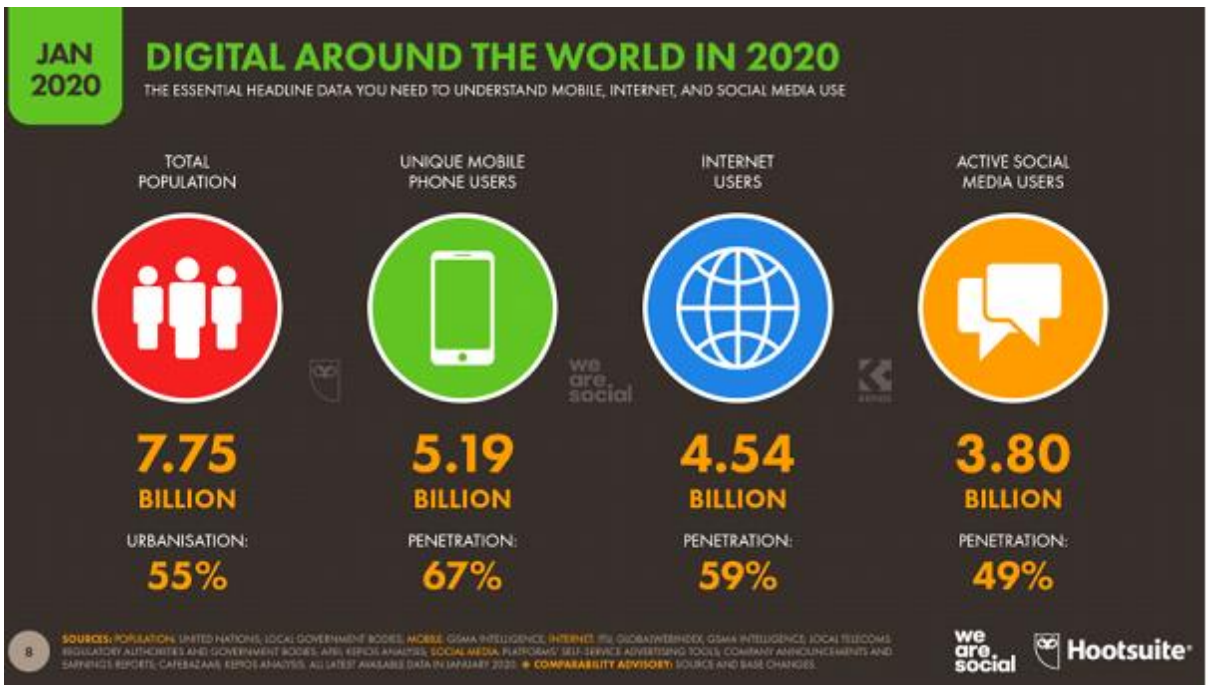

Рис.2.1 Цифровий світ у 2020

Середньостатистичний користувач проводить в інтернеті 6 годин 43 хвилини кожен день. Це на 3 хвилини менше, ніж рік тому, але як і раніше становить понад 100 днів на користувача на рік. Якщо залишити близько 8 годин на добу на сон, це означає, що зараз понад 40% часу неспання ми проводимо в інтернеті.

У сукупності глобальна аудиторія інтернету буде онлайн 1,25 мільярда років за один тільки 2020 рік, і третина цього часу піде на соціальні мережі. Кількість часу, який люди проводять в інтернеті, сильно відрізняється в різних країнах. Так у Філіппінах це 9 годині 45 хвилин в день, а в Японії – 4 години 22хвилини.

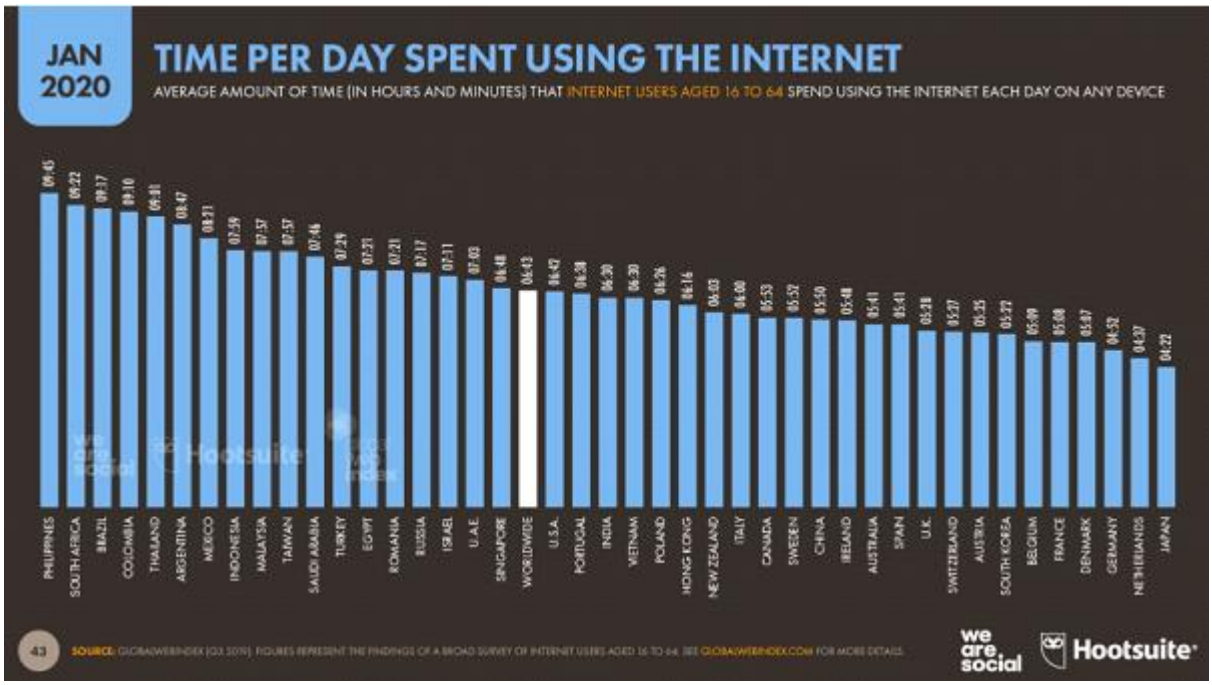

Рис.2.2 Кількість годин у день які користувачі проводять в мережі інтернет

Аудиторію соціальних мереж також часто називають «користувачами». Можемо припустити, це пов'язано з тим, що кожна людина в соціальних мережах не просто вбирає надану інформацію, він дійсно «користується» мережами. Соціальні мережі влаштовані так, що користувач сам настроює потік

споживаної інформації. Вибирає коло спілкування за допомогою вступу в ті чи інші віртуальні спільноти або підписок на сторінки будь-яких користувачів.

В журналістиці термін аудиторія визначається як «сукупність людей - адресатів журналістських творів, що виникає на основі спільності їх інформаційних інтересів і потреб, а також форм, способів і каналів їх задоволення».

У випадку з соціальними мережами загальним можна з твердою впевненістю назвати тільки канал комунікації – Інтернет. Однак у них може не бути ні спільних інтересів, ні потреб, які вони прагнуть задовольнити за допомогою соціальних медіа. Аудиторія мереж дуже різноманітна, сприймає інформацію по-різному в залежності від статі, віку, інтересів та інших характеристик. І щоб зрозуміти, яким чином на цю аудиторію можна впливати, перш за все, необхідно проаналізувати, хто ж є об'єктом по той бік монітора.

Хто ще не в мережі?

Сьогодні трохи більш як 40% від загальної чисельності населення світу – приблизно 3,2 мільярда людей – ще не підключені до інтернету. Понад мільярд «не підключених» живуть в Південній Азії (31% від загального числа). На країни Африки припадає 27%, тобто 870 мільйонів чоловік по всьому континенту.

У цих регіонах є залежність між рівнем доступу в інтернет і віком користувачів: в онлайн не виходять більша частина населення Африки у віці до 20 років і понад 460 мільйонів чоловік у віці до 13 років в Південній Азії.

Має значення і стать. За даними Міжнародного союзу електрозв'язку (ITU), жінки рідше мають доступ в інтернет, ніж чоловіки. Гендерний розрив також спостерігається серед аудиторії соціальних мереж. Наприклад, сьогодні жінки в Південній Азії користуються соціальними мережами в три рази рідше в порівнянні з чоловіками. Більша частина жінок, які проживають в Індії зараз, взагалі не знають про існування мобільного інтернету.

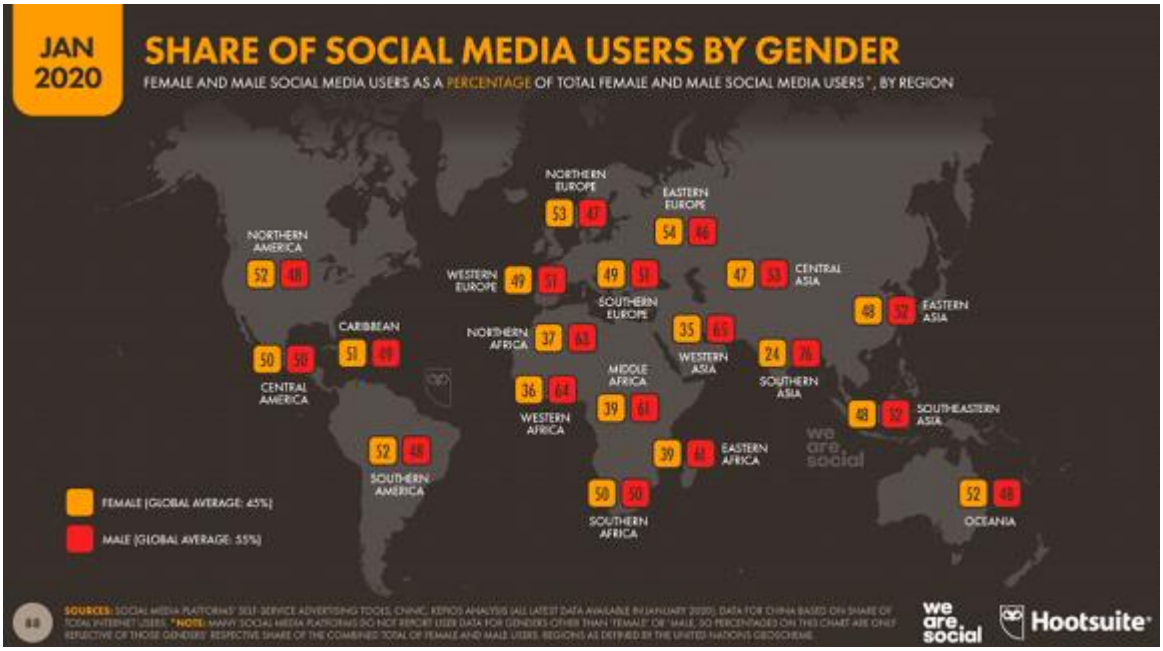

Рис.2.3. Види користувачів соціальних мереж за гендером

Види аудиторії в науці заведено виділяти відповідно до тими чи іншими характеристиками. Ми вдамося до цього ж способу класифікації. І.М. Блохін виділяє кілька груп соціальних характеристик аудиторії:

1. Соціально-демографічні: стать, вік, місце проживання, національність, мову.

2. Соціально-професійні: спеціалізація, рід занять, професійний статус, тип підприємства (підприємства, установи, організації).

3. Соціокультурні характеристики: освіта, віросповідання, субкультурні та контркультурні особливості, форми проведення дозвілля.

4. Споживчі характеристики: рівень доходу, споживання окремих товарів і послуг.

5. Політико-ідеологічна група.

У ній аудиторія ділиться на:

1. Політично позитивно активну, голосує «за»;

2. Політично негативно активну, голосує «проти» або «проти всіх» (аудиторія «протестного» електорату).

3. Політично пасивну, абсентеїстської налаштовану (абсентеїзм – прояв байдужості до політичного життя, ухилення від участі в ній.;

4. Політично активну, ідеологічно орієнтовану.

Розглянемо види аудиторії, спираючись на них.

Але спочатку відзначимо, що користувачем може бути як приватна особа, так і організація. Спочатку всіх користувачів по типу заповнення анкети можна розділити на «відвертих» (які заповнюють анкету максимально чесно реальними даними), «стриманих» (заповнюють анкету правдивими даними, але вказують про себе дуже небагато: стать, вік, ім'я і країну, наприклад), і «фейки» (так в мережі називають користувачів, які вказують вигадані дані або ж видаються кимось іншим). Чи не заповнювати анкету зовсім як правило не можна: такому користувачеві обмежують доступ до багатьох функцій сервісу.

Також, за типом сторінки можна виділити три види користувачів: з відкритою сторінкою (весь вміст профілю є іншим людям), з частково закритою сторінкою (доступ заблокований тільки для осіб, які не є «друзями», або тільки до деяких рубриках профілю), з повністю закритою сторінкою.Чи можемо виділити види користувачів по типу цілей використання соціальної мережі.

Для мобільних телефонів. Цей вид користувачів відвідує соціальні мережі, щоб відпочити, отримати задоволення. Для цього в мережах існує безліч гумористичних спільнот, онлайн-ігор, відео- і аудіо контент.

Так, в «Facebook» в групі «Смійся до сліз» регулярно публікуються анекдоти, комікси, карикатури. А в спільноті «Краща музика на всі випадки життя» в «ВКонтакте» можна знайти безліч найрізноманітніших музичних композицій і навіть додати у свій плейлист.

