МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет імені Петра Могили
Факультет комп'ютерних наук
Кафедра інтелектуальних інформаційних систем

ДОПУЩЕНО ДО ЗАХИСТУ
Завідувач кафедри інтелектуальних
інформаційних систем, д-р техн. наук, проф.
_____Ю. П. Кондратенко
«____»_____2022р.

БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

СИСТЕМА МОДЕЛЮВАННЯ ПРОЦЕСІВ СПАМ-ФІЛЬТРАЦІЇ

Спеціальність 122 «Комп'ютерні наук»

122 – БКР – 401з.210901101

Виконала студентка 4-го курсу, групи 401з
_____ В.В. Романець
«20» червня 2022 р.

Керівник: канд. техн. наук, доцент
_____М.О. Таранов
«20» червня 2022 р.

Миколаїв – 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет ім. Петра Могили
Факультет комп'ютерних наук
Кафедра інтелектуальних інформаційних систем

Рівень вищої освіти **бакалавр**
Спеціальність **122 «Комп'ютерні науки»**
(шифр і назва)
Галузь знань **12 «Інформаційні технології»**
(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри інтелектуальних інформаційних систем, д-р техн. наук, проф.

_____ Ю. П. Кондратенко

«____» _____20___р.

З А В Д А Н Н Я
на виконання кваліфікаційної роботи

Видано студенту групи 401з факультету комп'ютерних наук Романець Вікторії Валентинівні.

1. Тема кваліфікаційної роботи «Система моделювання процесів СПАМ-фільтрації».

Керівник роботи Таранов Микита Олександрович.
Затв. наказом Ректора ЧНУ ім. Петра Могили від «___» _____ 20___ р. № ____

2. Строк представлення кваліфікаційної роботи студентом «___» _____ 20__ р.

3. Вхідні (початкові) дані до роботи: методи та засоби захисту електронної пошти.

Очікуваний результат: визначення на законодавчому та технічному рівні способів боротьби з spam-листами, дослідження технічних методів фільтрації листів, розрахунок техніко-економічного обґрунтування, розробка та впровадження системи фільтрації spam-листів, працюючої на рівні протоколу POP3 та аналізуючої зміст вхідних листів користувачів, що дозволяє знизити економічні втрати від spam-листів.

4. Перелік питань, що підлягають розробці (зміст пояснювальної записки):

– математичні основи спам-фільтрації;

– алгоритми, що застосовуються для спам-фільтрації;

– порівняльний аналіз результатів застосування обраних алгоритмів спам-фільтрації.

5. Перелік графічного матеріалу: презентація.

6. Завдання до спеціальної частини: «Захист від іонізуючих випромінювань»

7. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис
Спеціальна частина з охорони праці	ст.викл. Макарова О.В.	

Керівник роботи __Таранов М.О_____

(наук. ступінь, вчене звання, прізвище та ініціали)

_____

(підпис)

Завдання прийнято до виконання ___Романець В.В._____

(прізвище та ініціали)

_____

(підпис)

Дата видачі завдання «_ __ » _____ _____ 2022 р.

КАЛЕНДАРНИЙ ПЛАН
виконання бакалаврської кваліфікаційної роботи

Тема: Система моделювання процесів СПАМ-фільтрації_____

№	Найменування роботи	Початок	Закінчення	Примітки
1	Подання заяви на затвердження теми та керівників БКР	26.10.2021	30.10.2021	Виконано
2	Отримання завдання на виконання БКР	24.11.2021	24.11.2021	Виконано
3	Складання календарного плану роботи на весь період виконання БКР	7.12.2021	10.12.2021	Виконано
4	Отримання завдання на переддипломну практику	22.05.2022	22.05.2022	Виконано
5	Проходження переддипломної практики, збір та аналіз матеріалів до БКР	23.05.2022	04.06.2022	Виконано
6	Розробка звіту з переддипломної практики	04.06.2022	06.06.2022	Виконано
7	Виконання БКР: аналіз сучасного стану задачі відслідковування очей, огляд існуючих технологій, розробка ПЗ	28.02.2022 та 06.06.2022	27.03.2022 та 19.06.2022	Виконано
8	Попередній захист БКР на засіданні комісії кафедри	30.05.2022	31.05.2022	Виконано
9	Доробка та остаточне оформлення БКР	02.06.2022	20.06.2022	Виконано
10	Подання БКР рецензенту	16.06.2022	18.06.2022	
11	Подання БКР, її електронної копії та інших документів (відгуку, рецензії) до захисту	20.06.2022	22.06.2022	Виконано
12	Захист БКР перед екзаменаційною комісією (ЕК)	27.06.2022	29.06.2022	Виконано

Розробив студент __Романець В.В._____ _____
(прізвище, ім'я, по батькові студента) (*підпис*)

Керівник роботи __ Таранов М.О._____ _____
(*посада, прізвище, ім'я, по батькові)* *(підпис)*

«_11_» _____12_____ 2021 р.

АНОТАЦІЯ

бакалаврської кваліфікаційної роботи студентки групи 401з ЧНУ ім. Петра Могили
Романець Вікторії Валентинівни
Тема: «Система моделювання процесів СПАМ-фільтрації»

Темою БКР є дослідження методів SPAM-фільтрації електронної пошти, розробка алгоритму та на його основі системи SPAM-фільтрації. Предметом дослідження в данної роботи є технічні методи фільтрації листів, спрямовані на зниження економічних та часових втрат від spam-листів. Об'єктом дослідження виступають процеси фільтрації кореспонденції типового підприємства.

Методологічною та теоретичною основою роботи є праці фахівців в області розробки й впровадження систем фільтрації spam-листів, теорії ймовірності, статистики, надійності, а також аналіз наукової літератури, підручників та посібників з досліджуваної проблеми.

Метою роботи є розгляд методів та засобів захисту електронної пошти, а також принципів створення захищеної електронної пошти в організації з розробкою системи фільтрації spam-листів для типового підприємства, що дозволить підвищити загальний рівень безпеки компанії та ефективність роботи співробітників.

Практична значимість роботи визначається тим, що її результати дозволяють визначити на технічному рівні способи боротьби зі spam-листами. Результатом даної роботи є визначення на законодавчому та технічному рівні способів боротьби з spam-листами, дослідження технічних методів фільтрації листів, розрахунок техніко-економічного обґрунтування, розробка системи фільтрації spam-листів, працюючої на рівні протоколу POP3 та аналізуючої зміст вхідних листів користувачів, що дозволяє знизити економічні втрати від spam-листів.

Область застосування для створеної системи фільтрації spam-листів безмежна, оскільки можливе застосування на будь-якому підприємстві з будь-якою кількістю персоналу та окремими користувачами.

Ключові слова: електронна пошта, SPAM-фільтрація, баєсовський фільтр.

Пояснювальна записка до дипломної роботи складається з 60 сторінок, 28 рисунків, 6 таблиць, 22 джерел інформації.

ABSTRACT

The theme of the thesis s the reasearch of methods of SPAM-filtering e-mail, the development of algorithm and system for SPAM-filtering. The subject of the study in the thesis is the technical methods of filtering letters, aimed at reducing the economic and temporal losses from spam-sheets. The object of research is the improvement of the filtration system of the correspondent of a typical enterprise.

The methodological and theoretical basis of the work is the work of specialists in the field of developing and implementing spam filtering systems, probability theory, statistics, reliability, as well as analysis of scientific literature, textbooks and manuals on the problem under study.

The purpose of the thesis is to consider the methods and means of protecting e-mail, as well as the principles of creating a secure e-mail in the organization, with the development of a spam filtering system for a typical enterprise that will improve the overall level of company security and employee efficiency.

Practical significance of work is determined by the fact that its results allow to determine technical level ways to combat spam-sheets. The result of this diploma project is to determine at the legislative and technical level ways to combat spam sheets, research of technical methods of filtering sheets, calculation of technical-economic substantiation, development and implementation of spam filtering system working at the level of the POP3 protocol and analyzing the content of user inputs, which allows to reduce the economic of waste of spam-mails.

The scope of application for the created system of filtering spam-sheets is limitless, since it is possible to apply to any enterprise with any number of staff and individual users.

Key words: e-mail, spam filtering, Bayes filter.

The explanatory note to the diploma work consists of 60 pages, 29 drawings, 6 tables, 22 sources of information.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет імені Петра Могили
Факультет комп'ютерних наук
Кафедра інтелектуальних інформаційних систем

Пояснювальна записка

до кваліфікаційної роботи

на тему:

«Система моделювання процесів СПАМ-фільтрації»

Спеціальність 122 «Комп'ютерні науки»

122 – БКР – 401з.210901101

Виконала студентка 4-го курсу, групи 401з
_____*В.В.Романець*
(підпис, ініціали та прізвище)
«___» _____ 2022 р.

Керівник: _____
(наук. ступінь, вчене звання)
_____*М.О.Таранов*
(підпис, ініціали та прізвище)
«___» _____ 2022р.

Миколаїв – 2022

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БД – база даних

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

СУБД – система управління базами даних

ADO – ActiveX Data Objects

CGI – Common Gateway Interface

COM – Component Object Model

DDL – Data Definition Language

DKIM – DomainKeys Identified Mail

DML – Data Manipulation Language

DNS – Domain Name System

IP – Internet Protocol

MIME – Multipurpose Internet Mail Extensions

MS – Microsoft

OLE – Object Linking and Embedding

POP3 – Post Office Protocol

SMS – Short Message Service

SMTP – Simple Mail Transfer Protocol

SPF – Sender Policy Framework

SQL – Structured Query Language

SSL – Secure Sockets Layer

ВСТУП

Протягом останніх років spam-листи перетворились з легкого дратуючого фактора в одну з найсерйозніших загроз безпеки інформації. Непрохані повідомлення переповнюють індивідуальні поштові скриньки та паралізують роботу серверів. Час, який співробітники змушені витрачати на розбір та прочитання spam-листів, постійно зростає - а разом з ним і фінансові втрати компаній (складові вже, за різними оцінками, від $50 до $200 на рік у розрахунку на одного співробітника). У 2018 році доля спаму в світовому поштовому трафику, за інформацією «Лаборатории Касперского», склала 66,8 %.

За останні роки було винайдено чимало способів боротьби з небажаною кореспонденцією. На жаль, зловмисники відслідковують дії фільтрів і винаходять все нові прийоми для їх обходу. До того ж нерідко фільтрація spam-листів приносить більше шкоди, ніж користі: разом з настирливою рекламою не доходять до адресата і важливі ділові або особисті повідомлення. Незважаючи на всілякі спроби боротьби з небажаною кореспонденцією, звіт, наданий компанією «MessageLabs» показує, що spam-листи обходяться Європі в 10,2 млрд. євро на рік.

Таким чином, всі дослідження в галузі боротьби з непотрібною кореспонденцією надзвичайно актуальні в даний час.

На даний момент існує величезна кількість програм фільтрації електронної кореспонденції, як для домашніх користувачів, так і для корпоративних клієнтів. Проблемами фільтрації spam-листів зайняті як великі компанії, так і окремі розробники. До найбільших компаній, що займаються створенням систем фільтрації електронних листів, відносяться «Лаборатория Касперского», «McAfee», «Symantec» та інші. Серед корпоративних рішень в галузі фільтрації spam-листів слід виділити наступні продукти: «Kaspersky Anti-Spam» («Лаборатория Касперского»), «SpamKiller» («McAfee»), «Premium AntiSpam» («Symantec»). За твердженням розробників, дані програмні продукти володіють високими показниками фільтрації spam-листів (92 – 97 %) та низькою кількістю помилкових спрацьовувань. Однак вартість даних систем фільтрації ($ 10 - $ 20 за

одну поштову скриньку на рік) є серйозним стримуючим чинником у придбанні даних програмних продуктів.

Мета дипломної роботи полягає в розробці методу spam-фільтрації електронної пошти та проєктування на його основі системи фільтрації spam-листів, що дозволить підвищити загальний рівень безпеки підприємства та зменшити час, який витрачається на розбір непотрібної кореспонденції.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Опис предметної області

SPAM існує тому, що є економічні передумови для його існування. Якщо розглядати SPAM як об'єкт інформаційного обміну, то між його суб'єктами встановлюються певні економічні відносини. До суб'єктів таких відносин ставляться:

1) Замовники (зацікавлені в широкому поширенні за каналами електронної пошти певної інформації). Саме замовники спочатку інвестують в SPAM частину своїх фінансових засобів, призначених на рекламу продуктів, рішень і послуг.

2) Творці/розповсюджувачі SPAM (спамери, які роблять і поширюють SPAM, і несумлінні провайдери, які зацікавлені в збільшенні обсягу використання трафіку). У спамерів, у свою чергу, існує свій поділ праці: серед них можна виділити дві категорії: «нападники» і «розсилочники». «Нападники» проникають у будь-які доступні комп'ютери й установлюють на них «троянські» програми, що забезпечують сховане розсилання SPAM. «Розсилочники» працюють із використанням звичайного списку. Саме вони являються основними покупцями списків поштових адрес.

3) Споживачі SPAM. Споживачами SPAM стають поневолі усі, оскільки одержують SPAM не залежно від свого бажання. Багато розуміють, що частина трафіку була задіяна на транспортування SPAM, і змушені його оплачувати. Крім того, існує деяке протиріччя в діях споживачів. З одного боку, вони різко виступають проти SPAM, з іншого боку - іноді піддаються на «угоди» і реагують на рекламу (інакше замовники не витрачали б гроші впусту) [1].

Економічні зв'язки між суб'єктами SPAM-відносин наведено на рисунку 1.1.

Розв'язати проблему SPAM можна тільки шляхом усунення умов його існування. По-перше, можна постаратися зруйнувати економічні відносини між суб'єктами, що беруть участь у виробництві й споживанні SPAM. Наприклад, виключити хоча б один суб'єкт із даного ланцюжка. Адже якщо не буде замовників

або споживачів, тоді творці SPAM «зникнуть» як такі. По-друге, розгорнути активну боротьбу з SPAM, що повинна вестися на всіх можливих фронтах, починаючи з кінцевих користувачів, закінчуючи державними й громадськими організаціями.

У цей час існує кілька різних організаційних способів боротьби з SPAM. До них ставляться:

1) Юридичні способи. Припускають прийняття законів про заборону SPAM, створення державних служб для виявлення й переслідування спамерів, наділення провайдерів певною відповідальністю й повноваженнями з фільтрації пошти. Організаційні міри підприємств щодо дотримання корпоративної інформаційної політики.

2) Соціальні способи. Створення умов, в яких SPAM стає процедурно неможливим або економічно невигідним. Припускають введення нових способів обміну електронною поштою - підтвердження відправлення листів, введення платних електронних марок, платних повідомлень (наприклад, Facebook із грудня 2015 року тестує систему оплати за відправлення повідомлень незнайомим користувачам) тощо. Створення співтовариств і об'єднань (наприклад, провайдерів) для боротьби з спамерами.

3) Пропаганда. Припускає роз'яснення негативної ролі SPAM як на державному, так і суспільному рівнях.

4) Технічні способи. Припускають впровадження технічних засобів контролю за поширенням SPAM, виділення SPAM з інформаційного потоку, а також його блокування[2].

