

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА**

ТРОЯН АНАСТАСІЯ ВЯЧЕСЛАВІВНА

Допускається до захисту:
завідувач кафедри загального та
прикладного мовознавства і
слов'янської філології,
д.філол.н., доцент
_____ Ситар Г.В.
«_____» _____ 2021 р.

**АЛГОРИТМ СТВОРЕННЯ ТЕКСТІВ МАСОВОЇ РОЗСИЛКИ:
ЛІНГВІСТИЧНІ ОСОБЛИВОСТІ ТА ТЕХНІЧНИЙ АСПЕКТ**

Спеціальність 035 Філологія

Кваліфікаційна робота

Науковий керівник:
І.В. Гарбера, доцент
кафедри загального та прикладного
мовознавства і слов'янської філології,
к.філол.н.

Оцінка: _____ / _____ / _____
Голова ЕК: _____

Вінниця 2021

АНОТАЦІЯ

Троян А.В. Алгоритм створення текстів масової розсилки: лінгвістичні особливості та технічний аспект. Спеціальність 035 «Філологія», освітньо-професійна програма «Прикладна лінгвістика». Донецький національний університет імені Василя Стуса, Вінниця, 2021. 67 с.

У кваліфікаційній роботі розглянуто теоретико-методологічні основи дослідження текстів масової розсилки. Доведено, що спам являє собою окремий мовленнєвий жанр інтернет-дискурсу. Проаналізовано потужний потенціал шкідливості спам-розсилки та основні методи ефективної боротьби з ним. Описано технічні та лінгвістичні особливості текстів масової розсилки. Доведено, що основним засобом створення спам-текстів є маніпуляційність використовуваних у процесі цього технологій. Описано функціонал та представлено приклад використання самостійно розробленої програми Find Spam – для технічного аналізу створюваних текстів масової розсилки.

Ключові слова: маніпуляція, масова розсилка, програма, спам, текст.

Рис. 25. Схема 1. Бібліографія: 48.

Troian A.V. Algorithm for Creating Mass Mailing Texts: Linguistic Features and Technical Aspect. Specialty 035 “Philology”, Program “Applied Linguistics”. Vasyl’ Stus Donetsk National University, Vinnytsia, 2021. 67 p.

In the qualification work the theoretical and methodological bases of research of texts of mass mailing are considered. It has been proven that spam is a separate speech genre of Internet discourse. The powerful potential of spam mail and the main methods of effective combating it are analyzed. Technical and linguistic features of mass mailing texts are described. It is proved that the main means of creating spam texts is the manipulation of the technologies used in this process. The functionality is described and an example of using the independently developed program Find Spam is presented – for the technical analysis of the created texts of mass mailing.

Keywords: manipulation, mass mailing, program, spam, text.

Fig. 25. Scheme 1. Bibliography: 48.

ЗМІСТ

ВСТУП	5
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЙНІ ОСНОВИ ДОСЛІДЖЕННЯ ТЕКСТІВ МАСОВОЇ РОЗСИЛКИ	
1.1. Спам як окремий мовленнєвий жанр інтернет-дискурсу	7
1.2. Потенціал шкідливості спам-розсилки та основні методи ефективної боротьби з ним	21
РОЗДІЛ 2. ТЕХНІЧНІ ТА ЛІНГВІСТИЧНІ ОСОБЛИВОСТІ ТЕКСТІВ МАСОВОЇ РОЗСИЛКИ	
2.1. Технічні / лінгвістичні маніпуляційні технології як засіб створення текстів масової розсилки	34
2.2. Приклади реалізації маніпуляційних технологій у спам- текстах	43
РОЗДІЛ 3. ПРОГРАМА ДЛЯ ТЕХНІЧНОГО АНАЛІЗУ СТВОРЮВАНИХ ТЕКСТІВ МАСОВОЇ РОЗСИЛКИ: АЛГОРИТМ ВИКОРИСТАННЯ	
3.1. Функціонал програми Find Spam	50
3.2. Приклад використання програми Find Spam	52
ВИСНОВКИ	60
СПИСОК ЛІТЕРАТУРИ	64
Додаток А. Апробація роботи	68

ВСТУП

Сучасні масові текстові розсилки все більше й частіше захоплюють наш інтернет-світ. Проблема розсилок не нова. Кожен отримувач на мобільний телефон, електронну пошту, месенджер, у соціальній мережі різноманітні небажані повідомлення з рекламою – спам.

Актуальність кваліфікаційної роботи зумовлена потребою виокремлення кваліфікаційних параметрів та опису нюансів створення текстів масової розсилки, що допоможе звичайному користувачеві швидко й ефективно відрізнити корисний лист від спаму.

Мета дослідження: проаналізувати ключові лінгвістичні особливості текстів масової розсилки як окремого жанру інтернет-дискурсу та створити спеціальну програму, що дозволяє автоматично проаналізувати контент на предмет його заспамленості.

Для успішної реалізації мети необхідно вирішити такі **завдання**: 1) узагальнити існуючі наукові погляди на тексти масової розсилки (спам-тексти) як окремих дискурсивний жанр; 2) проаналізувати загрози, спричинені небажаною масовою текстовою розсилкою, та основні методи боротьби з нею; 3) схарактеризувати кваліфікаційні технічні ознаки, лінгвістичні особливості й типології спам-текстів; 4) описати маніпулятивні технології, використовувані спамерами в текстах масової розсилки; 5) розробити програму Find Spam, основна функція якої – виокремлювати ключові спам-слова.

Об'єктом кваліфікаційної роботи є тексти масової розсилки, **предметом** – їх лінгвістичні особливості й технічний аспект створення.

Методи дослідження. Мета й завдання кваліфікаційної роботи зумовили необхідність застосування низки *загальнонаукових методів*: логіко-поняттєвий метод, метод узагальнення та систематизації, описовий метод. Як *спеціальні методи* застосовано дискурсивний аналіз (з метою виокремлення ключових лінгвістичних, технічних, психологічних параметрів спам-текстів) і метод програмування (використаний для розробки програми Find Spam).

Матеріал дослідження становлять близько 100 спам-листів з метою виокремлення ключових слів, що використовують спамери для розсилки користувачам.

Новизна роботи визначується тим, що нами розроблено спеціальну програму, яка покликана допомогти звичайному користувачеві відрізнити звичайний текст від заспамленого.

Теоретичне значення роботи: у роботі узагальнено існуючі наукові погляди на тексти масової розсилки як окремий дискурсивний жанр; проаналізовано загрози, спричинені спамом, та основні методи боротьби з ним; схарактеризовано кваліфікаційні технічні ознаки, лінгвістичні особливості й типології текстів масової розсилки; описано маніпулятивні технології, використовувані спамерами.

Практичне значення роботи. Результати дослідження можуть знайти практичне використання у вишівських курсах із дискурсології, комунікативної лінгвістики, теорії алгоритмів, програмування.

Апробація. Результати роботи апробовано шляхом участі в: науковому студентському форумі «Детермінанти девіантної поведінки: злочинний вимір» (28 квітня 2021 р., Вінниця) з науковою публікацією «**Маніпуляційні технології як засіб створення текстів масової розсилки**»; XIV Міжнародному науково-теоретичному і навчально-прикладному семінарі «Лінгвіст-програміст» (11-12 травня 2021 р., Вінниця) з науковою публікацією «**Алгоритм створення текстів масової розсилки: лінгвістичні особливості та технічний аспект**»; XVII Всеукраїнській науково-методичній конференції студентів та молодих вчених «Прикладна лінгвістика 2021: проблеми та рішення» (13 травня 2021 р., Миколаїв) з науковою публікацією «**Маніпулятивний вплив у сучасному рекламному дискурсі**».

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку літератури, додатку.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЙНІ ОСНОВИ ДОСЛІДЖЕННЯ ТЕКСТІВ МАСОВОЇ РОЗСИЛКИ

1.1. Спам як окремий мовленнєвий жанр інтернет-дискурсу

Спам постає окремим, унікальним мовленнєвим жанром сучасного інтернет-дискурсу. Щоб зрозуміти специфіку останнього, варто усвідомити своєрідність поняття дискурсу в цілому.

У сучасній лінгвістичній науці поняття «дискурс» трактують неоднозначно, що пов'язано з його багатофункціональністю та широким використанням у різних галузях. Існує низка поглядів на сутність поняття «дискурс», усі вони базовані на різному розумінні терміна. Дослідженню дискурсу присвячено роботи таких зарубіжних вчених, як Е. Бенвеніст, М. Стаббс, Д. Шифрін, В. Красних, В. Звягінцев, В. Карасик та ін. Над проблемою витлумачення дискурсу працюють також такі відомі українські вчені: А. Загнітко, Ж. Краснобаєва-Чорна, І. Шевченко, К. Серажим, Ф. Бацевич, О. Селіванова та ін. Однак, у науці досі не існує чіткого визначення поняття дискурсу.

Термін «дискурс» використовуваний у різних науках – таких, як психологія, філософія, соціологія, антропологія, етнологія, юриспруденція, педагогіка, політологія, економіка, семіотика, літературознавство. Важливим він є і для різних напрямів лінгвістики: психолінгвістики, когнітивної лінгвістики, прагмалінгвістики, етнолінгвістики. Звичайно, різні точки зору при вивченні дискурсу в його різних аспектах згодом лише взаємодоповнять одна одну та збагатять лінгвістичну науку, проте кожна із зазначених дисциплін по-своєму підходить до вивчення дискурсу, саме через це неможливо витлумачити один єдиний термін, що буде однаково розглядати дискурс з усіх його граней. Наприклад, у філософії «дискурс» застосовується на позначення утворення, що має мисленнєво-комунікативну природу та належність до об'єктів, які можуть інтерпретуватися лише у світлі нелінійної парадигми [16].

За «Лінгвістичним енциклопедичним словником» В. Ярцевої, «Дискурс (від франц. discours – мова) – зв’язний текст у сукупності з екстралінгвістичними – прагматичними, соціокультурними, психологічними та іншими факторами; текст, що розглядається у контексті подій; мовлення, що розглядається як цілеспрямований соціальний акт, як компонент, що бере участь у взаємодії людей і механізмах їх свідомості (когнітивних процесах). Дискурс – це мовлення, що «занурене в життя». Слідуючи цьому, «дискурс», на відміну від терміна «текст», не застосовується до старовинних та інших текстів, зв’язки яких з живим життям не відновлюються безпосередньо» [18, с. 136].

Л. Гренобл у статті «Discourse Analysis» зазначає, що спочатку термін «дискурс» у англійській науковій літературі позначав контрольований мисленнєвий процес, результат якого повинен бути впорядкованим і чітко вписуватися в ідейний контекст. Дискурсологія має й іншу назву «аналіз дискурсу» – термін, уперше вжитий американським лінгвістом, фундатором дистрибутивного та трансформаційного аналізу З. Харрисом у значенні методу аналізу зв’язного мовлення, який служить для опису меж простого речення і для зв’язку мови з культурою [24, с. 625]. Як термін лінгвістики поняття дискурсу З. Харрис вперше вжив у 1952 році у статті, що була присвячена аналізу мови реклами.

За К. Серажим, «... під дискурсом ми розуміємо складний соціолінгвістичний феномен сучасного комунікативного середовища, який, по-перше, детермінується (прямо чи опосередковано) його соціокультурними, політичними, прагматично-ситуативними, психологічними та іншими (конститууючими чи фоновими) чинниками, по-друге, має «видиму» – лінгвістичну (зв’язний текст чи його семантично значущий та синтаксично завершений фрагмент) та «невидиму» – екстралінгвістичну (знання про світ, думки, настанови, мету адресанта, необхідні для розуміння цього тексту) структуру і, по-третє, характеризується спільністю світу, який «будується» впродовж розгортання дискурсу його репродуцентом (автором) та інтерпретується його реципієнтом (слухачем, читачем тощо). Дискурс – це,

образно кажучи, життя тексту в нашій свідомості, це накладання інформації, яку ми отримуємо з цього тексту, і нашого знання про обставини, спонуки його породження на ментально-чуттєве інформаційне поле нашого індивідуального «Я»» [25, с. 13].

Французький мовознавець Е. Бенвеніст зазначає, що «дискурс – складне комунікативне явище, яке охоплює й соціальний контекст, що створює уявлення як про учасників комунікації, так і про процеси творення й сприйняття повідомлення. У широкому смислі слова дискурс є складною єдністю мовної форми, значення й дії, що можна охарактеризувати за допомогою розуміння комунікативної події чи комунікативного акту. Перевага такого розуміння полягає в тому, що дискурс не обмежується рамками конкретного мовного висловлювання, а саме межами тексту» [3, с. 19].

За О. Кубряковою, під дискурсом треба мати на увазі «іменний когнітивний процес, пов'язаний з реальним творенням мови, створенням мовного твору, текст є кінцевим результатом процесу мовної діяльності, що виливається в певну закінчену (і зафіксовану) форму» [17, с. 324].

В. Звягінцев вважає, що дискурс – це елементарна одиниця тексту, тобто складне ціле, або змістова єдність, що вирізняється на рівні мови та, як правило, реалізується у вигляді речень, які пов'язані між собою смисловими зв'язками. Не менш поширеним є розглядання *discourse* як довільного фрагменту тексту, що складається більше ніж з одного речення або незалежної частини речення. Здебільшого, хоча не завжди, концентрується навколо певного опорного концепту; створює загальний контекст, що описує діючих осіб, об'єкти, обставини, час, вчинки тощо, визначаючись не стільки послідовністю речень, скільки тим спільним для творця дискурсу та його інтерпретатора світом, що будується під час розгортання дискурсу – це погляд, «етнографія мовлення» [10, с. 10].

Ж. Краснобаєва-Чорна зазначає, що «найтипівішими є дві дефініції дискурсу: 1) одиниця, що складається з двох значущих компонентів – динамічного процесу мовленнєвої діяльності з обов'язковою апеляцією до

соціального контексту та її результату, тобто тексту; 2) родовий термін, що об'єднує всі різновиди використання мови (текст, діалог тощо). Проблема визначення ускладнюється тим, що дискурс має комплексний характер і виступає об'єктом міждисциплінарного вивчення: крім традиційної лінгвістики, дискурс досліджують комп'ютерна лінгвістика та штучний інтелект, психологія та педагогіка, філософія та логіка, антропологія й етнологія, літературознавство та семіотика» [16, с. 13].

Навіть якщо у сучасній науково-лінгвістичній літературі й немає однозначного тлумачення дискурсу, то існує багато праць, присвячених його дослідженню, і ця кількість, на нашу думку, постійно зростає й зростатиме в майбутньому. До того ж, бурхливий розвиток інноваційних технологій, зокрема у мережі Інтернет, дещо змінює традиційні уявлення про дискурс та його жанри, що дає можливість повніше зрозуміти їх динамічну, чутливу до нових суспільних реалій процесуальну сутність.

Отже, розвиток технологій має істотний вплив як на структуру жанрової системи інтернет-комунікації, так і на саму дискурс-комунікацію в рамках того або того жанру [6, с. 20]. Для аналізу дискурсу застосовується метод дискурс-аналізу, який полягає у виявленні як вербальних компонентів, так і прагматичних чинників [10, с. 15]. М. Макаров наголошує: «Дискурс-аналіз ідейно тримається на трьох китах – трьох найважливіших категоріях: дії, (по)будові та варіативності. Коли люди щось говорять або пишуть, вони тим самим здійснюють соціальні дії. Конкретні властивості цих соціальних дій визначаються тим, як усний дискурс чи письмовий текст побудовані, за допомогою яких саме ресурсів, відібраних мовцем з усього розмаїття мовних засобів, функціональних стилів, риторичних прийомів тощо. З одного боку, цікавим є сам процес побудови дискурсу. З іншого боку, оскільки усний дискурс чи письмовий текст вплетені до живої тканини соціальної діяльності та міжособистісної взаємодії, їхня варіативність утілює особливості різних соціально-діяльнісних контекстів і намірів авторів» [20, с. 88]. Велика увага до дискурсології зумовила розробки етнографічного напрямку аналізу дискурсу,

який мав на меті дослідити вплив культурних і соціальних чинників на процеси мовленнєвого спілкування, зокрема, з'ясувати правила конверсаційної взаємодії, процедури інтерпретації з урахуванням фонових знань учасників спілкування; встановити особливості зміни комунікативних ролей і їхню соціокультурну детермінованість; визначити правила виведення (*conversational inferences*) тощо [10].