Комунікація. Користувачі цієї групи шукають в мережах спілкування. Вони можуть поговорити з «друзями» або з іншими користувачами. У деяких співтовариствах ввечері створюються чати для людей, які самотні, ігри, знайомства. Також користувач може написати що-небудь на своїй «стіні» або в форумі і вступити в дискусію з тим, хто прокоментує запис. Також можна вступити в суперечку або бесіду з ким-небудь під фотографією «друга»,

наприклад. Користувачі цього типу часто «онлайн», регулярно перевіряють список вхідних повідомлень в надії, що їм будь-хто написав. Вони активно вступають в діалог з будь-якого приводу навіть з незнайомими людьми.

Інформування. Користувачі цього типу шукають в мережі «чогось новенького», активно споживають інформацію. Причини цього можуть бути різні: цікавість, професійна необхідність, хобі. Наприклад, людина, активно захоплюється в'язанням, буде шукати нові схеми і способи в'язки, віртуальні магазини з продажу пряжі та спиць і т.п. Ця аудиторія активно підписується на безліч спільнот, що цікавить їх тематики, проводять в мережі дуже багато часу, обробляю новинну стрічку. Якщо ж людина активно цікавиться новинами світу, він віддасть перевагу підписатися на компанії ЗМІ, щоб і в мережі отримувати новини та посилання на статті.

Отримання прибутку. Останнім часом користувачі все частіше прагнуть заробляти за допомогою соціальних мереж. Це відноситься як до приватних осіб, так і комерційним організаціям. Наведемо приклади. Користувач може створити спільноту в мережі, залучити передплатників цікавим контентом. Коли їх буде досить багато, почнуть надходити пропозиції про розміщення реклами (природно, за винагороду). Тобто, схема схожа з отриманням прибутку в ЗМІ. Використовують для отримання прибутку віртуальний простір і комерційні організації.

Можемо виділити два види такої діяльності.

Перший – просування в соціальних мережах бренду з метою залучення клієнтів. Як приклад можемо навести спільноту «Рафаелло» в «Facebook». Свою діяльність спільнота почала в співробітництві з дуже популярною в той час онлайн-грою. У групі не було реклами продукції цієї фірми, приймання замовлень на доставлення, презентації асортименту і вказівки цін. Організатори займалися проведенням конкурсів, інтерактивних ігор та публікацією цікавих фактів про солодощі. Таким чином здійснювалося просування бренду і залучення покупців.

Другий – створення «інтернет-магазину», вітрини вже чинного сайту-магазину або магазину не віртуального. Наведемо як приклад спільнота магазину «Куфе бижу». Мережа магазинів займається продажем намистин і фурнітури. Крім традиційних та онлайн-магазинів, фірма здійснює продаж товару завдяки спільноті в мережі, презентуючи товар і спілкуючись з потенційними покупцями.

Самопрезентація, просування. Користувачі цієї групи прагнуть представити себе (або кого-небудь) в мережі. Наприклад, художник або поет викладає свої роботи в профілі або створює спільноту. До цього ж виду відносимо організації, які просувають себе (або кого-небудь) за допомогою мережі. Цей вид схожий з попередньою групою, однак якщо вище йшлося про видалення прямий комерційного прибутку, то тут її може і не бути. Так, наприклад ГУ МВС України має свою спільноту в мережі «Поліція України», де формує ставлення аудиторії до відомства, проводячи конкурси та звітуючи про роботу. Часто також створюються спільноти політичних партій, рухів для залучення прихильників.

Соціально-демографічні характеристики користувачі можуть вказати у своїх анкетах: стать, дату народження, мова, сімейний стан, рідне місто.

Стать можна відзначити «чоловічий» або «жіночий», тут суворо (у всякому разі у вітчизняних соціальних медіа). А ось країну і місто можна вибрати із запропонованого списку або ввести самому.

Наприклад, в соціальній мережі «ВКонтакте» країну «Україна» вказали 23 812 055 чоловік. Для порівняння: «Японія» вказана в анкеті у 18 243 чоловік.

Оскільки в нашому дослідженні розглядаються українські користувачі та популярні в Україні соціальні мережі, за місцем проживання можемо розділити аудиторію на три групи:

1. проживають на території України;
2. проживають за кордоном;
3. люди, які вказали вигадану країну (така можливість є, наприклад в аудиторії «Facebook»).

Мову в соціальних мережах можна використовувати будь-яку з чинних. Однак в аналізованому нами сегменті мереж більшість користувачів спілкуються російською та англійськими мовами. Сімейний стан користувач може не вказувати або вибрати найбільш слушний термін зі списку. За цією ознакою розділимо аудиторію на людей, які перебували у шлюбі, які перебувають у незареєстрованих відносинах, які не перебувають в будь-яких відносинах («в активному пошуку», наприклад.)

У «Facebook» статус «одружений» вказали 17 825 238 осіб, а «неодружений» 12. 246 988 осіб, в «активному пошуку» трохи понад 9 тисяч осіб.

Можна виділити наступні види аудиторії:

- дитяча (7-15 років),
- молодіжна (16-30 років),
- середнього (30-50 років)
- старшого віку (старше 50 років).

У групі соціально-професійних характеристик розглянемо аудиторію в залежності від роду занять. Чи можемо виділити три групи осіб:

У соц.мережах можна вказати в анкеті місце навчання або роботи.

До соціокультурних характеристикам, як уже говорилося вище, відносяться: освіта, віросповідання, субкультурні та контркультурні особливості, форми проведення дозвілля.

За рівнем освіти виділимо наступні види аудиторії: без освіти, школярі, студенти, які закінчили навчальний заклад.

Виявити їх допомагають не тільки анкетні дані, а й численні спільноти, які об'єднують користувачів зі схожими інтересами та нагальними питаннями. Цікаво, що часто спільнота навіть не заявляє: для якої аудиторії створювалась, її наповнення робить це саме.

Так, наприклад, у соціальній мережі «Instagram» в спільноті «MDK» можемо зустріти жарти на тему студентського життя і передплатники у неї в

основному студенти. А ось в товаристві «Корпорація добра» багато «постів» на тему школи та серед передплатників багато школярів.

Віросповідання також вказується в анкетах в мережі (але не у всіх). Також його вказують як «світогляд». На основі анкет виділимо групи: юдеї, католики, православні, протестанти, мусульмани, буддисти, конфуціанці, пастафаріанці (пародійна релігія), світські гуманісти (філософська течія), атеїсти і люди, які не відносять себе до жодної з груп.

Що стосується споживчих характеристик, виділити групи за рівнем доходу досить складно, адже він може бути дуже різним. У соціальних мережах він видно з фотографій (якщо в кадр потрапляє обставини житла або гаджети) і підписам під записами «опубліковано за допомогою IPhone».

Що стосується політико-ідеологічної групи характеристик, слідом за дослідниками виділимо чотири види аудиторії: політично позитивно активну, політично негативно активну, політично пасивну, політично активну (ідеологічно орієнтовану).

Позитивно-активна аудиторія активно цікавиться політичними новинами і бере участь в обговореннях в тематичних спільнотах, формуючи своє ставлення до тієї чи іншої партії або навіть захищаючи її в суперечці з опонентами.

Негативно-активна аудиторія активно вступає в політичні суперечки, критикуючи того чи іншого політика або партію. Політичноактивна аудиторія не цікавиться політичними новинами, в обговореннях не бере. Ідеологічно орієнтована аудиторія виступає за ту чи іншу партію (політика), вступає в конструктивні суперечки з опонентами, орієнтується в політичному житті держави і може відстояти свою точку зору, спираючись в тому числі і на факти з історії.

Чисельність аудиторії соціальних медіа стрімко зростає, видове різноманіття знаходиться в постійному русі. Вчені відзначають, що користувачі мережі вже сформувалися як субкультура, яка може стати «інформаційною культурою, характерною для більшої частини російського суспільства,

органічною частиною культури нації в цілому». Детальніше про особливості культури соціальних мереж і вплив їх на свідомість людини поговоримо в наступних пунктах роботи.

2.2. Форми інформаційних операцій в соціальних мережах

Існують три типи інформаційних операцій такі як :

1. Фізичний вимір має інформаційно-технічний вплив
2. Інформаційний вимір має соціально-технічний вплив,
3. Пізнавальний вимір – має надання інформаційного впливу на представників командного складу ВС супротивника.

Основне завдання інформаційних операцій полягає в маніпулюванні масами на рівні свідомості, найчастіше з метою:

- внесення в суспільну та індивідуальну свідомість певних ідей і поглядів;
- дезорієнтації та дезінформації мас;
- ослаблення певних переконань;
- залякування.

З огляду на наведене, серед загроз національним інтересам і національній безпеці в Законі України "Про основи національної безпеки України" (стаття 7) серед потенційних загроз в інформаційній сфері окремо зазначається:

"... намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення невірогідної, неповної або упередженої інформації."

Основою сучасних інформаційних операцій є принципи синергетики.

Синергетичні підходи базуються на розгляді суспільства як надзвичайно складної системи, кожен елемент якої має безліч ступенів свободи, і тому гарантують коректність результатів моделювання лише на якісному рівні. Тому, не роблячи глобальних узагальнень, зупинимося лише на окремих прикладах, на підставі аналізу яких отримані деякі рекомендації.

Звичайна мережева інформаційна атака сьогодні відбувається здебільшого в веб середі. Для цього, як правило, створюється і деякий час функціонує веб-сайт (назвемо його «першоджерелом»), при цьому він публікує цілком коректну інформацію.

В час «Х» на його сторінці з'являється документ, зазвичай компромат на об'єкт атаки, вірогідний або сфальсифікований. Потім відбувається так звана «відмивання інформації». Документ передруковують інтернет-видання двох типів – зацікавлені в атаці й ті, кому просто не вистачає інформації для заповнення свого інформаційного поля. У разі претензій все передруковувати видання посилаються на «Першоджерело», і в крайньому разі, на прохання / вимогу об'єкта атаки видаляють зі своїх веб-сайтів інформацію. Першоджерело при необхідності також знімає інформацію або зовсім ліквідує (після чого виявляється, що воно зареєстроване в Інтернеті на нереальну особу). Разом з тим інформація вже розійшлася, завдання першоджерела виконана, атака стартувала. У всіх на слуху інформаційна кампанія, спрямована проти «Промінвестбанку», що почалася в кінці вересня 2008 р.

За допомогою системи контент-моніторингу InfoStream, що сканує всі основні інформаційні веб-сайти України в режимі реального часу, була визначена динаміка публікацій на веб-сайтах повідомлень, в яких згадувався «Промінвестбанк» за три місяці – вересень, жовтень і листопад. Ця динаміка свідчить про невелику кількість публікацій за першу половину вересня, проте потім пішов ряд публікацій, що компрометують голови правління В. Матвієнко, що викликало відносно невеликий резонанс. Як виявилося згодом, ці публікації були лише «Артпідготовкою». 26 вересня з'явилися перші повідомлення про можливе банкрутство банку, кількість яких цілком відповідає лавиноподібного процесу, обмеженому лише числом веб-сайтів, здатних публікувати подібну інформацію.Втім, цей процес вийшов на стабільно-середній рівень до грудня 2008 р.

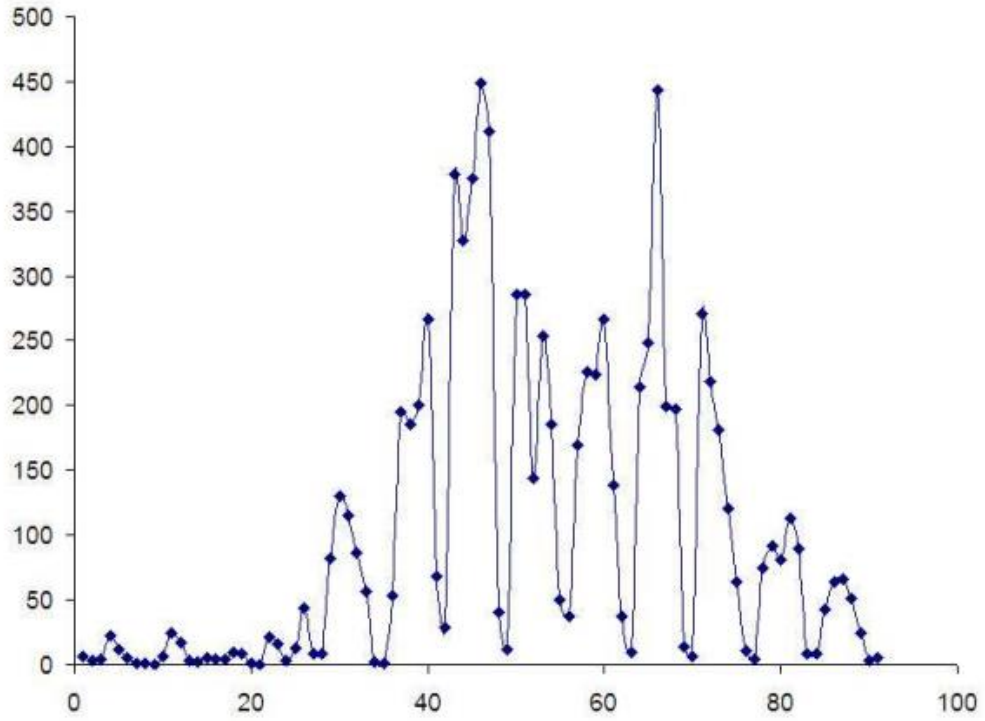

Рис.2.4. Системи контент-моніторингу InfoStream.

Розглянуті практичні приклади дозволили зробити деяку загальну методику проведення оборонної інформаційної операції з використанням

системи контент-моніторингу веб-ресурсів. Припустимо, об'єктом агресивної інформаційної операції є компанія «АБВ». Пропонується такі 12 кроків протидії:

1. Збір інформації з публікаціями в «чужих» (що не мають відношення до «АБВ») ЗМІ про компанії.