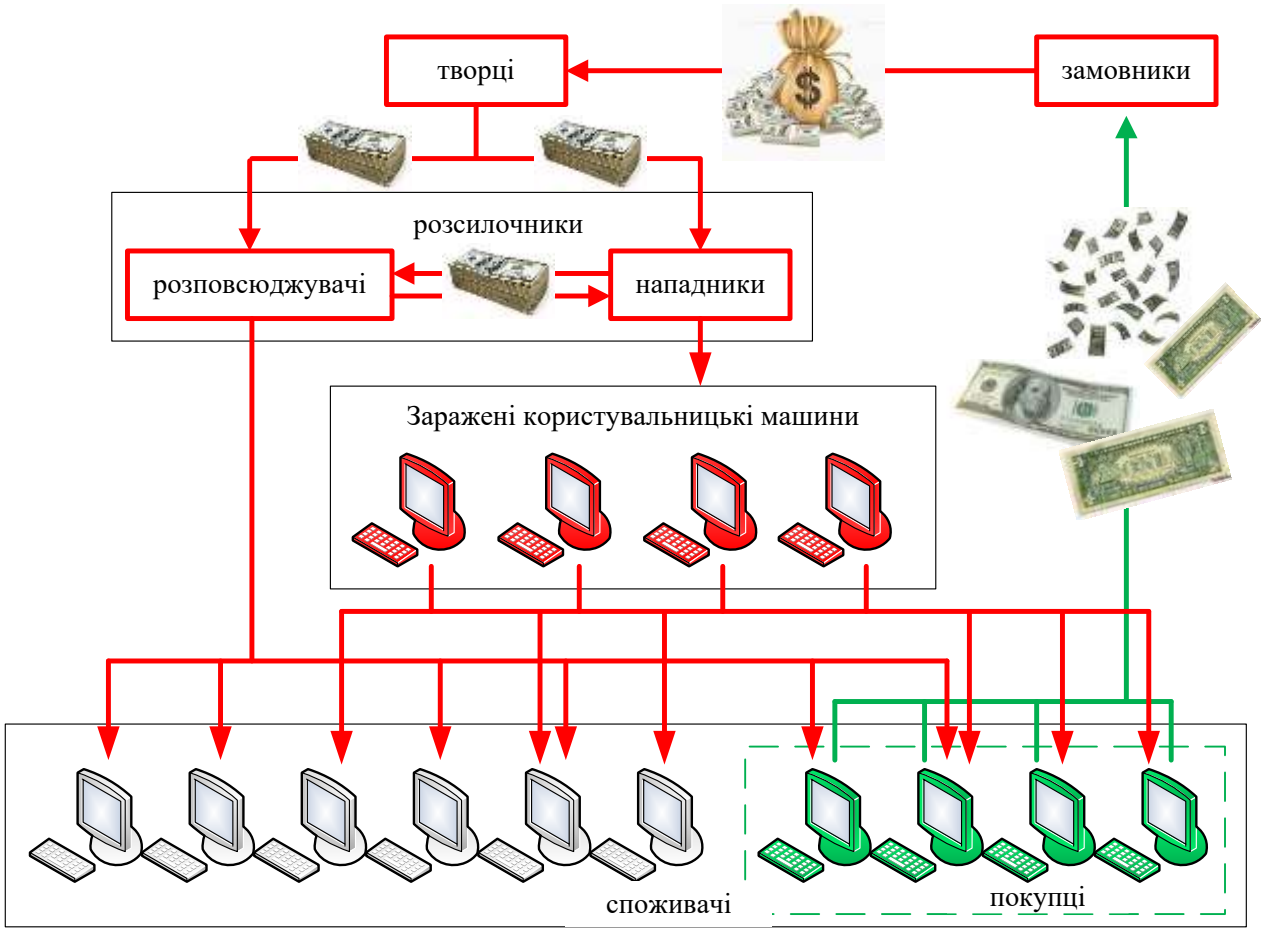


Рисунок 1.1- Економічні зв'язки між суб'єктами SPAM-відносин

Існує велика кількість різновидів спаму. Їх можна умовно розподілити за засобом розповсюдження та за видами (рисунок 1.2.)

Вспливаючі (pop-up) вікна/консолі

Особливо часто такий спам зустрічається на сайтах, розрахованих на відвідувачів з країн СНД. За кожну консоль власник заробляє не більше цента. Тому найжадібніші роблять по три і більше консолі. Також консолями вони можуть підвищити рейтинг свого сайту в рейтингах. Виходить замкнуте коло: більше консолей - більше рейтингів - більше відвідувачів - більше консолей. Зазвичай такі консолі «вискакують», коли відвідувач залишає сайт. Бувають і такі, що відкривають додаткові вікна і при вході на сайт.

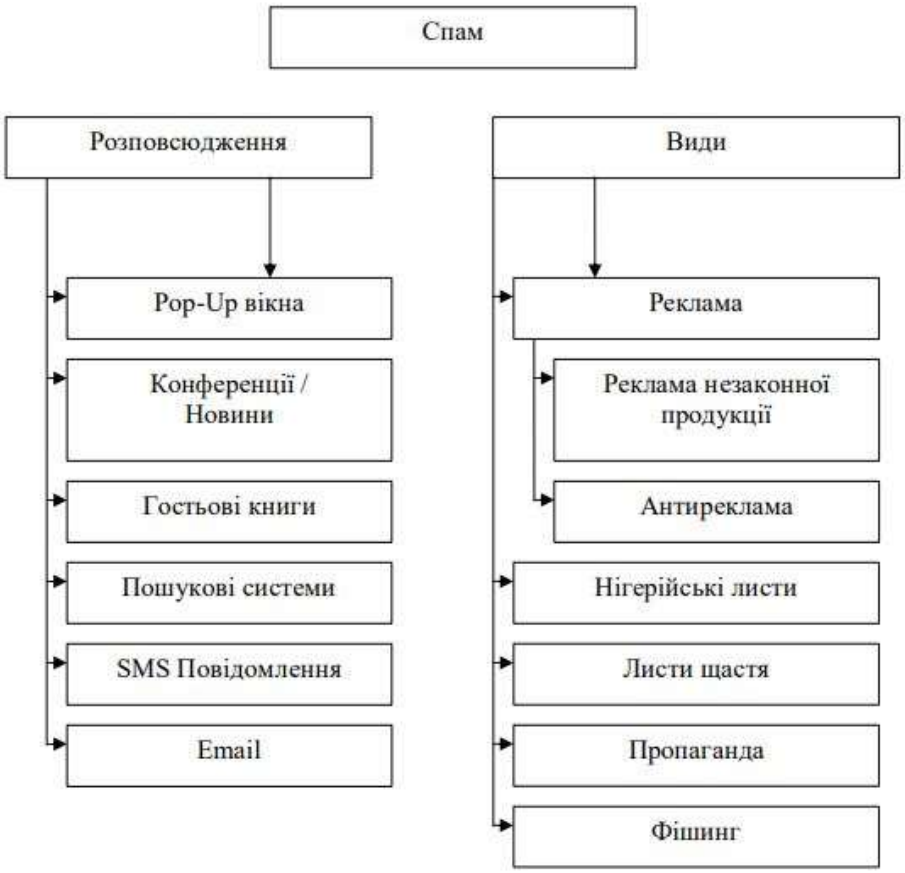


Рисунок 1.2 – Способи розповсюдження та види поштового спаму

Спам в конференціях/новинах

Як правило, кожна веб-конференція присвячена якійсь вузькій темі. За правилами конференцій рекламні повідомлення іноді допускаються, але не частіше, ніж один раз на тиждень. Спамерів правила не цікавлять. Вони можуть відправляти свою рекламу кожен день і одночасно в кілька конференцій. При чому навіть не за тематикою конференції. Подібне можна зустріти на форумах, дошках оголошень та чатах.

Спам в гостьових книгах

Іноді власники сайтів розміщують гостьові книги, в яких відвідувачі можуть написати свої зауваження, побажання. Але спамери і тут не соромляться. Їх не хвилює зміст сайтів. Вони просто шукають посилання на гостьові книги і розміщують в них свою рекламу.

Спам в пошукових системах

Деякі власники для залучення відвідувачів на свій сайт через пошукові системи вставляють у сторінки невидимий текст з найпопулярнішими словами. Користувач, через пошукову систему, набравши фразу «безкоштовний Інтернет», потрапляє на такий сайт і нічого очікуваного не знаходить.

Спам в SMS повідомленнях

Багато компаній, в першу чергу європейські, розглядають нове покоління мобільних телефонів в якості ідеальної платформи для розміщення реклами. Дійсно, власники таких телефонів - це потенційні клієнти, які постійно перебувають в межах доступу і при цьому мають можливість миттєво відгукнутися на рекламну пропозицію. SMS-сервіс в США може зникнути через спам. Аналітики вважають, що спам (нав'язувані рекламні оголошення), який надходить на мобільні телефони у вигляді коротких повідомлень (SMS), може поставити під загрозу подальше використання самої системи коротких повідомлень. Як правило, вхідні SMS безкоштовні, але деякі великі стільникові оператори США, такі як AT&T Wireless і Sprint, беруть за них плату [1].

Спам в електронній пошті Інтернет (Email)

Це найпоширеніший вид спаму. Рекламу можуть посилати конкретно на ваш Email або відразу на безліч адрес. Повідомлення можуть містити тільки одну рекламу, але можливі і приписки.

Види спаму в електронній пошті:

1) Найбільш розповсюдженою є реклама. Багато невеликих компаній, які ведуть легальний бізнес, використовують спам розсилку, з метою реклами своїх товарів. Не дивлячись на те що, такий вид розповсюдження інформації може виявитися занадто нав’язливим і відштовхнути потенційних клієнтів від покупки, головним плюсом такої реклами є низька вартість та одноразове охоплення великої аудиторії. Проте нерідкі випадки коли така реклама викликала зворотний ефект, викликала настороженість одержувачів і відштовхувала їх.

2) Реклама незаконної продукції. Інформація про продукцію, про яку не можна повідомити іншими легальними, публічними способами, часто стає змістом

спам-повідомлень, наприклад: контрафактні товари, обмежені по обороту ліки, незаконно отримана інформація, контрафактне програмне забезпечення.

3) Також зустрічається таке явище як антиреклама будь-якої продукції, компанії, або ресурсу, з метою зганьбити конкурентів або виставити товар в поганому світлі, що заборонено законодавством про рекламу.

4) Нігерійські листи - окремий вид спаму, спрямований на виманювання грошей у одержувача. Свою назву отримав тому, що більшість таких листів приходило з африканської країни - Нігерії. Відповідні листи містять повідомлення про те, що одержувач листа може отримати велику суму грошей, найрізноманітнішим чином, а відправник може допомогти з цим. Спійманого «на гачок» користувача відправник просить вислати невелику суму грошей, під приводом покриття витрат на відкриття рахунку або витрат на оформлення документів. Виманювання цієї невеликої суми і є метою спамерів.

5) Листи щастя або магічні листи - повідомлення нерідко нібито магічного, релігійно-містичного змісту, що розсилаються по електронній пошті, в соціальних мережах, мережах обміну миттєвими повідомленнями і тому подібних, декільком адресатам. Текст листа будується таким чином, щоб одержувач повірив у реальну дієвість отриманого, і поширив лист далі. У таких повідомленнях найчастіше використовуються тексти, що здаються дуже правдоподібними, описуються випадки з життя, які нібито трапилися в дійсності, наприклад про нещасні випадки з отримувачами або їх родичами, що не переслали дане повідомлення. Мети як такої не переслідує, окрім як поширення самого повідомлення і засмічення поштової скриньки. З часом текст листа може змінюватися шляхом навмисного редагування користувачами, або в наслідок описок.

6) Пропаганда - розповсюдження різних політичних, релігійних та інших поглядів, фактів і чуток, найчастіше свідомо неправдивих, з метою формування хибної громадської думки.

7) Також існує таке явище як розсилка спаму від імені іншої людини, найчастіше досить відомої, але часом страждають і звичайні користувачі. Метою

такої розсилки є спроба викликати негативне ставлення до «жертви». Від таких розсилок нерідко страждають різні компанії, бренди, а часом і Інтернет-ресурси.

8) Фішинг - спроба спамера «вивудити» у користувача, що отримав лист, номер його кредитної карти, пароля доступу в платіжну систему тощо. Такі листи зазвичай намагаються замаскуватися під повідомлення від офіційних представників банку або платіжної системи. Йдеться про те, що необхідно підтвердити відомості про рахунок, а в іншому випадку рахунок буде заблокований, надається посилання на сайт шахраїв, оформлений для правдоподібності під сайт банку, з формою для заповнення. Нічого не підозрюючи користувач, власноруч передає зловмисникам всі необхідні дані, після чого благополучно втрачає з рахунку всю суму, або її частину, як пощастить [2-4].

У таблиці 1.1 надано оцінку корисності й небезпеки spam-листів.

1.2 Аналіз існуючих методів усунення spam-листів

Поширення величезної кількості SPAM-повідомлень вимагає істотних вкладень у технологію розсилань. Фахівці в області боротьби з SPAM-листами виділяють наступний технологічний ланцюжок створення й поширення SPAM-листів:

1) збір і верифікація e-mail адрес одержувачів (класифікація адрес за типами);

2) підготовка «точок розсилання» - комп'ютерів, через які будуть розсилатися spam-листи;

3) створення програмного забезпечення для розсилання;

4) пошук клієнтів;

5) створення рекламних оголошень для конкретного розсилання;

6) поведення розсилання.

Кожний окремий крок у технологічному ланцюжку може виконуватися незалежно [3].

В даний час використовується декілька методів фільтрації електронної пошти.

Таблиця 1.1 - Оцінка корисності й небезпеки spam-листів

Вид spam-повідомлень	Користь	Небезпека
Реклама незаконної продукції	іноді	може мати елементи контролю, віруси або небезпечні посилання
Реклама	-//-	-//-
Пропаганда	-//-	-//-
«Ланцюгові листи»	інформація про використання адреси	-//-
Листи з вірусами	-//-	призводить до порушення роботи ПК
Поштові черв'яки	-//-	завантаження трафіку
DoS і DDoS-атаки	-//-	можливість втрати потрібної інформації
Фішинг	-//-	небезпечні посилання
Нігерійські листи	-//-	завантаження трафіку і втрачений час
Backscatter	-//-	-//-
Повідомлення антивірусних програм і spam-фільтрів	-//-	-//-
Антиреклама	-//-	-//-
Не замовлена розсилка	-//-	-//-
Листи від імені іншої особи, для появи до нього негативного ставлення	-//-	-//-
Листи з проханням про матеріальну допомогу	-//-	-//-

Статистичні методи фільтрації спаму

Ці методи використовують статистичний аналіз змісту листа для прийняття рішення, чи є він спамом. Найбільшого успіху вдалося досягти за допомогою алгоритмів, заснованих на теоремі Байеса. Для роботи цих методів потрібно «навчання» фільтрів, тобто потрібно використовувати розсортовані вручну листи для виявлення статистичних особливостей нормальних листів і спаму. Після навчання на досить великій вибірці, вдається розпізнати до 95-97 % спаму [6].

Змішані методи

Крім «наївного» Байєсівського підходу є й інші способи скомбінувати-об'єднати окремі ймовірності для різних слів. Ці методи відрізняються від «наївного» методу припущеннями, які вони роблять про статистичні властивості вхідних даних. Дві різні гіпотези призводять до радикально різних формул для об'єднання окремих ймовірностей [7].

Наприклад, для перевірки припущення про сукупності окремих ймовірностей, логарифм створення якого з точністю до константи підпорядковується розподілу хі-квадрат з 2N ступенями свободи, можна використовувати формулу (1.1):

$$p = C^{-1}(-2\ln(p_1 p_2 \ldots p_N), 2N), \qquad (1.1)$$

де C^{-1} - зворотна функції хі-квадрат.

Метод Марківської дискримінації

Окремі ймовірності можуть бути об'єднані також методами Марківської дискримінації.

Даний метод простий (алгоритми елементарні), зручний (дозволяє обходитися без «чорних списків» і подібних штучних прийомів), ефективний (після навчання на досить великій вибірці відсікає до 95-97% спаму, і в разі будь-яких помилок його можна «довчати» . Загалом, є всі показання для його повсюдного використання, що і має місце на практиці - на його основі побудовані практично всі сучасні спам-фільтри.

Втім, у методу є і принциповий недолік: він базується на припущенні, що одні слова частіше зустрічаються в спам, а інші - у звичайних листах, і неефективний, якщо дане припущення невірно. Втім, як показує практика, такий спам навіть людина не в змозі визначити «на око» - тільки прочитавши лист і зрозумівши його сенс. Існує метод Байесового «отруєння», що дозволяє додати багато зайвого тексту, іноді ретельно підібраного, щоб «обдурити» фільтр.

