math_2022_037

Міністерство освіти і науки України

Чернівецький національний університет

імені Юрія Федьковича

Факультет математики та інформатики
(повна назва інституту/факультету)

Кафедра математичного моделювання
(повна назва кафедри)

Розробка веб-додатку для верифікації електронних адрес з використанням Abstract API

Кваліфікаційна робота

Рівень вищої освіти - другий (магістерський)

Виконала:
студентка 6 курсу, групи 607
спеціальності 124 – Системний аналіз
(назва спеціальності)
Дибкалюк Юлія Володимирівна
(прізвище, ім'я та по-батькові)
Керівник проф. Черевко І.М.
(науковий ступінь, вчене звання, прізвище та ініціали)

До захисту допущено:

Протокол засідання кафедри № __

від „___" грудня 2022 р.

зав. кафедри _____ проф. Черевко І.М.

Чернівці – 2022

Анотація

У роботі здійснено огляд сервісу електронної пошти, проаналізовано найбільш популярні постачальники електронної пошти, описано явище спаму та способи захисту від нього. Наведено опис та аналіз різних інструментів для верифіації та валідації електронних адрес, їх особливості та прикладні інтерфейси.

Розроблено веб-додаток засобами мови програмування JavaScript для валідації та верифіації електронних адрес використовуючи Abstract API.

Abstract

The paper reviews the e-mail service, analyzes the most popular e-mail providers, describes the phenomenon of spam and methods of protection against it. A description and analysis of various tools for verification and validation of electronic addresses, their features and application interfaces are given.

A web application was developed using the JavaScript programming language for validating and verifying email addresses using the Abstract API.

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів наукових досліджень інших авторів мають посилання на відповідне джерело.

_____ Ю.В. Дибкалюк
(підпис)

Зміст

Вступ

Електронна пошта — відомий сервіс для обміну повідомленнями та файлами, який використовується як для простого спілкування, так і для корпоративного. Сучасні постачальники послуг електронної пошти окрім зручного інтерфейсу надають додаткові інструменти для організації роботи: календар, адресна книга, синхронізація з іншими пристроями.

Даний сервіс зручно використовувати для розсилки. Але для того, щоб розсилка була ефективною потрібно переконатись в дійсності електронних адрес у списку розсилки. Це допоможе уникнути потраплянню листів до папки зі спамом та відправлення повідомлення на вже неіснуючі або невалідні адреси. Після таких дій буде можливість краще оцінити ефективність розсилки.

В даній роботі описані відомі інструменти для верифіації та валідації електронних адрес, їх особливості та прикладні інтерфейси.

Використовуючи платформу Node.js та мову програмування JavaScript розроблено веб додаток, за допомогою якого можна зручно перевірити електронні адреси. Для перевірки застосовується прикладний інтерфейс Abstract API.

1.Електронна пошта

Електронна пошта (від англ. electronic — електронна, mail — пошта) — це спосіб надсилання та отримання текстових повідомлень та прикріплених до них файлів у вигляді листів через Інтернет з використанням цифрових пристроїв таких як комп'ютери та мобільні телефони.

Сучасні системи електронної пошти базуються на моделі зберігання й пересилання. Сервери електронної пошти приймають, пересилають, доставляють і зберігають повідомлення. Ні користувачі, ні їхні комп’ютери не зобов’язані одночасно бути онлайн. Щоб надіслати або отримати повідомлення, їм потрібно підключитися, як правило, до поштового сервера або інтерфейсу веб пошти.

Її схожість на звичайну пошту полягає в тому, що обидві передають повідомлення. Проте електронна пошта зараз є однією з найбільш використовуваних.

1.1. Переваги електронної пошти

Існує багато переваг електронної пошти та використання електронної пошти порівняно з традиційною. Цей вид зв'язку дозволяє ефективно передавати інформацію в режимі реального часу, до того ж в найрізноманітнішому вигляді.

Користування електронною поштою не вимагає додаткових витрат, що робить цю форму передачі інформації наразі найдешевшою. Сплачується лише підключення до мережі Інтернет, тобто не потрібно платити за кожне відправлене і отримане повідомлення.

Електронна пошта є швидкою та простою в використанні. Створений електронний лист легко може бути надісланий та отриманий адресатом в будь-якій точці світу через Інтернет.

Також вона дозволяє виключити помилки, можливі при передрукуванні інформації, і не вимагає додаткової перевірки та вичитування. Передача

інформації, за допомогою електронної пошти, чітко фіксується як у відправника так і в одержувача. У відповідних директоріях вказуються число, година і хвилина відправлення й отримання інформації.

Крім того, якщо інформація не була отримана адресатом, це також фіксується як невідправлена кореспонденція. Все це дозволяє чітко враховувати відправлену і отриману пошту без додаткових витрат часу і зусиль на її реєстрацію.

Надіслані та отримані повідомлення можна безпечно зберігати та легко шукати. Незалежно від місця перебування можна отримати доступ до папки "Вхідні" та переглянути свої повідомлення разом із прикріпленими файлами до них, за умови підключення до Інтернету. Набагато легше переглядати старі повідомлення електронної пошти, ніж старі замітки, написані на папері.

Оскільки електронна пошта є безпаперовою, зменшуються витрати на папір, що фактично зменшує шкоду, яку використання паперу завдає навколишньому середовищу.

До переваг також можна віднести досить масове охоплення, масштаби якого включають всіх користувачів мережі Інтернет. Електронна пошта дозволяє краще вивчати й обслуговувати споживачів фірми, активно розвивати ділові відносини з її партнерами. При цьому практично миттєво можна зробити скільки завгодно копій інформації і в разі потреби доповнити і розіслати її за потрібними адресами, що також значно спрощує роботу з матеріалами і документами в компанії. Техніка і час передачі інформації численним адресатам такі ж зручні, як і для передачі інформації одному респонденту.

Електронна пошта дозволяє відправляти й отримувати повідомлення різного виду: не тільки набрані текстові повідомлення, але і файли з баз даних, текстові файли, фотографії, таблиці, аудіо повідомлення. В цьому випадку інформація передається в електронному форматі, що дозволяє відправникові і одержувачеві не витрачати часу на її додаткову обробку,

оскільки відсутня необхідність введення друкарської інформації або її перетворення в електронну форму.

В залежності від провайдера, існують різні інструменти підвищення продуктивності: календар, адресна книга, доступ до веб-сервісів. Наприклад, все більш стає популярною можливість для реєстрації використовуючи обліковий запис електронної пошти.