2. Побудова графіка – динаміки появи повідомлень про компанії «АБВ» в мережевих ЗМІ.

3. Аналіз динаміки з ретроспективою в 6-12 місяців за допомогою методів аналізу часових рядів. Після цього аналізується контент публікацій в порогових точках, визначаються моменти, тривалість, періодичність впливу, прив'язка моментів впливу до інших подій з області інтересу об'єкта.

4. Визначення джерел, що публікують найбільшу кількість негативу (публікацій з негативною тональністю) про компанію «АБВ».

5. Визначення «першоджерел» публікацій в ЗМІ.

6. Визначення ймовірних «замовників».

7. Визначення сфер спільних інтересів компанії «АБВ» і потенційних «замовників» (Шляхом виявлення загальних інформаційних характеристик – пересічних «Інформаційних портретів» системи InfoStream, що будуються для об'єкта і «Замовника»), ранжування потенційних «замовників» по їх інтересам.

8. Визначення критеріїв інформаційних впливів на основі найрейтинговіших інтересів.

9. Моделювання інформаційних впливів, для чого знаходяться зв'язку «замовника» – найбільш пов'язані з ним особи та організації, аналізується динаміка впливу з боку замовника і будується прогноз цієї динаміки, аналізується контент публікацій в порогових точках кривої динаміки – визначаються критичні точки впливу.

10. Прогнозуються подальші кроки впливу шляхом аналізу аналогічної динаміки публікацій для інших компаній в ретроспективної бази даних системи InfoStream.

11. З урахуванням реалій і публікацій з ретроспективної бази даних оцінюються ймовірні наслідки.

12. Організовується інформаційна (і не тільки) протидія. Приклади публікацій в контексті протидії знаходяться в ретроспективної бази даних.

Наведений план, очевидно, є рафінованим, орієнтованим виключно на дані контент-моніторингу веб-ресурсів. Природно, на практиці орієнтація лише на єдиний тип джерел може призвести до дефіциту інформації, необхідної для прийняття рішень, неточностей, а часом – до неінформованості.

Лише застосування комплексних систем, які базуються на використанні численних джерел і баз даних, поряд з наведеними вище можливостями системи контент моніторингу, може гарантувати ефективну інформаційну підтримку при протидії інформаційним операціям.

Тепер розглянемо приклади використання інформаційних операцій у самих соціальних мережах.

Окремим прикладом використання Росією ботів у Twitter, що впливали на політичні уподобання громадян інших держав був акаунт «@TEN_GOP», котрий був дуже помітним «голосом» в американських правих, за яким стежили понад 130 000 осіб, а деякі помічники Трампа робили репости його записів під час передвиборчої кампанії. Коли діяльність цього облікового запису була припинена у липні 2017 року, то в мережі навіть почалися протести американських правих радикалів, не згодних із закриттям аканту. Але вже в жовтні Twitter підтвердив, що акаунт «@TEN_GOP» був фейковим і керувався російським оператором, пов'язаним із так званою «фабрикою тролів» в Санкт-Петербурзі.

@TEN_GOP був шедевром дезінформації та маскування: російський акаунт, який маскувався під американця понад 18 місяців, обманюючи друзів і ворогів президента Дональда Трампа в засобах масової інформації, в соціальних мережах і навіть в кампанії Трампа.

Його успіх прийшов від його поетапного підходу. По-перше, він наслідував справді вкрай правим коментаторам, публікуючи гіперпартизанські твіти, і привертав їхню увагу згадкою і похвалою. Їх відповіді дали йому видимість легітимності, яка дозволила йому взаємодіяти з високопоставленими фігурами, в тому числі в кампанії, і цитуватися справжніми ЗМІ.

Всюди він зберігав свій обраний характер, публікуючи твіти, в яких говориться, що він американський патріот, прихильник Трампа і крайніх правих, ворог ісламу і критик лібералізму. Ряд аналітиків запідозрив і в кінцевому підсумку довів, що він росіянин за походженням; але їх коментарів було недостатньо, щоб припинити публікацію.

Коротка, але вражаюча кар'єра @TEN_GOP показує, наскільки Америка залишається відкритою для спроб іноземного впливу. Це була анонімна обліковий запис, що не має зв'язку з республіканською партією, з якою вона пов'язувала себе, однак вона придбала величезну довіру, спочатку в крайньому правому куті, а потім в основному потоці, виключно завдяки своїм партизанським постам. Крайні праві коментатори підтримали це; головні

джерела і політики цитували це; ліберали напали на нього; всі були обдурені цим. Поки користувачі соціальних мереж продовжують сліпо приймати й ділитися анонімними, гіпер-партизанськими обліковими записами, вони залишаються відкритими для всіх облікових записів наступника, якою тепер керують оператори @TEN_GOP, – і для будь-яких інших дезінформаційних акторів, що володіють достатніми навичками маскування. В лютому 2018 року

Міністерство юстиції США висунуло звинувачення на адресу «Агентства інтернет-досліджень» у змові проти Сполучених Штатів та втручанні у вибори 2016 року.

15 березня 2018 року адміністрація Президента США Дональда Трампа запровадила фінансові санкції проти «Агентство інтернет-досліджень», також відома як AZIMUT LLC; MEDIASINTEZ LLC;MIXINFO LLC; NOVINFO LLC), деяких пов'язаних з нею компаній, ФСБ та ГРУ.

23 березня 2018 року соціальна мережа Tumblr повідомила про блокування та видалення 84 облікових записів, які були пов'язані з «Агентством інтернет-досліджень» та поширювали дезінформацію під час виборів 2016 року. Ці облікові записи не платили за рекламу, натомість були зосереджені на поширенні повідомлень, які б мали вигляд звичайних повідомлень від звичайних користувачів.Американська сага про те, хто у кого і з чиєю допомогою вкрав / додав голосу на президентських виборах 2016 року, триває.

Переживши розслідування прокурора Мюллера, президент Трамп тепер переходить в атаку на свого супротивника Хілларі Клінтон, чия демократична партія звинувачує його в «змові з Москвою».

Президент США оголосив у своєму Twitter'e про те, що це Хілларі і її команда маніпулювала підрахунком голосів:

«Вау, тільки що вийшла доповідь! Google маніпуляціями додав від 2,6 мільйона до 16 мільйонів голосів за Хілларі Клінтон на виборах 2016 року! Це публікує прихильник Клінтон, що не Трампа! На Google треба подати в суд. Моя перемога була навіть більше, ніж думали! @ Judicial Watch ».

Трамп не пояснив, яку доповідь він має на увазі, хоча поставив посилання на правову організацію «Judicial Watch». Зате ми самі поцікавилися, звідки виходить ця інформація?

Так, в Twitter'е «Judicial Watch» є новина на цю тему. Однак, найцікавіше, що претензії – якщо не звинувачення – на адресу Google і Хілларі Клінтон прозвучали за кілька днів до цього в стінах Конгресу США. Про що і повідав місту і світу "Judicial Watch».

Кілька днів тому на засіданні сенатського юридичного підкомітету з Конституції Роберт Епштейн (Dr. Robert Epstein), психолог з каліфорнійського «Американського інституту поведінкових досліджень і технологій» (American Institute for Behavioral Research and Technology - Vista, California) стверджував, що «biased search results generated by Google's search algorithm likely impacted undecided voters in a way that gave at least 2.6 million votes to Hillary Clinton, whom I supported ». – «необ'єктивними результати пошуку інформації, згенеровані алгоритмом пошуку Google, ймовірно, вплинули на виборців, які до цього не вирішили, кому віддати свій голос на виборах, таким чином, що Хілларі Клінтон, яку я підтримував, отримала додатково не менше 2,6 мільйона голосів ».

Ще раз: «Хіларі Клінтон отримала додатково не менше 2,6 мільйона голосів». При цьому Епштейн впевнений, що широкі маніпуляції подібного роду можуть принести на виборах 2020 до 15 мільйонів голосів! Трамп у своєму твіти помилився з цією цифрою ...

І далі – «... This system must be built to keep an eye on big tech in 2020 року, because if these companies all support the same candidate, they will have the power to shift 15 million votes to that candidate. To let big tech get away with subliminal manipulation on this scale would be to make the free and fair election meaningless ». – «Система (протидії) повинна бути створена, щоб у 2020 році наглядати за новими технологіями, оскільки, якщо ці компанії (Google та ін.) Підтримують одного і того ж кандидата, вони будуть в змозі перевести на нього 15 мільйонів голосів. Дозволити нової технології вийти з-під контролю з її підсвідомими

маніпуляціями подібного масштабу – значить, зробити вільні та чесні вибори безглуздими ».

У дослідженні, яке цитував Роберт Епштейн, було зібрано сотні тисяч результатів з пошукової системи, зібрані напередодні виборів 2016 року, і був зроблений висновок про те, що феномен, званий «ефектом маніпуляції пошуковою системою», дійсно вплинув на число голосів ... в користь Хілларі.

Brexit

Brexit міг би не статися, якби не витік даних користувачів Facebook у 2016 році. Про це, виступаючи перед членами комітету Палати громад британського парламенту, сказав колишній співробітник британської компанії Cambridge Analytica Крістофер Уайлі, повідомляє Bloomberg.

За його словами, Cambridge Analytica отримала сотні тисяч фунтів стерлінгів від лобістів виходу Сполученого Королівства зі складу Євросоюзу.

Як стверджує Уайлі, для розробки алгоритму впливу на громадську думку застосовувався додаток для аналізу особистості, розроблений дослідником Кембриджського університету Олександром Коганом, і персональні дані 50 млн користувачів Facebook, які опинилися в розпорядженні компанії. На думку екс-працівника Cambridge Analytica, на результати референдуму вплинув обман.

Скандал навколо ймовірного витоку даних користувачів Facebook розгорівся 19 березня. Телеканал Channel 4 News зняв на приховану камеру розмову з главою британської компанії Cambridge Analytica Олександром Нікс, який зізнався, що понад 200 разів впливав на виборчі кампанії по всьому світу.

Вперше про можливе застосування Cambridge Analytica методів психометрії писав в грудні 2016 року швейцарський журнал Das Magazin. Компанія намагалася моделювати переваги користувачів соцмереж, показуючи їм релевантну політичну рекламу.

Референдум про вихід Великобританії з ЄС відбувся 23 червня 2016 року. Згідно з його результатами, 51,9% британців проголосували за вихід країни зі спільноти, 48,1% – хотіли залишитися в ЄС.

Офіційна процедура виходу Британії з ЄС стартував 29 березня 2017 року і зайняла два роки.

Які витрати на передвиборчу кампанію і рекламу були ми розглянемо далі. Безумовно, вибори в США найдорожчі у світі. У наведеній нижче таблиці вказана інформація про витрати на проведення президентських кампаній головних кандидатів Демократичної та Республіканської партій. Жирним шрифтом виділено кандидат, який отримав перемогу. Таблиця заснована на даних Федеральної виборчої комісії США.

Таблиця 2.1.

Витрати на передвиборчу кампанію і рекламу в США

Рік	Республіканська партія	Демократична партія
2000	**Джордж Буш - 280 млн $**	Альберт Гор - 231 млн $
2004	**Джордж Буш - 251 млн $**	Джон Керри - 392 млн $
2008	Джон Маккейн - 333 млн $	**Барак Обама - 730 млн $**
2012	Митт Ромни - 443 млн $	**Барак Обама - 652 млн $**
2016	**Дональд Трамп - 429 млн $**	Хиллари Клинтон - 898 млн $

Говорячи про вибори які пройшли у 2016 році в США, за даними ФБК, на лютий 2016 року в виборчі комітети всіх учасників в цілому надійшло 503,7 млн. $., З яких республіканці залучили 268,6 млн., А демократична партія – 234,8 млн., решта – близько 0,3 млн. долл. За даними газети «Нью-Йорк таймс», представники 158 найбагатших сімей штатів до кінця вересня 2015 року, тобто в ще на самому початку проведення агітаційних заходів, на просування найбільш значущих кандидатів від республіканців (крім Д. Трампа) і демократів (крім Б. Сандерса) вклали близько 176 млн. $. (Половину від загального обсягу на той період).

Мільярдер Дональд Трамп, який представляє республіканців, до початку праймеріз практично повністю фінансував свою виборчу кампанію коштом особистих капіталовкладень, які склали понад 90%, його опонент, позасистемний кандидат демократів Б. Сандерс просував свої ідеї шляхом пожертвувань фізичних осіб з порівняно низькими доходами.

Найбільше коштів безпосередньо на рахунок виборчого фонду отримала представниця Демократичної партії Х. Клінтон з сумою в 130,4 млн. $., З яких 120,5 млн. Були пожертвувані фізичними особами, а на внески ККД припадало близько 1 млн., 500 000 її власних грошей., а ще різні трансферти в розмірі 4,4 млн.дол.

Клінтон і Трамп по-різному витрачали гроші своїх кампаній. Трамп витратив на рекламу 68 млн. $ Проти 237 млн. $ Клінтон і при цьому ні на день не сходив зі сторінок новинних порталів і газет, завдяки своєму скандальному і яскравого іміджу.

Таким чином, можна зробити кілька важливих зауважень. Якщо ще у 2000 році сукупний обсяг виборчих фондів політичних партій в США становив 511 млн. $, То у 2016 році 1,38 млрд. $, Що у 2,7 рази більше. Наведена статистика свідчить про зростальний вплив грошей в політиці та про перетворення капіталу в засіб досягнення політичної влади, хоча перемоги на президентських виборах гроші гарантувати не можуть.