Ще один не принциповий недолік, пов'язаний з реалізацією - метод працює тільки з текстом. Знаючи про це обмеження, спамери почали вкладати рекламну

інформацію в картинку. Текст в листі або відсутній, або не несе сенсу. Проти цього доводиться користуватися або засобами розпізнавання тексту («дорога» процедура, застосовується тільки при крайній необхідності), або старими методами фільтрації - «чорні списки» і регулярні вирази (так як такі листи часто мають стереотипну форму) [8].

Таким чином, існують два основних підходи до фільтрації spam`у - за формальними ознаками повідомлення (за способом посилки й оформленням) і за його змістом (рисунок 1.3).

Рисунок 1.3. - Технологічні підходи до боротьби зі spam-листами

Семантичні методи припускають розпізнавання за змістом листа (словосполучення, евристики, статистика) або розпізнавання за зразками листів (за сигнатурами, з голосуванням тощо).

Формальні методи включають фільтрацію за списками (поштових адрес, IP-адрес) і за формальними ознаками листа (наявність багатьох відправників, відсутність одержувача, формат, розмір тощо).

1.3 Постановка задачі

Метою роботи є дослідження методів spam-фільтрації та розробка програмного продукту захисту електронної пошти від спаму для будь-якого підприємства, що збільшить продуктивність його роботи. Розроблюваний програмний продукт повинен забезпечувати виконання таких основних операцій:

- отримання електронних повідомлень з поштового сервера;
- читання отриманих повідомлень з їх подальшою класифікацією;
- можливість окремого перегляду spam-повідомлень;
- збереження поточного повідомлення в базі даних із spam-коефіцієнтом.

Завдання кваліфікаційної роботи:

1) Розглянути технічні методи фільтрації spam-листів.
2) Вивчити можливості поштових протоколів для боротьби з непотрібною кореспонденцією.
3) Виконати моделювання процесу spam-фільтрації.
4) Розробити програму «Поштовий клієнт».
5) Реалізувати в даній програмі алгоритм фільтрації листів.

Технічне завдання на розробку проекту корпоративної системи фільтрації електронної пошти наведено в додатку А.

2 МОДЕЛЮВАННЯ ПРОЦЕСІВ СПАМ-ФІЛЬТРАЦІЇ

2.1 Ескізний проект

2.1.1 Математичні основи фільтрації (теорема Байеса)

Проблема семантичного аналізу листів пов'язана з обробкою не точної інформації. Одним з підходів до цього завдання може служити імовірнісне моделювання предметної області. Найбільш широке поширення одержали системи, засновані на теоремі Байєса.

Уперше даний підхід до аналізу електронних листів застосував Пол Грем. У своїй статті «A plan for spam», що була опублікована в серпні 2002 року, Пол Грем затверджував, що проблему spam-листів можна зупинити, використовуючи фільтрацію за змістом листа на основі ймовірносно-статистичних методів.

Пол Грем запропонував кожному слову, що зустрічається в переписці, або фразі привласнювати два значення:

- імовірність його наявності в spam-листах;
- імовірність його присутності в листах, дозволених для проходження.

Баланс цих двох значень і визначає ймовірність того, що лист, у якому зустрічаються дані слова або фрази, є spam-листом.

Весь підхід ґрунтується на тій логіці, що зловмисники можуть іти на будь-які виверти з IP-адресами й редагуванням тексту повідомлень, але донести інформацію до одержувача вони все-таки повинні. Якщо послане ними повідомлення через змушене застосування різних прийомів обходу фільтрів буде незрозуміло читачам, то користі від такого розсилання не буде ні якою. Читати «між рядків» користувач не буде. Виходить, зловмисники все-таки повинні написати в листі щось зрозуміле, закличне до якоїсь дії. Ця ознака spam-листа і є основою для роботи фільтрів, побудованих на статистичних алгоритмах Байєса.

Суть формули полягає в тому, що ймовірність події може бути досить точно обчислена, якщо зібрано статистику здійснення події в минулому. У застосуванні до spam-листів це звучить приблизно так: якщо 80 % листів, що містять словосполучення «мовний англійський», були spam-листами, то й наступний лист із таким словосполученням - spam, причому з більшою часткою ймовірності. Щоб оцінити цю частку, використається математичний апарат, а саме теорема Байєса.

Теорема виражається формулою Байєса:

$$P(H|X) = \frac{P(X|H) \cdot P(H)}{P(X)}, \qquad (2.1)$$

де P(H|X) - імовірність гіпотези H при настанні причини X ;

P(X|H) - імовірність присутності причини X при істинності гіпотези H;

P(H) - апріорна ймовірність гіпотези H;

P(X) - імовірність настання причини X.

Ця формула лежить в основі багатьох сучасних систем штучного інтелекту, призначених для роботи в умовах невизначеності. Такі системи дають імовірнісну оцінку, тому звичайно не заміняють експерта, а роблять йому підтримку в ухваленні рішення.

На практиці, коли є n гіпотез, використається формула Байєса в загальній формі:

$$P(H_i|X) = \frac{P(X|H_i)P(H_i)}{\sum \quad P(X|H_k)P(H_k)}, \qquad (2.2)$$

де $P(H_i|X)$ - імовірність істинності гіпотези H_i при заданій причині X;

$P(H_i)$ - апріорна ймовірність гіпотези H_i;

$P(X|H_i)$ - імовірність наявності причини X, якщо істина гіпотеза H_i;

n - число можливих гіпотез.

Якщо причину можна представити у вигляді вектора $X = (X_1, X_2, \dots, X_m)$, кожний компонент якого має умовну ймовірність щодо гіпотези H_i $P(X_j|H_j)$, то для

обчислення умовних імовірностей $P(X|H_i)$ використається припущення про умовну незалежність вектора X (саме системи класифікації, побудовані на такому припущенні, називаються байєсовськими класифікаторами). У цьому випадку умовна ймовірність обчислюється за формулою:

$$P(\mathrm{X}|H_i) = \prod_{j=1}^{m} P(X_j|H_i)\,. \qquad (2.3)$$

При навчанні фільтра масив електронних листів ділиться на два класи: spam і корисна кореспонденція. Для кожного слова обчислюється частота його зустрічі в обох класах листів.

Позначається $F_S(W_i)$ – кількість spam-листів, у яких зустрілося слово W_i, а $F_{NS}(W_i)$ – кількість корисних листів, у яких зустрілося слово W_i. У завданні дві гіпотези: H_S – лист є spam`ом, H_{NS} – корисний лист. Тоді ймовірність того, що поява слова W_i у листі означає spam, обчислюється за формулою:

$$P(W_i|H_s) = \frac{F_s(W_i)}{F_s(W_i) + F_{\mathrm{NS}}(W_i)}, \qquad (2.4)$$

а ймовірність того, що слово W_i не вказує на spam у листі:

$$P(W_i|H_{\mathrm{NS}}) = \frac{F_{\mathrm{NS}}(W_i)}{F_s(W_i) + F_{\mathrm{NS}}(W_i)}. \qquad (2.5)$$

Вектор W включає всі слова нового листа. Тоді для нового листа ймовірність того, що воно spam, обчислюється за формулою Байєса в такий спосіб:

$$P(H_S|W) = \frac{\prod P(W_j|H_s)}{\prod P(W_j|H_s) + \prod P(W_j|H_{\mathrm{NS}})}, \qquad (2.6)$$

З огляду на формулу (2.1) і вважаючи апріорні ймовірності обох гіпотез однаковими, одержується :

$$P(H_S|W) = \frac{P(W|H_s)P(H_s)}{P(W|H_s)P(H_s) + P(W|H_{\text{NS}})P(H_{\text{NS}})}, \quad (2.7)$$

Дана формула визначає ймовірність того, що лист із даним набором слів, сформованою базою spam і «не spam» слів є spam`ом.

Віднесення листа до spam`у або корисних листів виконується з врахуванням заданого програмістом, адміністратором або користувачем порога, значення якого становлять 0,6 - 0,8. Після ухвалення рішення по листу в базі даних обновляються імовірнісні бази для слів, які входять до нього [15].

2.1.2 Алгоритм фільтрації вхідної почти

Уся пошта що надходить до клієнта повинна аналізуватися та записуватися з результатами аналізу до бази даних. Алгоритм аналізу листа зображено на рисунку 2.1. Коефіцієнт спаму потрібен для подальшої вибірки поштовим клієнтом із заданими параметрами.

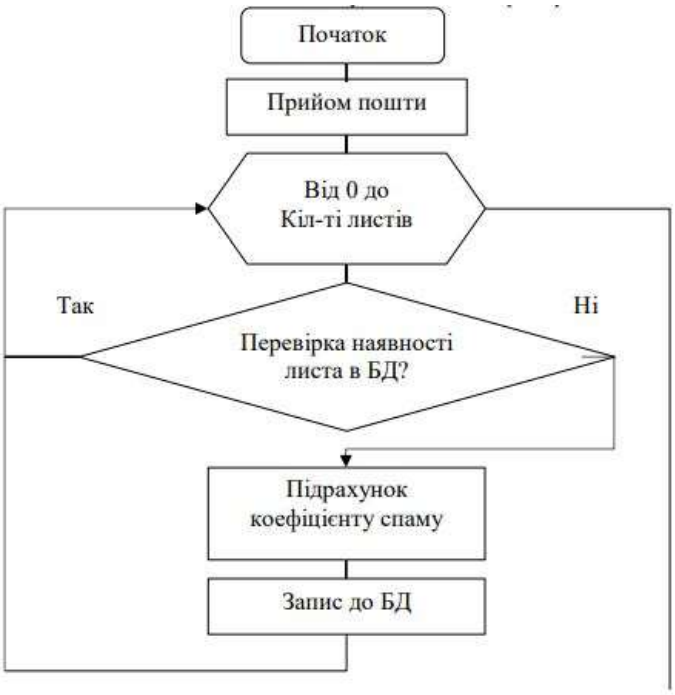


Рисунок 2.1 – Алгоритм фільтрації пошти

Фільтр використає два методи фільтрації:

- фільтрація за «чорними» і «білими» списками e-mail адрес;
- статистична фільтрація на основі теореми Байєса по тілу листа й заголовку «Subject».

Фільтр перевіряє адресу в заголовку «From» листа вхідної пошти користувачів в «чорних» і «білих» списках. Якщо адреса знайдена в «чорних» списках, лист уважається SPAM, якщо в «білих» - уважається легітимним. Після цього текст листа заноситься в SPAM або ham словники відповідно. У початок заголовка «Subject» SPAM-листа додається позначка «***SPAM***», після аналізу тексту листа, у його заголовок додаються два поля: X-MSpam і X-MSpam-Index з відповідному аналізу значеннями й лист пересилається одержувачеві.

Якщо відправник листа невідомий (відсутній у списках), фільтр намагається визначити «SPAMність» листа на основі теореми Байєса й привласнити йому число від 0 до 1. Чим ближче цей показник до 1, тим імовірніше, що лист - SPAM і навпаки (чим ближче показник до 0, тим більше шансів, що лист легітимне). Для обчислення індексу «спамності», фільтр «пробігає» по всіх словах у тілі листа й заголовку «Subject» і визначає для кожного слова ймовірність того, що лист SPAM або не SPAM. При перевищенні показником заданої границі, лист класифікується як SPAM, адреса відправника заноситься в «чорний» список, а словник SPAM-слів поповнюється словами даного листа. Якщо індекс «SPAMності» не перевищив нижню границю, лист уважається легітимним, слова цього листа поповнюють словник ham-слів, а адреса відправника додається в «білий» список. При індексі SPAMності, що перебуває між нижньою й верхньою границею, лист не класифікується, словники spam і ham слів залишаються незмінними, «білі» і «чорні» списки також не міняються.

Завдання класифікації повідомлень на SPAM-листи й легітимну пошту є нетривіальною. У зв'язку із цим програмне забезпечення, що займається фільтрацією SPAM-листів, може допускати помилки. Помилки бувають двох видів:

1) Помилки першого роду (false positive) - пропуск SPAM-листа через його знаходження в «сутінковій зоні» або подолання наявного рівня захисту - недостатня повнота методу.

2) Помилки другого роду (false negative) - помилкові спрацьовування, при яких потрібна кореспонденція помилково ставиться до SPAM-листів - точність методу.

2.2 Технічний проект

2.2.1 Складові частини системи та взаємодія між ними

У програмі можна виділити наступні загальні структурні одиниці:

– SpamMain (Головний модуль програмного комплексу. У ньому забезпечується користувацький інтерфейс для налаштування фільтру та перегляду списку отриманих листів);

– MailDetailView (Модуль для перегляду отриманого повідомлення);

– SpamWords (Модуль, що забезпечує перегляд та редагування словнику spam слів);

– SpamSettings (Модуль для налаштування параметрів з’єднання з поштовим сервером);

– DataModule (Модуль з’єднання програми з базою даних);

– IdMessage (Даний модуль містить опис класів, що розбивають лист на логічні частини для його подальшого аналізу);

– IdPOP3 (Даний модуль забезпечує з’єднання додатку з поштовим сервером);

– IdSSLIOHandlerSocketOpenSSL (Даний модуль забезпечує підтримку SSL шифрування з’єднання з поштовим сервером.);

Структурну схему модулів програми, що розроблена в проекті для аналізу пошти зображено на рисунку 2.2.

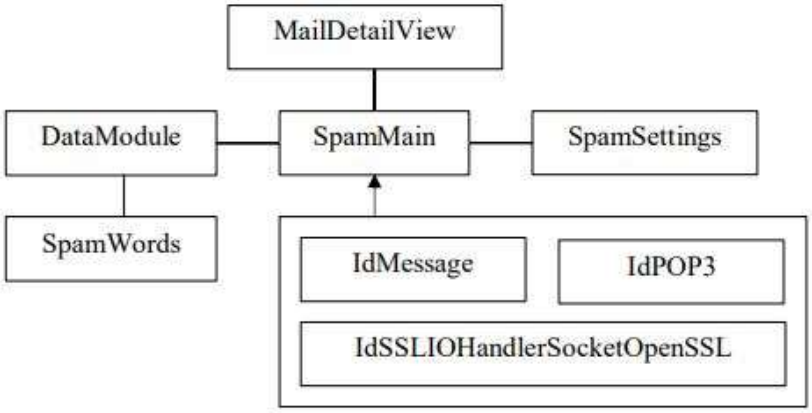


Рисунок 2.2 – Структурна схема модулів програми «Поштовий клієнт»

2.2.2 База даних програмного комплексу

База даних - спільно використовуваний набір логічно пов'язаних даних [16]. Це єдине сховище даних, яке одноразово визначається, а потім використовується одночасно багатьма користувачами.

Система управління базами даних (СУБД) - це програмне забезпечення, за допомогою якого користувачі можуть визначати, створювати і підтримувати базу даних, а також здійснювати до неї контрольований доступ [16].

При створенні архітектури доступу до даних використовувалася технологія ADO (Microsoft ActiveX Data Objects) - модель багатокомпонентних об'єктів - засіб розробки розподілених додатків середнього рівня, що дозволяє реалізувати сервіси проміжного шару усередині серверів автоматизації або компонентів Microsoft Component Services, є розширенням архітектури COM до рівня мережних додатків [17]. Структурну схему такого роду організації роботи представлено на рисунку 2.3.

Робоча станція – віддалений комп'ютер, на якому встановлено клієнтську частину програмного комплексу. Серверна частина програмного комплексу може бути встановлена як на окремому комп'ютері, підключеному до локальної мережі або Інтернет, так і безпосередньо на комп'ютері, на якому встановлений сервер бази даних СУБД.