В останні роки спостерігається соціальний інтерес до знань закономірностей людського спілкування. Сьогодні сфера вживання терміну «дискурс» є настільки широкою (філософія, соціологія, логіка, семіотика, теорія комунікації, лінгвістика тощо), що доводиться говорити про полісемію цієї термінологічної одиниці, а з розвитком інтернет-технологій, дискурс потрапляє також і у сферу інтернет-простору.

Відтак, під дискурсом сучасна лінгвістика (до уваги не беремо філософські інтерпретації цього поняття, оскільки нас дискурс цікавить передусім як об'єкт лінгвістичного дослідження) розуміє:

1. Зв'язний текст у сукупності з екстралінгвістичними – прагматичними, історико- та соціокультурними, психологічними та іншими – чинниками (це найбільш визнане сучасними мовознавцями тлумачення ввів у науковий обіг Т. ван Дейк, таких поглядів дотримуються і І. Штерн, В. Петров, Ю. Караулов та ін.).

2. Текст, узятий у подієвому аспекті; мовлення, яке розглядається як цілеспрямована соціальна дія, як компонент, що бере участь у взаємодії людей і механізмах їхньої свідомості (когнітивних процесах). Тобто дискурс – це подія, у центрі якої словесний компонент; комунікативний акт, узятий не тільки як цілісна структура, але і як повна тяглість, що включає і розмаїття його оцінок учасниками та спостерігачами, і навіть його наслідки (Н. Арутюнова, Г. Кук, К. Пайк та ін.).

3. Текст, що утворився в процесі дискурсії, коли значення «на виході» стає адекватним авторському задуму. Дискурсія починається там, де з'являються додаткові змісти, що відрізняються від буквального розуміння тексту.

Наближення до розуміння цих додаткових змістів комплектує майбутній дискурс. Таким чином, у цьому трактуванні дискурс є ментальним утворенням, що виникає у свідомості читача в процесі такого сприйняття тексту, яке відштовхується від буквального розуміння, й існує стільки, скільки триває процес його сприйняття й розуміння (В. Костомаров, Н. Бурвикова та ін.).

4. Сукупність тематично, культурно або інакше взаємопов'язаних текстів, що допускає розвиток доповнення іншими текстами (А. Баранов, Д. Добровольський та ін.).

5. Спілкування, що розглядається як реалізація певних дискурсивних практик. Тобто це – плинна мовленнєва діяльність у тій чи тій сфері, калейдоскоп висловів, фраз, аналітичних статей та інформаційних повідомлень, публічних виступів, інтерв'ю, коментарів, кулуарних обмінів думками, що характеризує буття у часі (М. Фуко, А.-Ж. Греймас, Ж. Курте та ін.).

На думку К. Серажим, «жодне з цих трактувань дискурсу (кожне породило цілу низку додаткових визначень) не охоплює усіх аспектів його природи, не відображає особливостей його породження та функціонування в сучасному комунікативному просторі» [25, с. 12].

Також, згідно з Н. Арутюновою, дискурс – «текст, занурений у життя» з усіма відповідними «формами життя» [2, с. 137]. Однією з таких особливих «форм» визначаємо «життя» й комунікацію носіїв мови в мережі Інтернет, що постає ще більш затребуваною й перспективною площиною людського існування у наших сьогоденішніх «дистанційованих» від реального життя умовах. Інтернет, будучи високотехнологічним і в той же час високодинамічним комунікативним простором, знаходиться в постійному русі, постійній еволюції. Відповідно, з'являються абсолютно нові форми інтернет-комунікації, а старі видозмінюються тим чи тим чином [6, с. 20].

У зв'язку з інтенсивним впровадженням в життя суспільства комп'ютера та інтернету формується особливий вид дискурсу – інтернет-дискурс. Своєрідною є сфера його появи та поширення – електронна, глобальна, інтерактивна. Специфіка інтернет-дискурсу проявляється в усіх «мовних»

площинах: є особливості графічні та орфографічні, лексичні, граматичні. З'являється принципово новий тип дискурсу – усно-письмовий. Інтернет-дискурс являє собою процес створення тексту в сукупності з його прагматичними, соціокультурними, психологічними факторами, цілеспрямованими соціальними діями, що включає в себе взаємодію людей і механізмів їх свідомості – когнітивних процесів. І, відповідно, стає дедалі поширенішим такий вид мовленнєвого жанру в інтернет-дискурсі, як спам.

Існують різні визначення спаму, частина з яких не зовсім розкриває суть поняття [43]. Чітке визначення спаму необхідне для збору статистики про спам і розуміння суті цього явища, а також може знадобитися для введення різних контрелементів, що стосуються комерційної поведінки, психології одержувача спаму, розширення законодавчих контекстів, економічної і технічної сторони справи.

На думку англійського лінгвіста К. Фейнштайна, «спам – це електронне повідомлення, яке розсилають за вказівкою організації (або конкретної особи), яка не має жодного відношення та інтересу до отримувача» [28, с. 21]. На його думку, будь-який лист, що містить рекламу та не узгоджений з отримувачем, є спамом, а люди, які його поширюють, – поширювачі спаму або ж спамери (англ. spammers). Також К. Фейнштайн додає, що спамом може бути лист, розісланий не лише за допомогою пошти, а й за допомогою соціальних мереж чи месенджерів.

Спам (spam, junk mail) – це електронні текстові та / або мультимедійні повідомлення різного змісту, зазвичай рекламного характеру, які без попередньої згоди (замовлення) споживача умисно масово надсилаються на його адресу електронної пошти або кінцеве обладнання абонента (крім повідомлень оператора чи провайдера щодо надання послуг). Подальше отримання таких повідомлень споживач не може припинити шляхом інформування про це замовника чи відправника. Найчастіше рекламні тексти розсилає робот або людина, яка отримує за розсилку гроші.

У найгіршому своєму вияві «спам – це один із видів надокучливої реклами, яка розповсюджується за допомогою електронної пошти» [21, с. 5].

Можна сказати, що спам – це анонімна масова непрошена розсилка. У цьому визначенні важливе кожне включене в дефініцію слово:

- анонімна (більшість повідомлень надходить в основному саме від автоматичних розсилок, з прихованою або фальсифікованою зворотною адресою);
- масова (ці розсилки саме масові, і лише вони є справжнім бізнесом для спамерів і справжньою проблемою для користувачів);
- непрошена (очевидно, що підписні розсилки і конференції не повинні підпадати під це визначення).

У більшості трактувань можна виділити певні спільні риси, які підходять під таке визначення: «спам – розсилка по електронній пошті повідомлень, іноді систематична, з непотрібною зазвичай інформацією у великих об'ємах особам, що не мають ніяких контактів з людиною, яка розсилає ці повідомлення і чий електронні адреси були отримані незаконним шляхом» [43]; «зазвичай під терміном «спам» розуміється систематична розсилка електронних повідомлень комерційного характеру особами, що приховують або підроблюють свої справжні координати» [45]; «спам визначається як будь-які непотрібні електронні повідомлення, що приходять на електронну пошту у великих кількостях. Це визначення швидше характеризує масові електронні розсилки» [42].

Згідно з даними Організації економічного співробітництва і розвитку (ОЕСР), у всіх визначеннях спаму можна виділити головні й додаткові його ознаки. До головних належать незатребуваність повідомлень, надісланих у великій кількості, і їх комерційний характер. Будь-яка людина, що отримала величезну кількість листів, відразу зрозуміє, що це спам. Спам має також додаткові ознаки, але не завжди лист, що відзначається ними, є спамом: адреси користувачів задіяні без їх дозволу; розсилається непотрібна інформація; розсилка є систематичною; відправника не хвилює склад аудиторії, головне –

кількість; повідомлення приходять щодня; відправник приховує / підробляє свої справжні координати; рекламуються нелегальні товари; інформація в повідомленнях є хибною зазвичай.

Не дивлячись на складність виділення єдиного визначення спаму, що точно і чітко визначає це явище, за допомогою існуючих визначень спаму можна стверджувати: спам – це електронне повідомлення, отримане по мережі Інтернет; спам приходить без попереднього запиту або згоди. Тобто, якщо одержувач погоджується на розсилку, то це вже не спам; спам розсилається у великих кількостях (відправник розсилає багато однакових повідомлень, а одержувачі вибираються випадково). Ці три параметри характерні для масових незатребуваних електронних повідомлень; також це співпадає з визначенням, поданим організацією SpamHouse [46]. Ця організація оперує саме вищеназваним визначенням спаму, хоча тут можна додати і четвертий пункт: спам повинен містити рекламу якого-небудь товару або послуги. Більшість повідомлень належать саме до цієї категорії і називаються рекламними повідомленнями.

Реклама, яка надсилається за допомогою спаму, має суттєві відмінності від звичайної, по-перше – звичайна реклама поширюється традиційними способами: через телебачення, радіо або ж друковані видання. До того ж, користувач у будь-який момент може відмовитися від нецікавої для нього реклами, на відміну від спаму.

Існують три основні відмінності спаму від звичайної реклами:

- 1) повідомлення без запиту на нього: одержувачі не виявляли бажання отримувати інформацію випадкового змісту від невідомих осіб;
- 2) безадресні розсилки: розповсюджувачі спаму не знають, хто саме стане його одержувачем;
- 3) масовість розсилки: спам розсилається величезними «тиражами», досягаючи часом десятків мільйонів копій.

У залежності від того, де поширюється спам, виділяють:

- поштовий спам (один із найпоширеніших, розповсюджуваний лише через пошту);
- спам на блогах;
- спам на форумах (розсилання рекламних повідомлень учасникам форуму без їхньої згоди);
- спам на дошках оголошень;
- вискакуючі вікна (pop-up) (випливаючі вікна, що містять рекламу та, зазвичай, заважають прочитанню інформації на сторінці; поширений на більшості сайтів);
- пошуковий спам, або веб-спам (використовується для того, щоб впливати на результати пошуку, таким чином, пошукові технології не можуть правильно ранжувати сайти й видавати саме ті сторінки, які справді релевантні запитам);
- спам у соціальних мережах та на сайтах знайомств;
- спам у SMS-повідомленнях та у месенджерах;
- мережевий спам (повідомлення по мережі, яке містить рекламу).

До потенційного споживача спам потрапляє шляхом масової розсилки. Одинадцятитомний «Словник української мови» (СУМ-11) дає таке визначення останній: «РОЗСІЛКА, и, жін., розм. Дія за значенням розсилати і розіслати. *Розсилка листів.*». Тобто, масова розсилка спаму – це інструмент комунікації з аудиторією, суть якого полягає у відправленні одного повідомлення багатьом контактам із певною метою. Зазвичай це здійснюється через сервіси розсилок, а список адресатів складається заздалегідь і називається базою для розсилки.

Різновиди розсилок можна виділяти за різними критеріями:

- за способом відправлення – ручні та автоматичні (залежить від того, відправляє маркетолог повідомлення самостійно або використовує певний сервіс розсилки);
- за механікою запуску – масові й тригерні (масові розсилки зазвичай відправляються одноразово певній групі абонентів; тригерні –

розсилаються користувачам за сценарієм залежно від дій, які вони здійснюють на сайті, в додатку або під час взаємодії з розсилками (сценарії можна адаптувати відповідно до потреб); одними з найпопулярніших тригерних розсилок є листи до дня народження клієнта, покинуті кошики і перегляди, повідомлення про статус замовлення і доставки);

- за регулярністю – регулярні та ситуативні (планована постійна комунікація належить до першого типу, а одноразові розсилки, актуальні у певний момент, – до другого);
- за контентом – промо, інформаційні, поведінкові та транзакційні (якщо контент повідомлення складається з рекламної інформації – це промо; із навчальної, новин компанії – інформаційна розсилка; також є повідомлення, які відправляються як реакція на певну дію / бездіяльність);
- за метою – привітальні, вітальні та ін. (більш вузька класифікація ґрунтується на приводі для відправлення повідомлення);
- за каналами – Email, SMS, месенджери, Push-повідомлення.

За останнім параметром розглянемо тексти масової розсилки детальніше:

Email-розсилка. Це лист, відправлений на електронну пошту. Має найбільший допустимий обсяг тексту і кількість використовуваних елементів. Наприклад, технологія AMP (Accelerated Mobile Pages, технологія прискорення роботи мобільних сторінок), що дозволяє виконати необхідну дію без переходу на сайт, серед розсилок доступна тільки для імейл. Метою Email-розсилки може бути просування бізнесу, інформування про новини компанії, проведення масових акцій, вітання зі святами та знаковими подіями.

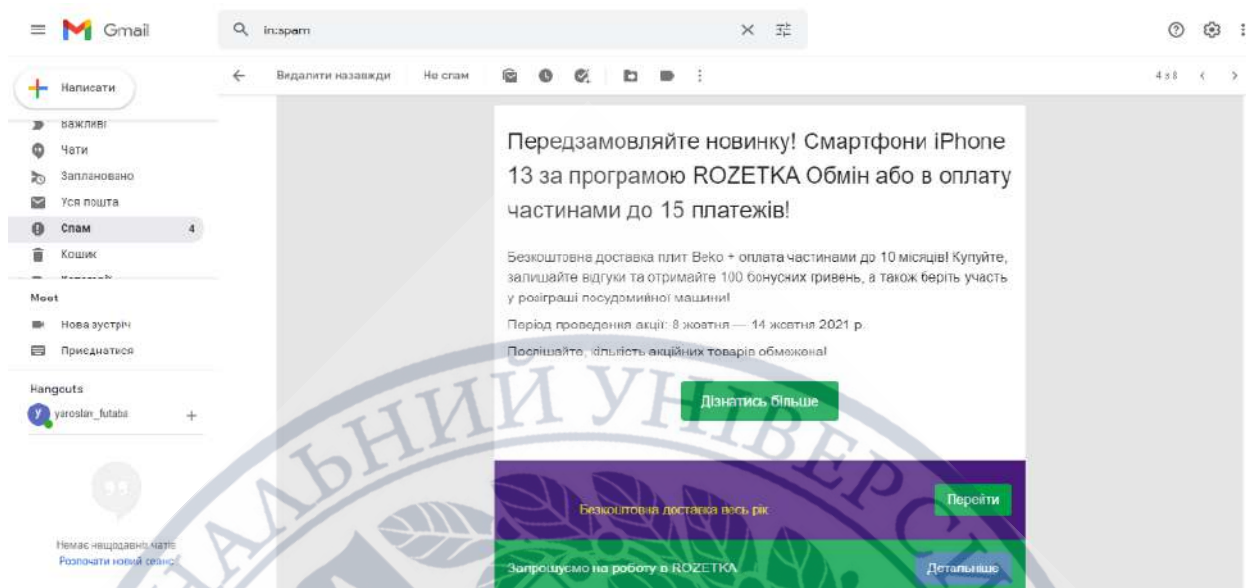


Рис. 1.1. Приклад Email-розсилки

SMS-розсилка. Відправлене на номер телефону одержувача коротке текстове повідомлення (до 70 символів) з інформацією про знижки, акції, підтвердження замовлення або доставки. SMS-повідомлення і досі дієві та ефективні. Використовують цей канал для додаткової стимуляції продажів і нагадування про важливі події та акції.