В даний час одним з основних видів зв'язку між компаніями та між компаніями і споживачами є електронна пошта. У ряді країн вже видані законодавчі акти, що підтверджують право враховувати цифрові підписи в комерційних документах (контрактах, угодах та ін.), які пересилаються електронною поштою. За правовим статусом він прирівнюється до власноручного підпису (печатки) у разі, якщо електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису [1].

Цінною перевагою електронної пошти в порівнянні зі звичайною також є можливість швидкої розсилки одного повідомлення за багатьма адресами відразу. Це знайшло відображення ще в одній з важливих можливостей електронної пошти — списках розсилки (англ. mailing lists). Вони полегшують листування з іншими користувачами, які мають спільні інтереси.

Повідомлення, відправлене на поштовий сервер, буде розіслане всім, хто підписався на цей список розсилки, тобто його отримають одразу тисячі користувачів. Підписатися на такі списки може кожний, хто має електронну поштову адресу.

1.2 Постачальники послуг електронної пошти

Постачальник послуг електронної пошти – це компанія, яка пропонує користувачам інструменти для надсилання та отримання електронних листів через браузер або окрему програму електронної пошти. Ці служби мають зручні та прості у використанні інтерфейси, які допомагають користувачам

упорядковувати свою пошту та ефективно керувати своїми списками розсилки.

Реклама електронною поштою є більш відомим каналом просування, ніж інші засоби масової інформації, тому все більше постачальників почали пропонувати окремі типи допомоги.

Вони надають інструментарій для створення і розсилки кампанії електронної пошти та на адміністрування, яке організація надає, щоб допомогти клієнт ефективно здійснити маркетингову кампанію електронною поштою.

Деякі постачальники просто забезпечують такі основні функції, як збереження списку адрес електронної пошти та надсилання повідомлень.

Але вибрати найкращого постачальника електронної пошти може бути складно, оскільки потрібно багато чого враховувати, особливо в наші дні віддаленої роботи. В цьому розділі розглянемо популярних постачальників електронної пошти таких як Gmail, Yahoo mail, AOL mail, Outlook та iCloud mail.

1. Gmail від Google

Gmail є найбільш використовуваним і популярним постачальником послуг електронної пошти з понад 1,2 мільярда користувачів у всьому світі [2].

(Рис.1 Логотип Gmail)

Особливості:

- Gmail поєднується з іншими службами Google, такими як Документи Google, Диск Google і Календар Google.

- Google підходить для всіх типів користувачів, однак це найбільше допомагає користувачам системи Android. Оскільки користувачі Android мають Google Play Store та потребують облікового запису Gmail для завантаження програм.
- Gmail пропонує великий простір для зберігання на Google Drive (безкоштовний і платний),
- Багатофункціональне редагування вмісту листів та першокласний захист від спаму та окремі вкладки для пропозицій.
- Можливість створення персональної адреси електронної пошти, наприклад: name@yourbusiness (бізнес план)

2. Outlook

(Рис.2 Логотип Outlook)

Outlook спочатку був заснований Microsoft як Hotmail. Microsoft Outlook є поштовим клієнтом, який використовується для надсилання та отримання електронних листів за допомогою доступу до електронної пошти Microsoft Exchange Server [3]. Він також надає доступ до контактів, календаря електронної пошти та функції керування завданнями. Він має понад 400 мільйонів користувачів у всьому світі і вважається найбільшою конкуренцією Gmail.

Користувачі Android не обмежуються лише використанням Gmail. Такі популярні платформи, як Xbox, Windows, Skype також використовують Outlook для своїх електронних листів.

Особливості:

- Фокусована папка вхідних повідомлень. Outlook надає пріоритет електронним листам, які ви отримуєте від найважливіших контактів.
- Інтеграція з іншими продуктами Microsoft: Word, PowerPoint та Excel.
- Навігація з голосовим керуванням.

Однак інколи обробка займає деякий час, а через сфокусовану папку "Вхідні" важливі електронні листи іноді можуть потрапляти до спаму.

Є один недолік використання Outlook – він не відстежує ваші електронні листи.

3. AOL Mail

(Рис.3 Логотип AOL Mail)

AOL — це безкоштовний постачальник електронної пошти, яку Verizon придбала в 2015 році [4].

Цей постачальник є дуже простим сервісом електронної пошти, який можна використовувати лише для надсилання та отримання електронних листів.

Особливості:

- Передбачений механізм захисту від листів, що можуть містити віруси.
- Унікальний режим панелі читання, у якому можна читати електронну пошту, не виходячи з папки "Вхідні" або можливість запропонувати електронному листу з’явитися збоку.

- Дозволяється вкладати лише ті файли, що зберігаються локально, не підтримується вкладення файлу з онлайн-сховища.

AOL не є надзвичайним, але ідеально підходить для базових функцій електронної пошти. Найкраща функція, яку він пропонує — необмежений обсяг пам’яті.

4. Yahoo Mail

(Рис.4 Логотип Yahoo Mail)

Yahoo Mail — це постачальник електронної пошти, що розпочав свою діяльність 8 жовтня 1997 року американською компанією Yahoo, Inc. Пропонує безкоштовне користування обліковим записом електронної пошти. З додатковою щомісячною платою можна отримати більше можливостей для роботи з іншими їх платформами як Yahoo Finance [5].

Особливості:

- Легкий в керуванні мобільний додаток зі зручним інтерфейсом.
- Тема та макет папки "Вхідні", які можна самостійно налаштувати.
- Прикріплені файли повинні бути доступними локально, Yahoo не підтримує вкладення онлайн-файлів.

Однак, якщо порівняти Yahoo з іншими постачальниками, він має менше фільтрів або сортування.

5. iCloud Mail

(Рис.5 Логотип iCloud Mail)

iCloud Mail — це постачальник послуг електронної пошти, яким керує компанія Apple.

Більшість користувачів iCloud Mail є користувачами Apple. iCloud є одним із постачальників електронної пошти, який також надає доступ до електронної пошти на різних пристроях. При отриманні iCloud+, можна отримати можливість надсилати та отримувати електронну пошту зі спеціального домену електронної пошти. Але наразі ця функція доступна не в усіх країнах і регіонах [6].

Найкраще в iCloud Mail – це те, наскільки він бездоганно інтегрований у macOS та IOS.

Незважаючи на те, що iCloud Mail відкритий для всіх, іноді його вважають непридатним для користувачів, які не інвестують в екосистему Apple.