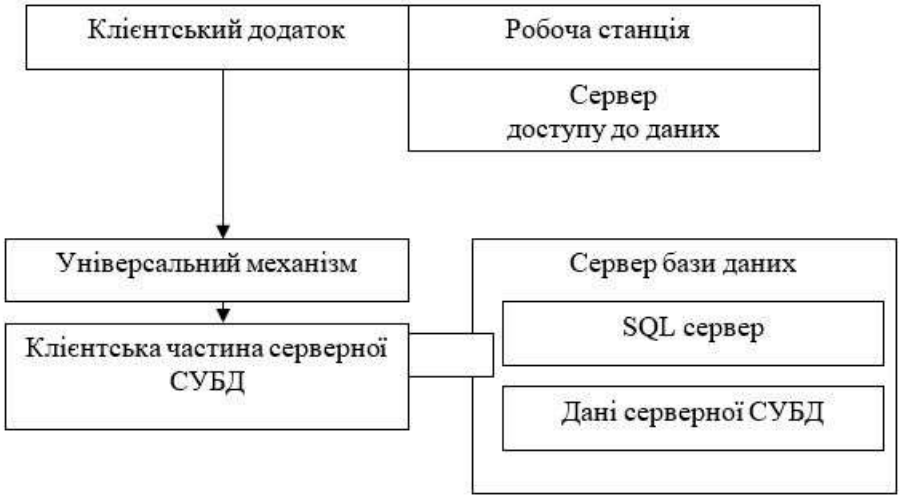


Рисунок 2.3 – Схема організації зв’язку між клієнтською та серверною частинами

Мова SQL має два основних компоненти [18]:

1) мову DDL (Data Definition Language), призначену для визначення структур бази даних та управління доступом до даних (оператори CREATE TABLE; DROP TABLE; ALTER TABLE; CREATE INDEX; DROP INDEX);

2) мову DML (Data Manipulation Language), призначену для вибірки і оновлення даних (оператори SELECT, INSERT, UPDATE, DELETE, COMMIT – фіксація змін, ROLLBACK – відміна внесених змін).

Основні оператори:

- PRIMARY KEY - ознака створення ключового поля;
- FOREIGN KEY - ознака створення поля зв'язку з іншою таблицею;
- CREATE TABLE - команда створення таблиці в поточній БД;
- USE - зробити активною конкретну БД;
- CREATE DATABASE - команда створення нової БД.

Для роботи з БД використовувався Microsoft SQL Server 2014, який базується на мові запитів SQL. За допомогою SQL було створено нову базу даних з назвою DB_Mail за допомогою команди:

```
CREATE DATABASE DB_MAIL.
```

Також були створені дві таблиці за допомогою наступних команд:

```
USE DB_MAIL
CREATE TABLE Mail
(
id_Mail INT Identity (1,1) NOT NULL PRIMARY KEY,
MNumber INT NOT NULL,
MRecipient CHAR(64) NOT NULL,
MSender CHAR(64) NOT NULL,
MSubject CHAR(128),
MBody TEXT,
MDate DATE NOT NULL,
MRatio FLOAT
)
CREATE TABLE Spam
(
id_Spam INT Identity (1,1) NOT NULL PRIMARY KEY,
SWord CHAR(64) NOT NULL,
SRatio FLOAT
)
```

Запити на вибірку

SQL-запит – це запит, який складається з послідовності SQL-інструкцій [19]. Ці інструкції задають команди, які потрібно виконати із вхідним набором даних для створення вихідного набору.

Існує кілька типів запитів:

- на вибірку;
- на відновлення;
- на додавання;
- на видалення;
- перехрестний запит;
- створення таблиць;

Найпоширенішим є запит на вибірку. Структура найпростішого запиту на вибірку даних:

SELECT список результуючих стовпчиків

FROM список таблиць-джерел даних

WHERE умова виводу стрічок;

Ключове слово SELECT означає запит на подання інформації. Вона буде подана у вигляді результуючої таблиці, рядки якої задовольнятимуть умові. Стовпчики, на основі яких формуються результуючі, або перевіряється умова, повинні належати таблицям перерахованим у списку [19]. Якщо список результуючих стовпчиків співпадає із списком єдиної таблиці-джерела, то такий список зручно представляти у скороченому вигляді за допомогою зірочки - *.

Зберігаємі процедури

Зберігаємі процедури представляють собою набір команд, що складається з одного або декількох операторів SQL або функцій та зберігається в базі даних у відкомпільованому вигляді [19].

Синтаксис оператора створення нової або зміни наявної зберігаємої процедури в позначеннях MS SQL Server:

{CREATE | ALTER } PROC[EDURE] имя_процедуры [;номер]

[{@имя_параметра тип_данных } [VARYING] [=default][OUTPUT]][,...n]

[WITH { RECOMPILE | ENCRYPTION | RECOMPILE,

ENCRYPTION }]

[FOR REPLICATION]

AS

sql_оператор [...n]

Для виведення лише повідомлень, розрахований коефіцієнт спамності для яких не перевищує значення спамності 0,65 створено процедуру SpamFilter:

```
CREATE PROC SpamFilter
@Ratio Float
AS
BEGIN
SELECT DISTINCT MSubject as 'Тема', MDate as 'Дата'
FROM Mail
```

```
WHERE @Ratio < MRatio
ORDER BY MDate
END
```

Процедура MailExitst перевіряє наявність листа з певним номером у базі даних:

```
CREATE PROC MailExist
@num Integer
AS
BEGIN
SELECT COUNT(MNumber)
FROM Mail
WHERE MNumber = @num
END
```

У таблицях 2.1, 2.2 зображено фізичну модель даних із вказаними типами та описом полів.

Таблиця 2.1 – Прийнята пошта «Mail»

Назва поля	Тип поля	Опис поля
id_Mail	int	Код листа в базі даних
MNumber	int	Номер листа на сервері
MRecipient	char(64)	Отримувач
MSender	char(64)	Відправник
MSubject	char(128)	Тема листа
MBody	text	Зміст листа
MDate	date	Дата
MRatio	float	«spam`ність»

Таблиця 2.2 – Список spam-слів «Spam»

Назва поля	Тип поля	Опис поля
id_Spam	int	Код слова
Sword	char(64)	spam-слово

Sratio	float	«spam`ність»

2.3 Робочий проект

2.3.1 Опис процедур і функцій

Використані в розробленій програмі «Поштовий клієнт» процедури і функції наведено у таблиці 2.3.

Таблиця 2.3- Процедури і функції фільтра spam-листів

Процедура або функція	Опис	Вхідні дані	Вихідні дані
function CheckPOPResponse: boolean	Перевірка підключення до поштового сервера	Логін і пароль для підключення до поштового сервера	Статус підключення до поштового сервера
procedure Save_Set_INI	Збереження настроювань програми в INI файл	Настроювання для збереження у файл	Файл настроювань
procedure Load_Set_INI	Завантаження настроювань програми з INI файлу		Поточні настроювання програми
procedure Load_Settings	Завантаження всіх настроювань програми з INI файлу	Дані про базу даних, настроювання підключення до поштового сервера	Файл настроювань або поточні настроювання програми

Продовження таблиці 2.3

procedure LoadBaseFromList	Завантаження листів з бази даних	Форма для завантаження листів з бази даних	Завантажені листи
procedure GetLoadMail	Завантаження листів з	База даних для збереження	База даних повідомлень

	поштового сервера	повідомлень	
Процедура або функція	Опис	Вхідні дані	Вихідні дані
procedure ParseMail (const s: String)	Додавання всіх листів у базу даних	Повідомлення для аналізування	Проаналізоване повідомлення
procedure AnalizMessage (Lb_t1,Lb_t2:TLabel)	Аналізування повідомлень на прочитанність	База даних повідомлень	База даних повідомлень
procedure AnalizMessage (Lb_t1,Lb_t2:Tlabel)	Аналізування повідомлень на прочитанність	База даних повідомлень	База даних повідомлень
procedure LogOutMess (I_Beg, I_Col:Integer)	Відправлення даних на лог форму	Дані про повідомлення	Данні для лог форми
procedure EnabMail (CHK:Boolean; i_tip:Integer)	Визначення доступних функцій при роботі з повідомленнями	Тип повідомлення	Функції для роботи з повідомленнями
procedure NewStatusMess (Stat_Mess:Boolean; Index1:Integer)	Установка нового статусу повідомленню	Новий тип повідомлення	Повідомлення нового типу
procedure NewMess (Status_Mess:Boolean)	Установка нового статусу повідомленню якщо виділено кілька штук	Новий тип повідомлення, повідомлення	Повідомлення нового типу
procedure NewMoveMess (Tip_:Integer)	Переміщення повідомлень по каталогах	База даних повідомлень	Переміщене повідомлення
procedure SetMessFilter (AdoTabTemp:TADOTable;Filter_Mess:String)	Установка фільтра	Таблиця повідом-лень	Результати фільтрування

Продовження таблиці 2.3

procedure InSlovar	Додавання з аналізуванням нових слів у словник	Таблиця словник	Оновлена таблиця словник
Процедура або	Опис	Вхідні дані	Вихідні дані

функція			
function PoiskInSlovar (Temp_Str:String): Boolean	Пошук і аналізу-вання слів у словнику	Таблиця словник, Таблиця повідом-лень	Коефіцієнт спамності

2.3.2 Функціональні можливості системи

Система являє собою шлюз, що працює на рівні протоколу SMTP, для вхідної пошти користувачів філії від головного поштового сервера серверу філії й для вихідної пошти користувачів філії.

Фільтр у своїй роботі використає два методи фільтрації:

− статистична фільтрація на основі теореми Байєса по тілу листа й заголовку «Subject»;

− фільтрація по «чорним» і «білим» списках e-mail адрес;

Система дозволяє робити:

а) фільтрацію вихідної пошти (лист вважається SPAM і далі не відправляється при розбіжності адреси користувача, що встановив smtp-з'єднання із заголовком «From» листа);

б) фільтрацію вхідних листів для кожного користувача на індивідуальній основі по власних словниках слів (spam і ham) і спискам e-mail адрес (black і white) - фільтр обчислює індекс «спамности» листа, не відсіяного «чорним» списком, додає адреса в заголовку «To» в «білий» список, а слова листа в ham-словник при впізнанні в якості легітимного (у противному випадку, дані листи не впливають на словник і списки адрес).

в) настроювання системи:

− на фільтрі вказується адреса й порт корпоративного сервера вихідної пошти.

− на клієнтському комп'ютері вказується адреса шлюзу фільтрації й порт, до якого він підключений (за замовчуванням 25).

г) «навчання» програми (відправленням листа на свою поштову адресу):

– при первісному нагромадженні статистики дані листи заносяться у відповідні словники залежно від позначки на початку теми повідомлення («spam» або «ham»), а адреса відправника у відповідний список залежно від того, указав користувач цей лист як spam або як ham;

д) у випадку виникненні помилок при класифікації листів фільтр визначає помилку, що була допущена - при помилці першого роду (фільтр порахував spam легітимним листом) слова цього листа віддаляються з ham-словника й заносяться в spam-словник, а адреса відправника листується в «чорний» список, при помилці другого роду виробляються зворотні дії.

Після зміни словників, що виходять листи в яких адреси в заголовках «From» і «To» збігаються з адресою користувача, що встановив smtp-з'єднання, віддаляються фільтром.

2.3.3 Робота із програмою «Поштовий клієнт»

При першому запуску база повідомлень порожня (рисунок 2.4).

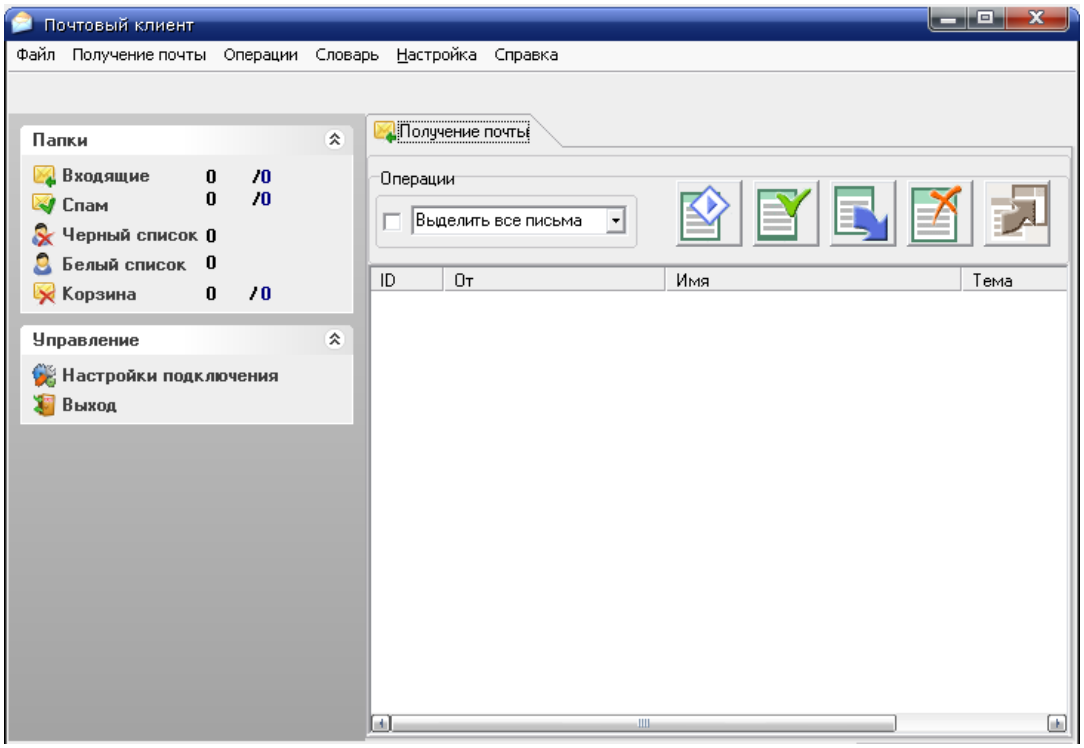


Рисунок 2.4 - Головна форма програми

Для налаштування програми натискується «Налаштування - Налагодження підключення» або кнопку на панелі «Налагодження підключення»

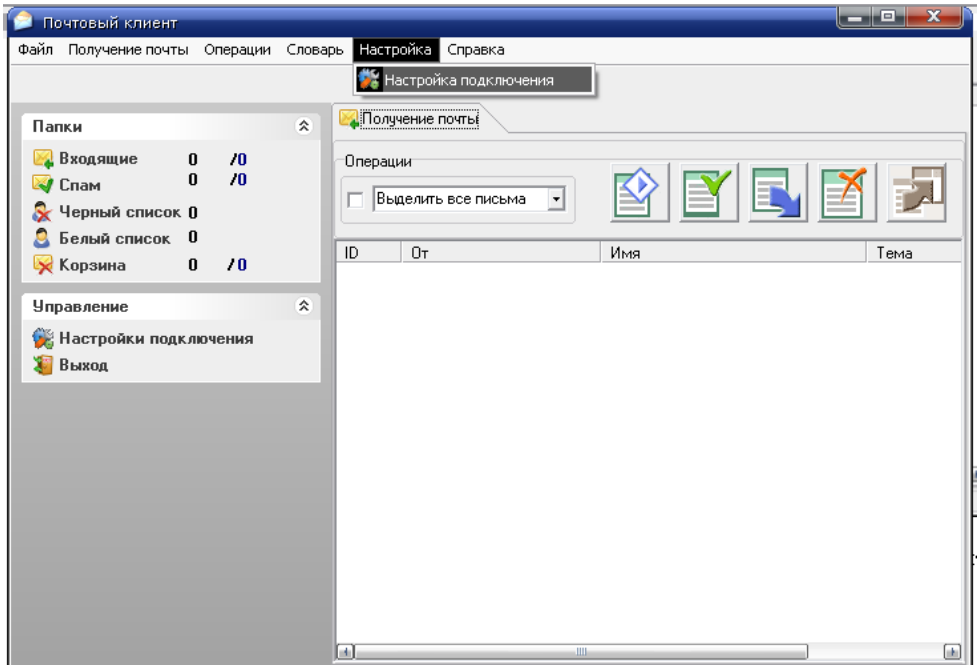


Рисунок 2.5 - Вхід в налаштування програми з системного меню

На формі, що з'явилася задаються основні налаштування підключення до поштового сервера і шлях до бази даних для збереження повідомлень. Є можливість приховувати символи паролю (рисунок 2.6) або показувати без маски (рисунок 2.7).