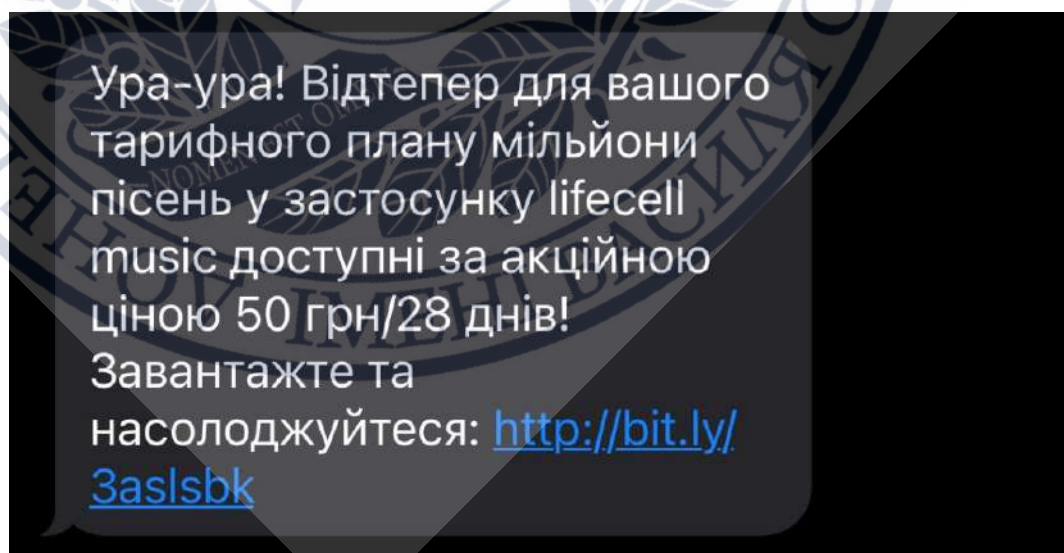


Рис. 1.2. Приклад SMS-розсилки

Push-розсилка. Повідомлення, які виводяться на екрані користувача поверх усіх вікон. Можуть бути у форматі web і для мобільних пристроїв.

Web-push-розсилка – хороший інструмент для нагадування про компанію, реклами товару або старту розпродажу. У повідомленні можна використовувати текст, банер, посилання і кнопки. Проводьте А/В-тестування, персоналізуйте звернення, випробовуйте різні креативи – і ви неодмінно отримаєте результат.

Mob-push-повідомлення. Відправляються з додатків, усе інше працює на мобільних пристроях користувачів аналогічним чином.



Рис. 1.3. Приклад Push-розсилки

Розсилка у Viber. Розсилка в месенджері, який використовують до 260 млн. користувачів в усьому світі (за версією проєкту Kantar CMeter). Великий обсяг знаків текстових повідомлень (до 1000), можливість додавати фото, посилання, а також кнопку, роблять цей канал одним із найзручніших у комунікації. Робота з цим каналом надає більше простору для креативу. Для старту необхідно отримати дозвіл на розсилки і зареєструвати альфа-ім'я. Вартість відправлення одного повідомлення коштуватиме дешевше, ніж SMS. Мінімальний бюджет для запуску Viber-розсилки через eSputnik у 2020 році знижено вдвічі.

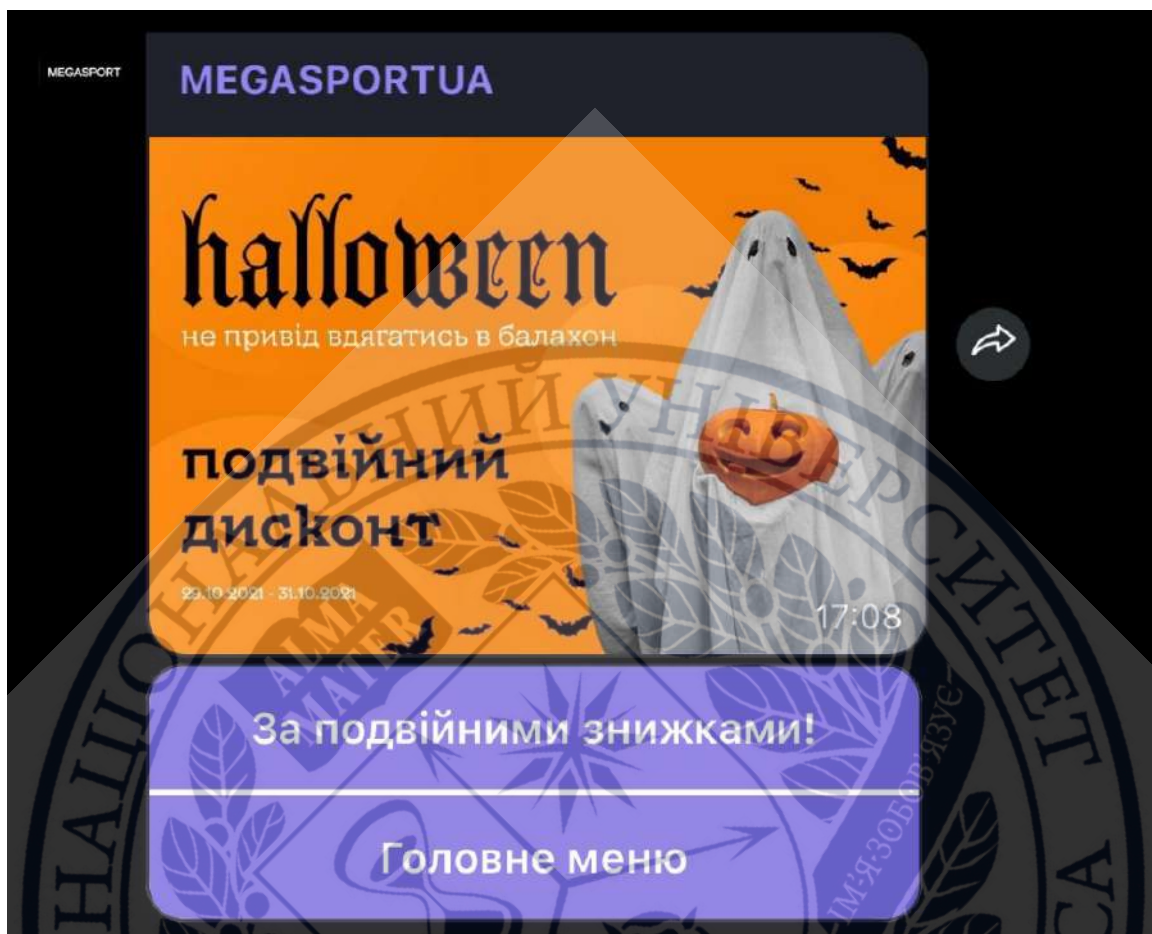


Рис. 1.4. Приклад розсилки у Viber

За допомогою сервісу eSputnik можна налаштовувати унікальні сценарії з використанням усіх необхідних каналів: Email, SMS, Push, Viber. Такий підхід допоможе досягти найбільшої ефективності для маркетингу в цілому і посилити результати одного каналу за допомогою інших. Наприклад, можна запустити Email-розсилку, потім запустити SMS усім, хто не прочитав, і нагадати про важливу подію – згорання бонусів, закінчення акції, наявність важливого товару на складі та ін. Ті самі Push-повідомлення добре працюють як додатковий «підігрівуючий» інструмент для основних розсилок.

1.2. Потенціал шкідливості спам-розсилки та основні методи ефективної боротьби з ним

Спам-повідомлення ділять залежно від цілей, що переслідує спамер. Ф. Воройський зазначає, що спамер – це особа, що розсилає спам: «... для боротьби зі спамом і особами, що його розсилають (спамери)...» [5, с. 507]. Спамери роблять масові розсилки з метою отримання прибутку, наприклад, у повідомленні може міститися реклама товару або послуги чи заклик брати участь у політичних кампаніях тощо. Інші розсилають повідомлення шахрайського характеру або поширюють шкідливі програми (віруси, «троянські коні»).

Найперше, що необхідно зробити спамеру, – це роздобути базу контактів (список поштових скриньок, номери телефонів для СМС-спаму). Домогтися цього можна кількома шляхами. Найпростіше купити базу контактів, вони продаються у вільному доступі. Основними параметрами таких баз є:

- актуальність (свіжі поштові скриньки, якими справді користуються);
- обсяг (якомога більший);
- специфіка (мільйон нових довільних контактів гірший, ніж сто тисяч адрес спеціальних адресатів – потенційно «зацікавлених»).

Спамер також може самостійно зібрати базу. В інтернеті є безкоштовні програми-роботи, завантажити які може кожен. Така програма починає по черзі відкривати одну сторінку в інтернеті за іншою. Упродовж дня подібний робот може переглядати до мільйона сторінок, продуктивність залежить від каналу зв'язку та ефективності програми. Програма аналізує код сторінки та збирає поштові скриньки. Якщо збирач інформації хоче отримати спеціалізовані скриньки, можна навчити свою програму вибирати окремі групи e-mail. Узяти на будь-якій пошуковій системі групу сайтів, наприклад, присвячених лінгвістиці, і почати працювати тільки з ними.

Найбільша проблема спамера – технології розсилки. Старі методи вже не діють, тому доводиться постійно вигадувати щось нове. Можна сказати, що розсилка спаму виглядає так: є комп'ютер, з якого надсилатимуть послання, є

текст повідомлення, є мільйон одержувачів. Якщо просто почати надсилати рекламу з комп'ютера, то вона відразу потрапить у спам-фільтри. Захисні системи чітко стежать, щоб постійний текст не розсилався у великих кількостях. Тому спамерам доводиться постійно використовувати обхідні шляхи. Найперше, починають від адресата до адресата змінювати текст повідомлення (змінювати місцями абзаци), або пишуться різні номери телефонів чи даються посилання на різні сайти (можна автоматично зробити 1000 сторінок у мережі з різними адресами, звідки відвідувач «перекидатиметься» на потрібний). Інша форма обходу спам-фільтрів – надсилати повідомлення не з одного комп'ютера. Хакер-маркетолог створює так звану бот-мережу, тобто він заражає, наприклад, 10 тис. комп'ютерів, з яких починається розсилення спаму. Оскільки повідомлення йдуть із різних адрес, це допомагає обійти захист. З погляду інформаційної безпеки, незатребувані комерційні електронні повідомлення впливають тільки на доступність інформації. Пропускна спроможність каналу зв'язку може повністю використовуватися для скачування цих повідомлень, і ресурс мережі Інтернет, до якого користувач намагається дістати доступ, опиниться недоступний.

Спам, розісланий з метою реклами товару або послуги, позначають як «незатребувані комерційні електронні повідомлення». Часто такі повідомлення розглядаються компаніями як важливий метод залучення клієнтів, оскільки розсилка повідомлень поштою – це найдешевший спосіб розповісти про товар або послугу. Проте більшість таких повідомлень розсилаються не самими компаніями, а спамерами, які отримують певну винагороду за розсилку спаму. Не дивлячись на мізерну кількість відповідей на спам-повідомлення, замовники все одно отримують прибуток. Згідно ОЕСР [43] 8% з опитаних призналися, що придбали товари, що рекламуються через спам. Дослідження показали, що навіть якщо відсоток тих, що відповіли, складатиме 0.001%, реклама через електронні повідомлення у будь-якому випадку вигідна.

Рекламні повідомлення можуть містити політичну або релігійну пропаганду. Наприклад, у 2003 році члени Конгресу США розіслали виборцям сотні тисяч повідомлень [48]. За негативністю впливу на захищеність інформації

повідомлення некомерційного характеру аналогічні першим, тобто впливають тільки на доступність інформації.

Деякі спамери розсилають повідомлення з фальсифікованою інформацією, тобто шахрайські листи. Фальсифіковані повідомлення розсилаються з метою змусити одержувача повірити, що яка-небудь вигадана подія є правдою, причому такі повідомлення часто супроводжуювані проханням розіслати цей лист якомога більшій кількості людей (ланцюгові листи). Деякі повідомлення попереджають про віруси, «черв'яків» або «троянських коней», інші містять недостовірну інформацію про які-небудь політичні або суспільні події, іноді в повідомленнях міститься прохання про добродійність або пропозиції комерційного характеру, наприклад, в повідомленні може знаходитися сертифікат на отримання безкоштовного подарунка від фірми.

Листи фальсифікованого змісту, надіслані з метою отримати певну матеріальну вигоду, називають *скам*. Прикладами можуть служити листи з проханням переказати гроші на рахунок жертв природного лиха.

Одним із видів шахрайських листів є *фішингові листи*, надіслані нібито від імені відомої компанії. Метою подібних листів є отримання у користувачів конфіденційних даних про паролі і коди доступу, наприклад, листи з «банку» з проханням підтвердити дані кредитної карти. Подібні листи, окрім порушення доступності зовнішніх ресурсів, порушують ще й конфіденційність інформації – такої, як номери банківських карт або паролі доступу до систем дистанційного управління рахунком.

Joe jobs – це обманне повідомлення, надіслане від імені іншої людини з метою нанесення шкоди репутації. Наприклад, Joe jobber може розіслати на тисячі адрес повідомлення з дитячою порнографією, при цьому зворотною адресою значитиметься, наприклад, User@Company.Ru, щоб обурені одержувачі цього повідомлення закидали скриньку User'a гнівними листами і репутація компанії Company була би підірвана. Назва joe jobs вперше була використана для опису подібної схеми, жертвою якої став хостер Джо Долл. Обліковий запис одного користувача був видалений з розсилки спаму для реклами своїх товарів;

у помсту той користувач розіслав на мільйони адрес ще більше спаму, але зворотною адресою значилася адреса Джо Долла [35, с. 3]. У цьому випадку має місце атака «Відмова в обслуговуванні», де ролі тих, що атакують, виконують одержувачі обманних повідомлень.

Шкідливі спам-програми розробляються з метою нанесення шкоди комп'ютерній системі і розсилаються під виглядом нешкідливого додатку до повідомлення. Віруси, «черв'яки», «троянські коні», програми-шпигуни і рекламні програми вкладаються в листи і запускаються при відкритті вкладеного файлу. Між спамом і шкідливими програмами існує взаємозалежність [44]: через спам розсилаються шкідливі програми, вони завдають шкоди комп'ютеру, щоб контролювати його на відстані і розсилати ще більше спаму. Такі комп'ютери називаються «зомбі». Таким чином, електронні листи зі шкідливими програмами порушують не тільки доступність зовнішніх ресурсів (за рахунок забивання вхідного каналу трафіком, що генерується при скачуванні спаму) і конфіденційність секретних даних (завдяки можливості деяких вірусів знаходити і відправляти господареві номери банківських карт і паролі доступу), але і цілісність всієї інформації, збереженої на комп'ютері (за рахунок здатності деяких вірусів зашифровувати всі знайдені документи).

Негативна квитанція – це недоставлене повідомлення, що посилається назад відправникові. Згідно дослідженню Ironport [40, с. 3], повідомлення, повернені на підроблені зворотні адреси невинних третіх осіб, складають близько 9% від всього електронного трафіку, що відповідає 1,67 млрд. повідомлень, що повернулися, на день [37, с. 5-6]. Негативна квитанція не є спамом як таким, але вона складає значну частину електронного трафіку, який збільшується через спам. Таким чином, негативні квитанції знижують тільки доступність зовнішніх ресурсів.

Згідно Ferris Research [38, с. 172-173], у 2010 році спам завдав американським компаніям збиток у розмірі \$8,9 млрд., а європейським – \$2,5 млрд. При цьому виявилось, що «закодування» непотрібною інформацією поштових скриньок не найстрашніше. Наприклад, 40% збитку викликано

падінням продуктивності праці – співробітники змушені відволікатися на спам. Виявилося, що в середньому співробітники витрачають 4,5 секунди лише на видалення одного такого листа.

Отже, боротьба зі шкодою, яку здатен нанести спам, є надзвичайно активною й необхідною. З цією метою створюються різноманітні проєкти.

Сучасна спам-розсилка поширюється в сотнях тисяч екземплярів лише за кілька десятків хвилин. Найчастіше спам йде через заражені шкідливими програмами комп'ютери користувачів – зомбі-мережі. Сучасна індустрія ІТ-безпеки пропонує безліч рішень, і в арсеналі антиспамерів є різні технології. Однак жодна з існуючих технологій не є досконалим протистоянням. Більшість сучасних продуктів використовують кілька технологій, інакше ефективність продукту невисока.