1.3 Розсилка

Список розсилки — це список адрес електронної пошти користувачів, які цікавляться тією самою темою, є членами однієї робочої групи або навчаються разом. Коли учасник списку надсилає примітку на спеціальну адресу групи, повідомлення електронної пошти транслюється всім учасникам списку. Ключовою перевагою списку розсилки є те, що коли нове повідомлення стає доступним, воно негайно доставляється до поштових скриньок учасників.

Електронні списки розсилки зазвичай повністю або частково автоматизовані за допомогою спеціального програмного забезпечення для списків розсилки та адреси розсилки, встановленої на сервері, здатному отримувати електронну пошту. Вхідні повідомлення надіслані на таку адресу обробляються програмним забезпеченням. Залежно від їхнього вмісту, вони обробляються програмою (у випадку повідомлень, що містять команди, спрямовані до самого програмного забезпечення) або розсилаються на всі адреси електронної пошти, підписані на список розсилки.

Часто доступний веб-інтерфейс, який дозволяє людям підписуватися, скасовувати підписку та змінювати свої уподобання. Загальним форматом для надсилання цих команд є надсилання електронного листа, який містить просто команду, за якою слідує назва електронного списку розсилки, до якого ця команда відноситься.

Сервери електронних списків розсилки можуть бути налаштовані на пересилання повідомлень передплатникам певного списку розсилки окремо, якщо вони отримані сервером списку, або у формі дайджесту.

Дайджест — це така форма електронного листа, у якому об’єднано всі повідомлення, отримані сервером списку в певний день. Такий лист надсилається абонентам один раз на день. Деякі списки розсилки дозволяють окремим передплатникам вирішувати, як вони бажають отримувати повідомлення від сервера списку.

З часом електронні розсилки все більше і більше почали використовувати для маркетингових схем, для надсилання листів потенційним та існуючим клієнтам компанії з метою сповіщення про акційні пропозиції, новини про роботу компанії, реклами.

Розсилки допомагають бізнесу постійно залишатися на зв'язку з клієнтом і звертатися до нього безпосередньо, а спеціальні сервіси відстежують його дії (відкриття листа, перехід за посиланнями).

Існує думка, що електронні розсилки застаріли, їхнє місце зайняли соціальні мережі та контекстна реклама. Але це не так. Реклама в соціальних мережах і пошукових системах розрахована на всіх можливих користувачів, а листи з розсилок потрапляють прямо в руки клієнтові. Маркетологи відстежують інтереси цільових аудиторій і намагаються складати листи так, щоб інформація була корисна і цікава.

Таким чином електронна розсилка стала персоналізованим маркетинговим інструментом, який не конкурує з іншими, а працює разом з ними.

Найчастіше в бізнесі розсилка використовується для новин, акцій та сповіщень.

Новини не обов'язково стосуються товарів — з них клієнт може дізнатися про розширення технічної бази, участі керівництва в міжнародній конференції, соціальних аспектах бізнесу. Така інформація піднімає рейтинг бізнесу і формує позитивне враження у клієнтів. Найчастіше в листі міститься не сам матеріал, а пропозиція перейти на сторінку блогу та прочитати статтю.

Розсилка про акції або спеціальні пропозиції зазвичай містить листи, де пропонують придбати товар зі знижкою або взяти участь в розіграші призів. Це допомагає клієнтам заощаджувати і отримувати додаткову вигоду, а бізнесу — збільшувати кількість лояльних покупців.

До сповіщень відносяться повідомлення нерекламного характеру, це скоріше сповіщення про важливі для клієнта події: відкриття або закриття певного закладу, зміни в графіку, зміни тарифів, нагадування про необхідність продовження терміну дії.

Розсилки часто плутають зі спамом, остільки останній — синонім настирливої поведінки відправника. Але це абсолютно різні речі, і у кожної з них є свої характерні особливості.

Електронна розсилка покликана побудувати довготривалі відносини з клієнтом, її механізм відкритий і прозорий.

Після запуску електронної розсилки є можливість отримати повідомлення про листи, які не були доставлені. Такі листи називаються поверненими, доставити їх неможливо через серверні помилки. Такі помилки доставки є двох видів: м'які та жорсткі [7]. Потрібно уважно проаналізувати звіт, щоб визначити точну причину повернення листа. Після чого вирішити, чи варто продовжувати робити відправлення розсилки на цю адресу.

Жорстка відмова — це повернення листа відправнику, оскільки адреса отримувача не існує. Така відмова вказує, що відправка листів на цю адресу є неможливою. Найчастіші проблеми такої помилки:

- некоректне написання електронної адреси;
- адреса, що більше не існує;
- домен, на якому зареєстрована адреса, більше не існує;
- заблоковано поштовий сервер отримувача;
- велика кількість м'яких відмов при відправленні на дану адресу.

М'яка відмова – це повернення листа відправнику у випадку тимчасової недоступності електронної адреси користувача. Можливими причинами такої помилки можуть бути:

- надто великий розмір листа;
- сервер отримувача тимчасово не працює;
- ваші листи багато користувачі відмітили як спам;
- відправник заблокований.

У випадку м’якої відмови є можливість відправити лист повторно. Якщо причиною є тимчасові проблеми на сервері, достатньо відправити лист пізніше. При поверненні листа через блокування адреси відправника, причини можуть бути наступні:

- відправник робить масові розсилки з безкоштовної електронної адреси (в таких адресах є певні правила боротьби зі спамом), тому ваші листи блокуються;
- адреса електронної пошти або IP відправника занесені до чорного списку;
- сервер отримувача вважає листи спамом.

Після визначення причини її необхідно усунути перед повторним відправленням листа.

1.4. Спам

Спам — масове розсилання кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати. Часто спам надсилається електронною поштою, але він також може поширюватися через текстові повідомлення, телефонні дзвінки чи соціальні мережі.

Натхненням для використання терміну "спам" для опису масових небажаних повідомлень стала сценка Монті Пайтона, у якій актори заявляють, що всі повинні їсти спам, хочуть вони цього чи ні [8]. Подібним чином, спам повідомлення турбують всіх хто має адресу електронної пошти, незалежно від того, зацікавлені вони тією інформацією чи ні.

1.4.1. Види спаму

Спамери використовують багато форм зв’язку для масової розсилки своїх небажаних повідомлень. Деякі з них є маркетинговими повідомленнями

про продаж небажаних товарів. Інші види спаму можуть поширювати зловмисне програмне забезпечення, обманом змусити вас розкрити особисту інформацію або налякати, щоб отримувач подумав, що йому потрібно заплатити, щоб уникнути проблем.