Тепер розглянемо методи і техніки аналізу великих даних

Вікіпедія станом на середину 2018 року давала таке визначення терміну Big Data:

«Великі дані (Big Data) – позначення структурованих і неструктурованих даних величезних обсягів і значного різноманіття, які ефективно обробляються горизонтально масштабованими програмними інструментами, що з'явилися в кінці 2000-х років і альтернативних традиційним системам управління базами даних і рішень класу Business Intelligence».

Як бачимо, в цьому визначенні присутні такі терміни, як «величезних», «значного», «ефективно» і «альтернативних». Навіть сама назва вельми

суб'єктивна. Наприклад, 4 Терабайта (місткість сучасного зовнішнього жорсткого диска для ноутбука) – це вже великі дані чи ще ні? До цього визначення Вікіпедія додає наступне: «в широкому сенсі про "великі дані" говорять як про соціально-економічний феномен, пов'язаний з появою технологічних можливостей аналізувати величезні масиви даних, в деяких проблемних областях – весь світовий обсяг даних, і випливаючи із цього трансформаційні наслідки».

Аналітики компанії IBS «весь світовий обсяг даних» оцінили такими величинами:

2003 р. – 5 ексабайт даних (1 ЕБ = 1 млрд гігабайтів)

2008 р. – 0,18 зеттабайт (1 ЗБ = 1024 ексабайта)

2015 р. – понад 6,5 зеттабайт

2020 р. – 40-44 зеттабайт (прогноз)

2025 р. – цей обсяг зросте ще в 10 разів

У доповіді також наголошується, що більшу частину даних генерувати будуть не звичайні споживачі, а підприємці.

Можна користуватися і більш простим визначенням, цілком відповідним думці журналістів і маркетологів.

«Великі дані – це сукупність технологій, які покликані здійснювати три операції:

1. Обробляти великі в порівнянні з «стандартними» сценаріями обсяги даних.

2. Вміти працювати зі швидко надходячими даними в дуже великих обсягах. Тобто даних не просто багато, а їх постійно стає все більше.

3. Вміти працювати зі структурованими та слабо структурованими даними паралельно і в різних аспектах .

Вважається, що ці «вміння» дозволяють виявити приховані закономірності, що вислизають від обмеженого людського сприйняття. Це дає безпрецедентні можливості оптимізації багатьох сфер нашого життя: державного управління, медицини, телекомунікацій, фінансів, транспорту,

виробництва і так далі. Тож не дивно, що журналісти та маркетологи настільки часто використовували словосполучення Big Data, що багато експертів вважають цей термін дискредитованим і пропонують від нього відмовитися.

Більш того, в жовтні 2015 року компанія Gartner виключила Big Data з-поміж популярних трендів. Своє рішення аналітики компанії пояснили тим, що до складу поняття «великі дані» входить велика кількість технологій, вже активно застосовуються на підприємствах, вони частково належать до інших популярних сфер і тенденціям і стали повсякденним робочим інструментом.

Хоч би що там було, термін Big Data як і раніше широко використовується.

Три "V" (4, 5, 7) і три принципу роботи з великими даними

Визначальними характеристиками для великих даних є, крім їх фізичного обсягу, і інші, що підкреслюють складність завдання обробки та аналізу цих даних. Набір ознак VVV (volume, velocity, variety – фізичний обсяг, швидкість приросту даних і необхідності їх швидкої обробки, можливість одночасно обробляти дані різних типів) був вироблений компанією Meta Group у 2001 році з метою вказати на рівну важливість управління даними по всім трьом аспектам. Надалі з'явилися інтерпретації з чотирма V (додавалася veracity – правдивість), п'ятьма V (viability – життєздатність і value – цінність), сім'ю V (variability – мінливість і visualization – візуалізація). Але компанія IDC, наприклад, інтерпретує саме четвертий V як value (цінність), підкреслюючи економічну доцільність обробки великих обсягів даних у відповідних умовах. Виходячи з вищенаведених визначень, основні принципи роботи з великими даними такі:

Горизонтальна масштабованість. Це – базовий принцип обробки великих даних. Як вже говорилося, великих даних з кожним днем стає все більше. Відповідно, необхідно збільшувати кількість обчислювальних вузлів, за якими розподіляються ці дані, причому обробка повинна відбуватися без погіршення продуктивності.

Відмовостійкість. Цей принцип випливає з попереднього. Оскільки обчислювальних вузлів в кластері може бути багато (іноді десятки тисяч) і їх кількість, не виключено, що буде збільшуватися, зростає і ймовірність виходу машин з ладу. Методи роботи з великими даними повинні враховувати можливість таких ситуацій і передбачати превентивні заходи.

Локальність даних. Через те, що дані розподілені по великій кількості обчислювальних вузлів, то, якщо вони фізично знаходяться на одному сервері, а обробляються на іншому, витрати на передачу даних можуть стати невиправдано великими. Тому обробку даних бажано проводити на тій же машині, на якій вони зберігаються.

Ці принципи відрізняються від тих, які характерні для традиційних, централізованих, вертикальних моделей зберігання добре структурованих даних. Відповідно, для роботи з великими даними розробляють нові підходи та технології.

Технології та тенденції роботи з Big Data. Спочатку в сукупність підходів і технологій включалися засоби масової-паралельної обробки невизначено структурованих даних, такі як СУБД NoSQL, алгоритми MapReduce і засоби Hadoop. Надалі до технологій великих даних стали відносити й інші рішення, що забезпечують подібні за характеристиками можливості по обробці надвеликих масивів даних, а також деякі апаратні засоби.

MapReduce – модель розподілених паралельних обчислень в комп'ютерних кластерах, представлена компанією Google. Відповідно до цієї моделі додаток поділяється на велику кількість однакових елементарних завдань, що виконуються на вузлах кластера та потім природним чином приводяться в кінцевий результат.

NoSQL (від англ. Not Only SQL, не тільки SQL) – загальний термін для різних не реляційних баз даних і сховищ, що не позначає якусь одну конкретну технологію або продукт. Звичайні реляційні бази даних добре підходять для досить швидких і однотипних запитів, а на складних і гнучко побудованих

запитах, характерних для великих даних, навантаження перевищує розумні межі та використання СУБД стає неефективним.

Hadoop – вільно поширюваний набір утиліт, бібліотек і фреймворк для розробки та виконання розподілених програм, що працюють на кластерах з сотень і тисяч вузлів. Вважається однією з основоположних технологій великих даних.

R – мова програмування для статистичної обробки даних і роботи з графікою. Широко використовується для аналізу даних і фактично став стандартом для статистичних програм.

Апаратні рішення. Корпорації Teradata, EMC і ін. Пропонують апаратно-програмні комплекси, призначені для обробки великих даних. Ці комплекси поставляються як готові до установки телекомунікаційні шафи, містять кластер серверів і програмне забезпечення, що керує для масово-паралельної обробки. Сюди також іноді відносять апаратні рішення для аналітичної обробки в оперативній пам'яті, зокрема, апаратно-програмні комплекси Hana компанії SAP і комплекс Exalytics компанії Oracle, дарма що те, що така обробка з самого спочатку не є масово-паралельною, а обсяги оперативної пам'яті одного вузла обмежуються декількома терабайтами.

Консалтингова компанія McKinsey, крім розглянутих більшістю аналітиків технологій NoSQL, MapReduce, Hadoop, R, включає в контекст можливість застосування для обробки великих даних також технології Business Intelligence і реляційні системи управління базами даних з підтримкою мови SQL.

Міжнародна консалтингова компанія McKinsey, що спеціалізується на вирішенні завдань, пов'язаних зі стратегічним управлінням, виділяє 11 методів і технік аналізу, які можна застосувати до великих даними.

- Методи класу Data Mining (видобуток даних, інтелектуальний аналіз даних, глибинний аналіз даних) – сукупність методів виявлення в даних раніше невідомих, нетривіальних, практично корисних знань, необхідних для прийняття рішень. До таких методів, зокрема, відносяться навчання

асоціативними правилами (association rule learning), класифікація (розбиття на категорії), кластерний аналіз, регресійний аналіз, виявлення та аналіз відхилень і ін.

- Краудсорсинг – класифікація і збагачення даних силами широкого, невизначеного кола осіб, які виконують цю роботу без вступу в трудові відносини.
- Змішування та інтеграція даних (data fusion and integration) – набір технік, що дозволяють інтегрувати різнорідні дані з різноманітних джерел з метою проведення глибинного аналізу (наприклад, цифрова обробка сигналів, обробка природної мови, включаючи тональний аналіз, та ін.)
- Машинне навчання, включаючи навчання з учителем і без вчителя – використання моделей, побудованих на базі статистичного аналізу або машинного навчання для отримання комплексних прогнозів на основі базових моделей
- Штучні нейронні мережі, мережевий аналіз, оптимізація, в тому числі генетичні алгоритми (genetic algorithm – евристичні алгоритми пошуку, які використовуються для вирішення завдань оптимізації та моделювання шляхом випадкового підбору, комбінування і варіації шуканих параметрів з використанням механізмів, аналогічних природному відбору в природі)
- Розпізнавання образів
- Прогнозна аналітика
- Імітаційне моделювання (simulation) – метод, що дозволяє будувати моделі, що описують процеси так, як вони проходили б насправді. Імітаційне моделювання можна розглядати як різновид експериментальних випробувань
- Просторовий аналіз (spatial analysis) – клас методів, які використовують топологічну, геометричну і географічну інформацію, видобуту з даних
- Статистичний аналіз – аналіз часових рядів, A / B-тестування (A / B testing, split testing – метод маркетингового дослідження; при його використанні контрольна група елементів порівнюється з набором тестових груп, в яких один

або кілька показників були змінені, для того щоб з'ясувати, які зі змін покращують цільовий показник)

- Візуалізація аналітичних даних – подання інформації у вигляді малюнків, діаграм, з використанням інтерактивних можливостей та анімації як для отримання результатів, так і для використання в якості вихідних даних для подальшого аналізу. Дуже важливий етап аналізу великих даних, що дозволяє представити найважливіші результати аналізу в найбільш зручному для сприйняття вигляді.

У третьому розділі даної роботи автор розповість про рекомендації щодо кібергігієни, розробки і покращення нових технологій та реалізацію методики виявлення потенційно небезпечних повідомлень в соціальних мережах.

А далі ми з Вами розглянемо особливості розробки системи пошуку потенційно небезпечних повідомлень в соціальних мережах та методи боротьби з ними.

ВИСНОВКИ ДО ДРУГОГО РОЗДІЛУ

Ми живемо в епоху швидких змін. Їх прискорення формує інформаційне суспільство, для якого характерний дефіцит інформації, потрібної для прийняття рішень. Це позбавляє людину самостійного мислення, перетворюючи його на слухняного учня експертів, які часто виявляються агентами впливу зацікавлених осіб. Виникають небачені раніше можливості опановування капіталом і владою шляхом інформаційних операцій і війн. У другому розділі роботи автор розкрив тему аудиторії та характеристики українських соціальних мереж. Дослідив які бувають типи інформаційних операцій у соціальних мережах, роздивились приклади використання інформаційних операцій у самих соціальних мережах, та довів, що Brexit міг би не статися, якби не витік даних користувачів Facebook у 2016 році.

Також були розглянуті методи, техніки, принципи аналізу роботи з великими даними.Тепер зрозуміло,що таке спам, як його визначити та чому спам – це небезпечно для Вас та Ваших гаджетів.

РОЗДІЛ 3. РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ПОТЕНЦІЙНО НЕБЕЗПЕЧНИХ ПОВІДОМЛЕНЬ В СОЦІАЛЬНИХ МЕРЕЖАХ

3.1. Особливості розробки системи пошуку потенційно небезпечних повідомлень в соціальних мережах та методи боротьби з ними

У сучасному суспільстві електронна пошта і соціальні мережі стали незамінним засобом практично моментально обміну інформацією в діловій і особистій сферах. Однак при такому великої переваги в цьому процесі є і ряд негативних моментів.

Йдеться про спам – масову неперсоніфіковану розсилку комерційної, політичної та іншої реклами або іншого виду повідомлень особам, які не виражав бажання їх отримувати, яка не тільки викликає роздратування і невдоволення одержувачів корисної інформації, втрату їхнього особистого часу, відволікає від виконання службових обов'язків, а й значно збільшує навантаження на комунікації, підвищує трафік, знижує ефективність роботи серверів. Для обходу антиспам-фільтрів окремі користувачі або організації, зацікавлені в збільшенні, наприклад, рекламної розсилки, намагаються використовувати будь-яку можливість. Тому так актуальна потреба в розробці нових підходів, що дозволяють підвищити ефективність виділення небажаної й дуже часто шкідливої кореспонденції і виключити її з потоків вхідних повідомлень.

Формулювання завдання і пропонований метод її рішення:

До технологій, що дозволяє отримати високоефективні рішення, що перевершують по своїй результативності інші часто використовувані підходи, відносяться ті, які реалізовані в рамках систем штучного інтелекту (СШІ). Людина як засіб боротьби зі спамом має здатність виявлення його ознак, ґрунтуючись на власному досвіді та перевагах, знаннях про добровільні

новинних і рекламних підписках, його робота не зводиться до шаблонів і тому високоефективна. Саме тому завдання розробки засобів боротьби зі спамом в цей час зосереджене на наділення їх навичками і якостями, властивими людині, з одного боку, а з іншого боку – на використанні оптимізаційних механізмів.