Методи можуть застосовуватися на різних стадіях відправки спаму. Вони можуть бути задіяні на стадії роботи поштового клієнта, МТА поштового провайдера відправника, поштового вузла поза поштовим провайдером відправника і одержувача або клієнта одержувача [1]. На перших двох стадіях можна застосувати превентивні заходи. Бажано зупинити спам якомога раніше, щоб не витратилися такі ресурси, як ширина смуги пропускання і час скачування. Проте, найпоширеніші технічні методи боротьби зі спамом застосовуються на стороні одержувача.

Маршрути розсилки спаму можуть розрізнятися. Іноді спамери встановлюють власного агента пересилки (MTA) і розсилають повідомлення безпосередньо провайдеру поштових послуг (ESP – E-mail service provider) одержувача. Іншим способом може бути дослідження інфраструктури ESP (посилаючи повідомлення через MTA).

Загалом методи боротьби зі спамом можна розділити на коротко-, середньо- і довгострокові. Механізми фільтрації і блокування розглядаються як короткострокові методи, оскільки їх застосування може бути обмежене інфраструктурою місцевої поштової організації з незначними модифікаціями.

Деякі методи, засновані на DNS, які впливають на структуру і вміст в записах DNS, можуть запускатися місяцями або навіть роками. Методи, засновані на інфраструктурі відкритих ключів (PKI – Public key infrastructure) і методи, засновані на ресурсах, можуть виявитися довгостроковими, зважаючи на значні зміни й розширення інфраструктури. Уся різноманітність методів боротьби зі спамом показана на схемі 1.1.



Схема 1.1. Технічні методи боротьби зі спамом

Найбільш поширеними є декілька методів. Першим є **чорні списки**. Вони ж DNSBL (DNS-based Blackhole Lists). Це одна з найстаріших антиспам-технологій. Блокують пошту з IP-серверів, перелічених у списку. Плюси: чорний список на 100% відсікає пошту з підозрілого джерела. Мінуси: дають високий рівень помилкових спрацьовувань, тому слід застосовувати з обережністю.

Контроль масовості (DCC, Razor, Pyzor). Технологія передбачає виявлення в потоці пошти масових повідомлень, які абсолютно ідентичні або майже не відрізняються. Для побудови працездатного «масового» аналізатора потрібні величезні потоки пошти, тому цю технологію пропонують виробники, що мають значні обсяги пошти, яку вони можуть аналізувати. Плюси: якщо технологія спрацювала, вона гарантовано визначила масову розсилку. Мінуси:

по-перше, «велике» розсилання може виявитися не спамом, а цілком легітимною поштою (наприклад, Ozon.ru тисячами надсилають практично однакові повідомлення, але це не спам); по-друге, спамери вміють «пробивати» такий захист за допомогою інтелектуальних технологій, – вони використовують програмне забезпечення, що генерує різний контент (текст, графіку тощо) у кожному спамерському листі, у зв'язку з чим контроль масовості не спрацьовує.

Перевірка інтернет-заголовків повідомлення. Спамери пишуть спеціальні програми для створення спамерських повідомлень та їх миттєвого поширення. При цьому вони припускаються помилок в оформленні заголовків, у результаті спам далеко не завжди відповідає вимогам поштового стандарту RFC (Request for Comments), що описує формат заголовків. За цими помилками можна визначити спамерське повідомлення. Плюси: процес розпізнавання та фільтрації спаму прозорий, регламентований стандартами та досить надійний. Мінуси: спамери швидко навчаються і помилок у заголовках спаму стає дедалі менше. Використання тільки цієї технології дозволить утримати не більше третини всього спаму.

Контентна фільтрація. Також одна зі старих, перевірених часом і досвідом технологій. Спамерське повідомлення перевіряється на наявність специфічних для спаму слів, фрагментів тексту, картинок та інших характерних рис. Контентна фільтрація починалася з аналізу теми повідомлення та його частин, які містили текст (plain text, HTML), але зараз спам-фільтри перевіряють всі частини, включаючи графічні вкладення. У результаті аналізу може бути побудована текстова сигнатура або зроблено підрахунок «спамерської ваги» повідомлення. Плюси: гнучкість, можливість швидкого «тонкого» налаштування. Системи, що працюють на такій технології, легко підлаштовуються під нові види спаму та рідко помиляються з розмежуванням спаму та звичайної пошти. Мінуси: зазвичай потрібні повсякчасні систематичні оновлення. Налаштуванням фільтра займаються спеціально навчені люди, іноді цілі антиспам-лабораторії. Така підтримка дорого коштує, що впливає на вартість спам-фільтра. Спамери винаходять спеціальні трюки для обходу цієї

технології: вносять до спаму випадковий «шум», що ускладнює пошук спамерських характеристик повідомлення та їх оцінку. Наприклад, використовують у словах небуквені символи (ось так, наприклад, може виглядати при використанні цього прийому слово alcohol: a_l_k_o_h_o_l_ або @lkohol генерують варіативне кольорове тло у зображеннях тощо.

Контентна фільтрація: байєс. Статистичні байєсівські алгоритми також призначені для аналізу контенту. Байєсівські фільтри не потребують постійного налаштування. Усе, що їм потрібно, – це попереднє навчання. Після цього фільтр підлаштовується під тематику листів, типову для цього конкретного користувача. Відтак, якщо користувач працює в системі освіти та проводить тренінги, то особисто у нього повідомлення такої тематики не будуть розпізнаватися як спам. Для тих, кому пропозиції відвідати тренінг не потрібні, статистичний фільтр віднесе повідомлення до спаму. Плюси: індивідуальне налаштування. Мінуси: найкраще працює на індивідуальному потоці пошти. Налаштувати байєс на корпоративному сервері з різними видами пошти – складне завдання. Головне, що кінцевий результат буде набагато гіршим, ніж очікується. Якщо користувач не навчає фільтр, технологія не буде ефективною. Спамери цілеспрямовано працюють над обходом байєсівських фільтрів, і це їм вдається.

Грейлістинг. Тимчасова відмова у прийомі повідомлення. Відмова йде з кодом помилки, який розуміють усі поштові системи. Через деякий час вони повторно надсилають повідомлення. А програми, які розсилають спам, у такому разі повторно листа не надсилають. Плюси: швидке вирішення проблеми. Мінуси: затримка у доставці пошти. Для багатьох користувачів таке рішення є неприйнятним.

Існують цілі організації з метою ефективної протидії спаму.

Так, Spamhaus Project – це міжнародна некомерційна організація, яка відстежує спам і пов’язані з ним кіберзагрози, такі як фішинг, зловмисне програмне забезпечення та ботнети, надає оперативні й високоточні дані про загрози в режимі реального часу для основних мереж, корпорацій та постачальників безпеки, а також співпрацює з правоохоронними органами для виявлення і переслідування джерел спаму та шкідливого програмного забезпечення по всьому світу (див. Рис. 1.5).

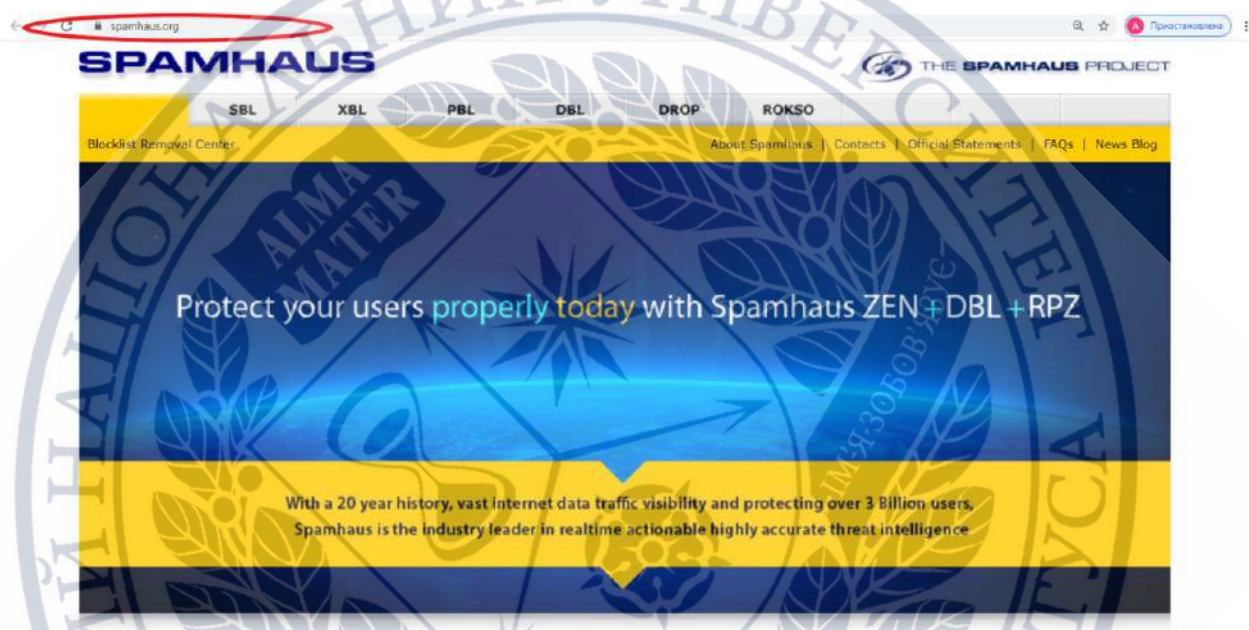


Рис. 1.5. Сайт проєкту Spamhaus

Заснований проєкт у Лондоні в 1998 році, проте зараз Spamhaus базується в Андорра-ла-Велья (столиця Андорри) і керується спеціальним персоналом з 38 слідчих, експертів-криміналістів та мережових інженерів, які працюють у 10 країнах світу. У реальному часі Spamhaus захищає понад 3 мільярди поштових скриньок користувачів і відповідає за блокування переважної кількості спаму та шкідливого програмного забезпечення, що надсилається в інтернеті. Дані Spamhaus сьогодні використовуються більшістю інтернет-провайдерів, постачальників послуг електронної пошти, корпорацій, університетів, урядів та військових мереж. Фактична кількість захищених поштових скриньок у

реальному часі опублікована в розділі «База користувачів Spamhaus» зліва на головній сторінці (див. Рис. 1.6).



Рис. 1.6. Розділ «База користувачів» Spamhaus

Окрім списків блоків на основі DNS (DNSBL), Spamhaus виробляє спеціальні дані для використання з брандмауером інтернету та обладнанням маршрутизації, – такі як списки DROP Spamhaus, дані C&C Botnet та дані зони реагування Spamhaus (RPZ) для DNS-розпізнавачів, що захищають мільйони користувачів інтернету, які натискають на шкідливі посилання у фішингових повідомленнях та електронних листах.

Щоб задовольнити суспільний попит на свої DNSBL, Spamhaus побудував одну з найбільших інфраструктур DNS у світі. Мережа Spamhaus складається із понад 80 загальнодоступних серверів DNSBL, розміщених у 18 країнах, обслуговує мільярди запитів DNSBL щодня безкоштовно.

Нагороди, вручені Spamhaus, включають такі:

- Нагорода за боротьбу з кіберзлочинністю (від Національного альянсу кібер-криміналістів і навчання Федерального бюро розслідувань (NCFTA)).

Загалом словник містить 40 визначень. Одним із центральних визначень є дефініція спаму. На думку авторів, слово «спам» у застосуванні до електронної пошти означає «небажана масова електронна пошта». Небажане означає, що одержувач не надав перевіреного дозволу на надсилання цього конкретного повідомлення. Масове означає, що повідомлення надсилається як частина більшої колекції повідомлень, усі з яких мають по суті ідентичний вміст. Повідомлення є спамом, лише якщо воно є і незапрошеним, і масовим. Небажана електронна пошта – це звичайна електронна пошта (запити щодо першого контакту, запити щодо роботи, запити продажів). Масова електронна пошта – це також звичайна електронна пошта (інформаційні бюлетені для передплатників, комунікації з клієнтами, списки обговорень). Електронне повідомлення вважається спамом, якщо особистість і контекст одержувача не мають значення, оскільки повідомлення однаково застосовне до багатьох інших потенційних одержувачів; одержувач не надав перевіреного, свідомого, явного і досі відкликаного дозволу на його надсилання.

Різні юрисдикції запровадили своє «законодавство» для контролю за тим, що вони називають спамом. Кожен закон по-своєму розглядає спам і, як наслідок, часто має різні визначення того, що він охоплює, незалежно від того, називають це спамом чи ні. Spamhaus використовує стандартне визначення – це незатребувані масові електронні листи (Unsolicited Bulk Email), яке підкреслює, що це не про вміст, а про згоду.

Незалежно від того, чи є повідомлення про небажану масову електронну пошту (UBE) рекламою, шахрайством, порнографією, листом з проханням або пропозицією безкоштовного обіду, – зміст не має значення – якщо повідомлення було надіслано небажано та масово, повідомлення є спамом. Спам не є піднабором UBE (Непотрібна групова електронна пошта). Непотрібна групова електронна пошта (UBE) – це електронна пошта, яка не є бажаною або не запитується одержувачем та надсилається у великій кількості (оптом). Більшість UBE призначені для рекламних цілей. Постачальники інтернет-послуг (ISP) можуть отримати списки, що блокують найбільш стійких відправників UBE. Це

захищає клієнтів від небажаних, дратівливих та іноді шкідливих UBE. Цей термін широко відомий як спам електронної пошти. Автори проєкту виділяють такі ключові параметри щодо небажаної розсилки електронної пошти:

1. Надсилання небажаної масової електронної пошти (UBE) заборонено усіма постачальниками інтернет-послуг по всьому світу.
2. Список блокування спаму від Spamhaus (SBL), яким послуговується більше 3 мільярдів користувачів інтернету, базовано на міжнародно прийнятому визначенні спаму як «небажаної масової електронної пошти». Тому будь-хто, хто надсилає UBE в інтернеті, незалежно від того, комерційний це контент чи ні, незаконний чи ні, виступає повноцінним відправником спаму – а отже, і справжнім спамером. Усі відправники UBE мають повністю усвідомлювати, що вони порушують умови ділових контрактів свого інтернет-провайдера (з потенційним ризиком втратити свої облікові записи та вільний доступ до інтернету, якщо вони надішлють UBE); вони потраплять до списку блокування спаму (SBL), якщо і надалі надсилатимуть UBE.

Отже, вся електронна пошта, надіслана небажано та масово, є спамом. Ця відмінність є важливою, оскільки законодавці витрачають надмірну кількість часу, намагаючись регулювати вміст спам-повідомлень, і при цьому стикаються з проблемами свободи слова, не усвідомлюючи, що проблема спаму пов'язана виключно зі згодою потенційного користувача.

Отже, у Розділі 1 розглянуто теоретико-методологічні основи дослідження текстів масової розсилки. Доведено, що спам являє собою окремий мовленнєвий жанр інтернет-дискурсу. Проаналізовано потужний потенціал шкідливості спам-розсилки та основні методи ефективної боротьби з ним.

РОЗДІЛ 2. ТЕХНІЧНІ ТА ЛІНГВІСТИЧНІ ОСОБЛИВОСТІ ТЕКСТІВ МАСОВОЇ РОЗСИЛКИ

2.1. Технічні / лінгвістичні маніпуляційні технології як засіб створення текстів масової розсилки

У сучасному світі неможливо уявити торгівлю без текстів масової розсилки та реклами у них. Задля попиту на товари маркетологи вдаються до різноманітних технологій впливу на покупця, зокрема і до маніпуляції.

Науковці по-різному підходять до дослідження маніпуляції. Одні з них вивчають маніпуляцію як засіб впливу на масову свідомість у контексті інформаційних процесів (І. Винокуров, Д. Волкогонов, Г. Гуртовой, Ю. Єрмаков, С. Кара-Мурза, Г. Ковалев, В. Крисько, Ю. Крижанська, В. Куликов, П. Лайнбарджер, Г. Мельник, С. Репко, Г. Почепцов, В. Севрюгін, В. Третьяков та ін.). Вони визначають маніпуляцію як негативне явище із руйнівним впливом на масову свідомість, що передбачає зміну спрямованості активності людей та здійснюється настільки майстерно, що залишається непоміченою ними.