Фільтри від спаму електронної пошти виловлюють багато таких типів повідомлень, а оператори телефонного зв'язку часто попереджають вас про "ризик спаму" від невідомих абонентів. Через електронну пошту, текстове повідомлення, телефон або соціальні мережі, деякі спам-повідомлення все ж таки проходять. В такому випадку отримувач хочете мати можливість розпізнати їх та уникнути можливих загроз. Нижче наведено кілька типів спаму, на які варто звернути увагу.

Фішингові електронні листи — це тип спаму, який кіберзлочинці надсилають багатьом людям, сподіваючись "зачепити" хоча б декількох одержувачів. В цьому разі спамер намагається виманити в одержувача листа номери його кредитних карток чи паролі доступу до електронних платіжних систем. Такий лист, зазвичай, маскується під офіційне повідомлення від адміністрації банку. У ньому говориться, що одержувач повинен підтвердити відомості про себе, інакше його рахунок буде заблоковано. Наводиться адреса сайту, яка належить спамерам, із формою, яку треба заповнити. Серед даних, що потрібно повідомити, знаходяться необхідні шахраям.

Наступним видом спаму є підробка електронної пошти. Підроблені електронні листи імітують або підробляють електронний лист від законного відправника та просять вас вжити певних дій. Добре виконані підробки містять знайомий бренд і вміст, часто від великої відомої компанії, такої як PayPal або Apple. До поширених спам-повідомлень електронної пошти відносяться:

- Вимога про оплату неоплаченого рахунку;
- Запит на скидання пароля або підтвердження облікового запису;

- Перевірка покупок, які ви не робили;
- Запит на оновлену платіжну інформацію;
- Шахрайство служби технічної підтримки;

У шахрайстві технічної підтримки спам-повідомлення вказує на те, що у вас є технічна проблема, і вам слід зв’язатися зі службою технічної підтримки, зателефонувавши за номером телефону або натиснувши посилання в повідомленні. Ці типи спаму також часто повідомляють, що вони надходять від великої відомої технологічної компанії.

Якщо ви вважаєте, що у вас є технічна проблема або зловмисне програмне забезпечення на вашому комп’ютері, планшеті чи смартфоні, вам слід завжди відвідувати офіційний веб-сайт компанії. Саме там заходиться законна контактна інформація, за якою можна звернутися про допомогу.

Шахрайство часто пов’язано з поточними подіями. Гарячі теми в новинах можна використовувати в спам-повідомленнях, щоб привернути вашу увагу. У 2020 році, коли світ зіткнувся з пандемією Covid-19 і спостерігалося збільшення кількості робочих місць з дому, деякі шахраї розсилали спам-повідомлення, обіцяючи віддалену роботу з оплатою в біткоїнах. У тому ж році ще одна популярна тема спаму була пов’язана з пропозицією фінансової допомоги малому бізнесу, але шахраї зрештою попросили надати реквізити банківського рахунку.

Шахрайство з попередньою оплатою. Цей тип спаму, який іноді називають електронними листами "нігерійського принца", оскільки він був передбачуваним відправником повідомлень протягом багатьох років, обіцяє фінансову винагороду, якщо отримувач спочатку відправить грошовий аванс. Відправник зазвичай вказує, що цей готівковий аванс є певною комісією за обробку або заставою для розблокування більшої суми, але після оплати вони зникають. Щоб зробити це більш особистим, подібний тип шахрайства

полягає в тому, що відправник видає себе за члена сім’ї, який потрапив у біду та потребує грошей, але якщо ви платите, результат, на жаль, аналогічний.

Шкідливий спам. Скорочення від "спам зловмисного програмного забезпечення" або "зловмисний спам", це таке спам-повідомлення, яке доставляє зловмисне програмне забезпечення на ваш пристрій. При натисканні на посилання або відкриття вкладення електронної пошти, користувач може отримати певний тип зловмисного програмного забезпечення, включаючи програми-вимагачі, трояни, боти, викрадачі інформації, криптомайнери або шпигунські програми. Звичайним це відбувається шляхом додавання шкідливих сценаріїв до вкладення знайомого типу, таких як документ Word, PDF-файл або презентація PowerPoint. Після відкриття вкладеного файлу сценарії запускаються та приносять шкідливе програмне забезпечення.

1.4.2. Як захиститись від спаму

Хоча повністю уникнути спаму може бути неможливо, є певні кроки, які можна вжити, щоб захистити себе від спаму.

Насамперед навчитися розпізнавати фішинг. Кожен може стати жертвою фішингових атак тому, що отримувач може поспішати й випадково відкрити зловмисне посилання. Але якщо з’явиться новий тип фішингової атаки, розпізнати його може бути складно. Тож щоб захистити себе, варто перевіряти деякі ключові ознаки того, що отримане повідомлення є не просто спамом, а саме фішингом.

Варто звертати увагу на електронну адресу відправника, якщо електронний лист від компанії є законним, вона має відповідати домену компанії, яку він, представляє. Іноді вони очевидні, наприклад example@qwerty09348.biz, але іноді зміни менш помітні, наприклад example@paypa1.com замість paypal.com.

Остерігайтеся будь-яких підозрілих посилань, включно з кнопками в електронному листі. Якщо ви отримуєте повідомлення від компанії, у якій у вас є обліковий запис, доцільно увійти до нього, щоб побачити, чи є там повідомлення, а не просто натиснути посилання в повідомленні без попередньої перевірки. Ви можете зв'язатися з компанією, щоб запитати, чи підозріле повідомлення є законним чи ні. Якщо у вас є сумніви щодо повідомлення, не натискайте жодних посилань.

Також варто звернути увагу на граматичні помилки. Ми всі допускаємо їх, але компанія, яка розсилає законні повідомлення, ймовірно, не матиме багато пунктуаційних помилок, поганої граматики та орфографічних помилок. Це може бути ще одним червоним прапорцем, який вказує на те, що електронний лист може бути підозрілим.

Багато фішингових повідомлень видають себе за надходження від великих відомих компаній, сподіваючись зловити в пастку читачів, які мають справу з компанією. Інші спроби фішингу пропонують щось безкоштовно, наприклад готівку або бажаний приз. Занадто хороші пропозиції в неочікуваних листах, можуть бути попередженням про те, що спам-повідомлення намагається щось отримати від вас, а не навпаки.

Якщо ви не очікуєте електронного листа з вкладенням, будьте обережні, перш ніж відкривати або завантажувати їх. Використання програмного забезпечення для захисту від зловмисних програм може допомогти, скануючи файли, які ви завантажуєте.