Подібний висновок заснований на результатах порівняльного аналізу роботи ряду чинних методів виявлення спаму за різними параметрами. дослідження показали, що доцільно розробити новий, який базується на евристичних методах оптимізації, підхід до вирішення поставленого завдання виявлення спаму, який би мав малу частоту помилкових спрацьовувань, але до того ж володів великою ефективністю на початковій стадії навчання. Серед різноманітних компонент CI, що моделюють різні процеси живої природи, одним з найбільш перспективних методів виявлення спаму є створення штучних імунних систем (ІВС, або Artificial Immune Systems, AIS), де програмним шляхом представлені, досліджуються і використовуються властивості та механізми живих організмів, забезпечують їх виживання. У даній постановці описана вище завдання вимагає забезпечення виживання в потоці електронної пошти корисної інформації та відсіювання небажаної.

Біологічним прототипом ІВС є імунна система людини, а точніше обробка інформації в ній молекулами білків. Ця система являє собою складну адаптивну структуру, яка використовує комбінацію різних механізмів захисту від зовнішніх і внутрішніх патогенів, в тому числі будь-яких мікроорганізмів, здатних викликати патологічний стан (хвороба) людини. Основні сучасні методи боротьби зі спамом можна розділити на наступні категорії:

- методи, засновані на аналізі змісту листа;
- «Білі» і «чорні» списки;
- детектори масових розсилок;
- методи, засновані на верифікації зворотної адреси відправника та його домену та ін.

Водночас слід зазначити, що методи боротьби зі спамом, засновані на лінгвістичних сигнатури, правилах фільтрації повідомлень, стають все менш

ефективними, т. к. вимагають значного збільшення трудовитрат фахівців на підтримку бази сигнатур і правил в актуальному стані. Деякі з перерахованих вище методів боротьби зі спамом були введені в розроблений програмний комплекс для проведення порівняльного аналізу їх результатів з ре злиттів функціонування пропонованого підходу на основі ІВС.

Евристичний підхід до визначення спаму

Структура імунної системи. Захисна система людини має ієрархічну багаторівневу структуру. Перший фізичний бар'єр на шляху бактерій і вірусів – це шкірний покрив. Другий рівень захисту – біохімічний, реалізується за допомогою продуктів потових, слинних та інших залоз. Третій і четвертий рівні представлені вродженим і набутим імунітетом.

Імунітет – здатність спеціальних клітин організму впізнавати, зв'язувати й виводити з нього речовини та структури, що походять з клітин інших організмів або втратили схожість з клітинами власного тіла, – чужорідних агентів (патогенів). Вроджений і набутий імунітет працюють саме в зазначеній послідовності. Спочатку неспецифічну реакцію на патоген здійснює вроджена імунна система. Якщо ж вроджена імунна система з патогеном не справляється, то в сутичку з ним вступає придбана імунна система.

В імунній відповіді організму беруть участь два типи клітин – фагоцити та лімфоцити.

Фагоцити – це клітини імунної системи, основною функцією яких є поглинання антитіл (а також мертвих або тих, хто гине клітин організму). Основна роль фагоцитів – здійснення функції вродженої імунної системи.

Найбільшою мірою для використання в інтелектуальних системах (ІС) підходить набутий імунітет, який реалізується призначеними для цієї мети клітинами – лімфоцитами. Людина, ІС якого є біологічним прототипом ІВС, зберігає своє здоров'я до тих пір, поки рівень активності лімфоцитів, а значить і його імунітет, достатньо високі. Для підтримки цієї здатності на бажаному для організму рівні потрібно також збереження певного рівня активності деяких видів клітин. Підтримка ж імунітету людини на необхідному рівні, в свою

чергу, досягається завдяки безперервним впливам на його організм патогенів, які називаються антигенами. Якщо людину звільнити від подібних впливів, створити йому стерильне середовище проживання, його імунітет ослабне.

Антигени – макромолекулярні сполуки з жорсткою структурою (білки, пептиди, полісахариди, нуклеїнові кислоти, комплексні сполуки та ін.), Які викликають імунну відповідь організму – імунні реакції, що підтримують активність лімфоцитів. Можна сказати, що антигени – це агенти, у відповідь на появу яких в організмі імунна система утворює спеціальні реагують з ними антитіла.

За функціональними ознаками розрізняють кілька типів лімфоцитів, головними з яких є В-лімфоцити, які здійснюють розпізнавання антигенів і вироблення антитіл. Серед В-лімфоцитів виділяють клітини «пам'яті», що живуть відносно довго і зберігають в собі інформацію про зустрінутих раніше організмом чужорідних білках. Розпізнавання антигенів В-лейкоцитами засноване на комплементарності між рецепторами цих клітин

і активними ділянками антигену, що утворюють його область зчеплення.

Комплементарністю називають просторову взаємодоповнюваність молекул або їх частин, що приводить до утворення зв'язків між ними. У антитіл може бути тільки один рецептор, в той час як антигени можуть мати їх велике число. При розпізнаванні В-лімфоцитами антигенів збіг образу антигену в рецепторах і зустрінутого антигену може бути неповним.

Дуже важливою характеристикою обговорюваних процесів взаємодії в ІВС антигену та антитіла є значення функції афінності (лат. Affinitas – спорідненість), кількісно описує силу взаємодії речовин. Значення функції афінності можна визначити за законом що діє мас як відношення концентрації комплексу «антиген - антитіло» до добутку концентрацій компонентів.

Штучна імунна система. Для створення ІВС необхідно виділити її основні компоненти та визначити математичну модель їх функціонування. Перед ІВС виявлення спаму стоїть завдання створення механізму визначення

приналежності повідомлення до одного з двох підмножин: «спам» – «не спам», тобто завдання класифікації.

З точки зору розв'язування задачі виділимо наступні властивості ІС:

1. Розпізнавання свого і чужого – одна з основних задач ІС.

2. Виділення особливостей. Кожна антиген-клітина служить фільтром, який фокусує увагу лімфоцитів-рецепторів.

3. Різноманітність. Імунна система використовує комбінаторний механізм для освіти безлічі різних рецепторів лімфоцитів, гарантуючи, що хоча б один лімфоцит з усієї сукупності зможе взаємодіяти з будь-яким відомим або невідомим антигеном.

Навчання складається в зміні концентрації лімфоцитів, яке відбувається при первинному відповіді й закладено в механізмі поповнення клонів з урахуванням поточного стану системи.

Пам'ять – це невелика частина лімфоцитів, що знаходяться в активованому стані.

1. Розподілений пошук. За своєю суттю ІС – це розподілена система.

2. Саморегуляція. Залежно від властивостей антигену, регуляція імунної відповіді може бути як локальної, так і системною.

3. Граничний механізм. Імунна відповідь і клонування клітин відбувається лише після

1. подолання деякого порогу, що залежить від сили хімічних зв'язків.

4. Спільна стимуляція. Активація В-лімфоцитів жорстко регулюється за допомогою додаткового стимулюючого сигналу від хелперних Т-лімфоцитів, що допомагає усвідомлювати різницю між небезпечними та безпечними антигенами.

5. Ймовірне виявлення. Перехресні реакції в ході імунної відповіді - це процес стохастичний. Лімфоцит може взаємодіяти з декількома структурно подібними антигенами. Найбільш відомою з теорій, що пояснюють механізм виробництва антитіл ІС, є клонально-селекційна теорія Бернета, відповідно до якої при розпізнаванні. По-клітин антигену вони стимулюються і починають

синтезувати антитіла з тієї ж специфічністю шляхом клонування. При цьому число клонів, вироблених В-лімфоцитів, пропорційно рівню його стимуляції.

Процес, який викликає клонування тільки тих По-клітин, які синтезують потрібний тип антитіл, називають колосальним відбором. Можна сказати, що клональний відбір створює подпопуляцію В-клітин, призначену для боротьби з відповідним антигеном.Після придушення проникнення в організм даного антигена велика частина клонованих В-клітин руйнується. Решта клітини реалізують функцію імунної пам'яті, так що подальший вплив схожого антигену призводить до більш швидкої імунної реакції. Даний підхід ліг в основу запропонованої методики детектування спаму. Слід зазначити, що нині для генерації і відбору клону розроблений цілий ряд алгоритмів, і цей напрямок продовжує постійно розвиватися. Рухом цього процесу, природно, керують ті що підлягають вирішенню прикладні завдання, де необхідна оптимізація, і переважно за допомогою оптимізаційних механізмів живої природи. відомі, наприклад, алгоритми адаптивного клонування, що пропонують деякі зміни на основі аналізу операторів для вибору кількості мутацій і кількості клонів; алгоритми, інтегрують локальний пошук з глобальним пошуком і багато інших.

Детектування спаму на основі ІВС

Лімфоцити на своїй поверхні містять безліч рецепторів, пов'язаних з певною частиною патогена. Лімфоцит може позначати як «чужого» об'єкта той патоген, на який зреагував його рецептор. В активний стан лімфоцит переходить після того, як певна кількість його рецепторів зреагує на патоген. Після цього відбувається ряд хімічних реакцій, які в підсумку знищують патоген.

Використовувана в роботі модель виявлення спаму включає тільки один клас детекторів. Рецептор і патоген спочатку представлені у вигляді рядків, а хімічний зв'язок між ними

змодельована на основі відповідності цих рядків. Ступінь відповідності двох рядків може обчислюватися різними методами. Одним з них є метод обчислення ступеня відповідності рядків із застосуванням модифікованого

фонетичного алгоритму Soundex. Принцип даного алгоритму заснований на приведенні тексту до нижнього регістра, виключення прогалин, розділових знаків, голосних букв, м'якого і твердого знаків і розбитті приголосних букв на групи з порядковими номерами. Відповідність букв і цифр, які заміняють

Букви й цифра-заміна:

Б, П 1

В, Ф 2

Г, К 3

Д, Т 4

З, З 5

Ж, Ш, Щ 6

Х, Ц, Ч 7

Л, М, Н 8

Р, Й 9

Для визначення ступеня відповідності двох рядків доцільно застосувати коефіцієнт Танімото:

$$k = \frac{c}{a + b - c}$$

де k - коефіцієнт Танімото від 0 до 1; a, b - кількість елементів в першому і в другому множинах; c - кількість спільних елементів у двох підмножинах.

Основна мета еволюційних методів оптимізації взагалі та генетичних алгоритмів (ГА) зокрема полягає у визначенні кращих представників своєї популяції, найбільш пристосованих до поточних умов, і передачі генів майбутнім поколінням. Для інтелектуальної системи детектування спаму визначено ряд наступних операторів: формування початкової популяції та навчання лімфоцитів, оператор мутації (ОМ), оператор рекомбінації або

кросовера (ОК), оператор репродукції (ОР), – які відіграють важливу роль в роботі ІВС. Така система при своєму запуску потребує попереднього навчання.

Імунологічне навчання клітин. Розглянемо механізм навчання з точки зору ІВС. На початку роботи моделюється детектор, який буде реагувати на спам: визначається довжина рядка детектора і відбувається її генерація випадковим чином на основі генератора псевдовипадкових чисел. На цьому етапі навчання детектори реагують і на «спам», і на «не спам».

Активовані детектори на цій стадії процесу навчання програма знищує. Для початкового навчання детекторів в ІВС задається період навчання Т. Під час імунологічного навчання детектори повинні взаємодіяти з «легальної» кореспонденцією. Після завершення періоду навчання в разі активації детектора ІВС отримає сигнал про те, що була розпізнана чужорідна клітина – спам.

Специфічні особливості операторів ІВС. У підвищенні точності детектування небажаної кореспонденції незамінну роль відіграє ОМ. Мутація – стійка зміна генотипу, що відбувається під впливом зовнішнього або внутрішнього середовища. Оператор мутації, включаючи в процес пошуку хромосоми з новими властивостями, сприяє розширенню області пошуку, дозволяючи системі вийти за межі локального екстремуму. Вважається, що ОМ реалізує «безстатеве» розмноження і є основною пошуковим оператором еволюційних алгоритмів. Для здійснення мутації рядків можуть бути застосовані різні види ОМ. Найпростішим ОМ є одноточковий. При його реалізації випадково вибирають ген в батьківській хромосомі та, обмінюючи його на поруч розташований ген, отримують хромосому нащадка. При використанні двоточкового ОМ випадковим чином вибираються дві точки розрізу з подальшою перестановкою генів.

3.2 Реалізація методики виявлення потенційно небезпечних повідомлень в соціальних мережах та методи боротьби з ними

У цьому розділі даної роботи автор розповість про рекомендації щодо кібергігієни, розробки та покращення нових технологій та реалізацію методики виявлення потенційно небезпечних повідомлень в соціальних мережах.

Нині реалізовані такі методи швидкого збору даних про розсилки (перераховані в порядку убування поширеності у світі):

– приймання спаму в спеціальні «пастки» (honeypot) – E-mail адреси, призначені тільки для прийняття спаму;

– голосування користувачів – користувач, який отримав спам, нотифікує про це систему збору даних, надаючи зразок спаму;

– аналіз всієї проходить через поштову систему пошти з повідомленням контрольних сум окремих повідомлень на центральний сервер.

на такий-то лист поскаржилися стільки-то раз», будуються списки масових на даний момент часу розсилок, які стають доступними учасникам системи в реальному часі. Поштові системи, прийнявши лист, можуть дізнатися його статус і чи відкинути (знищити, перенаправити в архів або карантин) як спам, або передати одержувачу.

Збір спаму за допомогою адрес-«пасток»

Найбільша мережа адрес-пасток для аналізу спаму в реальному часі організована і підтримується компанією Brightmail (www.brightmail.com).