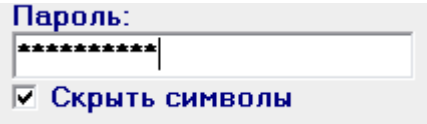


Рисунок 2.6 - Пароль зі схованими символами

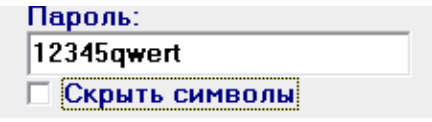


Рисунок 2.7 - Пароль без маски

Після внесення всіх налаштувань натискається кнопка «Зберегти» або «Відмінити».

Після внесення всіх налаштувань приймається пошта з поштового сервера. Для цього натискується «Одержання пошти-Прийняти нову пошту».

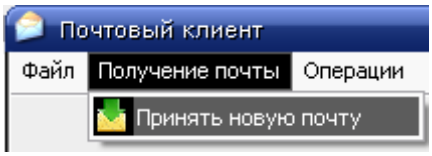


Рисунок 2.8 - Прийом пошти з поштового сервера

Після підключення до поштового сервера з'явиться вікно, що відображає загальну кількість повідомлень і кількість прийнятих повідомлень.

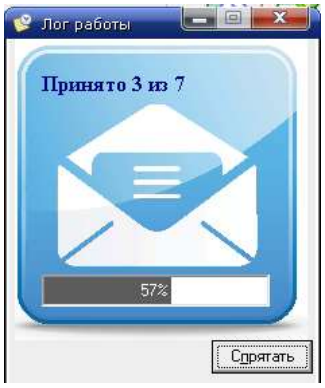


Рисунок 2.9 - Інформування про прийом нових повідомлень

Після натискання кнопки сховати відбувається аналіз прийнятих повідомлень. Результат аналізу відображається на формі, скан якої наведено на рисунку 2.10.

На наведеній на рисунку 2.11 формі відображений прийом сімох повідомлень з яких три повідомлення є спамом. Відповідно три адреси занесені в «Чорний список», листи переміщені в «Спам», а словник оновлен новими словами.

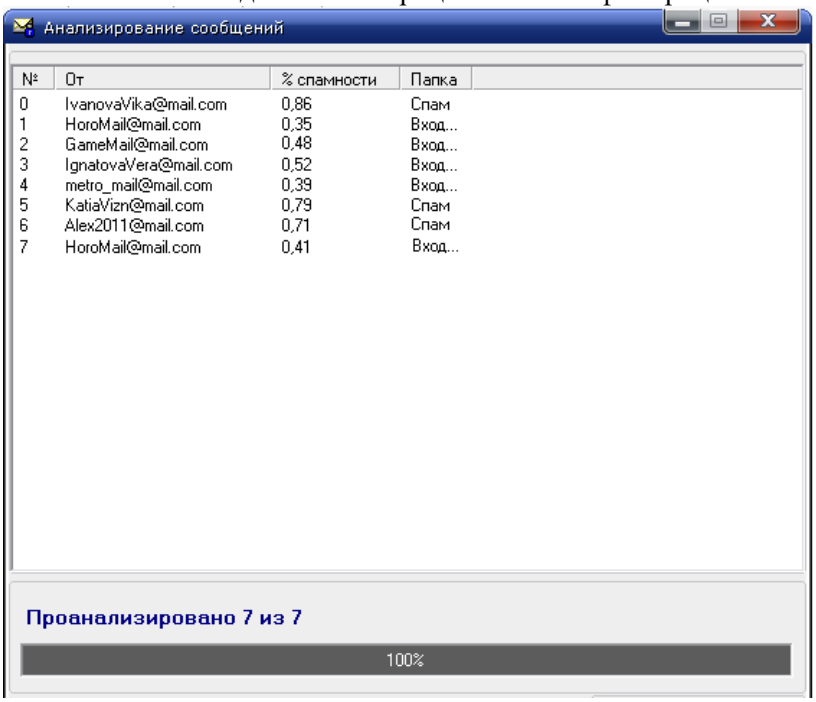


Рисунок 2.10 - Форма з результатом аналізу листів

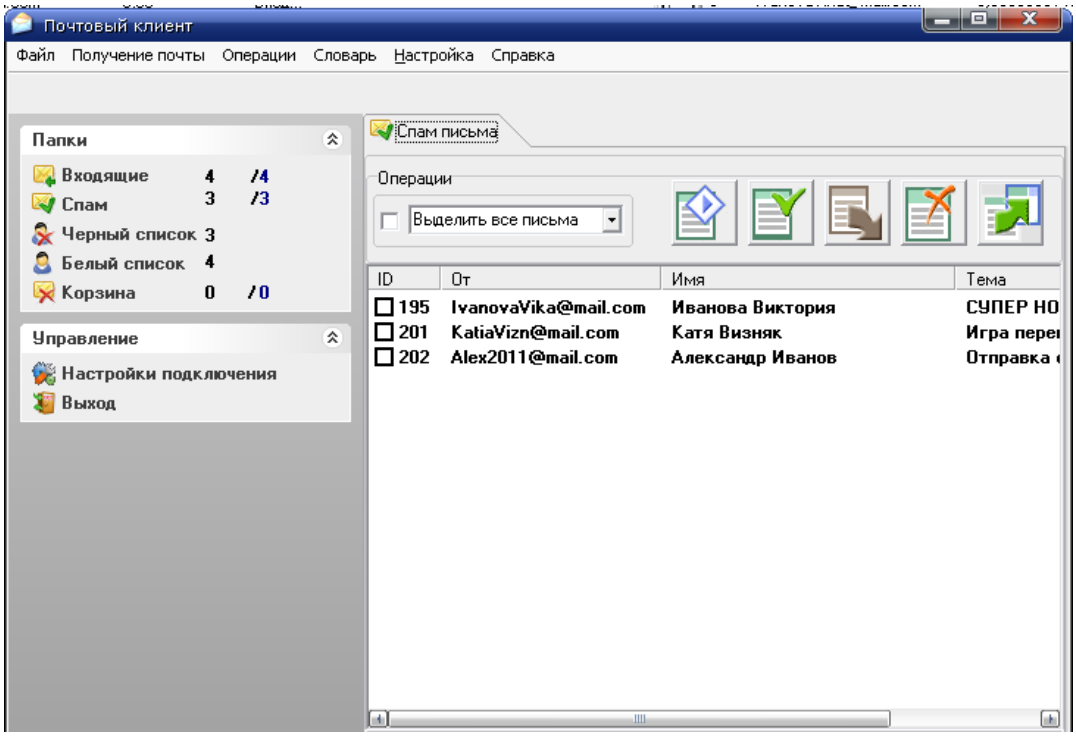


Рисунок 2.11 - Форма з прийнятим SPAMом

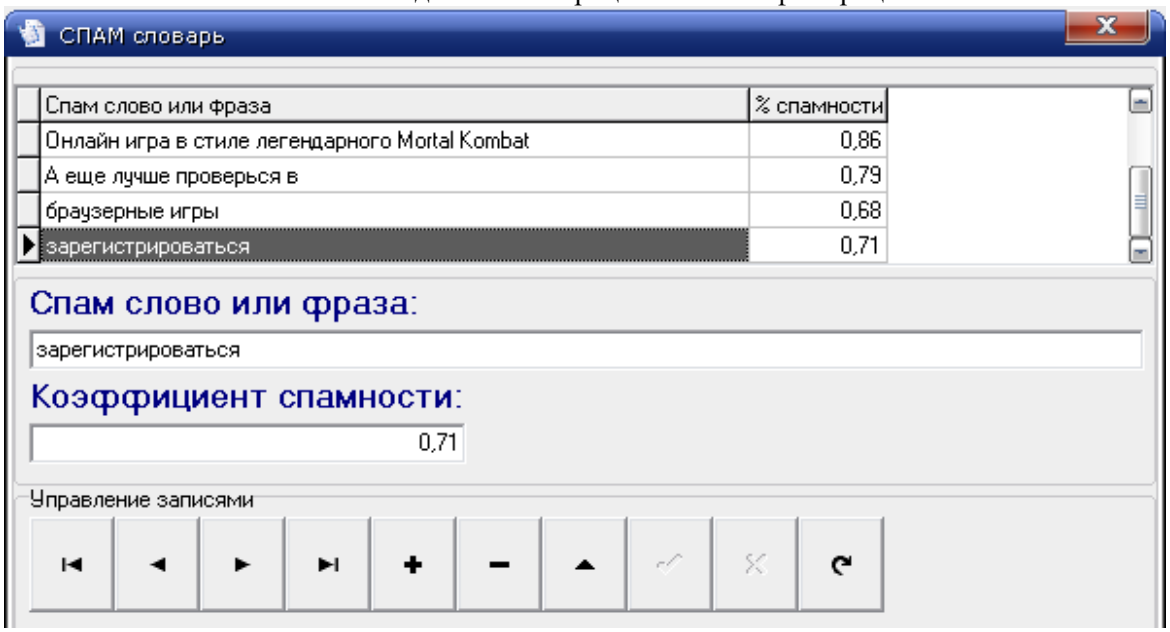


Рисунок 2.12 - Форма SPAM словника

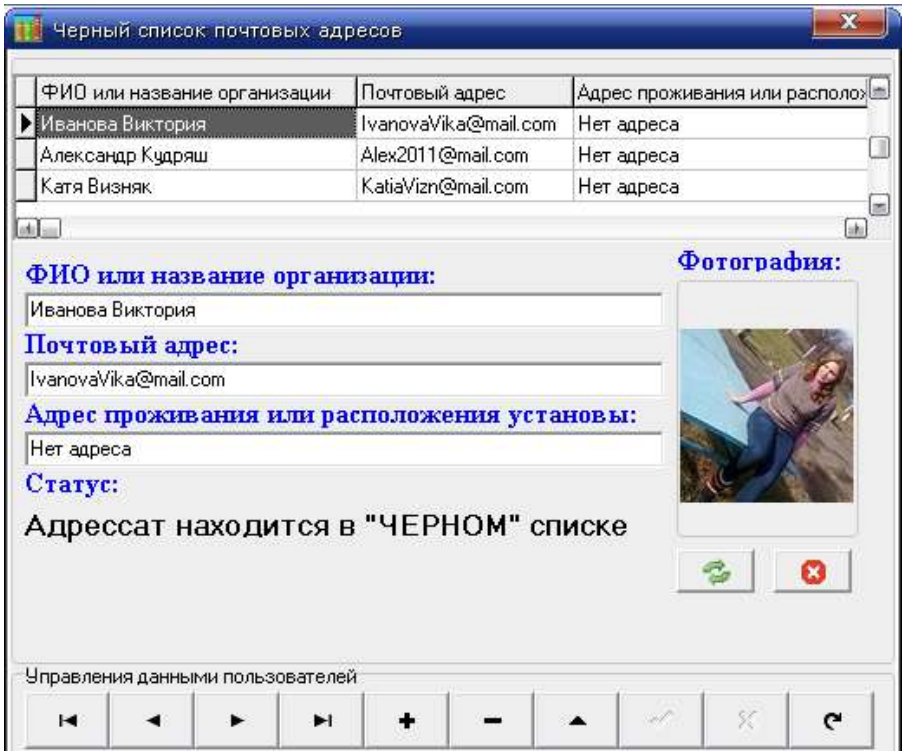


Рисунок 2.13 - Форма «Чорного списку»

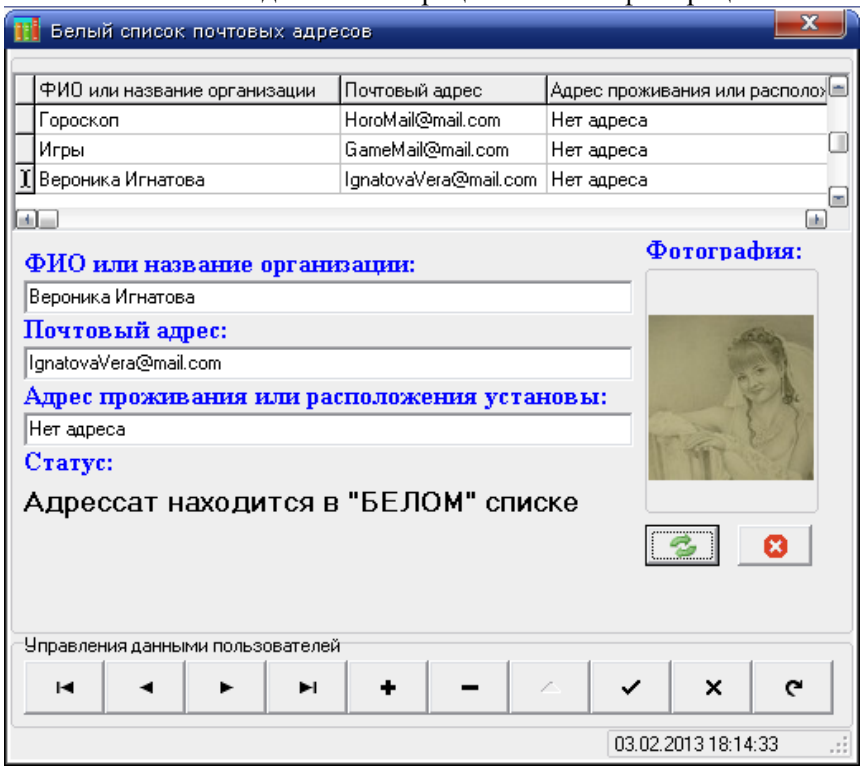


Рисунок 2.14 – Форма «Білий» список

Для керування повідомленнями використовується головна форма (рисунок 2.15).

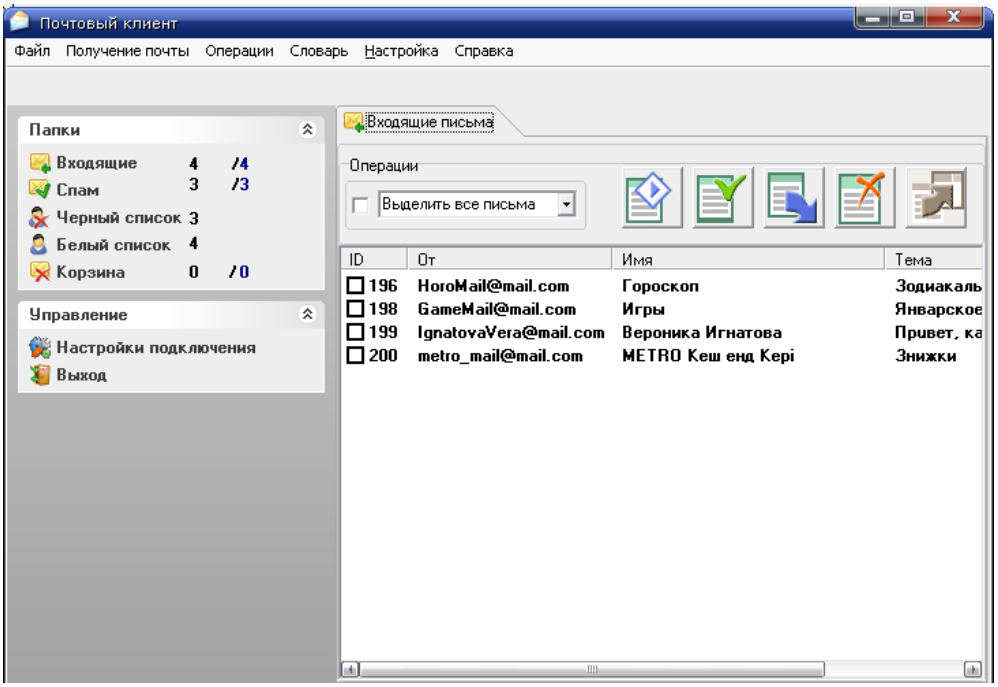


Рисунок 2.15 - Головна форма

Для відображення листів можна скористатися прапорцем біля спадного списку, що має кілька варіантів виділення (рисунок 2.16).