Значна частина різноманітних впливів у рекламній діяльності є не чим іншим, як формою маніпуляції. Великий психологічний словник за редакцією Б. Мещрякова та В. Зінченко дає таке визначення терміну «маніпуляція»:

1. Ручна операція, ручна дія, демонстрація фокуса, що заснований на спритності рук.
2. Махінація, обман, шахрайство.
3. Комунікативний вплив, який призводить до актуалізації в об'єкта впливу певних мотиваційних станів (а разом з тим почуттів, уподобань, стереотипів), що спонукають його до поведінки, бажаної (вигідної) для суб'єкта впливу; при цьому не передбачається, що він обов'язково має бути не вигідним для об'єкта впливу.

Американський соціальний психолог Роберт Чалдіні виділяє безліч типових ситуацій маніпуляції: прохання про допомогу, послугу; вплив продавця і реклами на покупця; політична пропаганда; виховання дітей тощо. Він же представив список осіб, для яких маніпуляції являють собою «засоби виробництва»: збирачі коштів різних фондів; вуличні торговці; ділки, бізнесмени, торгові агенти; вербувальники; працівники реклами, піарники (від «Public relations»), іміджмейкери; вуличні жебраки та ін.

Маніпуляція – це прихований вплив на почуття, думки, твердження та установи людини, на меті якого є зміна цих думок на ті, що потрібні маніпулятору. Т. ван Дейк охарактеризував маніпуляцію так: «Це здійснення неправомірного впливу за допомогою дискурсу: маніпулятори змушують інших вірити в те, що відповідає інтересам маніпулятора і суперечить найкращим інтересам об'єкта маніпуляції» [33].

Маніпулятивний вплив є багатокомпонентним явищем. У науковій літературі йдеться про прийоми, способи, засоби впливу. Можна зазначити, що цей вплив присутній у всіх сферах людського життя, особливо у тих, які оточують нас кожен день, зокрема в рекламі. Успішною маніпуляцією можна назвати тоді, коли реципієнт сприймає її як природний та неминучий процес [29].

У зв'язку із масовим поширенням реклами інформаційних продуктів і послуг важливим постає такий її вид розповсюдження, як масова розсилка, або спам.

У цьому контексті знов актуалізуємо повне визначення спаму: це електронні текстові та / або мультимедійні повідомлення різного тематичного змісту, зазвичай рекламного характеру, які без попередньої згоди / замовлення потенційного споживача умисно масово надсилаються на його адресу електронної пошти / кінцеве обладнання абонента (крім повідомлень оператора чи провайдера щодо надання спеціальних послуг).

Загалом, підвищення ролі реклами у суспільстві пов'язане з тим, що, надаючи детальну інформацію про товар, вона створює попит на нього і врешті-решт спонукає придбати або вибрати ту чи ту послугу, тому вплив на масову

свідомість є невід'ємною частиною під час створення реклами. На думку дослідників, на структуру тексту реклами впливають аудиторія, характер товару, носій реклами (ТБ, журнал, газета, радіо, інтернет тощо). Окрім того, реклама має бути емоційною і надавати правдиву інформацію про товари чи послуги, їхні «принади» мають бути доказовими, доступно виголошеними. Усі сучасні реклами найчастіше мають таку структуру, що й розкриває сутність того чи того товару або послуги: слоган – заголовок – основний текст – ехо-фраза (резюме).

Більшість науковців суголосні в тому, що в рекламі значну роль відіграють психологічні чинники, і виділяють п'ять своєрідних «центрів тяжіння», а саме: «формат повідомлення, внутрішній світ споживача, органи чуття людини, логіка побудови рекламного повідомлення і форми подання статистичних даних» [15]. У свідомості людини виникає думка, що її щастя, успіх, підвищення статусу залежать саме від придбаної речі. Тобто, відбувається елементарне маніпулювання свідомістю людини. Зазначимо також, що маніпулятивні прийоми можуть бути як позитивними, так і негативними. Розглянемо деякі методики маніпуляції, що активно застосовувані у рекламних спам-текстах.

Однією з існуючих технік маніпулятивного впливу є застосування в рекламних повідомленнях масових розсилок так званого нейролінгвістичного програмування (НЛП).

Нейролінгвістичне (з грец. *neuron* – «нерв» і лат. *lingua* – «мова») програмування (з нім. *programieren* – «складати програми») (НЛП) – система опису структури суб'єктивного досвіду, що пояснює специфіку кодування набутої інформації; модель спілкування, яка ґрунтується на виявленні та використанні стандартів мислення; комплекс технік і операційних принципів, на основі яких моделюються ефективні стратегії мислення й поведінки.

Засновниками НЛП вважають Р. Бендлера та його учня Д. Грюндера, що вперше представили метод у 70-х роках ХХ століття. Нейролінгвістичне програмування як напрямок у психології покликане допомагати людині вносити в голову свого співрозмовника певні думки, які дозволяють змінити мислення й поведінку та досягти поставлених цілей, які не завжди є позитивними.

Прийоми НЛП застосовують у відносинах між людьми дуже широко, часто не усвідомлено. Найголовніше в НЛП – це робота з чужою свідомістю, яка здійснюється за допомогою використання спеціальних технік та прийомів: як вербальних, так і невербальних. За допомогою цього найрізноманітніші установки, які будуть вигідні одній людині, можуть бути закладені в мозок іншої.

Застосовують НЛП в різноманітних сферах, зокрема в рекламній. Так, одним з базових в НЛП є поняття репрезентативних систем особистості: візуальної, аудіальної, кінестетичної. Це пов'язано зі способами отримання, обробки та зберігання інформації у пам'яті людини. При розробці ефективного рекламного повідомлення необхідно використовувати всі три системи для формування у свідомості реципієнта найбільш повного і насиченого образу, а також з метою створення його універсальності в плані репрезентативних систем, оскільки найбільш швидке розуміння й сприйняття інформації людиною досягаються в тому випадку, якщо вона подається в характерній для неї репрезентативній системі.

На думку вчених Б. Поршнева, А. Брудного, у процесі реклами ефект від навіювання думок про перевагу певних продуктів чи послуг допоможе створити відповідний фон, який дослідник А. Брудний називає фасцінацією (від англ. *fascination* – «зачарування»). Прикладом фасцінації можуть слугувати музика чи колір, які роблять рекламу більш привабливою. Фактично відбувається змішання інформаційних каналів з метою продемонструвати усі характеристики товару: колір, звук, смак, аромат тощо. Більшість популярних нині кліпів пропонує безліч «райської насолоди», «спокуси смаком», містить сексуально забарвлені образи. Отже, клієнтам за допомогою вербальних та невербальних елементів намагаються вселити думку про те, що ці речі чи продукти викликають лише задоволення. Тобто, відбувається маніпулювання чуттєвим досвідом людини. Зазначимо, що в деяких випадках творці реклами використовують найрізноманітніші емоції, наприклад: радість, жалість, страх, заздрість тощо. Ці почуття мають на меті настільки заповнити людину, щоб вона не мала змоги

адекватно реагувати на ситуацію. Наприклад: «Ви ж не хочете захворіти? Тоді купіть наші вітаміни!».

Отже, психологічна маніпуляція в рекламі – це вплив на клієнта за допомогою прихованих технік, які змінюють її поведінку і спонукають до вигідної для маніпулятора дії. Однак важливо зрозуміти, що межа між маніпуляціями та техніками продажів дуже розмита. Звичайну знижку в магазині можна теж вважати маніпуляцією, адже вона часом стимулює людину до прийняття не вигідних для себе рішень.

У сучасних лінгвістичних дослідженнях рекламного дискурсу ми часто зустрічаємо твердження, що будь-який вплив реклами на масову свідомість автоматично вважають маніпуляцією. Стрімке поширення реклами у сучасному світі й зумовило актуальність нашого дослідження. Вплив на реципієнта у рекламі досліджували Є. Доценко, В. Зірка, С. Кара-Мурза та ін.

Є. Доценко, проаналізувавши значну кількість дефініцій терміну «маніпуляція» у вітчизняних та зарубіжних працях (Б. Бессонов, Д. Волкогонов, Р. Гудін, О. Йокояма, Л. Прото, У. Рікер, Дж. Рудінов, В. Сагатовський, Г. Шіллер, П. Робінсон та ін.), пропонує своє власне визначення: «Маніпуляція – це вид психологічного впливу, вправне здійснення якого призводить до прихованого спонукання в іншої людини намірів, котрі не співпадають з її актуальними бажаннями», наголошуючи на «прихованості» маніпуляції: «Маніпуляція – це психологічний вплив, спрямований на зміну напрямку активності іншої людини, здійснений настільки вміло, що залишається поза її увагою». Варто також наголосити на важливості фактору самостійності у прийнятті адресатом певного рішення, адже маніпуляція не передбачає тиску з боку адресанта чи примушення адресата до певної дії, отож результатом маніпулятивного впливу буде здійснення адресатом певного вчинку з власної волі та ініціативи [19, с. 303].

Маніпулятивний вплив у сучасному рекламному дискурсі можна розділити на три групи – лінгвістичний, квазілінгвістичний та нелінгвістичний.

До першої групи можна віднести суто мовні, тобто вербальні засоби впливу. Професор Г. Подшивайлова зазначає, що сюди входять стилістичні прийоми та засоби мовної виразності, і за їх допомогою досягається потрібний ефект – радість, страх, нагнітання тощо. До другої групи входять шрифти, також їх розмір та колір, розташування у друкованих виданнях. Вони сприймаються читачем через зоровий канал та імпліцитно впливають на нього, маніпулюючи на підсвідомому рівні, змушуючи його зробити певний висновок на користь творця реклами. До третьої групи входять усі невербальні елементи реклами, тобто – схеми, таблиці, фотоматеріали, зображення тощо. Раніше цій групі не приділялося багато уваги, адже вона вважалася несуттєвою в рекламному дискурсі. Однак вже давно відомо, що всі її елементи відіграють важливу роль у сприйнятті повідомлення аудиторією.

Сучасний інтернет-дискурс являє собою процес створення тексту в сукупності з його прагматичними, соціокультурними, психологічними факторами, цілеспрямовану соціальну дію, що включає взаємодію людей і механізмів їх свідомості – когнітивних процесів.

Обов'язковими елементами сучасного інтернет-дискурсу є вплив на читача та орієнтація на його вимоги. Щоб інформація дійшла до великої кількості населення, нерідко використовують спам як спосіб її передавання й поширення.

На думку англійського лінгвіста К. Фейнштайна, «спам – це електронне повідомлення, яке розсилають за вказівкою організації (або конкретної особи), яка не має жодного відношення та інтересу до отримувача» [28, с. 21]. На його думку, будь-який лист, що містить рекламу та не узгоджений з отримувачем, є спамом, а люди, які його поширюють, – поширювачі спаму, або ж спамери (англ. spammers). Також К. Фейнштайн додає, що спамом може бути розісланий не лише за допомогою пошти, а й за допомогою соціальних мереж чи месенджерів текст.

З самої назви вищерозглянутої концепції – нейролінгвістичне програмування – випливає, що в ній є три складові: одна складова стосується психофізіологічних аспектів володіння мовою, друга – пов'язана з лінгвістичною

сторonoю мовленнєвої діяльності, а третя – спрямована на дослідження впливу на людину в процесі мовного спілкування та на регулювання її поведінки [12, с. 243]. Отже, нейролінгвістичне програмування (Neurolinguistic Programming, НЛП) – це управління людською свідомістю за допомогою лінгвістичних конструкцій, архетипів, візуальних зображень тощо.

Існують такі види НЛП-технік:

1. Приєднання. Мабуть, найвідоміша і часто застосовувана техніка, про яку знають навіть ті, хто не вивчав основні напрямки нейролінгвістичного програмування. Вона служить для встановлення контакту з людиною, яка, побачивши незнайомця, інтуїтивно захищається від нього. Сенс простий: необхідно просто копіювати свого співрозмовника в чому-небудь. Це можуть бути пози, жести, міміка і навіть хода й темп дихання, голосу.

2. Рапорт. Це слово можна пояснити як «побудова довірливих відносин». Як створити простір, у якому твій новий співрозмовник довіриться тобі? Просто розкажіть, наскільки ви схожі і перебуваєте в одному човні. Відмінно це проілюструє фраза «Ми з тобою однієї крові» – людина не просто зменшить бар'єр між вами, але й почне несвідомо демонструвати свою довіру.

3. Три «так». Наступне, що може допомогти вам змусити людину сказати те, що потрібно, – це розгін ваших думок і мовлення в тому напрямку, де співрозмовник на кожне ваше питання зможе відповісти тільки «Так» – їх повинно бути три. Він впаде в якусь подобу трансу, у якому подіє той самий закон інерції – четвертою і п'ятою (й так далі) відповіддю також стане позитивна, стверджувальна.

4. Розрив шаблону. Що з себе являє розрив шаблону? Ви повинні сказати або зробити щось таке, що не впишеться в очікування співрозмовника. Говорючи простою мовою, слід вибрати модель поведінки, якою ви хочете переконати співрозмовника, і зробити абсолютно протилежну річ.

5. Переключення уваги. Суть техніки в тому, щоб швидко переключити увагу співрозмовника на іншу тему або річ, яка захопить його увагу, – адже мозок і зір людини здатні фокусуватися тільки на чомусь одному. З областю, яка

залишається поза увагою, можна робити все, що завгодно, – ось чому цей спосіб маніпулювання – один із найулюбленіших у ілюзійоністів і шахраїв.

6. Ведення. Ведення проводять вже тільки після того, як довіру людини отримано і, грубо кажучи, з нею можна робити все, що завгодно: говорити, що робити, куди йти тощо.

До основних нелінгвістичних маніпуляційних технологій відносять такі:

- експлуатація аудіопатернів: створення шляхом підлаштування до дихання, модуляції, інтонаційної гри додаткового образу, який ніби увиразнює, відтіняє, а за потреби спростовує та перекреслює той образ, що формується вербально;
- використання візуальних архетипів: спекулюючи тим, що підсвідомість людини містить певний архетип (символи, які всі сприймають емоційно однаково, позитивно або негативно), маніпулятор для просування політики, формування позитивного іміджу чи боротьби з останнім ставить його у відеоряд поруч з відповідними меті архетипами;
- маркування тексту – виділення в основному тексті (жирним шрифтом, іншим кеглем тощо) кількох слів або літер, які, якщо читати лише їх, мають свій окремий смисл;
- застосування субмодальностей – використання особливостей і характеристик зображення або звуку для створення необхідного позитивного чи негативного емоційного фону, формування певних схильностей до активності (пасивності) на підсвідомому рівні, які б уможливили контроль емоцій об'єктів маніпулятивного впливу різних субмодальностей;
- використання каталепсії (завмирання людини в певній позі; дія, пов'язана з розладом рухового апарату);
- вікова регресія – навмисне показування картин чи образів минулого, під час якого людину, групу або маси охоплює легкий транс ностальгії;

- руйнація (підміна) шаблонів – досягнення необхідних змін у світобаченні й діях людини, групи чи мас шляхом зміни (підміни) звичних, відпрацьованих алгоритмів (шаблонів, стереотипів) та нав'язування інших моделей поведінки;
- оцінювання поведінки як результату позитивного наміру: проведення чіткої межі, визнання різниці між намірами, які, на думку класика НЛП В. Сатір, є завжди позитивними, і реальною поведінкою, яка може не відповідати нормам моралі;
- гра на асоціації або дисоціації – спроба викликати в об'єкта впливу залежно від потреби (мети) асоціативний спогад, який зумовлює такі гострі переживання минулого досвіду, ніби все це відбувається зараз, або дисоційований спогад, у процесі якого людина виконує роль глядача, що просто проглядає відеозапис подій за участю іншої людини (асоційована позиція викликає сильні почуття, які створюють мотивацію для зміни поведінки, а дисоційована дає змогу отримати більше інформації й легше вивести об'єкт впливу з деморалізованого стану, мобілізувати всі його творчі ресурси для розв'язання проблеми);
- підлаштовування (вербальне та невербальне) до людини, групи, мас з метою здійснення психологічного маніпулятивного впливу шляхом входження в довіру, проникнення у підсвідомість – ведення.