Деталі реалізації відомі тільки з опублікованих цією компанією документів, згідно з ними мережу збору спаму складається більш ніж з мільйона поштових адрес-пасток; дані по спаму поповнюються і користувачами самої системи. На підставі отриманих спам-повідомлень складаються списки сигнатур повідомлень і списки правил аналізу заголовків, які доставляються передплатникам системи практично в реальному часі. Згідно з публікаціями компанії Brightmail, нею використовуються як чіткі сигнатури (hashes), що ідентифікують в точності дане повідомлення, так і нечіткі, які пристосовуються

до мінливих спамерських листів.Рішення Brightmail Anti-Spam є тільки на комерційній основі у вигляді plug-in до систем Sendmail і MS Exchange, online-сервісу і в складі деяких мережевих пристроїв (Network Appliances).

Внаслідок комерційного характеру системи отримати дані про її придатності для фільтрації російського спаму важко. Доступні лише дані тестів PC Magazine, згідно з якими рівень виявлення спаму склав 77.79%, а рівень помилкових спрацьовувань системи – 0.05% всіх повідомлень.яві

Аналогічна схема збору зразків спаму реалізована в системі SkyScan AS компанії MessageLabs. На основі маркетингових документів компанії, можна припустити, що використовуються методи дуже схожі на систему Brightmail; як і в разі Brightmail істотна інформація про систему практично ніде не опублікована.

У тестах PC Magazine сервіс SkyScan показав рівень виявлення спаму в 96% при частці помилкових спрацьовувань 0.48%

Підтримка великої кількості адрес-пасток вимагає великих людських і адміністративних ресурсів – це не повинні бути «порожні» адреси, вони повинні активно функціонувати – публікуватися на WWW-сайтах, форумах і конференціях, реєструватися в онлайн-сервісах і іншим чином імітувати поведінку звичайного користувача з точки зору спамера. По всій видимості, дана технологія може бути застосована тільки в умовах компанії-розробника антиспамерського ПО, або в умовах великого поштового сервісу. Створення подібної системи на базі тільки зусиль волонтерів представляється малоймовірним.

Голосування користувачів

Метод розподіленого виявлення спаму методом голосування користувачів полягає в наступному:

1. Поштова система, яка прийняла лист, розраховує його сигнатуру, передає її на сервер системи виявлення та отримує відповідь – спам це чи ні.

2. .Якщо користувач отримав лист, який він вважає спамом, то він може проголосувати «проти нього» – переправивши в систему збору даних повідомлення про те, що даний лист є спамом.

3. Якщо один лист (одна сигнатура) має досить багато голосів «проти», то система збору даних вважає даний лист спамом.

Вище описана схема реалізована в системі Vipul's Razor / Cloudmark SpamNet.

Ця система містить:

- мережа серверів під управлінням компанії Cloudmark;
- безкоштовне клієнтське ПЗ для Unix (як для поштових серверів, так і для поштових клієнтів) і безкоштовне право використання серверів системи;
- платна підписка на сервіс для клієнтів Windows
- платне серверне ПЗ для Windows-серверів і підписка на сервіс для корпоративних користувачів.

Початково система Vipul's Razor була цілком безкоштовною, проте після виходу Razor Version 2 (Razor v2, червень 2002 роки) встановилася описана вище схема – Безкоштовної версії для Unix-систем і платні для Windows.

У Razor v2 використовуються як чіткі контрольні суми тексту листа (SHA1), так і два варіанти нечітких:

- Nilsimsa – метод розрахунку нечітких сигнатур, які слабо змінюються при невеликій зміні вихідних даних (в даний час цей спосіб не використовується бо метод Nilsimsa давав помітне число помилкових спрацьовувань)
- Ephemeral Signatures – нетривалі сигнатури, засновані на випадковому відборі шматочків тексту для їх побудови (сервер повідомляє клієнтові необхідні дані для вибору, клієнт здійснює вибір і розрахунок сигнатури).

Вважається, що такі сигнатури спамерам складно підробити, через те, що заздалегідь невідомо, які ділянки тексту повідомлення будуть використані для аналізу листи.

Клієнтське ПЗ Razor / SpamNet підтримує механізми голосування «проти» тексту повідомлення (тобто за визнання його спамом) і голосування «за» (тобто реакція на помилкові спрацьовування системи). Для підтримки Ephemeral Signatures лист при голосуванні передається на сервер цілком.

Клієнти реєструються на сервері, отримуючи унікальний ідентифікатор, який використовується надалі при голосуваннях. Підтримується «Truth Evaluation System» – система розрахунку рівня довіри до окремих учасників голосування користувачам, заснована, по всій видимості, на порівнянні схожості розподілу голосувань даного користувача із середнім по системі в цілому.Правила системи забороняють автоматичне голосування «проти», за винятком використання адрес-пасток.

Статистика і якість роботи системи Razor / SpamNet:

В даний час система обробляє понад 100 млн. Повідомлень на добу.

Згідно з документами Cloudmark, рівень виявлення спаму даною системою досягає 95%. З іншого боку, статистика, яку публікує на сайті Cloudmark.com, показує, що частка виявленого спаму в усьому потоці пошти становить близько 25%. Через те, що загальна частка спаму в пошті в даний час складає близько половини (за даними Brightmail, MessageLabs і самої Cloudmark), то виходить, що насправді система Razor / SpamNet виявляє близько 50% спаму.

Згідно з тестами PC Magazine, рівень виявлення спаму цією системою складає 83%, рівень помилкових спрацьовувань – 6.7%

Для спаму, одержуваного в Росії, якість роботи Razor істотно гірше – по тестах автора на вибірці з 11600 спам-повідомлень, рівень виявлення спаму дорівнює 10%, хоча рівень помилкових спрацьовувань вкрай низький (одне повідомлення на 5000). По всій видимості, поширеність Razor в Україні невелика, відповідно і сигнатур україномовних листів в базі практично немає.

Проект Pyzor (pyzor.sourceforge.net) було розпочато, як клієнт до Razor, написаний на мові Python. Однак автора (Frank Tobin) турбував той факт, що серверна частина системи Razor не є відкритою (недоступна як у вигляді вихідних текстів, так і у вигляді виконуваних модулів), в результаті Pyzor нині реалізує свій алгоритм підрахунку контрольних сум (дайджест SHA по тексту листа, очищеного від html-тегів) і має окремий сервер контрольних сум. Об'єднання Pyzor-серверів в загальну мережу та обмін даних між серверами не передбачені.

Судячи з усього, проект покинутий автором і ніким більше не розвивається. В даному огляді Pyzor згаданий для повноти картини.

Аналіз всієї пошти, що поступає

Аналіз всієї проходить через поштову систему пошти має на увазі, що для кожного поштового повідомлення генеруються контрольні суми, які передаються на сервер збору статистики. У відповідь сервер повідомляє кількість зареєстрованих повторів даного листа. Починаючи з деякої кількості повторів можна вважати даний лист спамом. Очевидно, що подібна технологія не буде відрізняти легальні масові розсилки від спаму, отже, потрібні «білі списки» в які такі розсилки будуть внесені.

Дана технологія реалізована в проекті DCC – Distributed Checksum Clearinghouse. Програмне забезпечення DCC поширюється у вихідних кодах по дуже ліберальної ліцензії. Користувачам доступний як клієнт, який може бути використаний з наявною мережею DCC-серверів, так і свій сервер, який можна встановити або незалежно, або включити в загальну DCC-мережу. Включені в DCC-мережу сервера обмінюються даними про частотних контрольних сумах практично в реальному часі.

Система DCC підтримує як анонімних, так і авторизованих клієнтів. DCC-сервер можна налаштувати так, щоб повідомлення про спам він брав тільки від авторизованих користувачів. У системі реалізований і аналог механізму голосування – окреме повідомлення (його контрольна сума) може бути явно позначений як «спам» або «не спам».

В системі використовується відразу кілька типів контрольних сум – чітка сума MD5 по всьому тексту повідомлення, окремі контрольні суми за адресами відправника, одержувачів і частини заголовків листа і два типи нечітких сум, розрахованих на роботу з мінливим текстом листа.

Зараз публічна мережа DCC обробляє близько 40 млн. «Унікальних повідомлень» в добу (яку публікує статистика не враховує число окремих одержувачів кожного листа), але не маючи доступу до детальної інформації у нас немає можливості перевести це число у звичні одиниці. Точно так же, яку публікує статистика по виявленому спаму – близько 30% в середньому – наводиться в унікальних повідомленнях, перевести це в «звичайні відсотки» без додаткових даних не можна, через те, що незрозуміло, як з'ясувати долю повторюваних листів.

Тести автора даної статті, проведені по збірці одержуваного в Україні спаму, показують рівень виявлення спаму у 25% (у звичайних термінах) при нулі помилкових спрацьовувань (без урахування одержуваних легітимних розсилок з великим числом передплатників).

Порівняльний аналіз методів

Три розглянутих методи кардинально відрізняються за способом збору спаму, інші характеристики у них близькі – за отриманими зразками спаму генеруються сигнатури, поштова система може порівняти сигнатуру отриманого листа з відомими системі, а в разі збігу – вирішити, чи є отриманий лист небажаним.

Однак відмінності в способах збору призводять до істотної відмінності в поведінці розподілених систем в цілому.

Якість роботи:

Якість роботи (відсоток визначається спаму) розподілених систем залежить від ряду властивостей системи:

- Від показності вибірки – кількості різноманітного збирається спаму.

- Від відповідності вибірки, наявної в системі, потоку спаму конкретного користувача.
- Від методів побудови контрольних сум – наскільки якісно вони працюють з персоналізованих (з випадковими послідовностями) спамом.

Судячи з опублікованих даних, найбільш представницькою вибіркою нині володіють системи з пастками пошти, в першу чергу Brightmail, обробна близько 2 млрд. Повідомлень на добу. У заснованих на інших принципах збору спаму систем DCC і Razor потоки повідомлень мають приблизно один порядок – близько 100 млн. Повідомлень на добу (з урахуванням різниці методів підрахунку), проте в разі DCC в систему потрапляє інформація про все потоці пошти, а в разі Razor – тільки за вибором користувача, відповідно представництво DCC трохи вище. Принципи побудови нечітких контрольних сум в DCC і Razor схожі. Відповідно, якість роботи у DCC має бути вище внаслідок більшої показності – що і спостерігається в тестах.

Помилкові спрацьовування:

Помилкові спрацьовування – це помилкове прийняття за спам-повідомлення того, що не є спамом. Не маючи детальних даних по системи з пастками спам-пошти, розглядати цей аспект їх роботи неможливо. Розглянемо проблему помилкових спрацьовувань для двох, що залишилися класів систем:

1. Системи з голосуванням користувачів залежать у визначенні спаму від вибору користувачів. З досвіду автора, користувачі часто вважають спамом цілком «легальні» повідомлення – розсилки, на які вони підписалися і не знають, як відписатися, повідомлення від автоматичних поштових «роботів» і так далі. Рівень «шуму» на потоці скарг зазвичай становить не більше кількох відсотків. З іншого боку, зазвичай число скарг на легальні повідомлення менше скарг на масовий спам. З урахуванням вищесказаного, системи з голосуванням повинні або підвищувати «поріг спрацьовування» (число скарг, при якому лист вважається спамом), або миритися з помилкові спрацьовування, коли за спам приймаються легітимні розсилки. Судячи з появи механізму «голосування за» в

Razor v2, ця властивість є певною проблемою – повністю від помилкових спрацьовувань позбутися не вдається.

2. Системи з аналізом всієї пошти принципово мають на увазі можливість помилкового спрацьовування – для цих систем легальні розсилки й спам виглядають однаково. Іншими словами, поштові системи, що використовують DCC або аналоги повинні підтримувати білі списки для всіх легальних розсилок, які хочеться отримувати. У істотному ступені, проблема помилкових спрацьовувань перекладена на кінцевого користувача.Можливість компрометації розподілених систем.

Останнім часом відбуваються масові DoS-атаки на системи RBL, що говорить про накопичення спамерами достатніх ресурсів для спроб усунення що не подобається їм. З урахуванням цього факту, необхідно розглянути можливість компрометації розподілених систем збору статистики.

Компрометація подібних систем можлива у двох варіантах: або система різко знижує якість роботи (частку розпізнається спаму), або ж різко збільшується число помилкових спрацьовувань. Надалі будемо розглядати можливість компрометації тільки з використанням закладених в самі системи механізмів роботи.

Системи з пастками для пошти – якість їх роботи залежить від пошти, що надходить в пастки. Знизити якість роботи можна в ситуації, коли спам в ці пастки перестав приходити. З урахуванням кількості пасток в комерційних системах це малоймовірно. Кількість помилкових спрацьовувань можна збільшити, «завалив» пастки легітимною поштою. В обох випадках, для компрометації системи необхідно, щоб в руки спамерів потрапила значна частина списку пасток, компрометація без цього списку малореальна.

Системи з голосуванням користувачів. Якість роботи таких систем залежить від активності користувачів – число скарг на лист пропорційно масовості його розсилки та кількості користувачів системи. Таким чином, знизити якість розпізнавання можна шляхом зменшення кількості спаму приходить голосуючим учасникам, але саме цього вони й так домагаються.

Іншими словами, погіршення якості розпізнавання внаслідок зовнішнього впливу видається нереальним. Компрометація системи шляхом збільшення числа помилкових спрацьовувань є неможливою – для цього спамерам потрібно стати голосуючим учасником і голосувати «проти» легітимних розсилок.

Потенційно це можливо, дану проблему система Razor / SpamNet нейтралізує шляхом привласнення рейтингу голосуючим учасникам – для компрометації системи необхідна велика кількість голосуючих учасників з хорошим рейтингом. Це знову можливо, але вимагає вже великих організаційних ресурсів. Водночас, проблема ненавмисної компрометації бази даних Razor легальними розсилками є і сьогодні.