Постачальники послуг електронної пошти досить добре фільтрують спам, але коли повідомлення потрапляють до вашої папки "Вхідні", ви можете повідомити про них. Це стосується спам-дзвінків і текстових повідомлень, оскільки багато операторів також дають вам можливість повідомляти про спам. Ви також можете заблокувати відправника.

Повідомлення про спам може допомогти вашому постачальнику послуг електронної пошти чи оператору телефонного зв'язку краще виявляти спам.

Якщо законні електронні листи потрапляють до вашого фільтру спаму, ви можете повідомити, що їх не слід позначати як спам, і це також надає корисну інформацію про те, що не слід фільтрувати. Іншим корисним кроком є завчасне додавання відправників, від яких ви хочете отримувати листи, до свого списку контактів.

Найбільший потік спаму поширюється через електронну пошту. Рекордним роком став 2016 рік, коли потік спаму в загальному трафіку електронної пошти становив 65 % (за даними Cisco Systems) [9].

2. Валідація та верифікація електронних адрес

Надсилання електронних листів на неіснуючі адреси призводить до того, що вони повертаються до вашої папки "Вхідні". Високий показник відмов (тобто відсоток недоставлених електронних листів від усіх електронних листів у вашій кампанії) може завдати шкоди репутації вашого відправника.

Велика кількість відмов насторожує постачальника послуг електронної пошти, який позначає вас як потенційного спамера, оскільки вони зазвичай не піклуються про якість свого списку розсилки. Коли ваша репутація відправника постраждає, ваші електронні листи потраплять у папку "спам" або взагалі не будуть доставлені.

Найгірший сценарій, коли ви ігноруєте показник відмов, вищий за 2%, і нічого не робите з цим якнайшвидше, полягає в тому, що ваш домен може опинитися в чорному списку. В багатьох випадках вийти з чорного списку — це дуже важко або практично неможливо. Досить часто простіше створити новий домен, а потім видалити старий із чорного списку.

Тому, щоб запобігти цього сценарію потрібно ретельно подбати про якість свого списку розсилки. Не купувати готові списки розсилки та завжди перевіряти адреси електронної пошти незадовго до надсилання кампанії.

Отже, щоб розсилка була ефективною варто робити валідацію та верифікацію списку електронних адрес для неї. Це потрібно для збереження актуальності списку користувачів, адже щорічно 22.5% електронних адрес з різних причин стають недійсними [10]. Найчастіше це корпоративні адреси, які деактивуються після зміни роботи користувача.

2.1Валідація та верифікація

Валідація визначає чи адреса електронної пошти є дійсною. Перевіряється загальний формат адрес електронної пошти, включаючи друкарські помилки.

Верифікація перевіряє чи існує адреса електронної пошти. Це є набагато складнішим процесом, який потребує досвіду роботи з електронною поштою та пов’язаних із нею технологій.

Верифіковані електронні адреси набагато надійніші ніж лише валідовані електронні адреси.

2.2 Інструменти для верифікаці та валідації

Валідатор може бути як десктопним додатком, так і онлайн-сервісом. Останній варіант більш актуальний, тому що у цьому випадку не використовується ваша IP-адреса, а також сервіс постійно оновлюється розробником, який гарантує своєчасну технічну підтримку.

Ефективність валідатора залежить від алгоритму його роботи та кількості рівнів перевірки.

Інструменти бувають з великої кількістю особливостей, тому легко підібрати саме той сервіс, який буде максимально зручний та практичний у вашому робочому середовищі.

Відомим програмним інструментом є AtomPark.

(Рис.6 Логотип Atompark)

Подібне програмне забезпечення корисне, для великих компаній, де пошук та перевірка існування електронної пошти виконуються конкретним фахівцем. З їх допомогою досить просто фільтрувати великі списки для розсилки.

Перевагою таких інструментів є миттєва покупка, необмежена кількість перевірок адрес та доступність контактної бази без посередників. Але самостійне оновлення системи, необхідність у резервних копіях (відсутність хмарного сховища), перевірка електронних адрес тільки з одного пристрою, відсутність інтеграцій та специфічні системні вимоги виступають суттєвими недоліками.

Онлайн сервіси для верифікації, надають можливість хмарного зберігання даних. Це дозволяє, наприклад, знайти та перевірити електронну адресу та відправити на неї тригерного листа з будь-якого пристрою.

Зазвичай такі інструменти використовують модель підписки з щомісячними лімітами на перевірку контактів. Тим не менш, вони завжди пропонують безліч безкоштовних додатків та розширень, а також преміуми за потреби.

Така модель оптимальна для тих, хто хоче одноразово верифікувати невелику кількість електронних адрес або робить це раз у 1-2 місяці. Також, серед переваг, варто відзначити доступ до аккаунту з будь-якої точки світу, можливості командної роботи, відсутність обмежень у операційній системі та відкритий API.

Варто відзначити, що обидва типи інструментів для перевірки електронних адрес зазвичай пропонують як індивідуальну, так і масову перевірку електронних адрес.

2.3Аналіз відомих API для перевірки електронних адрес

Прикладний програмний інтерфейс (англ. Application Programming Interface, API) — набір визначень підпрограм, протоколів взаємодії та засобів для створення програмного забезпечення. Інтерфейс можна розглядати як контракт на обслуговування між двома програмами. Цей контракт визначає, як обидва спілкуються один з одним за допомогою запитів і відповідей. Документація API містить інформацію про те, як розробники структурують ці запити та відповіді.

В цьому пункті розглянуто відомі прикладні програмні інтерфейси для перевірки електронних адрес.

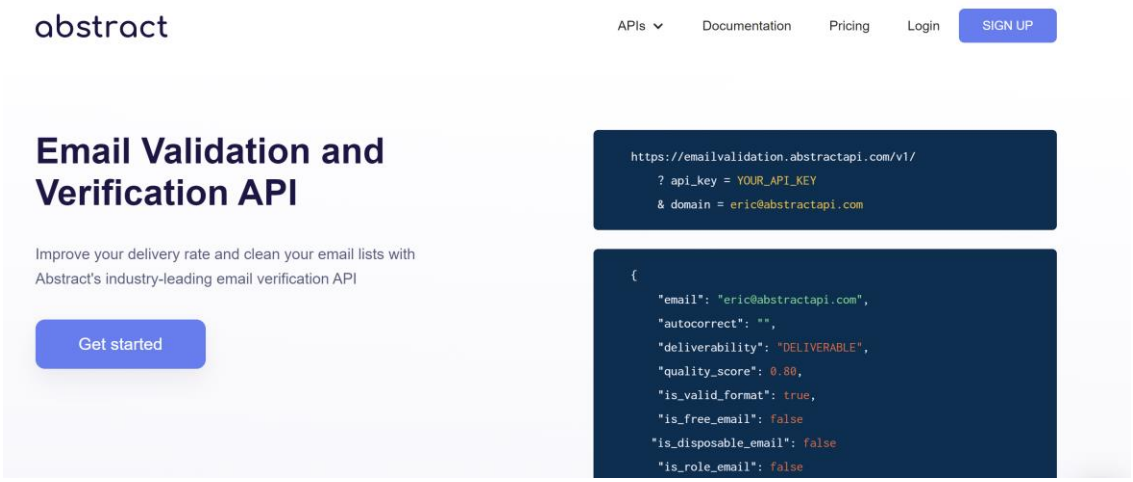
Abstract Email Verification API — це API перевірки електронної пошти, орієнтований на розробників, який використовують понад 100 000 стартапів і компаній, зокрема Shopify, Stanford, Payoneer [11].