Лінгвістичні технології використовують такі методи:

- зміна фокусу уваги в часовому просторі – блокування думок про минуле, орієнтація людини, групи, мас на позитивний результат на сучасному етапі і в майбутньому;
- імперативна персеверація – неодноразове повторення твердим гіпнотичним голосом певного твердження;
- прийом «зв'язки» – штучне умонтування необхідної інформації, потрібного відеоряду в позитивний чи негативний контекст залежно від мети, яку ставить перед собою маніпулятор;

- прийом «розкручування» – навмисна зміна – рівня або масштабу розгляду проблеми чи суперечності: може бути «розкручування вгору», яке дає змогу різко, до вищих цінностей, підсилити мотивацію на зміну; «розкручування вниз» – сприяє визначенню конкретних перешкод та способів виконання задуманого; «розкручування вбік» – уможливорює використання аналогії, чужого досвіду для розв’язання проблеми;
- рефреймінг (зміна) контексту – стимулювання здатності людини, групи, мас поглянути на поведінку чи подію під іншим кутом;
- прийом рефреймінгу змісту – зміна значення змісту поведінки, події без зміни контексту.

Окрім названих прийомів, при застосуванні лінгвістичних технологій використовують також прийоми рівності, псевдовибору, припущення (імплікації), «закладання міни», умотивованих пресупозицій (тверджень), створення «психічних вірусів», зміщення фокусу уваги, трюїзмів, конкретного образу, слів-команд, метафор і притч тощо.

2.2. Приклади реалізації маніпуляційних технологій у спам-текстах

Розглянемо кілька конкретних прикладів маніпуляції у текстах масової розсилки.

Одним із найбільш поширених прийомів у рекламі є прийом, який має назву «брак часу». Основна його мета – створення у покупця своєрідного психозу, у якому він біжить купувати рекламовану продукцію. Наприклад: *«Неймовірні знижки!», «Мегазнижки! Встигніть купити!», «Величезні знижки!»*. Досить часто тут використовують слова *«Тільки для Вас», «Саме зараз!»*, що створюють ситуацію нагнітання: *«Тільки сьогодні і тільки зараз! У нас знижки! Зимові знижки на взуття до -70%!»*.



Рис. 2.1. Приклад прийому «брак часу»

У зв'язку з цим використовують ще й прийом контрасту: «Найкраще шукай тут!». Хоча це один з видів інформаційно порожніх протиставлень, оскільки покупець у дійсності не знає, з чим порівнюється той чи той товар.



Рис. 2.2. Приклад прийому контрасту

Наступний прийом має назву «апеляція до прогресу». У його основі – уміння переконати клієнта, що цей конкретний продукт є абсолютно новим,

модним. Популярними у цьому випадку є словосполучення «новий сучасний дизайн», «оновлений смак», «новий запашний аромат» тощо.



Рис. 2.3. Приклад прийому «апеляція до прогресу»

Іноді в рекламі товару використовують звернення до добрих почуттів особистості, тобто відбувається своєрідна інтимізація комунікативного простору. Це такі теми, як зустріч з батьками, піклування про них, намагання допомогти матусі, спілкування з найближчими друзями тощо. Наприклад, уже впродовж тривалого часу реклама ювелірного заводу «Золотий вік» пропагує щире кохання між двома закоханими. Така реклама викликає позитивні емоції і, безумовно, викличе й бажання придбати товар для своєї другої половинки.



Рис. 2.4. Приклад прийому інтимізації

Автори реклами можуть вдаватися й до певного шантажу, звертаючись до інстинкту самозбереження: «Купіть наші вітаміни, щоб зберегти здоров'я своїх рідних», «Тільки наш диван виготовлений із 100%-во натуральних матеріалів», «Лише наші фрукти вирощені з любов'ю» тощо.



Рис. 2.5. Приклад прийому звернення до інстинкту самозбереження

Деякі види телереклам вдаються до свідомого використання ілюзії переконливості, посиляючись на численні «професійні думки стоматологів, гінекологів, педіатрів» або інших фахівців, які нібито мають достатньо даних, що підтверджують перевагу рекламованого товару над усіма іншими (наприклад, пігулки, які обіцяють швидке схуднення).

Нерідко для реклами запрошують відомих акторів, спортсменів, співаків. Цей прийом має назву «авторитет»: відомий ірландський боєць Конор Макгрегор заохочує користуватись Pari Match, Ігор Кондратюк вміло закликає купувати товари на Prom.ua тощо.



Рис. 2.6. Приклад прийому «авторитет»

У людей виробляється стереотипність мислення, що криється у такій фразі: «Якщо відомі та успішні люди пропонують цей товар, то я теж повинен це купити». У результаті це приведе до зростання продажу рекламованої продукції.

Значна роль у правильній побудові реклами належить таким засобам лінгвістичної маніпуляції:

1. У рекламних текстах надають перевагу означено-особовим реченням, присудок у яких виражений дієсловом наказового способу: «*Живи щасливо!*», «*Пий корисне!*», «*Отримуй радість від кожного дня!*», «*Купуй вигідніше!*» тощо. Уважається, що дієслова наказового способу недоконаного виду передають рішучість, різкість, а доконаного виду – виражають волевиявлення [7, с. 131]. У деяких випадках слова лунають пом'якшено: «*Зустрінь свято з Coca-Cola!*», «*Подаруй собі релакс!*» тощо. Оскільки дієслова наказового способу мають відтінок побажання, доброзичливої поради, то така реклама подобається споживачам і привертає їхню увагу. Такі структури сприяють досягненню головної мети реклами – швидко вплинути на того, хто її сприймає. До того ж вони короткі, тому легко запам'ятовуються.

2. Засобом спонування у рекламі, особливо на телебаченні, слугують квантитативно-генітивні речення. В українському телебаченні в мові реклами вони лунають здебільшого напередодні свят як привітання від тих чи тих виборчих блоків, партій: *«Щасливої Пасхи Вам та Вашим родинам!»*, *«Море сміху! Ласощів усяких!»* тощо.
3. Використовуються і лексеми з різноманітними суфіксами, що передають суб'єктивну оцінку: *«Називін! Для носів та носиків!»*.
4. Рекламі сприяє й гіперболізація тексту: реклама вафель *«Siesta»* *«Найхрумкіший смак!»*; реклама бритви *«Найкраще для чоловіків – «Gillette»!* тощо; використання ступенів порівняння: *«Добре, а з ЛЮКС ще краще!»* (реклама чіпсів «Люкс») та ін.
5. Часто вживаються евфемізми, особливо у політичній рекламі, що допомагають уникнути конфлікту в спілкуванні та під час виступів, приховати негативні факти. Наприклад, в американських ЗМІ безробітних називають *непрацевлаштованими*, бідних – *недостатньо привілейованими* тощо. Військовий конфлікт між Україною і Росією тривалий час називали *АТО*, а не війною.

Отже, у Розділі 2 описано технічні та лінгвістичні особливості текстів масової розсилки. Доведено, що основним засобом створення спам-текстів є маніпуляційність використовуваних у процесі цього технологій.

РОЗДІЛ 3. ПРОГРАМА ДЛЯ ТЕХНІЧНОГО АНАЛІЗУ СТВОРЮВАНИХ ТЕКСТІВ МАСОВОЇ РОЗСИЛКИ: АЛГОРИТМ ВИКОРИСТАННЯ

3.1. Функціонал програми Find Spam

Поштовим сервісам (Gmail, Mail.ru, Outlook тощо) важливо, щоб їхні користувачі не отримували регулярно створюваний шкідливий спам. З цією метою вони створили спам-фільтри – спеціальні алгоритми, які аналізують отримувані листи та вирішують, спам це чи ні. Спам-фільтри щодня перевіряють мільйони листів і чудово знають, які слова та фрази найчастіше використовують спамери. Коли спам-фільтр бачить ці слова в розсилці (такі слова ще називають стоп-словами), автоматично додає листа до категорії «Спам». На нашу думку, корисним і важливим є створення спеціального програмного забезпечення, яке б давало змогу кожному користувачеві самостійно перевіряти, чи є той чи той отриманий (чи створений ним самим) текст спамом. Основне функційне призначення розробленої нами програми Find Spam – здійснювати автоматизований лінгвістичний аналіз з метою перевірки, чи є той чи той створений контент спам-текстом.

Для якісної роботи нашої програми було опрацьовано 97 спам-листів з метою виокремлення ключових слів, що використовують спамери для розсилки користувачам. Загалом було виділено 116 слів.

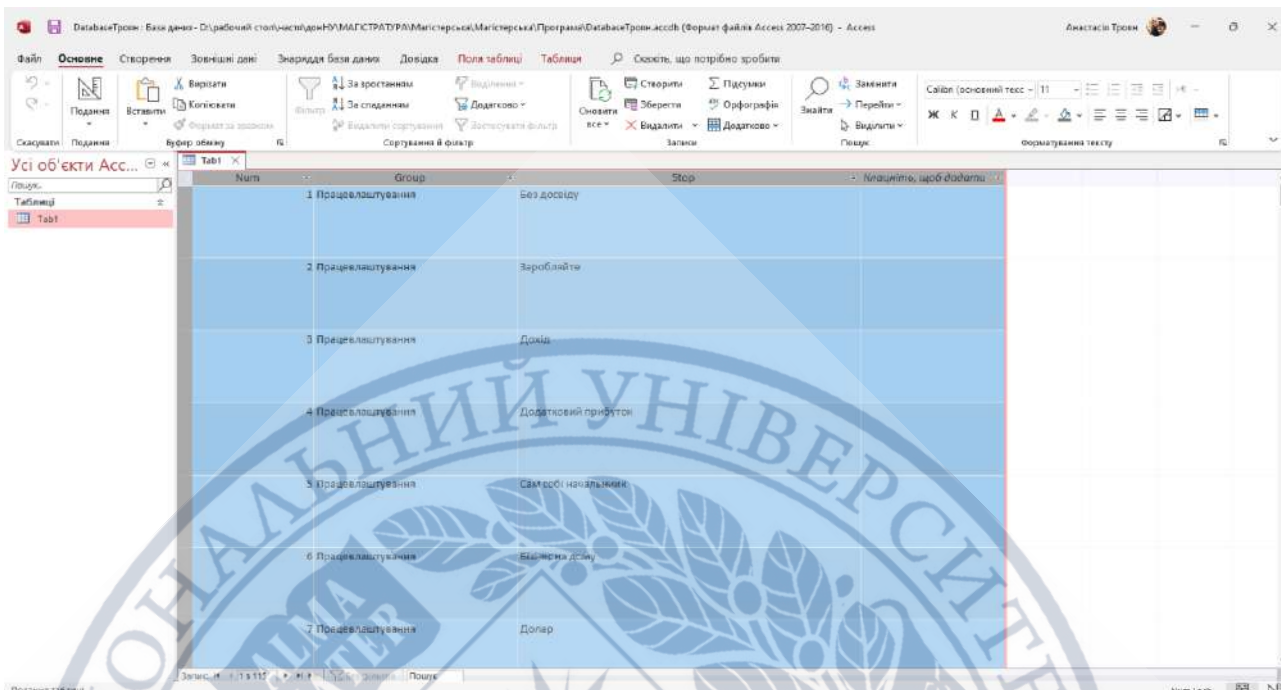


Рис. 3.1. Приклад оформлення таблиці спам-ключовиків в Access

Кожне з яких було віднесено до однієї з 7 тематичних груп: «Працевлаштування» (11 слів), «Фінанси» (32), «Загальне» (5), «Маркетинг» (9), «Здоров'я» (9), «Контент для дорослих» (4), «Пропозиції» (15), «Призи» (7), «Безкоштовні пропозиції» (5), «Заклик до дії» (18).

Створена нами програма може обробляти два види даних: посилання на контент та файл, який містить необхідний для перевірки текст. Програма виконує чотири функції: `def database()`, `def open_file(file_name)`, `def open_url(url)`, `def find_spam()`, та використовує три допоміжні бібліотеки: `requests`, `pyyodbc`, `os`:

- 1) `def database()` – призначена для отримання доступу до бази даних, що містить список спам-слів, за допомогою допоміжної бібліотеки `pyyodbc` (на виході повертає список спам-слів у форматі `list`);
- 2) `def open_file(file_name)` – призначена для отримання доступу до текстового файлу, у якому міститься текст для перевірки (приймає на вхід повний шлях до місця знаходження файлу у форматі `string`, повертає на виході вміст файлу у форматі `string`);

- 3) `def open_url(url)` – призначена для отримання доступу до контенту, що міститься за посиланням, за допомогою допоміжної бібліотеки `requests` (приймає на вхід посилання у форматі `string`, повертає на виході вміст посилання у форматі `string`);
- 4) `def find_spam()` – головна функція програми, працює циклічно до тих пір, поки користувач не введе ключ виходу з програми; отримує список спам-слів за допомогою функції `database()`; якщо сталася помилка та програма не змогла отримати доступ до бази, вона виведе на консоль помилку та завершить роботу; далі відбувається запит у користувача, який вид даних потрібно обробити: якщо користувач ввів «1», програма запросить у нього посилання на контент, якщо «2» – програма запросить повний шлях до файлу, який потрібно перевірити; якщо «0» – програма завершить роботу; якщо на будь-якому етапі вводу користувач введе некоректні дані, програма виведе помилку на консоль та зробить запит ще раз; в залежності від того, який ключ введе користувач, 1 чи 2, програма отримає контент за допомогою функцій `open_url(url)` або `open_file(file_name)`; далі програма формує статистику контенту: шукає у контенті співпадіння кожного слова зі списком спам-слів (якщо співпадіння є, вона запам'ятовує результат); на вихід програма повертає список всіх спам-слів та кількість співпадінь з проаналізованим контентом для кожного слова.

Допоміжна бібліотека `os` використовується для затримання вікна консолі після завершення роботи програми.

3.2. Приклад використання програми Find Spam

Запустити файл «`find_spam.exe`». Якщо програма не змогла підключитися до бази, вона виведе у вікно консолі помилку «Failed to open the database. Check the database and run the program again.».

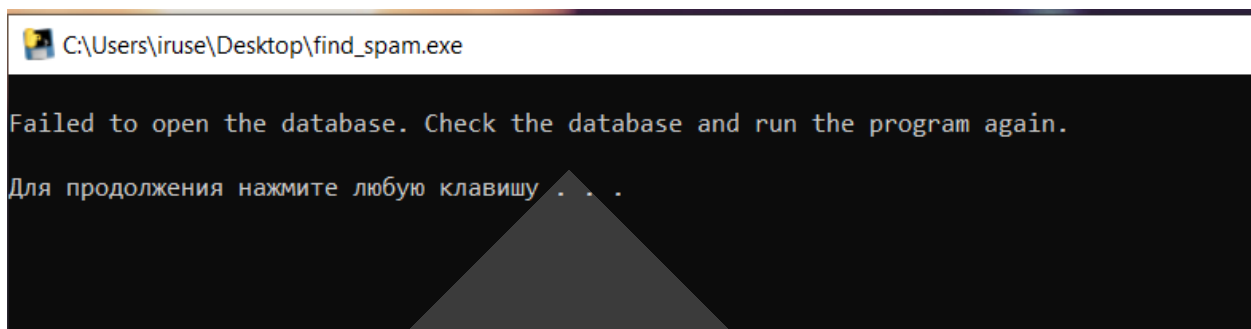


Рис. 3.2. Помилка відкриття програми

Якщо програма змогла отримати доступ до бази, вона виведе у вікно консолі запит до користувача:

«Press 1, if you want to check url.