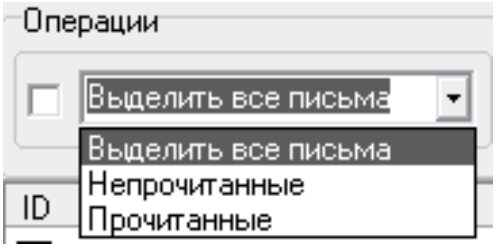


Рисунок 2.16 - Спадаюче меню розкривного списку

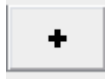
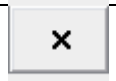
Для роботи з поштовими відправленнями передбачені кнопки, що мають функції, зазначені у таблиці 2.4.

Таблиця 2.4 - Процедури і функції фільтра SPAM-листів головної форми

Кнопка	Виконувана функція
	Помітити "НЕПРОЧИТАНИМ"
	Помітити "ПРОЧИТАНИМ"
	Перемістити в "СПАМ"
	Перемістити в "КОШИК"
	Відновити

У формі «Білий» список є можливість керування даними користувачів за допомогою кнопок, функції яких наведені у таблиці 2.5.

Таблиця 2.5 - Кнопки керування даними користувачів форми «Білий» список

Кнопка	Виконувана функція
	Перший запис
	Попередній запис
	Наступний запис
	Останній запис
	Додати запис
	Видалити запис
	Підтвердити зміни
	Видалити запис
	Обновити запис

В даному розділі описано функціональні можливості програмного комплексу «Поштовий Клієнт», призначеного для виявлення spam-листів у вхідній пошті. Лістинг головного модулю програми наведено в додатку Б.

3 РЕЗУЛЬТАТИ РОЗРОБКИ КОРПОРАТИВНОЇ СИСТЕМИ СПАМ-ФІЛЬТРАЦІЇ

3.1 Структурна схема потоків електронної пошти на підприємстві

Потоки електронної пошти на підприємстві організуються відповідно до політики з використання електронної пошти. Правила безпеки й інструкції можуть стати основою для скарг і судових процесів, але рятують від більших турбот, що заважають роботі організації й користувачів.

Політикою повинно бути передбачене:

- обмеження на особисту переписку співробітників із правом контролю компанією вхідної й вихідної електронної пошти.
- заборона співробітникам відповідати на spam або переходити за посиланнями, що містяться в ньому, у тому числі й за посиланнями «для відмови від розсилання»;
- заборона співробітникам завантажувати картинки при запиті поштового клієнта про дозвіл такого завантаження (якщо відправник не знайомий).

Політика підприємства повинна так само обмежувати вільне поширення електронної адреси компанії. Якщо буде потреба публікації адреси:

- використати CGI для зв'язку з користувачами замість публікації своєї адреси на сайті;
- представити адреса у вигляді картинки або представити в виді, який не читається, наприклад, «U_S_E_R_(a)_D_O_M_A_I_N_._N_E_T» із заміною на кирилицю схожих латинських символів.

Архітектура системи електронної пошти повинна забезпечувати належну доставку повідомлень як усередині організації, так і в Internet; система повинна допускати використання посередницьких програм, переадресації, шлюзів і ручного втручання в керування цією службою. Структурну схему потоків електронної пошти на типовому підприємстві зображено на рисунку 3.1.

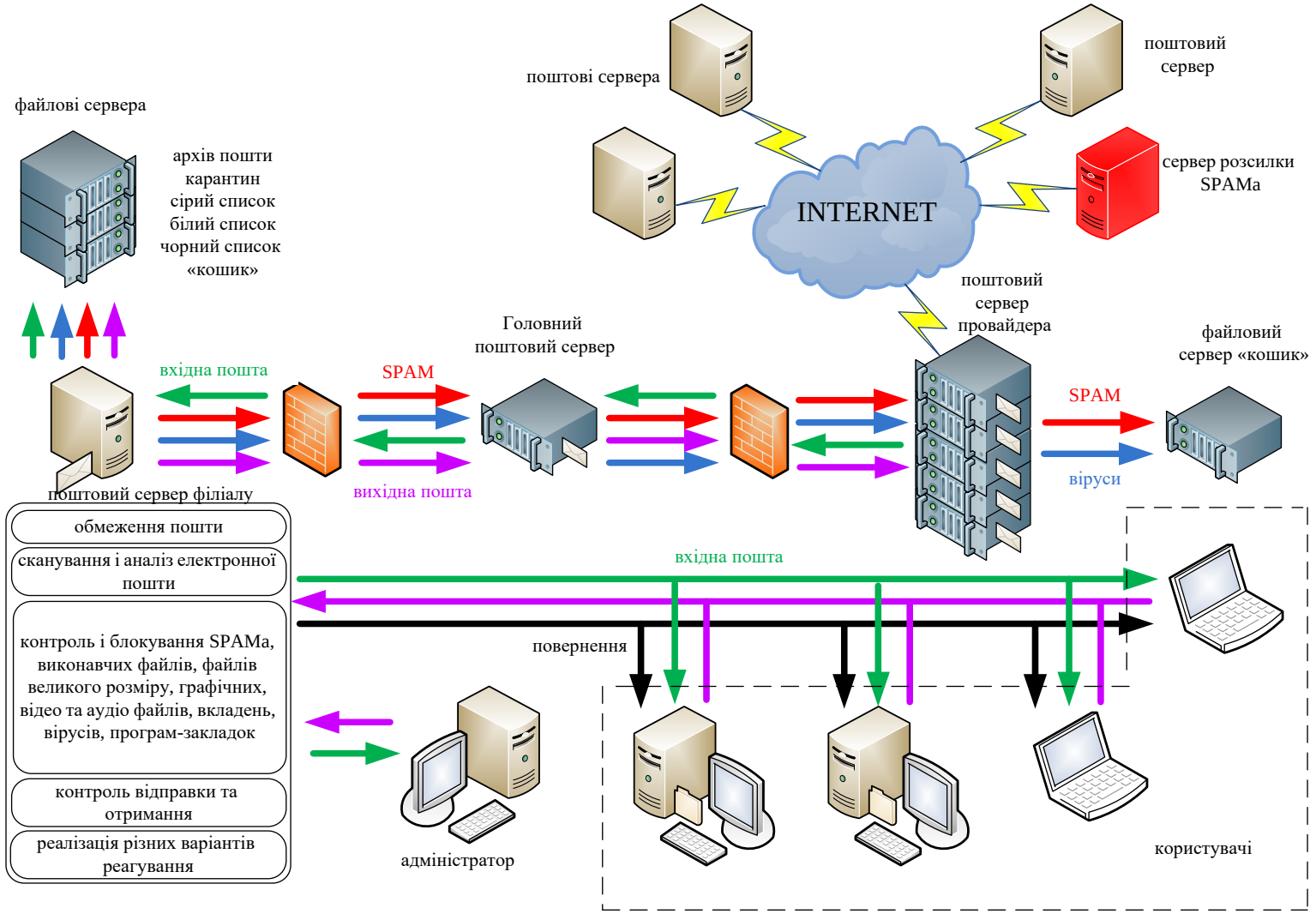


Рисунок 3.1 - Структурна схема потоків електронної пошти на підприємстві

3.2 Функціональні можливості системи

Архівування електронної пошти

Компанія архівує всі повідомлення, що надійшли й вихідні повідомлення електронної пошти, що проходять через його сервер, принаймні, три роки (строк позовної давності). На підставі інформації, що зберігається в архіві, можна проводити подальший аналіз поштового потоку компанії, коректувати роботу системи, здійснювати аналіз інцидентів, пов'язаних зі зловживаннями співробітниками компанії поштовим сервісом тощо.

Обмеження розмірів повідомлень електронної пошти

Інструкції підприємства повинні перешкоджати пересиланню даних, які приєднують до повідомлення, що вже зберігаються в системі (файлових серверах) або мережі; обмежувати розмір повідомлень електронної пошти, які відправляють і одержуються користувачами; передбачити виключення для користувачів, робота яких вимагає більших розмірів повідомлень (доступ до архіву для читання «своїх» листів). Адміністратор повинен розглядати й дозволяти виключення індивідуально.

Перенесення пересилки листів великого розміру

Пересилка листів великого розміру переноситься до того моменту, коли канал зв'язку менш завантажений (наприклад, вночі).

Контроль отримувача та відправника електронної пошти

Забезпечує фільтрацію поштового трафіку, реалізуючи частково при цьому функціональність міжмережного екрану (брандмауеру).

Сканування електронної пошти

Сканування вмісту листа забезпечує попередінй перегляд вмісту повідомлень на предмет витоку конфіденційної інформації, spam’у або вірусів.

Текстовий аналіз електронної пошти

Аналіз вмісту повідомлень електронної пошти за ключовими словами та виразами дозволяє виявити й вчасно запобігти витоку конфіденційної інформації, наявність забороненого змісту, зупинити розсилку SPAM. Аналіз тексту

повідомлень виконуються на основі семантичного аналізу, враховуючи лексико-граматичні граматичні конструкції слова.

Розбиття електронних листів на окремі частини

Розбір електронних листів на заголовки, тіло, окремо прикріплені файли забезпечує запобігання «небезпечних» прікріплень. Під час збору частин листа в одне ціле додається елемент результати перевірки (попередження щодо присутності вірусів).

Виявлення графічних, відео й звукових файлів

Мультимедійні файли займають великий розмір, тому їх пересилка електронною поштою може привести до втрати продуктивності мережних ресурсів. Можливість затримувати мультимедійні файли дозволяє підвищити продуктивність використання мережевих ресурсів.

Обробка стиснених/архівних файлів

Обробка стиснених/архівних файлів дає можливість перевіряти стислі файли на зміст у них заборонених матеріалів.

Розпізнавання exe-файлів

Exe-файли є файлами програм, мають великі розміри та найчастіше можуть будти заражені вірусами.

Контролювання спаму

Передача spam`у завантажує мережу. Тому наявність можливосю попередження та блокування spam`у забезпечує ефективне використання ресурсів мережі.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Чорноморський національний університет імені Петра Могили
Факультет комп'ютерних наук
Кафедра інтелектуальних інформаційних систем

Спеціальний розділ

ОХОРОНА ПРАЦІ

до кваліфікаційної роботи

на тему:

«СИСТЕМА МОДЕЛЮВАННЯ ПРОЦЕСІВ СПАМ-ФІЛЬТРАЦІЇ »

Спеціальність 122 «Комп'ютерні науки»

122 – БКР – 401з.210901101

Виконала сстудентка 4-го курсу, групи 401з
_____*В.В.Романець*
(підпис, ініціали та прізвище)
«___» _____ 202_ р.

Консультант:_____*ст. викладач каф. екології*
(наук. ступінь, вчене звання)
_____*Макарова О.В.*
(підпис, ініціали та прізвище)
«___» _____ 202_ р.

Миколаїв – 2022

4 ОХОРОНА ПРАЦІ

Використання комп'ютерної техніки, пов'язане з необхідністю рішення питань охорони праці користувачів комп'ютера.

Основоположним законодавчим документом в галузі охорони праці є Закон України "Про охорону праці", дія якого поширюється на всі підприємства, установи і організації незалежно від форм власності та видів діяльності, на усіх громадян, які працюють, а також залучені до праці на цих підприємствах. Цей закон визначає: «Охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності».

4.1Система управління охороною праці на підприємстві

Згідно з Законом України «Про охорону праці» та типовим положенням про службу охорони праці на будь-якому підприємстві незалежно від форми власності та виду діяльності, створюється комісія з питань охорони праці для організації виконання правових, організаційно-технічних, санітарно-гігієнічних, соціально-економічних і лікувально-профілактичних заходів, спрямованих на запобігання нещасним випадкам, професійним захворюванням і аваріям у процесі праці [20].

Основні завдання комісії з питань охорони праці підприємства:

- опрацювання ефективної системи управління охороною праці на підприємстві та сприяння удосконалення її діяльності кожного структурного підрозділу та кожного працівника;

-організація проведення профілактичних заходів, спрямованих на усунення шкідливих і небезпечних виробничих факторів, запобігання нещасним випадкам на виробництві;

- контроль за дотриманням працівниками вимог законів та інших актів з охорони праці;

- інформування та надання роз'яснень працівникам з питань охорони праці.

Документація при організації служби охорони праці оформлюється відповідно до вимог наступних документів:

- наказ про створення комісії з питань охорони праці;

- типові положення про комісію з питань охорони праці підприємства (ДНАОП 03.08.93 №72);

- закон України Про охорону праці;

- кодекс законів про працю України;

- державні міжгалузеві та галузеві нормативні акти про охорону праці, стандарти підприємства;

- положення про відділ з охорони праці.

У колективному договорі підприємства повинне передбачатися забезпечення працівникам соціальних гарантій у галузі охорони праці, а також комплексні заходи щодо досягнень встановлених нормативів безпеки, гігієни праці та виробничого середовища, підвищення існуючого рівня охорони праці, запобігання випадкам виробничого травматизму і професійних захворювань.

Працівники організації піддаються щорічним медичним оглядам.

Навчання та інструктаж працівників з питань охорони праці є складовою частиною системи управління охороною праці і провадиться з усіма працівниками в процесі їх трудової діяльності.

Періодично проводиться тестування співробітників на знання по охороні праці, що оформлюється протоколом.

Примірник інструкції з охорони праці повинен бути виданий працівникові за його професією або вивішений на його робочому місці.

Відповідно до п. 1.4. Типового положення про службу охорони праці СУОП створюється на підприємствах з кількістю працюючих 50 і більше осіб. Якщо підприємство має до 50 працівників, то функції служби охорони праці можуть виконувати особи з відповідною професійною підготовкою за сумісництвом. Передбачається, що при відсутності спеціалістів відповідної кваліфікації, можуть бути використані послуги асоціації спеціалістів з охорони праці [21].

При чисельності працюючих на підприємстві від 51 до 500 чоловік включно штат служби охорони праці складає один чоловік з інженерно- технічною освітою.

Сертифікація робіт з охорони праці здійснюється за допомогою перевірки і оцінки відповідності елементів діяльності роботодавця щодо забезпечення охорони праці державним нормативним вимогам охорони праці з урахуванням проведення атестації робочих місць за умовами праці та особливостей організації робіт з охорони праці в галузі зв'язку.

Практично усі заходи з охорони праці базуються на законодавчих і нормативних положеннях. Адміністрація для створення безпечних і нешкідливих умов праці працівників і для власної безпеки зобов'язана керуватися переліком основних нормативно-законодавчих актів і документів з охорони праці.

Аудит відповідності наявного переліку нормативно-правових актів існуючим вимогам приведено в таблиці 4.1.

Таблиця 4.1 - Нормативно-правова база з питань охорони праці

Нормативно-правові акти (Закони, накази, Положення, інструкції тощо)	Відповідність чинному законодавству
1) Закон України «Про охорону праці»	відповідає
2) Закон України «Про об'єкти підвищеної небезпеки»	відповідає
3) Типове положення про службу охорони праці	відповідає
4) Типове положення про навчання з питань охорони праці	відповідає
5) Типове положення про комісію з питань охорони	відповідає

праці	
6) Положення про розробку інструкцій з охорони праці	відповідає
7) Положення про медичний огляд працівників певних категорій	відповідає
8) Положення про порядок забезпечення працівників спеціальним одягом, спеціальним взуттям та іншими засобами індивідуального захисту	відповідає

Продовженння таблиці 4.1

9) Перелік посад, посадових осіб, які зобов’язані проходити попередню і періодичну перевірку знань з охорони праці	відповідає
10) Порядок проведення атестації робочих місць за умовами праці	відповідає
11) Положення про систему управління охороною праці	відповідає

4.2 Аналіз небезпечних і шкідливих факторів умов праці

Найбільш негативним фактором впливу на співробітників будь-якого офісного підприємства є комп'ютери.