Дане API перевіряє можливість доставки електронної пошти, виконуючи кілька перевірок і повертаючи їх у форматі JSON. Він включає наступне:

- Перевірка формату
- Виявлення друкарських помилок із пропозицією автоматичного виправлення
- Безкоштовне виявлення постачальника послуг електронної пошти
- Виявлення фіктивного постачальника електронної пошти
- Виявлення електронної пошти ролі (контакт, команда, тощо)
- Загальне виявлення електронної пошти

- Перевірка перевірки MX
- Перевірка доставки SMTP

Abstract — це один із API, який відповідає вимогам GDPR і CCPA, не зберігаючи електронної пошти.



(Рис. 7 Abstract API)

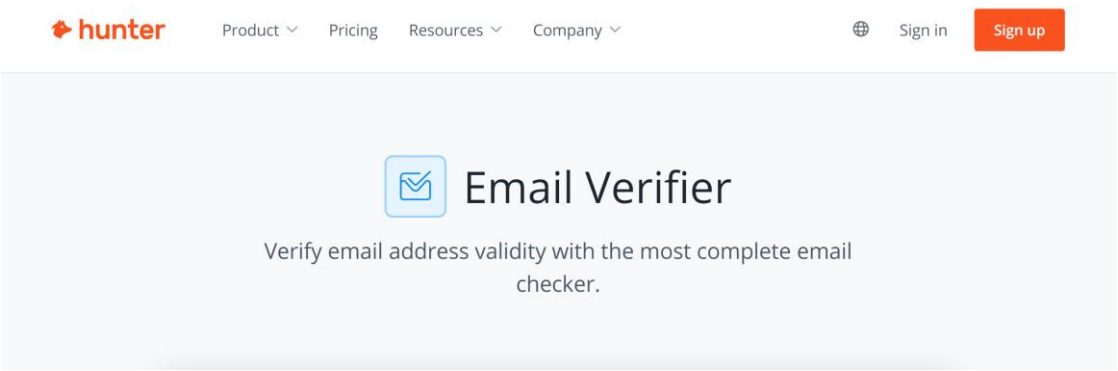
Hunter Mail Verifier показує кілька рівнів перевірки, включаючи формат, відповідь поштового сервера та інформацію про домен. Він показує доступність адреси електронної пошти з детальними перевірками разом із оцінкою надійності.

Також є можливість порівняння з унікальною базою, яка містить понад 100 мільйонів професійних електронних листів. Ви можете використовувати верифікатор для масової перевірки електронних листів, що означає, що ви можете підтвердити весь свій список електронних адрес [12].

Засіб перевірки електронної пошти підключається безпосередньо до SMTP-сервера в процесі перевірки електронної пошти, не надсилаючи електронні листи користувачам. Hunter виконує різні типи перевірок:

- Перевірка формату
- Друкарських помилок

- Виявлення електронної пошти ролі (контакт, команда, тощо)
- Загальне виявлення електронної пошти
- Перевірка перевірки MX
- Перевірка доставки SMTP



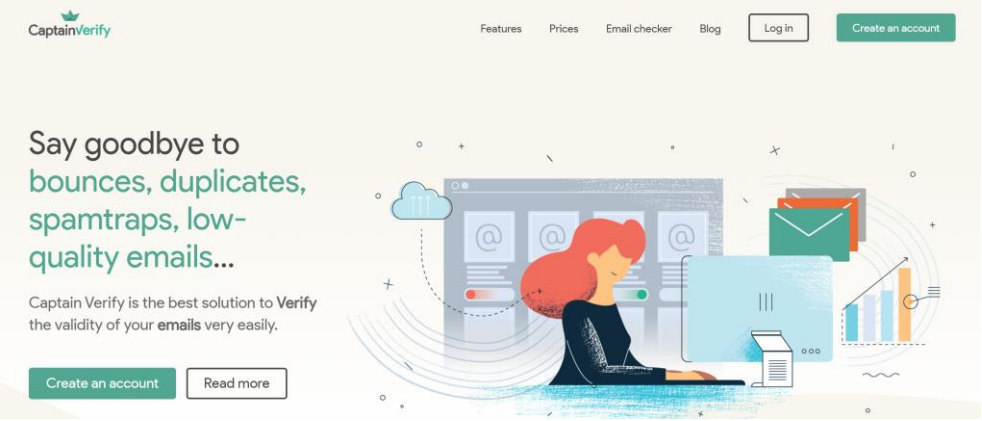
(Рис. 8 Hunter Mail Verifier)

Captain Verify дозволяє імпортувати ваші списки електронної пошти із зашифрованих файлів CSV і може ефективно їх аналізувати та перевіряти.

Після завершення перевірки електронної пошти ви зможете легко завантажити файл зі результатами. Captain Verify також легко та швидко перевіряє та очищає ваші списки розсилки. Це не залишає місця для недійсних або неправильно написаних електронних адрес.

Ви також можете сегментувати свої списки розсилки, уточнюючи всі дані для зручності. Крім того, таке рішення дозволяє покращити маркетингові кампанії та підвищити рентабельність інвестицій.

Captain Verify суворо дотримується норм GDPR і захищає інформацію про ваш бізнес і клієнтів. Також, він надає точний статистичний звіт на основі якості вашої бази даних [13].