Системи аналізу всієї пошти, що приходить. Дані системи будують об'єктивну статистику почти, що приходить, класифікуючи її по частоті, а не за змістом. Знизити частотність будь-якої розсилки без порушення цілісності системи є неможливим. Компрометація системи внаслідок помилкових спрацьовувань теоретично можлива тому немає способу перевірити реальне число одержувачів повідомлення, про який рапортує поштовий сервер.

В системі DCC закладена потенційна можливість приймати звіти тільки від авторизованих клієнтів, однак тепер ця можливість на публічній мережі DCC-серверів не використовується.

Необхідно відзначити, що компрометація шляхом збільшення числа помилкових спрацьовувань істотна тільки для легальних масових розсилок, компрометувати поодинокі повідомлення важко, бо для компрометації необхідно отримати зразок компрометованого листа до того, як його отримано більшістю одержувачів. Для звичайних листів це малореально. В той самий час, для легко компрометованого на сьогодні системи DCC проблема пропуску масових легальних розсилок є і без компрометації, їх в будь-якому випадку потрібно вносити в білий список.Аналіз всієї проходить через поштову систему пошти має на увазі, що для кожного поштового повідомлення генеруються контрольні суми, які передаються на сервер збору статистики. У відповідь сервер повідомляє кількість зареєстрованих повторів даного листа. Починаючи

з деякої кількості повторів можна вважати даний лист спамом. Очевидно, що подібна технологія не буде відрізняти легальні масові розсилки від спаму, отже, потрібні «білі списки» в які такі розсилки будуть внесені.

Дана технологія реалізована в проекті DCC – Distributed Checksum Clearinghouse. Програмне забезпечення DCC поширюється у вихідних кодах по дуже ліберальної ліцензії. Користувачам доступний як клієнт, який може бути використаний з наявною мережею DCC-серверів, так і свій сервер, який можна встановити або незалежно, або включити в загальну DCC-мережу. Включені в DCC-мережу сервера обмінюються даними про частотних контрольних сумах практично в реальному часі.

Система DCC підтримує як анонімних, так і авторизованих клієнтів. DCC-сервер можна налаштувати так, щоб повідомлення про спам він брав тільки від авторизованих користувачів. У системі реалізований і аналог механізму голосування – окреме повідомлення (його контрольна сума) може бути явно позначений як «спам» або «не спам».

В системі використовується відразу кілька типів контрольних сум – чітка сума MD5 по всьому тексту повідомлення, окремі контрольні суми за адресами відправника, одержувачів і частини заголовків листа і два типи нечітких сум, розрахованих на роботу з мінливим текстом листа.

Зараз публічна мережа DCC обробляє близько 40 млн. «Унікальних повідомлень» в добу (яку публікує статистика не враховує число окремих одержувачів кожного листа), але не маючи доступу до детальної інформації у нас немає можливості перевести це число у звичні одиниці. Точно так же, яку публікує статистика по виявленому спаму – близько 30% в середньому – наводиться в унікальних повідомленнях, перевести це в «звичайні відсотки» без додаткових даних не можна, через те, що незрозуміло, як з'ясувати долю повторюваних листів.

Тести автора даної статті, проведені по збірці одержуваного в Україні спаму, показують рівень виявлення спаму у 25% (у звичайних термінах) при

нулі помилкових спрацьовувань (без урахування одержуваних легітимних розсилок з великим числом передплатників).

Проблеми розподілених методів

Найбільш суттєвою проблемою для вищеописаних методів детектування масових розсилок є «персоналізація» спаму – кожний сучасне спамерський лист існує у величезній кількості варіантів з незначними відмінностями в тексті. Наскільки відомо автору, сьогодні жодна з розподілених систем повністю дану проблему не вирішила.

Водночас, шляхи вирішення досить зрозумілі – існує багатий розроблений математичний апарат, призначений для пошуку схожих текстів і фрагментів текстів (сигнатури Рабина і т.п.), який поступово починає використовуватися в розподілених системах виявлення спаму.

Друга наявна проблема пов'язана з помилковими визначеннями легальних розсилок як спаму. Ця проблема характерна як для методів, які аналізують всю пошту, так і, меншою мірою, для систем з голосуванням користувачів. Розв'язання цієї проблеми на локальному рівні можливо шляхом створення білих списків, що включають всі прийняті даної поштовою системою розсилки. На глобальному рівні можна створювати як загальні білі списки (з якоюсь політикою), або вводити методи, що дозволяють впевнено і надійно ідентифікувати джерело розсилки.

Таким методом може бути, наприклад, необов'язкова електронний підпис змісту легальних розсилок, що дозволяє впевнено ідентифікувати відправника. Підписані повідомлення могли б з гарантією проходити через поштові фільтри.

Друга існуюча проблема пов'язана з помилковими визначеннями легальних розсилок як спаму. Ця проблема характерна як для методів, які аналізують всю пошту, так і, меншою мірою, для систем з голосуванням користувачів. Розв'язання цієї проблеми на локальному рівні можливо шляхом створення білих списків, що включають всі прийняті даної поштовою системою розсилки. На глобальному рівні можна створювати як загальні білі списки (з

якоюсь політикою), або вводити методи, що дозволяють впевнено і надійно ідентифікувати джерело розсилки.

Таким методом може бути, наприклад, необов'язкова електронний підпис змісту легальних розсилок, що дозволяє впевнено ідентифікувати відправника. Підписані повідомлення могли б з гарантією проходити через поштові фільтри.

Перспективи та шляхи розвитку розподілених систем аналізу електронної пошти

Подальше вдосконалення розподілених систем аналізу електронної пошти можна розділити на два основних напрямки: поліпшення вже побудованих механізмів і створення принципово нових методів аналізу.

Удосконалення наявних механізмів розподілених систем, очевидно, буде включати боротьбу з описаними вище проблемами. Буде збільшуватися захищеність систем від компрометації, якість обробки листів з добавками випадкового тексту, знижуватися рівень помилкових спрацьовувань. Очевидно, що буде збільшуватися й охоплення розподілених систем – їх ефективність в боротьбі зі спамом автоматично буде призводити до появи нових клієнтів.Нові можливості розподілених систем аналізу. Володіння великим масивом одержуваних в реальному часі даних про поширення окремого повідомлення відкриває абсолютно нові можливості для надійного виявлення спаму. По всій видимості, великий ефект має дати об'єднання чинних методів фільтрації спаму (RBL, детермінований контентний аналіз, статистичний аналіз) з даними, що поставляються розподіленими системами.

Можна навести такі потенційні приклади:

- Автоматична побудова недовготривалих чорних списків IP-адрес в реальному часі. Якщо яке-небудь повідомлення, розкласифікувати як спам, розсилається в даний час з якогось списку IP-адрес, то весь цей список може бути тимчасово позначений як «чорний» і який-небудь захід пошти з цих машин – заборонений. Таке блокування може здійснюватися швидко, його можна робити тільки на час розсилки.

- Ретроспективний аналіз джерел спаму і побудова чорних списків на його основі. Спосіб передбачає аналіз джерел спаму, що розсилають повідомлення, які не були класифіковані як спам відразу (наприклад, через наявність в них великих обсягів випадкового тексту). Якщо дані розсилають тільки спам, то вони можуть бути поміщені в порівняно довгоживучі чорні списки.
- Аналіз активності окремих машин при розсилці пошти, виявлення «схем поведінки» користувальницької машини, що розсилає спам. По всій видимості, така машина повинна відрізнятися по поведінці, як від звичайного поштового сервісу, так і від призначеного для користувача комп'ютера.
- Накопичення та аналіз змін тексту всередині однієї масової розсилки (один основний текст зі змінними добавками). Можна як виділяти загальні частини таких повідомлень статистичними методами, так і досліджувати алгоритм випадкових змін з метою передбачення подальших варіацій.

Багаті потенційні можливості розподілених систем аналізу пошти мають в собі й приховані небезпеки – контроль над такою системою дає безліч потенційних можливостей контролю пошти, не пов'язаних з фільтрацією спаму. Для запобігання занадто великого інтересу до подібних систем, вони повинні накопичувати відомості тільки про масові розсилання, а не через електронну пошту в цілому.

Далі автор хоче надати рекомендації щодо кібергігієни, яка в наш час надзвичайно важлива.Хороша кібергігієна – це загальна практика, яка може допомогти вам забезпечити безпеку в мережі, але є кілька рекомендацій, які допоможуть вам забезпечити максимальну безпеку.

Кібергігієна – це правила дотримання простих правил цифрової безпеки при роботі з інтернетом, який став повноцінною частиною нашого життя. Тут можна провести паралель з правилами особистої гігієни: з одного боку, кібергігієна за своєю суттю така ж елементарна, а з іншого – необхідна на рівні щоденної звички.

Насправді три чверті користувачів інтернету знають, як важливо дотримуватися правил кібербезпеки. І все одно поширюють всюди свої паролі. Більше третини користувачів мають, як мінімум, одне незахищене пристрій, вразливе для кібершахраїв. А ще багато хто вважає, що публічні мережі Wi-Fi зручні для швидкої перевірки пошти, відправлення документів і входу у свої облікові записи. З власної волі вони піддають свою безпеку ризику заради безкоштовного інтернету. Ці дані говорять про те, що одна справа – знати правила, і зовсім інша – їх дотримуватися.

Ось чому важливо звертати увагу на проблему культури кібербезпеки, ключовим елементом якої є кібергігієна. Прості правила інформаційної безпеки формуються й оновлюються разом з розвитком технологій. Спрямовані ці правила на те, щоб скоротити ризики користувачів в умовах глобальної дигіталізації.

Всілякі інформаційні майданчики закликають користувачів інтернету користуватися антивірусом, створювати максимально складні паролі, не повторювати їх на різних ресурсах, використовувати двофакторну аутентифікацію всюди, де це можливо. Рекомендують шифрувати інформацію на жорстких дисках, USB-носіях і застосовувати функції шифрування для збереження конфіденційності листування в інтернеті.

У світі, де соціальні мережі стали обов'язковою частиною життя людини, а «крадіжка особистості» стає глобальною проблемою, ми повинні ставитися до схоронності особистої інформації як до матеріальної цінності.

Але чи достатньо в цифровому світі однієї лише кібергігієни як індивідуальної профілактики?

Кібергігієна, як і гігієна «звичайна», пройшла свої стадії становлення. Розвиваючись, з правил особистої профілактики гігієна перейшла до формування цілих заходів з оздоровлення груп населення. Далі, сучасна гігієна стала регулювати здоров'я людей на державному рівні. Це тому, що профілактика повинна бути системною: тільки так вона виконає свої функції та забезпечить безпечну повноцінне життя.

Сьогодні захищеність людей в інформаційному просторі не є ні потребою окремої групи осіб, ні привілеєм меншини. Це – потреба кожного громадянина.

І недотримання норм кібербезпеки навіть в невеликому обсязі може спричинити тотальне «зараження» інформаційного простору, а також порушення цифровий стабільності та стійкості держави.

Тому забезпечення безпеки інформаційного простору має сприйматися як гігієна – основа здорового життя. Причому, як для окремої людини, так і для всієї держави. Для громадянина це – особиста практика і прості правила безпечного використання інформаційних ресурсів. А для держави – законотворчість, створення об'єднань, державного і міждержавного співробітництва.

Отже. Чи вірно, що кібергігієна – це тільки дотримання громадянином заходів безпеки в інформаційному середовищі? Ні. Кібергігієна – поняття набагато ширше. Воно містить вивчення впливу на людину дигіталізації, розробку нормативів і заходів по інформаційному захисті громадян, з оздоровлення інформаційного середовища. І, звичайно, пропаганду знань основ кібербезпеки.

Розширення поняття кібергігієни допоможе збільшити рівень залученості громадян і держави в питання кібербезпеки. Просування її культури на рівні кожної людини, створення ініціативної служби кібербезпеки на рівні компанії й, нарешті, повне включення держави в питання створення кібербезпеки як екосистеми.

Ключові кроки для гарної комп'ютерної гігієни

Крок 1: Встановіть авторитетне антивірусне і шкідливе програмне забезпечення.

Перший і, можливо, найважливіший крок – установка антивірусного програмного забезпечення. Для чого? Антивірусне програмне забезпечення – це програма або комплекс програм, які сканують і знищують віруси або інші шкідливі програми. Це життєво важливий компонент вашої загальної кібергігієни в захисті від порушень безпеки, а також інших загроз.

Зокрема, антивірусне програмне забезпечення забезпечує захист, виконуючи ключові завдання, в тому числі такі.

Визначення конкретних файлів для виявлення шкідливого програмного забезпечення.

Планування і виконання автоматичного сканування.

Сканування або одного конкретного файлу, або всього вашого комп'ютера, або флеш-накопичувача, в залежності від ваших конкретних потреб.

Видалення шкідливого програмного забезпечення.

Підтвердження «здоров'я» вашого комп'ютера та інших пристроїв.

Крок 2: Використовуйте мережеві брандмауери

Використання мережевого брандмауера є ще однією ключовою звичкою для підтримки гарної комп'ютерної гігієни. Міжмережеві екрани є першою лінією захисту в мережевої безпеки, запобігаючи несанкціонований доступ користувачів до ваших веб-сайтів, поштових серверів і іншими джерелами інформації, доступ до яких можна отримати з Інтернету.