Виробнича діяльність операторів ПК має свої особливості, під впливом яких можуть формуватись розлади здоров'я [22]. До найважливіших факторів, характерних для роботи операторів ПК, що впливають на погіршення стану їх ЦНС належать:

- інформаційне перевантаження мозку в поєднанні з дефіцитом часу;
- тривожне очікування інформації, особливо тієї, що викликає необхідність прийняти рішення;
- велике зорове та нервово-емоційне напруження;
- гіподинамія;
- монотонія;

- висока відповідальність за кінцевий результат;
- тривала ізоляція у спілкуванні, зумовлена індивідуальним характером праці за ПК.

При експлуатації, відповідно до встановлених гігієнічно-санітарних вимог (ГОСТ 12.1.005-88, СН 4088-86) інститут підприємство зобов'язане забезпечити в приміщеннях з ПК оптимальні параметри виробничого середовища (таблиця 4.2).

Таблиця 4.2 – Норми мікроклімату для приміщень з ВТД

Пора року	Категорія робіт	Температура повітря, С, не більше	Відносна вологість повітря, %	Швидкість руху повітря, м/с
Холодна	Легка - 1 а	22...24	4...6	0,1
	Легка - 1 б	21...23	4...6	0,1
Тепла	Легка - 1 а	23...25	4...6	0,1
	Легка - 1 б	22...24	4...6	0,2

Природне освітлення в приміщеннях з ПК має здійснюватися через вікна, орієнтовані переважно на північ або північний схід і забезпечувати коефіцієнт природної освітленості не нижче ніж 1,5 %. Для захисту від прямих сонячних променів, які створюють прямі та відбиті відблиски з поверхні екранів ПК і клавіатури повинні бути передбачені сонцезахисні пристрої, вікна повинні мати жалюзі або штори.

Основні вимоги до виробничого приміщення для експлуатації ПК:

- воно не може бути розміщено у підвалах та цокольних поверхах;
- площа на одне робоче місце в такому приміщенні повинна становити не менше 6,0 м^2, а об'єм не менше 20,0 м^3;
- воно повинно мати природне та штучне освітлення відповідно до СНіПП-4-79;
- в ньому мають бути шафи для зберігання документів, магнітних дисків, полиці, стелажі, тумби тощо, з урахуванням вимог до площі приміщення;
- щоденно проводити вологе прибирання;

– поруч з приміщенням для роботи з ПК мають бути обладнані:

– побутова кімната для відпочинку під час роботи;

– кімната психологічного розвантаження.

Штучне освітлення в приміщеннях з робочим місцем, обладнаним ПК, має здійснюватися системою загального рівномірного освітлення. Як джерело штучного освітлення мають застосовуватись люмінесцентні лампи ЛБ [23].

Вимоги до освітлення приміщень та робочих місць під час роботи з ПК:

– освітленість на робочому місці повинна відповідати характеру зорової роботи, який визначається трьома параметрами: об'єктом розрізнення - найменшим розміром об'єкта, що розглядається на моніторі ПК; фоном, який характеризується коефіцієнтом відбиття; контрастом об'єкта і фону;

– необхідно забезпечити достатньо рівномірне розподілення яскравості на робочій поверхні монітора, а також в межах навколишнього простору;

– на робочій поверхні повинні бути відсутні різкі тіні;

– в полі зору не повинно бути відблисків (підвищеної яскравості поверхонь, які світяться та викликають осліплення);

– величина освітленості повинна бути постійною під час роботи;

– слід обирати оптимальну спрямованість світлового потоку і необхідний склад світла.

Гігієнічні норми до організації і обладнання робочих місць з ПК. При розташуванні елементів робочого місця користувача ПК слід враховувати [23]:

– робочу позу користувача;

– простір для розміщення користувача;

– можливість огляду елементів робочого місця;

– можливість ведення захистів;

– розміщення документації і матеріалів.

Конструкція робочого місця користувача ПК має забезпечити підтримання оптимальної робочої пози. Робочі місця з ПК слід так розташувати відносно вікон, щоб природне світло падало збоку, переважно зліва.

Робочі місця з ПК повинні бути розташовані від стіни з вікнами на відстані не менше 1,5 м, від інших стін — на відстані 1 м, відстань між собою - не менше ніж 1,5 м.

Для забезпечення точного та швидкого зчитування інформації в зоні найкращого бачення площина екрана монітора повинна бути перпендикулярною нормальній лінії зору. При цьому повинна бути передбачена можливість переміщення монітора навколо вертикальної осі в межах ±30° (справа наліво) та нахилу вперед до 85° і назад до 105° з фіксацією в цьому положенні.

Клавіатура повинна бути розташована так, щоб на ній було зручно працювати двома руками. Клавіатуру слід розміщати на поверхні столу на відстані 100...300 мм від краю. Кут нахилу клавіатури до столу повинен бути в межах від 5 до 15°, зап'ястя на долонях рук повинні розташовуватись горизонтально до площини столу.

Принтер повинен бути розміщений у зручному для користувача положенні, так, що максимальна відстань від користувача до клавіш управління принтером не перевищувала довжину витягнутої руки користувача.

Конструкція робочого стола повинна забезпечувати можливість оптимального розміщення на робочій поверхні обладнання, що використовується, з врахуванням його кількості та конструктивних особливостей (розмір монітора, клавіатури, принтера, ПК та ін.) і документів, а також враховувати характер роботи, що виконується.

Тривалість регламентованих перерв під час роботи з ЕОМ за восьми годинної денної робочої зміни залежно від характеру праці: 15 хвилин через кожну годину роботи - для розробників програм зі застосуванням ЕОМ; 15 хвилин через кожні дві години - операторів із застосуванням ЕОМ; 10 хвилин після кожної години роботи за ПК для операторів комп'ютерного набору.

Дотримання вимог цих правил може значно знизити наслідки несприятливої дії на працівників підприємства, шкідливих та небезпечних факторів, які супроводжують роботу з відеодисплейними матеріалами, зокрема можливість

зорових, нервово-емоційних переживань, серцево-судинних захворювань.

Електробезпека при роботі з комп'ютером

Електричні установки, до яких відноситься практично усе устаткування ЕОМ, представляють для людини велику потенційну небезпеку, оскільки в процесі експлуатації або проведенні профілактичних робіт людина може торкнутися частин, що знаходяться під напругою [22].

Будь-яка дія струму може привести до електричної травми, тобто до ушкодження організму, викликаного дією електричного струму або електричної дуги .

При розгляді питання забезпечення електробезпеки розробника необхідно виділити три основні чинники:

електроустановки робочого місця програміста;

допоміжне електроустаткування;

довкілля приміщення.

До електрооблаштувань робочого місця відносяться: комп'ютер, відеомонітор, принтер. До допоміжного устаткування відносяться лампи місцевого освітлення, вентилятори і інші електричні прилади. Електроустаткування, перелічене вище, відноситься до установок напругою до 1000 В.

Довкілля приміщень, впливає на електричну ізоляцію приладів і пристроїв, електричний опір тіла людини і може створювати умови для поразки електричним струмом.

Приміщення, обладнані обчислювальною технікою, як правило, належать до категорії приміщень без підвищеної небезпеки оскільки:

відносна вологість повітря не перевищує 75 %;

немає струмопровідного пилу;

температура не перевищує тривалий час +30 градусів;

відсутня можливість одночасного дотику людини з тими, що мають з'єднання із землею металевими конструкціями;

відсутність доступу до токоведущим частин устаткування;

немає струмопровідних підлог.

Таким чином, для запобігання електротравматизму користувача, необхідно дотримуватися вимог безпеки, як при роботі із звичайною побутовою технікою.

Пожежобезпека при роботі з комп'ютером

Відповідно ГОСТ 12.1.004-91 ССБТ Приміщення належить до категорії Д по взривопожаронебезпеці, оскільки не містить горючих речовин, але лише негорючі речовини і матеріали в холодному стані [22].

Пожежі в приміщенні, в якому знаходиться ЕОМ, представляють особливу небезпеку, оскільки зв'язані з великими матеріальними втратами. Як відомо пожежа може виникнути при взаємодії горючих речовин, окислення і джерел запалення. У приміщенні є присутніми усі три основні чинники, необхідні для виникнення пожежі. Горючими компонентами є: будівельні матеріали для акустичної і естетичної обробки приміщень, дверей, поли, папір, ізоляція кабелів та ін.

Протипожежний захист - це комплекс організаційних і технічних заходів, спрямованих на забезпечення безпеки людей, на запобігання пожежі, обмеження його поширення, а також на створення умов для успішного гасіння пожежі.

Джерелами запалення в приміщенні, що містить ЕОМ, можуть бути електронні схеми від ЕОМ, прилади, вживані для технічного обслуговування, облаштування електроживлення, де в результаті різних порушень утворюються перегріті елементи, електричні іскри і дуги, здатні викликати загоряння горючих матеріалів.

У сучасних ЕОМ дуже висока щільність розміщення елементів електронних схем. У безпосередній близькості один від одного розташовуються сполучні дроти, кабелі. При протіканні по них електричного струму виділяється значна кількість теплоти. При цьому можливе оплавлення ізоляції. Для відведення надмірної теплоти від ЕОМ служать системи вентиляції і кондиціонування повітря. При постійній дії ці системи є додатковою пожежною небезпекою.

Приміщення офісного підприємства необхідно обладнати засобами сповіщення про пожежу, а також засобами для гасіння пожежі - порошковими вогнегасниками.

ВИСНОВКИ

Результатом даної роботи є програмний продукт - корпоративний spam-фільтр «Поштовий клієнт», що працює на рівні протоколу POP3 і аналізує вхідну пошту користувачів.

Поставлена мета – дослідження методів спам-фільтрації, розробка системи фільтрації spam-листів, що дозволяє підвищити загальний рівень безпеки підприємства та зменшити час, що витрачається на розбір непотрібної кореспонденції, в результаті написання дипломної роботи досягнута.

Для досягнення мети були виконані наступні завдання:

– розглянуті технічні методи фільтрації spam-листів;

– вивчені можливості поштових протоколів для боротьби з непотрібною кореспонденцією;

– реалізовані алгоритми фільтрації листів.

В даний час здійснюється тестування програмного продукту.

Дешевизна електронної пошти, а також недосконаліть поштових протоколів, роблять даний спосіб вельми привабливим для поширення інформації. У зв'язку з цим, як показала практика, кількість spam-листів у загальному трафіку листів буде постійно збільшуватися, а зловмисники будуть шукати нові способи обходу spam-фільтрів. Вирішити проблему spam-листів раз і назавжди не представляється можливим у найближчому майбутньому. Можна лише підтримувати певний рівень фільтрації шляхом постійного відстежування нових видів spam-листів і розробки методів їх виявлення.

Дані факти ще раз підкреслюють перспективність розроблюваної теми та актуальність даного програмного комплексу.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Антиспам без секретов. практические рекомендации по борьбе с нелегальной расснлкой по электронной почте [PDF] [7p9imgi5pe80]. *E-book library. Search and download for free, instantly.* URL: https://vdoc.pub/documents/-7p9imgi5pe80 (дата звернення: 19.05.2022).

2. Вред от спама. *Энциклопедия «Касперского»*. URL: https://encyclopedia.kaspersky.ru/knowledge/damage-caused-by-spam/#:~:text=Нагрузка%20на%20коммуникации.,идет%20о%20рабочем%20почтовом%20ящике). (дата звернення: 19.05.2022).

3. Тематики спама. *Энциклопедия «Касперского»*. URL: https://encyclopedia.kaspersky.ru/knowledge/types-of-spam/#:~:text=Лидирующие%20тематики%20спама:&text=Медикаменты;%20товары%20и%20услуги%20для,Образование. (дата звернення: 19.05.2022).Спам и фишинг. Энциклопедия «Касперского». URL: http://surl.li/cfzda.

4. Спам, види спаму і боротьба зі спамом - Спам і боротьба із спамом - - Статті про віруси, антивіруси і антивірусні програми - Безкоштовні програми для комп'ютера. *Безкоштовні програми для комп'ютера - Безкоштовні антивіруси і антивірусні програми*. URL: https://best-free-soft.at.ua/publ/spam_vidi_spamu_i_borotba_zi_spamom/1-1-0-33 (дата звернення: 01.05.2022).

5. Учасники проектів Вікімедіа. Спам – вікіпедія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Спам (дата звернення: 01.05.2022).

6. Contributors to Wikimedia projects. Байесовская фильтрация спама – Википедия. *Википедия – свободная энциклопедия*. URL: https://ru.wikipedia.org/wiki/Байесовская_фильтрация_спама (дата звернення: 01.05.2022).

7. Учасники проектів Вікімедіа. Прихована марковська модель – Вікіпедія. *Вікіпедія*.

URL: https://uk.wikipedia.org/wiki/Прихована_марковська_модель (дата звернення: 01.05.2022).

8. Про інформацію. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 12.05.2022).

9. Цивільний кодекс України. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 12.05.2022)..

10. Про захист персональних даних. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 12.05.2022).

11. Про захист прав споживачів. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/1023-12#Text (дата звернення: 12.05.2022).

12. Про затвердження Правил надання та отримання телекомунікаційних послуг. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/295-2012-п/page (дата звернення: 12.05.2022).

13. Про рекламу. Офіційний вебпортал парламенту України. URL: http://zakon2.rada.gov.ua/laws/show/270/96-вр (дата звернення: 12.05.2022).

14. МНУ ім. В.О.Сухомлинського. URL: http://mdu.edu.ua/wp-content/uploads/gmit084.pdf (дата звернення: 14.05.2022).

15. Рудикова Л.В. Базы данных. Разработка приложений (для студента). *Учебно-методическая литература для учащихся и студентов. Студенческие работы, курсовые, контрольные, рефераты, ГДЗ*. URL: https://www.studmed.ru/rudikova-lv-bazy-dannyh-razrabotka-prilozheniy-dlya-studenta_4aa881dff2f.html (дата звернення: 19.05.2022).

16. Федоров А. елманова Л. - введение в OLAP .pdf. *DocMe.su: Сервис публикации документов*. URL: https://www.docme.su/doc/1763275/fedorov-a.--elmanova-l.---vvedenie-v-olap-.pdf (дата звернення: 19.05.2022).

17. Ульман Д. Базы данных на паскале. Москва : Машиностроение, 1990. 367 с.

18. SQL в Access: основні поняття, глосарій і синтаксис. *Microsoft Support*. URL: https://support.microsoft.com/uk-ua/office/sql-в-access-основні-поняття-глосарій-і-синтаксис-444d0303-cde1-424e-9a74-e8dc3e460671 (дата звернення: 27.05.2022).

19. Про охорону праці. *Офіційний вебпортал парламенту України*. URL: https://zakon.rada.gov.ua/laws/show/2694-12#Text (дата звернення: 27.05.2022).

20. ZakonOnline. Лист № 1.4/18-848 від 21.03.2011 Про типові програми навчальних. *Аналітично-правова система ZakonOnline*. URL: https://zakononline.com.ua/documents/show/125054___125054 (дата звернення: 27.05.2022).

21. Гандзюк М.П., Желібо Є. П., Халімовський М.О. Основи охорони праці. *Учебно-методическая литература для учащихся и студентов. Студенческие работы, курсовые, контрольные, рефераты, ГДЗ*. URL: https://www.studmed.ru/gandzyuk-m-p-zhel-bo-p-hal-movskiy-m-o-osnovi-ohoroni-prac-_7990db79f7e.html (дата звернення: 26.05.2022).