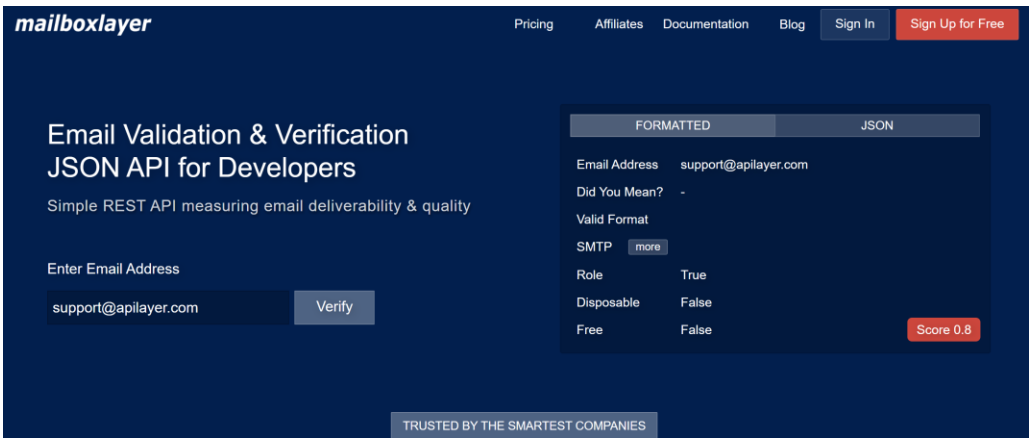
(Рис. 9 Головна сторінка Captain Verify)

Mailboxlayer — це прикладний інтерфейс для підтвердження та верифікації електронної пошти. Він оснащений розширеними інструментами, такими як перевірка синтаксису та друкарських помилок, фільтрація одноразових і безкоштовних постачальників електронної пошти, перевірка SMTP, перевірка якості електронної пошти та балів доставки.

Цей інструмент має зручну структуру URL-адреси, яку легко інтегрувати. Він використовує формат JSON, який також є легким і безпечним завдяки 256-бітному шифруванню HTTPS [14].

Mailboxlayer пов’язано з кількома базами даних, які регулярно оновлюються та містять постачальників електронної пошти, відокремлюючи одноразові та безкоштовні електронні листи від окремих доменів.

API Mailboxlayer полегшує зворотні виклики JSONP і пропонує форматування JSON для зручного переглядання даних про електронні адреси. Він відображає оцінки якості від 0 до 1; 0 — це погано, а 1 — добре. Це відображає якість і доступність електронної адреси.



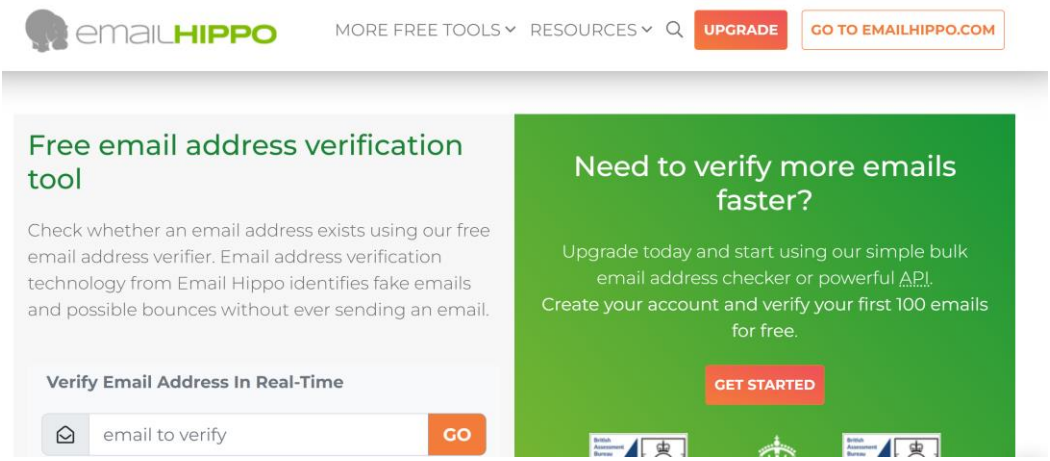
(Рис. 10 Головна сторінка Mailboxlayer)

За допомогою Email Hippo ви можете швидко перевіряти адреси електронної пошти у своєму списку. Це ідеальний варіант для інтеграції його у ваші продукти, пов'язані з електронною поштою, оскільки він дає результати в реальному часі та створює унікальний рейтинг довіри – Email Hippo Trust Score [15].

Ви можете використовувати його для фільтрації онлайн-реєстрацій, оновлення баз даних і очищення систем CRM. Отримати кращий контроль над своїм списком електронних листів, знаходячи електронні листи з низьким рівнем відкриття.

Email Hippo може виявляти рольові електронні листи, які зазвичай мають низький рівень відкриття порівняно з іменованими адресами. Він також перевіряє записи MX, щоб збільшити можливості доставки електронної пошти.

За допомогою Hippo можна навіть виявити домени з посиланнями на темну мережу. Знайти поштові сервери, щоб відфільтрувати шахраїв і перевірити потенційних клієнтів. Ви отримуєте повну інформаційну панель із інструментами звітування та макетами, визначеними користувачем, а також підсумками виявлення, які можна завантажити.



(Рис. 11 Головна сторінка Email Hippo)

Email Hippo надає результати з кількох точок даних і допомагає вам ефективно створювати робочі процеси. Він також перевіряє синтаксичні помилки в реальному часі, допомагаючи вам створювати та надсилати відповіді на сповіщення.

3. Розробка веб-додатку

3.1 Інструменти для розробки

Для розробки додатку використовувалась платформа Node.js. Дана платформа виводить мову JavaScript за межі браузера і дозволяє використовувати її на стороні сервера. В основі цієї платформи лежить виключно швидкий рушій JavaScript, запозичений з браузера Chrome V8, до якого додана надійна та швидка бібліотека асинхронного мережного введення і виведення.

Цю платформу розробив Райан Дав (RyanDahl) в 2009 році, після двох років експериментування зі створенням серверних вебкомпонентів на мові програмування Ruby та інших. В результаті своїх досліджень він прийшов до висновку, що замість традиційної моделі паралелізму на основі потоків слід звернутися до систем, що орієнтуються на подіях. Ця модель була обрана за простоту, за низькі накладні витрати, в порівнянні з ідеологією "один потік на кожне з'єднання", і за швидкодію [16].

Прийнята в платформі Node модель принципово відрізняється від поширених платформ для побудови серверів для додатків, в яких масштабованість досягається за рахунок багатопоточності. Стверджується, що завдяки подієво-орієнтованій архітектурі знижується використання пам'яті, підвищується пропускна здатність і спрощується модель програмування. Наразі платформа Node швидко розвивається, і багато хто вважає її привабливою альтернативою традиційному підходу до розробки веб-додатків. Також для цієї платформи зручно створювати та використовувати спеціалізовані пакети.