Press 2, if you want to check file.

Press 0, if you want to exit.»

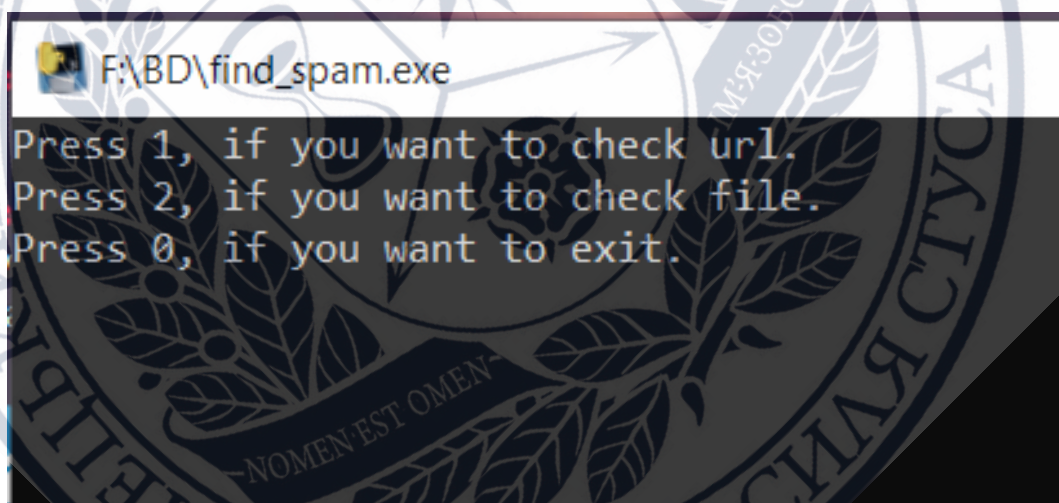


Рис. 3.3. Запит програми до користувача при її відкритті щодо типу наступної перевірки

Якщо ви введете некоректні дані, програма виведе у вікно консолі помилку «You pressed wrong key. Please, try again.» та запит на наступну перевірку:

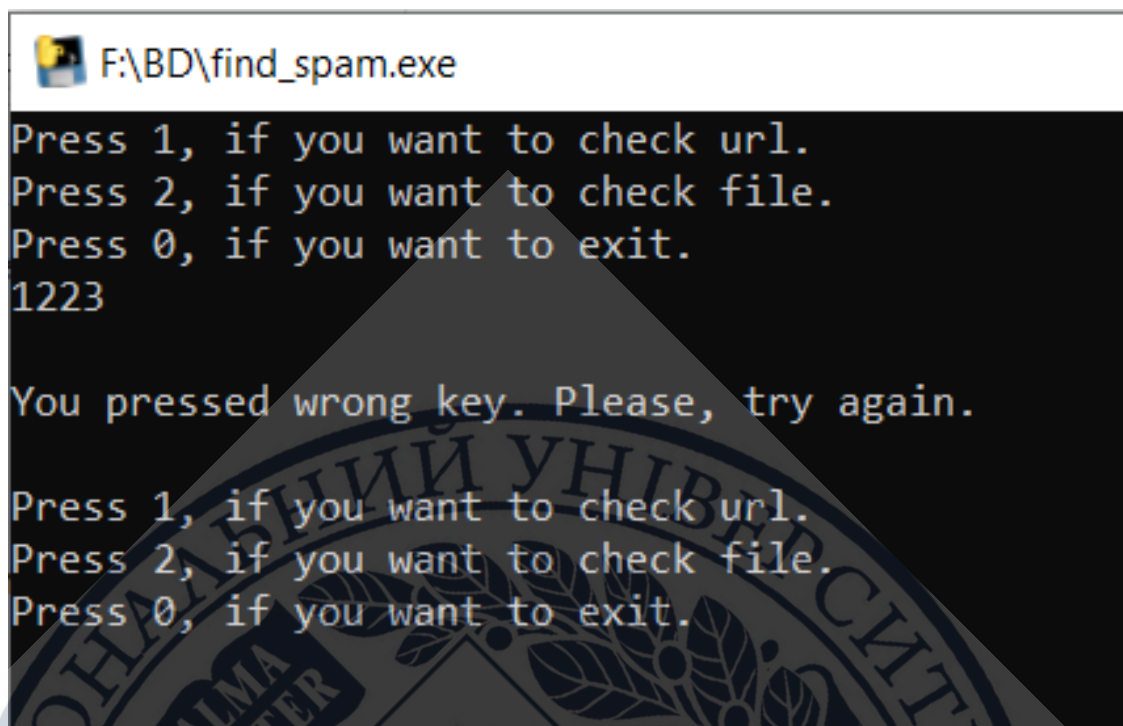


Рис. 3.4. Запит на наступну перевірку (якщо були введені некоректні дані)

Якщо ви ввели «1», програма виведе запит на введення посилання на контент «Please, enter the [url:](#)»

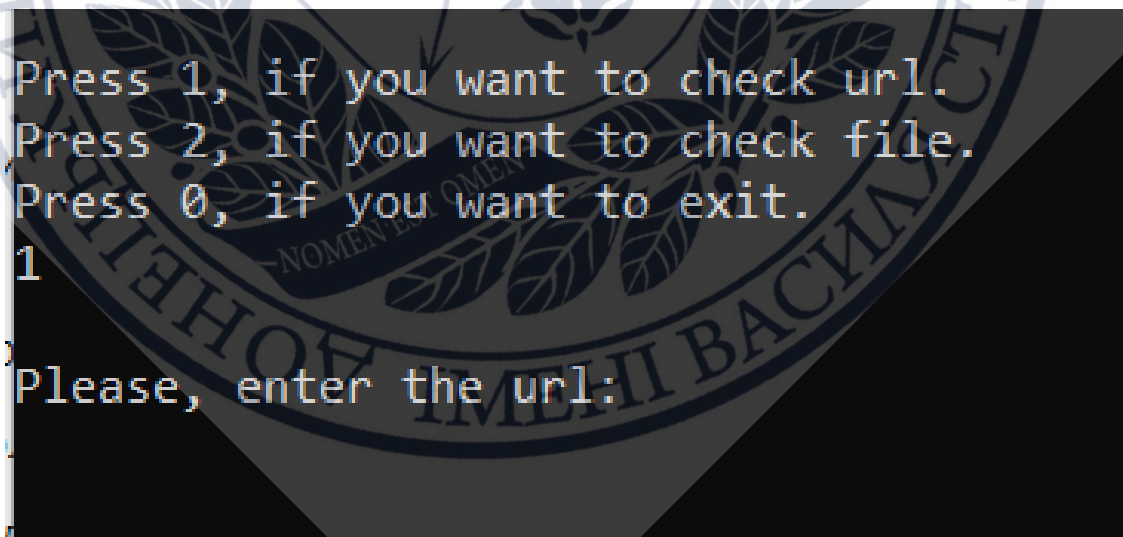


Рис. 3.5. Запит програми на введення посилання на контент

Якщо ви введете некоректне посилання, програма виведе у вікно консолі помилку «Page is not available. Try again» та запит на наступну перевірку:

```
Press 1, if you want to check url.  
Press 2, if you want to check file.  
Press 0, if you want to exit.  
1
```

```
Please, enter the url: zsdvdcfv
```

```
Page is not available. Try again
```

```
Press 1, if you want to check url.  
Press 2, if you want to check file.  
Press 0, if you want to exit.
```

*Рис. 3.6. Запит на наступну перевірку
(якщо було введено некоректне посилання)*

Якщо ввести коректне посилання та програма змогла отримати до нього доступ, вона виведе у вікно консолі результат: усі спам-слова та кількість співпадінь з контентом, що міститься за посиланням, яке ви ввели у програму. Після цього вона виведе запит на наступну перевірку:


```

F:\BD\find_spam.exe
Press 1, if you want to check url.
Press 2, if you want to check file.
Press 0, if you want to exit.
1
Please, enter the url: https://www.donnu.edu.ua/uk/#
унікальна пропозиція : 0
пропозиція обмежена : 0
ексклюзивна : 0
спеціальна : 0
гарантовані : 0
без ризику : 0
вигода : 0
гарантія : 0
без зобов'язань : 0
без вкладень : 0
умови : 1
термін : 0
перемога : 0
переможець : 0
виграші : 0
розіграші : 0
конкурси : 0
безкоштовний : 0
доступ : 1
встановлення : 0
сайти : 3
консультації : 0
позбудьтеся : 0
подзвони : 0
відкрийте : 1
натисні тут : 0
швидше : 0
порівняй : 0
збережи : 0
роздрукуй : 0
підпишись : 0
дійте зараз : 0
тільки сьогодні : 0
отримайте зараз : 0
почніть зараз : 0
прочитай : 0
не зволікайте : 0
прямо зараз : 0
чи не видаляйте : 0
приєднуйтеся : 0
без досвіду : 0
заробляйте : 0
дохід : 0

F:\BD\find_spam.exe
вклади : 0
банкрутство : 0
кредитор : 0
колектор : 0
дебет : 0
кредит : 3
виплати : 0
процентні ставки : 0
борги : 0
мінімальний платіж : 0
рефінансування : 0
100% : 44
мільйони : 0
тисячі : 0
приховані : 0
успіхи : 0
новинка : 0
реклама : 0
збільшення трафіку : 0
продаж : 0
знижки : 0
ринки : 0
не спам : 0
придбати : 0
розпродаж : 0
діагностика : 0
віагра : 0
хоропіння : 0
ліки : 0
харчова добавка : 0
лікування : 0
знижити вагу : 0
схуднення : 0
здоров'я : 0
18+ : 0
21+ : 0
xxx : 0
секс : 0
терміново : 0
збільшити : 0
продажі : 0
комерційна пропозиція : 0
кращу пропозицію : 0
Press 1, if you want to check url.
Press 2, if you want to check file.
Press 0, if you want to exit.

```

Рис. 3.7. Результат:

усі спам-слова та кількість співпадінь з контентом за посиланням

Якщо ви введете «2», програма виведе у вікно консолі запит на введення повного шляху до файлу, який потрібно перевірити «Please, enter path to file:»:

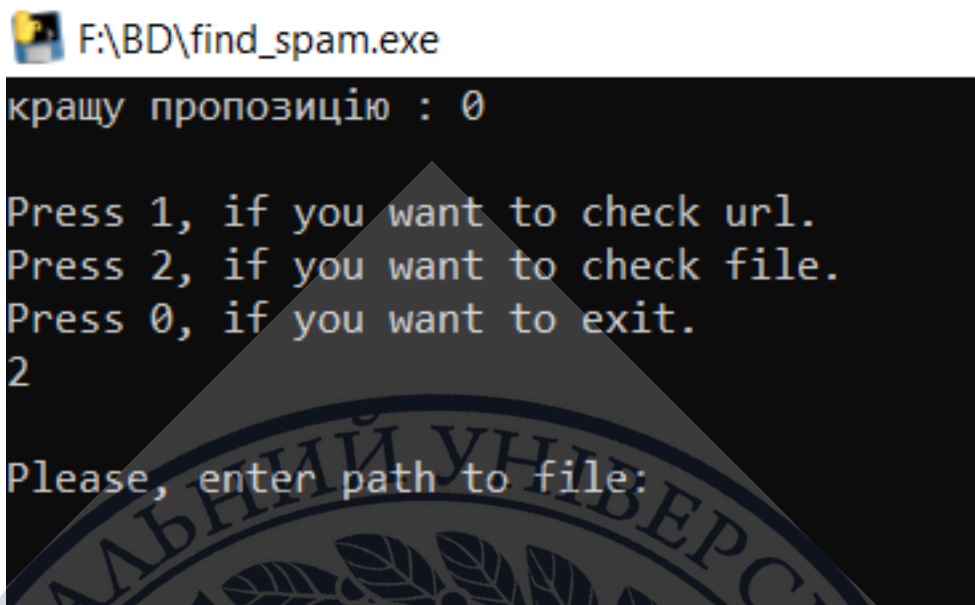
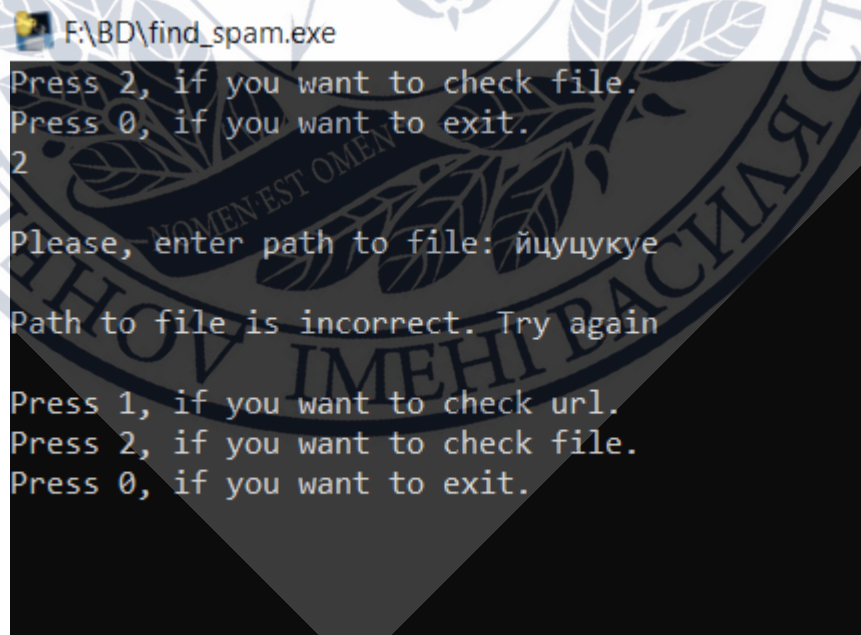


Рис. 3.8. Запит програми на введення повного шляху до файлу, який потрібно перевірити

Якщо ви введете некоректний шлях до файлу або програма не зможе знайти такий файл, вона виведе у вікно консолі помилку «Path to file is incorrect. Try again» та запит на наступну перевірку:



*Рис. 3.9. Запит на наступну перевірку
(якщо був введений некоректний шлях до файлу)*

Якщо ви введете коректний шлях до файлу, програма виведе у вікно консолі результат: усі спам-слова та кількість співпадінь з контентом, що міститься у цьому файлі. Після цього вона виведе запит на наступну перевірку:

```

F:\BD\find_spam.exe
кредитні картки : 0
без капіталовкладень : 0
акція : 0
вклади : 0
банкрутство : 0
кредитор : 0
колектор : 0
дебет : 0
кредит : 0
виплати : 0
процентні ставки : 0
борги : 0
мінімальний платіж : 0
рефінансування : 0
100% : 0
мільйони : 0
тисячі : 0
приховані : 0
успіхи : 0
новинка : 0
реклама : 0
збільшення трафіку : 0
продаж : 0
знижки : 0
ринки : 0
не спам : 0
придбати : 0
розпродаж : 0
діагностика : 0
віагра : 0
хропіння : 0
ліки : 0
харчова добавка : 0
лікування : 0
знижити вагу : 0
схуднення : 0
здоров'я : 0
18+ : 0
21+ : 0
xxx : 0
секс : 0
терміново : 0
збільшити : 0
продажі : 0
комерційна пропозиція : 0
кращу пропозицію : 0
Press 1, if you want to check url.
Press 2, if you want to check file.
Press 0, if you want to exit.

F:\BD\find_spam.exe
Press 1, if you want to check url.
Press 2, if you want to check file.
Press 0, if you want to exit.
2
Please, enter path to file: F:\BD\Текст 1.txt
унікальна пропозиція : 0
пропозиція обмежена : 0
ексклюзивна : 0
спеціальна : 0
гарантовані : 0
без ризику : 0
вигода : 0
гарантія : 0
без зобов'язань : 0
без вкладень : 0
умови : 0
термін : 0
перемога : 0
переможець : 0
виграші : 0
розіграші : 1
конкурси : 0
безкоштовний : 0
доступ : 0
встановлення : 0
сайти : 0
консультації : 0
позбудьтеся : 0
подзвони : 0
відкрийте : 0
натисні тут : 0
швидше : 0
порівняй : 0
збережи : 0
роздрукуй : 0
підпишись : 0
дійте зараз : 0
тільки сьогодні : 0
отримайте зараз : 0
почніть зараз : 0
прочитай : 0
не зволікайте : 0
прямо зараз : 0
чи не видаляйте : 0
приєднуйтеся : 0
без досвіду : 0
заробляйте : 0
дохід : 0
додатковий прибуток : 0

```

Рис. 3.10. Результат:

усі спам-слова та кількість співпадінь з контентом, що міститься у файлі

Якщо ви завершили всі перевірки, введіть «0». Програма виведе у вікно консолі повідомлення про завершення роботи:

 F:\BD\find_spam.exe

кращу пропозицію : 0

Press 1, if you want to check url.