22. Основи охорони праці - бібліотека buklib.net. *Головна - Бібліотека BukLib.net*. URL: https://buklib.net/books/21960/ (дата звернення: 27.05.2022).

ДОДАТОК А

Установка програми «Поштовий клієнт»

Для установки програми треба запустити файл «Setup mail client.exe» і далі слід виконати інструкцію із зазначенням потрібних параметрів (рисунки В.1 – В.7).

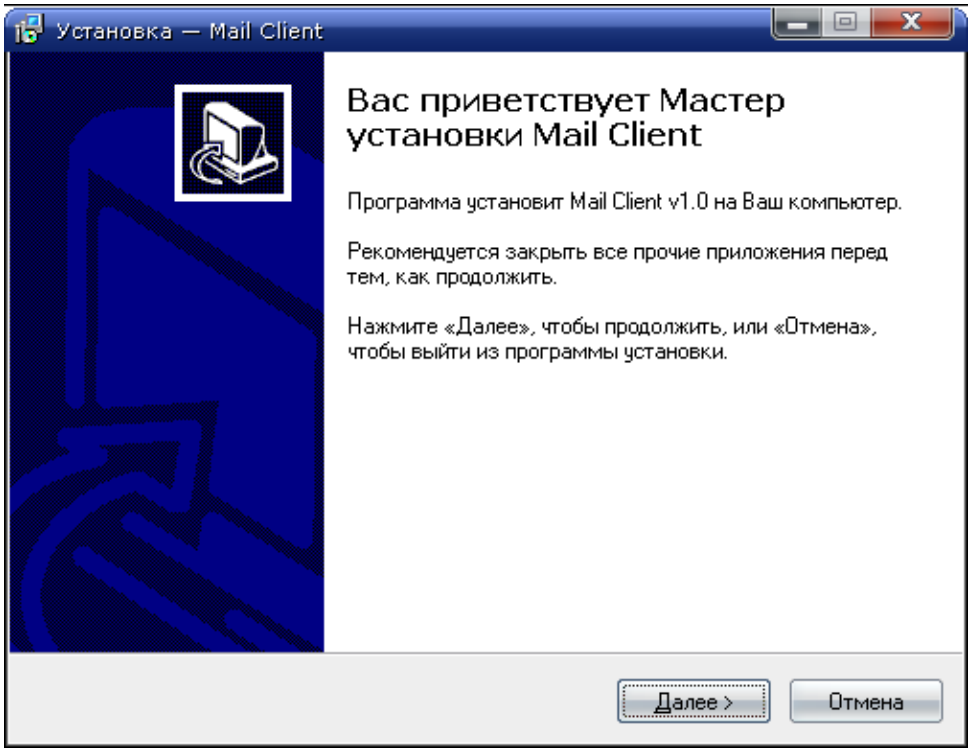


Рисунок В.1 - Майстер установки

На наступній формі зазначена папка для установки програми по типовому значенню, також є можливість вибору іншої папки якщо нажати «Огляд». Після цього натискається «Далі».

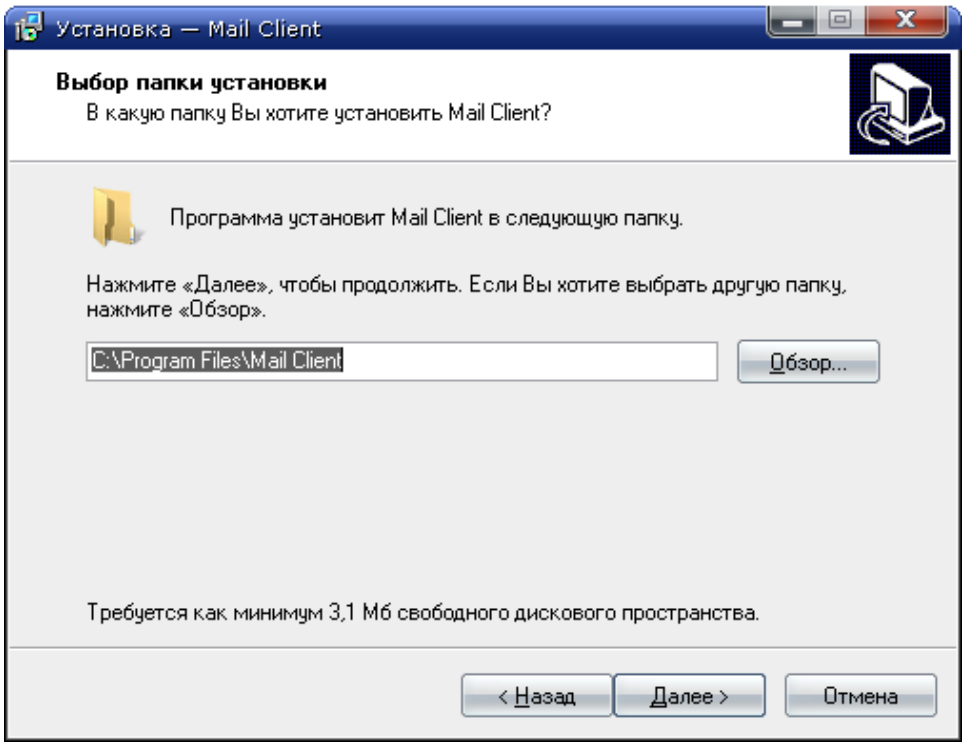


Рисунок В.2 - Вибір місця зберігання

На наступній формі вказується ім'я папки в меню ПУСК.

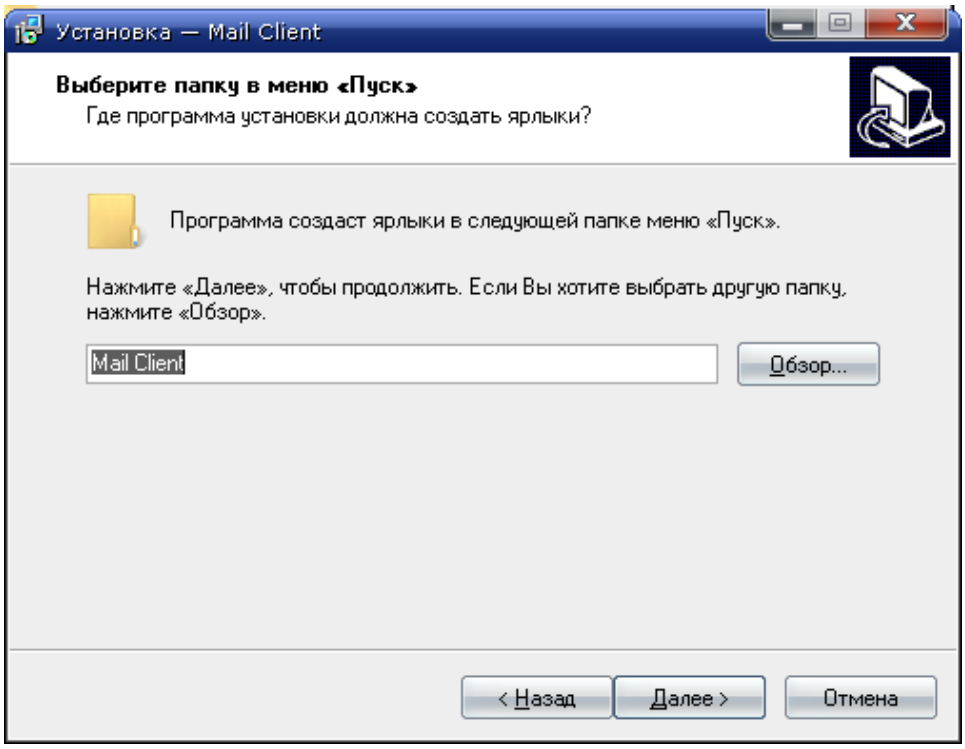


Рисунок В.3 - Вибір папки в меню «Пуск»

Для створення ярлика на робочому столі треба поставити позначку напроти пропозиції й натиснути «Далі»

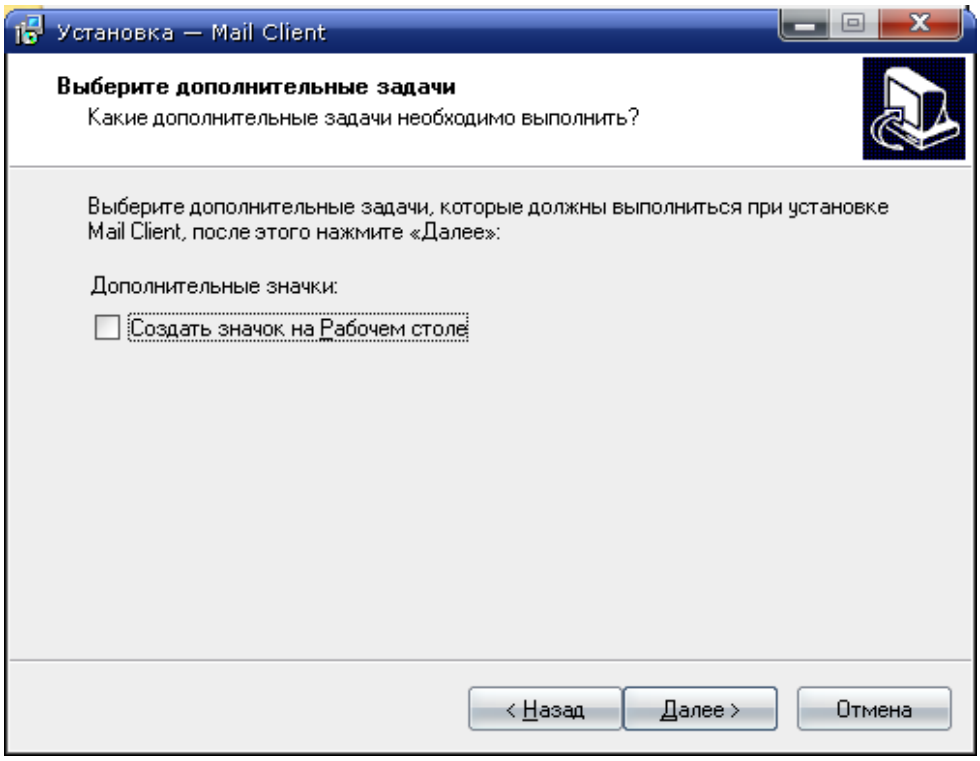


Рисунок В.4 - Пропозиція створити іконку запуску на робочому столі

Для установки програми натискується «Установити»

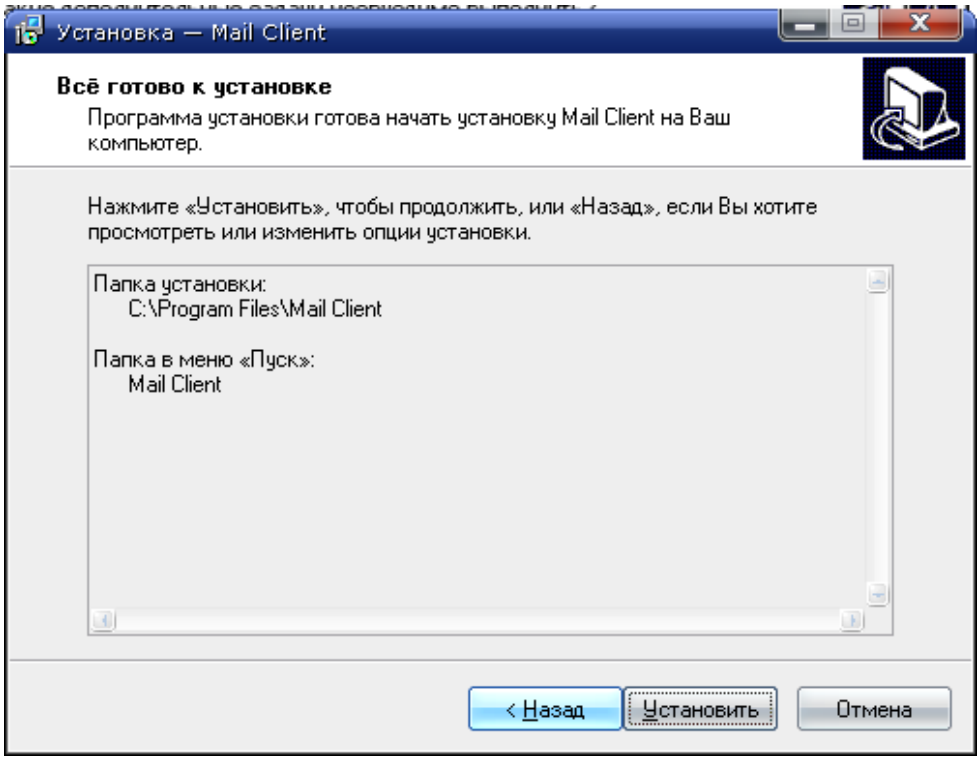


Рисунок В.5 - Перевірка уведених параметрів

По закінченні установки натискується «Завершити» із запуском програми або без вищезазначеного.

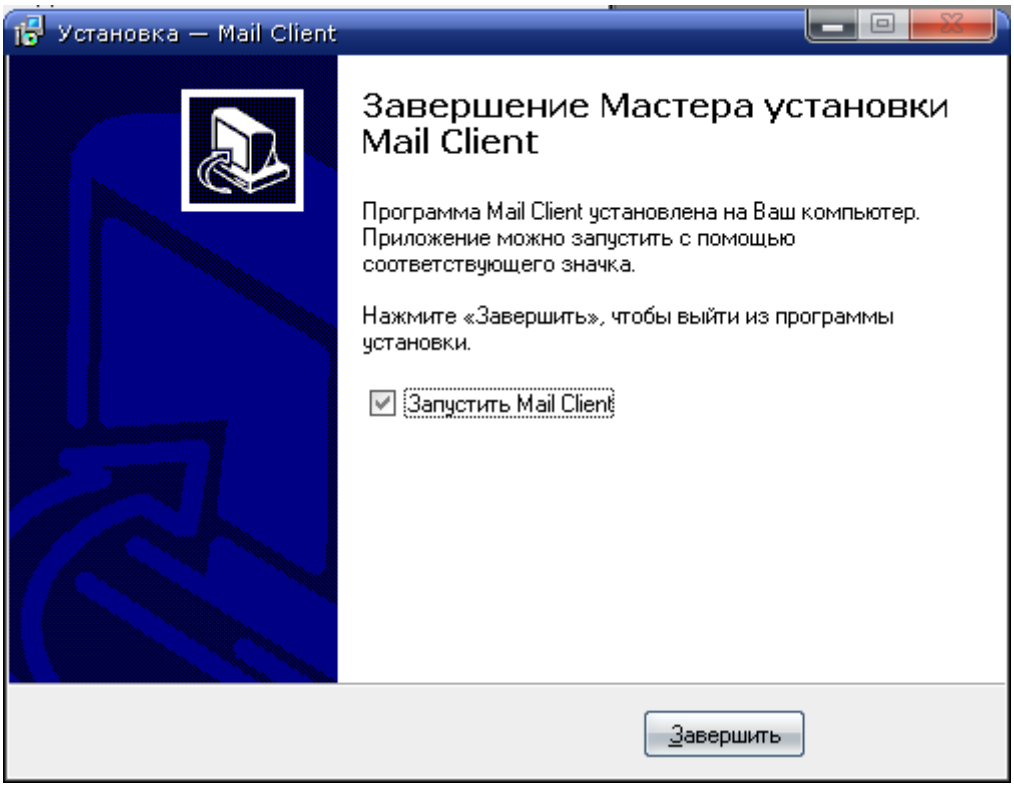


Рисунок В.6 - Завершення установки програми

Етап встановлення програмного продукту завершений. Відтепер програму можна запустити через «Пуск-Mail Client-Mail Client.exe» або видалити через «Пуск-Mail Client-Деінсталювати Mail Client».

Рисунок В.7 - Програма в меню «Пуск»