Крок 3: Регулярно оновлюйте програмне забезпечення

Регулярно оновлюйте свої додатки, веб-браузери та операційні системи, щоб переконатися, що ви працюєте з останніми програмами, в яких усунуті або виправлені можливі збої. Налаштування цієї функції на автоматичне оновлення допоможе забезпечити вам самі останні засоби захисту.

Ці оновлення особливо важливі, тому що вони часто включають виправлення програмного забезпечення. Розробники програмного забезпечення випускають виправлення безпеки щоразу, коли виявляють недоліки програмного забезпечення – недоліки, які можуть використовувати віруси або хакери. Розробники не завжди можуть попередити вас, коли був впроваджений критичний патч. Таким чином, регулярні оновлення гарантують, що ці патчі закриють всі відомі на момент їх випуску дірки у вашому програмному забезпеченні.

Крок 4: Встановіть надійні паролі

Установка надійних паролів для всіх ваших пристроїв має важливе значення. Ваші паролі повинні бути унікальними та складними, містити не менше 12 символів, а також цифри, символи, великі й малі літери. Регулярна зміна ваших паролів необхідна для того щоб зменшити ймовірність їх злому зловмисниками. Пам'ятайте! Кожен пароль повинен бути унікальним.

Додаткові елементи керування пристрою – паролі прошивки. У той час як шифрування диска перешкоджає доступу кіберзлодіїв до інформації, що зберігається на вашому пристрої, паролі вбудованого ПО захищають ваше обладнання, запобігаючи перезавантаження або скидання вашої машини без вашого пароля.

Крок 5: Використовуйте багатофакторну аутентифікацію

Двофакторна або багатофакторна аутентифікація – це найкраща практика, яка пропонує додатковий рівень захисту. Для двофакторної аутентифікації зазвичай потрібно, щоб ви вказали свій пароль та ім'я користувача, а також, скажімо, унікальний код, відправлений на ваш мобільний телефон. Це може бути все, що необхідно для деяких систем, але багатофакторна аутентифікація додає нові рівні безпеки з використанням біометричних даних, таких як розпізнавання осіб або відбитків пальців, щоб хакерам було важче отримати доступ до вашого пристрою та особистої інформації.

Крок 6: Використовувати шифрування пристрою

Хоча в більшості компаній автоматично застосовуються процеси шифрування даних, вам також може знадобитися шифрувати ваші пристрої та інші носії, що містять конфіденційні дані, включаючи ноутбуки, планшети, смартфони, знімні диски, стрічки для резервного копіювання та хмарне сховище. Фактично, багато пристроїв використовують шифрування за умовчанням для даних, що зберігаються на смартфонах. Деякі додатки використовують наскрізне шифрування, а інші служби шифрують дані на ваших пристроях і зберігають їх в хмарі. Інший варіант – використовувати зашифровану карту пам'яті USB для захисту конфіденційних даних.

Крок 7: Регулярно робіть резервні копії

Також розумно захищати ваші файли, створюючи резервні копії важливих файлів в автономному режимі, на зовнішньому жорсткому диску або в хмарі. Це може допомогти захистити від втрати даних, особливо якщо хакери отримують доступ до одного з ваших пристроїв.

Крок 8: Тримайте жорсткий диск в чистоті

Якщо ви продаєте свій ноутбук, планшет або смартфон, важливо, щоб ваша особиста або конфіденційна інформація при цьому не передавалася. Якщо ваш пристрій зламано, чистий жорсткий диск означає менше інформації, до якої здійснюється доступ.

Але простого видалення файлів або даних може бути недостатньо. Частиною хорошої кібергігієни є переформатування, а потім чистка жорсткого диска. Наприклад, якщо ви хочете продати свій комп'ютер і використовувати його для онлайн-банкінгу, вам слід розглянути можливість очищення диска для видалення програмного забезпечення і даних з жорсткого диска.

Крок 9: Захистіть свій маршрутизатор

Не забудьте захистити свою бездротову мережу. Це містить відключення та оновлення стандартної назви й пароля, з яким маршрутизатор прийшов від виробника, відключення віддаленого управління і вихід з системи під обліковим записом адміністратора після його налаштування. Крім того, переконайтеся, що ваш маршрутизатор пропонує шифрування WPA2 або WPA3, щоб підтримувати найвищий рівень конфіденційності інформації, що передається через вашу мережу.

ВИСНОВКИ ДО ТРЕТЬОГО РОЗДІЛУ

Пам'ятайте, що практикувати хороші звички кібергігієни це розумно. Якщо ви налаштуєте на своєму комп'ютері та інших пристроях авторитетні антивірусні програми, будете регулярно оновлювати їх, створювати надійні

паролі та містити все в чистоті, ви будете на шляху до створення кібернетичних звичок, які можуть допомогти вам убезпечити себе в мережі.

Наступ інформаційної ери призвів до того, що інформаційний вплив, що існував споконвіку у взаєминах між людьми, в наші дні все більш очевидно набуває характеру військових дій. Тепер накопичений значний досвід наукових досліджень у галузі інформаційного протиборства та інформаційно-психологічних війн. Який би зміст у поняття "інформаційна війна" не вкладався, воно народилося в середовищі військових і позначає, перш за все, жорстку, рішучу і небезпечну діяльність, яку можна порівняти з реальними бойовими діями. Ми живемо в епоху швидких змін. Їх прискорення формує інформаційне суспільство, для якого характерний дефіцит інформації, потрібної для прийняття рішень. Це позбавляє людину самостійного мислення.

Автор рекомендує дотримуватись елементарних правил кібергігієни,які детально розписав у третьому розділі своєї роботи.

ВИСНОВКИ

В ході виконання дипломної роботи були запропоновані методи для забезпечення інформаційної безпеки системи. В результаті роботи були розглянуті особливості політичного впливу в умовах інформаційної війни, форми інформаційних операцій в соціальних мережах і методи обробки великих обсягів інформації.

Автор визначив шо інформаційні війни ведуться на різних рівнях: від підприємства і корпорації до регіону, держави та світу.

Дослідження показує, що інформаційні війни практично однакові на корпоративному і державному рівнях.

Було визначенно, що здійснюються одні й ті ж помилки, відповідно уроки одного сектора можуть бути корисні іншому.

В епоху загальної інформатизації суспільство з об'єктивних і суб'єктивних причин все більшою мірою втрачає здатність до самоорганізації.

Було наведенно приклади, що контроль інформаційних війн концентрується в руках вузького кола осіб, які не несуть відповідальності перед суспільством за прийняття доленосного рішення.

Автор вважає, що ведення інформаційних війн стає долею маловідомих політтехнологів.

Реальність замінюється штучно створюваними віртуальними моделями, в межах яких створюються вигідні для політика масові думки, уявлення, переваги, реакції та ставлення до конкретних подій, процесів, явищ, а також народжує зразкову масову поведінку цільової аудиторії, на яку направлено маніпуляційний вплив. Маніпулювання суспільною свідомістю це прихований вплив на свідомість людей і управління їх поведінкою, побудоване на ігноруванні волі реципієнта, з метою спонукання аудиторії до конкретних вчинків, чужим їх поглядам, в інтересах суб'єкта політичної маніпуляції.

Приховування правди в комунікації є наслідком умисного подання дійсності в інтересах мовця, що неодмінно пов'язане з певним використанням

інформації. Цілеспрямоване спотворення інформації є найважливішою складовою маніпуляційного впливу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гузев С.А., Комиссарова М.Н. Информационные войны: типы и особенности // Современные наукоемкие технологии. 2013. №10(2)

2. Искусственные иммунные системы и их применение: сб. ст. / под ред. Д. Дасгупты. М.: Физматлит, 2016. 344 с

3. Бронников И.А., Буренко В.И., Нестерчук О.А. Модернизация политических институтов, процессов и технологий в условиях глобализации // под ред. О.Е. Гришина, А.К. Сковикова. М.: Изд-во Моск. гуманит. ун-та,2012.

4. Seth Stephens-Davidowitz [«Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are»]: IT Bestseller / Seth Stephens-Davidowitz: Dey Street Books, 2016. – 352 pages

5. Навіщо за нами стежать в соцмережах і хто продає наші дані? Велике інтерв'ю про Big Data [Електронний ресурс] https://www.youtube.com/watch?v=LZIpsq1YyBg

6. Is Big Data a Bubble Set to Burst? [Електроний ресурс] https://www.datacenterknowledge.com/archives/2015/03/30/big-data-bubble-set-burst

7. Большие данные [Електронний ресурс] https://ru.wikipedia.org/wiki/Большие_данные

8. Панарин И.Н. Технология информационной войны/И. Н. Панарин. - М.: КСП+, 2003. – 320 с.

9. Семененко В.А. Информационная безопасность: учебное пособие. 2-е изд., стереот. - М.: МГИУ, 2005. – 215 с.

10. Корнюшин, П.Н. Информационная безопасность / П.Н. Корнюшин, С.С. Костерин. - Владивосток: ТИДОТ ДВГУ, 2003. – 154 с.

11. Конев И. Р. Информационная безопасность предприятия / И. Р. Конев, А. В. Беляев. - СПб. : БХВ-Петербург, 2003. – 747 с.

12. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1/С.В. Кавун, В.В. Носов, О.В. Мажай. - Харків: Вид. ХНЕУ, 2008. – 352 с.

13. Теория информационной безопасности и методология защиты информации: учебное пособие. / И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина - Казань: Изд-во Казан. гос. техн. ун-та, 2008. – с. 358.

14. Сороковская А. А. Информационная безопасность предприятия : новые угрозы и перспективы [Електронний ресурс]. - Режим доступа : http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032–035.pdf. – Дата доступу : 08.06.2015

15. Курушин В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. – М. : Новый юрист, 2012.– 256 с.

16. Гатчин Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат. – СПб. : СПбГУ ИТМО, 2010. – 98 с.

17. Вишнівський В.В. Організація дистанційного навчання.Створення електронних навчальних курсів та електронних тестів.Навчальний посібник./ Вишнівський В.В., Гніденко М.П.,Гайдур Г.І., Ільїн О.О. – Київ: ДУТ, 2014. – 140с

18. Гайворонський М.В. Безпека інформаційно–комунікаційних систем./ Гайворонський М.В., Новіков О.М. – К.: Видавнича група BHV, 2009. – 608 с.

19. Дронь М.М., Малайчук В.П., Петренко О.М. Основи теорії захисту інформації: Навч. посібник. – Д.: Вид–во Дніпропетр. ун–ту, 2001. – 312 с.

20. Афанасьєв В. Соціальна інформація та управління суспільством. – М.: Знание, 2005, – 119 с.

21. Блек С. Паблик рилейшнз. Що це таке? М.: Наука, 2007, – 256 с.

22. Вершинін М.С. Політична комунікація в інформаційному суспільстві. М.: Ягуар, 2006, – 256 с.

23. Волковский Н.Л. История информационных войн. В 2 ч. Часть 1. / Н.Л.Волковский. СПб.: ООО «Издательство «Полигон», 2003.

24. Володин А.Г., Широков Г.К. Глобализация: истоки, тенденции, перспективы//Полис. №5. 1999.

25. Глобализация и мультикультурализм. Отв. Ред. П.С.Карабаев.М.: Изд–во

РУДН, 2005.

26. Глоссон Р. Природа войны // Война и геополитика. Выпуск 3. Время мира. Новосибирск, 2003.

27. Гриняев С. Взгляды военных экспертов США на ведение информационного противоборства. – Зарубежное военное обозрение. № 8, 2001.

28. Звіринців А.Б. Комунікаційний менеджмент: Робоча книга менеджера PR: 2–е вид., Испр. – СПб.: Союз, 2007, – 288с.

29. Информационная безопасность систем организационного управления. Теоретические основы [Текст]: в 2 т. / Н.А. Кузнецов, В.В. Кульба, Е.А. Микрин и др.; [отв. ред. Н.А.Кузнецов, В.В.Кульба] ; Ин–т проблем передачи информации РАН. – М.: Наука, 2006.

30. Каландара К.Х. Управління суспільною свідомістю. Роль комунікативних процесів. М.: Наука, 2006, – 154 с.

31. Крутских А., Федоров А. Про міжнародної інформаційної безпеки. М.: Слово, 2008, – 234 с.

32. Малькова Т.В. Маси. Еліта. Лідер. М.: Яуар, 2006, – 232 с.

33. Масова інформація в радянському промисловому місті: Досвід комплексного соціологічного дослідження / Під загальною редакцією Б.А. Грушина, Л.А. Оконнікова. – М.: 2006, – 347 с.

34. Новиков, Д.А. Рефлексивные игры [Текст] / Д.А.Новиков, Г.А.Чхартишвили – М.: СИНТЕГ, 2003.

35. Панарин И. Н. Информационная война и геополитика [Текст] / И. Н. Панарин – М.: «Поколение», 2006.

36. Почепцов Г.Г. Інформаційні війни. М.: ВЦ Гарант, 2008, – 453 с.

37. Расторгуєв С.П. Інформаційна війна. М.: Наука, 2008, – 235 с.

38. Рютінгер Р. Культура підприємництва. – М.: Лідер, 2006, 672 с.

39. Танскотт Д. Електронно–цифрове суспільство. Плюси і мінуси мережевого інтелекту. М.: Прогрес, 2006, – 673 с.

40. Техніка дезінформації та обману. – М.: Слово, 2008, – 139 с.

41. Тоффлер Е. Третя хвиля. М.: Пале, 2007, – 458 с.

42. Фірсов Б. Телебачення очима соціолога. – М. Слово, 2008, – 418 с.

43. Хаббард Л.Р. Проблеми роботи. – СПб.: Знання, 2008, – 342 с.

44. Хейне П. Економічний образ мислення. – М.: Слово, 2006, – 457 с.