Press 2, if you want to check file.

Press 0, if you want to exit.

0

Для продовження натисніть будь-яку клавішу . . .

Рис. 3.11. Повідомлення про завершення роботи

Натисніть будь-яку клавішу або закрийте вікно і робота програми буде завершена.

Отже, у Розділі 3 описано функціонал та представлено приклад використання самостійно розробленої програми Find Spam – для технічного аналізу створюваних текстів масової розсилки.

ВИСНОВКИ

У процесі дослідження дійшли таких висновків:

Спам – окремий, унікальний мовленнєвий жанр сучасного інтернет-дискурсу. Останній сформований у зв'язку з інтенсивним впровадженням в життя суспільства комп'ютера та інтернету. Сфера його появи та поширення – електронна, глобальна, інтерактивна. Специфіка інтернет-дискурсу репрезентована в усіх «мовних» площинах (графічні, орфографічні, фонетичні, лексичні, граматичні, стилістичні особливості). Процесуально інтернет-дискурс являє собою створення тексту в сукупності з його прагматичними, соціокультурними, психологічними факторами, цілеспрямованими соціальними діями, що включає в себе взаємодію людей і механізмів їх свідомості – когнітивних процесів.

Спам – це електронні текстові та / або мультимедійні повідомлення різного тематичного змісту, зазвичай рекламного характеру, які без попередньої згоди / замовлення потенційного споживача умисно масово надсилаються на його адресу електронної пошти / кінцеве обладнання абонента (крім повідомлень оператора чи провайдера щодо надання спеціальних послуг). Кваліфікаційними ознаками спаму є анонімність, масовість, непрошеність. Залежно від сфери поширення виокремлюють спам на пошті, на блозі, на форумі, на дошці оголошень, у соцмережі, у SMS, у вигляді вискакуючих вікон, веб-спам, мережевий спам.

Масова розсилка спаму – це інструмент комунікації з аудиторією, суть якого полягає у відправленні одного повідомлення багатьом контактам із певною метою. Це здійснювано через сервіси розсилок. Особа, що розсилає спам, – спамер. Список адресатів складено заздалегідь і названо базою для розсилки (її параметри – актуальність, обсяг, специфіка). Типологія розсилок укладена: за способом відправлення – ручні та автоматичні; за механікою запуску – масові й тригерні; за регулярністю – регулярні та ситуативні; за контентом – промо, інформаційні, поведінкові та транзакційні; за метою – інформаційні, комерційні,

привітальні, вітальні та ін.; за каналами – Email-розсилка, SMS-розсилка, Push-розсилка, Розсилка у Viber та інших месенджерах.

З функційного погляду також виокремлюють унікальні види спаму. Спам, розісланий з метою реклами товару або послуги, позначають як «незатребувані комерційні електронні повідомлення». Листи фальсифікованого змісту, надіслані з метою отримати певну матеріальну вигоду, називають скам. Одним із видів шахрайських листів є фішингові листи, надіслані нібито від імені відомої компанії. Joe jobs – це обманне повідомлення, надіслане від імені іншої людини з метою нанесення шкоди репутації. Шкідливі спам-програми розробляються з метою нанесення шкоди комп'ютерній системі і розсилаються під виглядом нешкідливого додатку до повідомлення. Негативна квитанція – це недоставлене повідомлення, що посилається назад відправникові.

Для боротьби зі шкідливим спамом використовують такі методи: контроль масовості (DCC, Razor, Pyzor), перевірка інтернет-заголовків повідомлення, контентна фільтрація, байєс, грейлінг. Крім того, існує Spamhaus Project – міжнародна некомерційна організація, яка відстежує спам і пов'язані з ним кіберзагрози (фішинг, зловмисне програмне забезпечення та ботнети), надає оперативні й високоточні дані про загрози в режимі реального часу для основних мереж, корпорацій та постачальників безпеки, співпрацює з правоохоронними органами для виявлення і переслідування джерел спаму та шкідливого програмного забезпечення по всьому світу.

У текстах масової розсилки широко використовуване нейролінгвістичне програмування – це управління людською свідомістю за допомогою лінгвістичних конструкцій, архетипів, візуальних зображень тощо. Серед його спам-технік: приєднання, рапорт, три «так», розрив шаблону, переключення уваги, введення. Серед інших маніпуляційних спам-технологій: експлуатація аудіопатернів, використання візуальних архетипів, маркування тексту, застосування субмодальностей, використання каталепсії, вікова регресія, руйнація (підміна) шаблонів, оцінювання поведінки як результату позитивного намір, гра на асоціації або дисоціації, підлаштовування (вербальне та

невербальне). Серед власне лінгвістичних спам-технологій: зміна фокусу уваги в часовому просторі, імперативна персеверація, прийом «зв'язки», прийом «розкручування», рефреймінг (зміна) контексту, прийом рефреймінгу змісту; прийоми рівності, псевдовибору, припущення (імплікації), «закладання міни», умотивованих пресупозицій (тверджень), створення «психічних вірусів», зміщення фокусу уваги, трюїзмів, конкретного образу, слів-команд, метафор і притч тощо. У рекламних спам-текстах надають перевагу означено-особовим реченням, присудок у яких виражений дієсловом наказового способу. Засобом спонукання у спам-рекламі слугують квантитативно-генітивні речення. Використовуються лексеми з різноманітними суфіксами, що передають суб'єктивну оцінку. Наявна гіперболізація спам-тексту. Часто вживані евфемізми.

Нами розроблена спеціальна програма Find Spam, мета якої – здійснювати автоматизований лінгвістичний аналіз з метою перевірки, чи є той чи той створений контент спам-текстом. Для якісної роботи було опрацьовано 97 спам-листів з метою виокремлення ключових слів, що використовують спамери для розсилки користувачам. Загалом було виділено 116 слів, кожне з яких було віднесено до однієї з 7 тематичних груп: «Працевлаштування» (11 слів), «Фінанси» (32), «Загальне» (5), «Маркетинг» (9), «Здоров'я» (9), «Контент для дорослих» (4), «Пропозиції» (15), «Призи» (7), «Безкоштовні пропозиції» (5), «Заклик до дії» (18).

Створена програма може обробляти два види даних: посилання на контент та файл, який містить необхідний для перевірки текст. Програма виконує чотири функції: `def database()`, `def open_file(file_name)`, `def open_url(url)`, `def find_spam()`, та використовує три допоміжні бібліотеки: `requests`, `pyyodbc`, `os`: 1) `def database()` – призначена для отримання доступу до бази даних, що містить список спам-слів, за допомогою допоміжної бібліотеки `pyyodbc` (на виході повертає список спам-слів у форматі `list`); 2) `def open_file(file_name)` – призначена для отримання доступу до текстового файлу, у якому міститься текст для перевірки (приймає на вхід повний шлях до місця знаходження файлу у форматі `string`,

повертає на виході вміст файлу у форматі string); 3) `def open_url(url)` – призначена для отримання доступу до контенту, що міститься за посиланням, за допомогою допоміжної бібліотеки `requests` (приймає на вхід посилання у форматі string, повертає на виході вміст посилання у форматі string); 4) `def find_spam()` – головна функція програми, працює циклічно до тих пір, поки користувач не введе ключ виходу з програми; отримує список спам-слів за допомогою функції `database()`; якщо сталася помилка та програма не змогла отримати доступ до бази, вона виведе на консоль помилку та завершить роботу; далі відбувається запит у користувача, який вид даних потрібно обробити: якщо користувач ввів «1», програма запросить у нього посилання на контент, якщо «2» – програма запросить повний шлях до файлу, який потрібно перевірити; якщо «0» – програма завершить роботу; якщо на будь-якому етапі вводу користувач введе некоректні дані, програма виведе помилку на консоль та зробить запит ще раз; в залежності від того, який ключ введе користувач, 1 чи 2, програма отримає контент за допомогою функцій `open_url(url)` або `open_file(file_name)`; далі програма формує статистику контенту: шукає у контенті співпадіння кожного слова зі списком спам-слів (якщо співпадіння є, вона запам'ятовує результат); на вихід програма повертає список всіх спам-слів та кількість співпадінь з проаналізованим контентом для кожного слова.

Допоміжна бібліотека `os` використовується для затримання вікна консолі після завершення роботи програми.

СПИСОК ЛІТЕРАТУРИ

1. Аракелова А.О. *Спам. Історія виникнення. Методи боротьби. Інформатика та інформаційні технології: студ. наук. конф., 20 квітня 2015 р.: матер. конф. Одеса, ОНЕУ. С. 99-102.*
2. Арутюнова Н.Д. *Дискурс. Лингвистический энциклопедический словарь.* М., 1990. С. 136-137.
3. Бенвенист Э. *Общая лингвистика.* М., 1974. 446 с.
4. Большой психологический словарь. Сост. и общ. ред. Б.Г. Мещеряков, В.П. Зинченко. М., 2009. 811 с.
5. Воройский Ф.С. *Информатика. Новый систематизированный толковый словарь-справочник (Введение в современные информационные и телекоммуникационные технологии в терминах и фактах).* М., 2003. 760 с.
6. Гудзь Н.О. *Интернет-дискурс як новий тип комунікації: структура, мовне оформлення, жанрові формати.* Сучасні лінгвістичні студії: навч. посіб. Житомир: ЖДУ ім. І. Франка, 2015. С. 61-87.
7. Данилова А.А. *Манипулирование словом в средствах массовой информации.* М., 2011. 232 с.
8. *Дискурс як когнітивно-комунікативний феномен / за ред. І.С. Шевченко.* Х., 2005. 356 с.
9. Доценко Е.Л. *Психология манипуляции: феномены, механизмы и защита.* М., 1997. 344 с.
10. Загнітко А.П. *Основи дискурсології: науково-навчальне видання.* Донецьк: ДонНУ, 2008. 194 с.
11. Звегинцев В.А. *Предложение и его соотношение к языку и речи.* М., 1976. 307 с.
12. Іщук Т. *Нейролінгвістичне програмування як ефективний метод навчання перекладу: аспект пізнавальної функції мови. Актуальні питання гуманітарних наук.* 2014. Вип. 8. С. 242-248.

- 13.Клапків Л.М., Клапків Ю.М., Свірський В.С. Фінансові ризики в діяльності страхових компаній: теоретичні засади, сучасні реалії та прагматизм управління: монографія. Івано-Франківськ: Видавець Кушнір Г.М., 2020. 171 с.
- 14.Классификация с помощью мешка слов. Руководство. URL: <http://datareview.info/article/klassifikatsiya-tekstov-s-pomoshhyu-meshka-slov-rukovodstvo/> (дата звернення – 25.11.2021)
- 15.Ковалевська Т.Ю. Реклама як маніпулятивний дискурс. *Мова та суспільство*. К., 2004. С. 51-56.
- 16.Краснобаєва-Чорна Ж.В. Дискурсологія: теоретико-прикладний аспект. Вінниця, 2017. 110 с.
- 17.Кубрякова О.С. Частины мови з когнітивної точки зору. М., 1997. 326 с.
- 18.Лингвистический энциклопедический словарь / гл. ред. В.Н. Ярцева. М., 1990. 682 с.
- 19.Лянг О. Маніпулятивний вплив у дискурсі комерційної реклами. *Наукові записки Кіровоградського державного педагогічного університету імені Володимира Винниченка. Сер.: Філологічні науки*. 2010. Вип. 89 (5). С. 303-307.
- 20.Макаров М.Л. Основы теории дискурса. М., 2003. 280 с.
- 21.Маринин С.А. Борьба со спамом и вирусами. М.: НТ Пресс, 2007. 48 с.
- 22.Методы автоматической классификации текста. URL: <http://www.swsys.ru/index.php?page=article&id=425> (дата звернення – 25.11.2021)
- 23.Подшивайлова Г.М. Мовні засоби маніпулятивного впливу в політичному дискурсі (на матеріалі друкованих російськомовних ЗМІ України): автореф. дис. ... канд. філол. наук. К., 2009. 20 с.
- 24.Селіванова О.О. Сучасна лінгвістика: напрями та проблеми: підручник. Полтава: Довкілля-К, 2008. 712 с.
- 25.Серажим К. Дискурс як соціолінгвальне явище: методологія, архітектоніка, варіативність. К., 2002. 392 с.

26. Синтаксический анализ в NLTK. URL: <https://habr.com/ru/post/340574/> (дата звернения – 25.11.2021)
27. Спам и фишинг в 2018. URL: <https://securelist.ru/spam-and-phishing-in-2018/93453/> (дата звернения – 25.11.2021)
28. Фейнштайн К. Защита ПК от спама, вирусов, всплывающих окон и шпионских програм. М., 2005. 240 с.
29. Шиллер Г. Манипуляторы сознанием. М., 1980. 326 с.
30. An introduction to machine learning with scikit-learn. URL: <https://scikit-learn.org/stable/tutorial/basic/tutorial.html>
31. Desktop Operating System Market Share Worldwide. URL: <http://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-201902-201902-bar> (дата звернения – 25.11.2021)
32. Desktop Windows Version Market Share Worldwide. URL: <http://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide#monthly-201902-201902-bar> (дата звернения – 25.11.2021)
33. Dijk van T.A. Discourse and manipulation. *Discourse and society*. London, 2006.
34. Does your PC have a good rep? URL: <https://www.cnet.com/news/does-your-pc-have-a-good-rep-to-send-e-mail-it-better/> (дата звернения – 25.11.2021)
35. Doll J. Spam Attack. URL: <http://www.joes.com/spammed.html> (дата звернения – 25.11.2021)
36. Eliminate Spam. URL: <http://awildduck.com/?p=277> (дата звернения – 25.11.2021)
37. Evett D.: 2006, Spam Statistics 2006, <http://spam-filterreview.toptenreviews.com/spam-statistics.html>. Pp. 5-6.
38. Ferris Research: 2005, The Global Economic Impact of Spam. Report #409. Pp. 172-173.
39. Garreta R. Learning scikit-learn: Machine Learning in Python. 2013. 108 p.

- 40.Ironport: 2006, Internet Email Traffic Emergency: Spam Bounce Messages are Compromising Networks, <http://www.ironport.com/bouncereport/>. P. 3.
- 41.Lutz M. Learning Python, 5th Edition. 2013. 648 p.
- 42.NLTK Workbook. URL: <http://www.nltk.org/book/ch06.html> (дата звернення – 25.11.2021)
- 43.OECD: 2004a, Background Paper for the OECD Workshop on Spam. Pp. 40-41.
- 44.OECD: 2004b, Report of the 2nd OECD Workshop on Spam. Pp. 17-18.
- 45.Richert W. Building Machine Learning Systems with Python. 2013. 290 p.
- 46.Spamhaus Project. URL: <https://www.spamhaus.org/organization/> (дата звернення – 25.11.2021)
- 47.The Government of Hongkong, Nigerian letters, <http://www.mfo.gov.hk/police/pda/con-tricks/con7.htm>. Pp. 2-3.
- 48.The New York Times: 2003, We Hate Spam, Congress Says (Except Ours), <http://www.nytimes.com>. P. 3.

Додаток А
Апробація роботи