В платформу Node не вбудована ні об'єктна модель документа (DOM), ні будь-які інші можливості браузера. Саме мова програмування JavaScript в поєднанні з асинхронним введенням та виведенням робить Node потужною платформою для розробки додатків.

При швидкому створенні додатків використовуючи платформу Node часто буває необхідний зручний і швидкий спосіб перетворити додаток в шаблон.

Препроцесор Jade використовується за умовчанням як механізм перегляду для Express, але синтаксис Jade може бути надмірно складним для багатьох моделей використання. EJS є одним з альтернативних варіантів, це — шаблонізатор для платформи Node.js. Його перевагами є простота у використанні та налаштуванні. Також наявна проста інтеграція з модулем Express для Node.js.

Використовується EJS, щоб при створенні додатку підключити повторювані частини сайту та передавати їх при завантаженні сторінки у браузері. Виправляти помилки EJS легко оскільки вони є звичайними винятками JavaScript із номерами рядків шаблону.

Шаблонізатор має велику спільноту активних користувачів, а бібліотека активно розвивається [18]. Його основні особливості:

- швидка компіляція та рендеринг

- прості шаблонні теги: <% %>
- можливість кастомізації тегів (наприклад, використання [? ?] замість <% %>)
- статичне кешування проміжного JavaScript
- статичне кешування шаблонів
- відповідає системі Express view

Для перевірки електронних адрес використовувався прикладний інтерфейс Abstract. API перевірки електронної пошти Abstract бере адресу електронної пошти та визначає, чи вона дійсна і наскільки ризикованою, на думку інтерфейсу це може бути.

API перевірки електронної пошти Abstract використовує різноманітні все більш складні та методи, які постійно оновлюються, щоб гарантувати виключення всіх недійсних або ризикованих електронних листів. Ці методи включають: перевірку синтаксичних помилок і друкарських помилок в адресі електронної пошти (наприклад, yuliia@gnamil.com), перевірка записів SMTP і MX у реальному часі за доменом електронної пошти, виконання складного регулярного виразу (regex) перевіряти електронну пошту та використання інших фільтрів, що підтримані машинним навчанням, для виявлення недійсних або ризикованих електронних листів.

Також він надає можливість ідентифікувати характеристики електронної пошти, наприклад, чи належить він безкоштовному постачальнику послуг електронної пошти (Yahoo або Gmail), чи постачальнику одноразових служб електронної пошти (Yopmail). Визначення "ролі" адреса електронної пошти (наприклад, team@ або @support).

Abstract підтримує одну з найбільших і найчастіше оновлюваних баз даних безкоштовних і одноразових адрес електронної пошти, що дозволяє ідентифікувати їх і вирішити фільтрувати їх чи ні.

Всі дані, які надсилаються до API перевірки електронної пошти Abstract і обробляються, захищені за допомогою 256-бітного шифрування SSL (HTTPS).

Для використання API потрібно мати унікальний ключ, що буде використовуватись при кожному запиті. Відповідь повертається в універсальному та легкому форматі JSON.

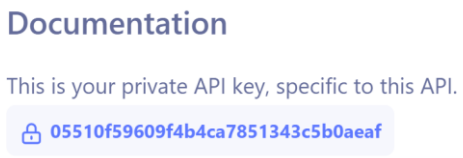
3.2. Етапи розробки веб-додатку

Метою було створення веб-додатку використовуючи платформу Node.js та Abstract API для верифікації та валідації електронних адрес. В додатку користувач може ввести електронну адресу, яку бажає перевірити та отримати результат про статус цієї адреси.

Першим кроком була ініціалізація проекту командою npm init, де вказується назва проекту, версія, опис, автор та ключові слова. Всі вище згадані дані записуються в файл package.json (Додаток 1). Також в цьому файлі в списку залежностей знаходяться всі необхідні додаткові модулі для розробки та роботи додатку.

Наступним кроком було створення файлу index.js (Додаток 2) в якому використовуючи веб-фреймворк Express запускається сервер на обраному порті. Після цього використовуючи відомі технології HTML/CSS та Bootstrap побудовано сторінки додатку. Додаток складається з трьох сторінок: welcome, index, info. Сторінка "welcome" є головною сторінкою з загальною інформацією про додаток та містить кнопку для переходу на сторінку "index", яка дає можливість ввести користувачу адресу для перевірки. Детальна інформація про валідацію та верифікацію міститься на сторінці "info" відповідно. Для динамічного створення сторінок використано шаблонізатор EJS.

Для використання прикладного інтерфейсу Abstract у власному додатку потрібен API ключ, щоб його отримати потрібно зареєструватись в їх системі.



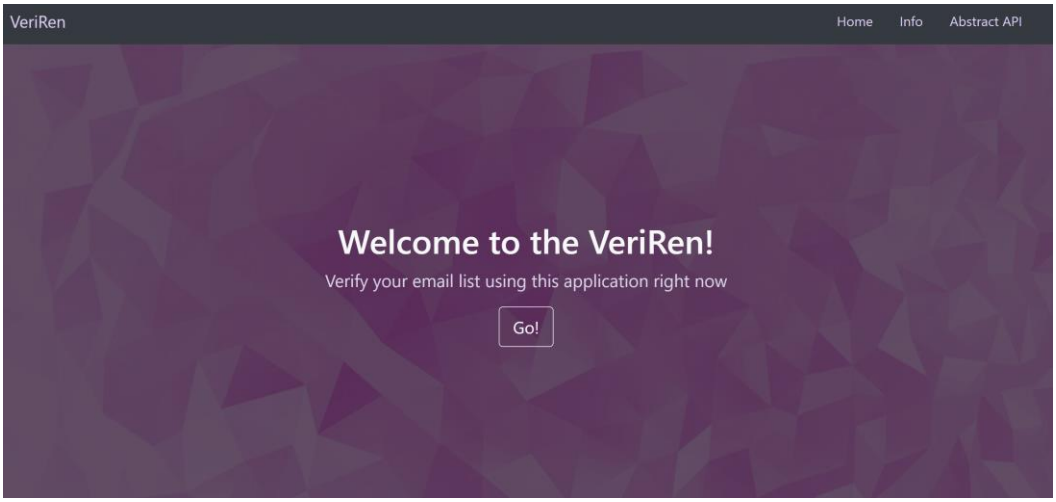
(Рис.12 API ключ Abstract)

Отримавши ключ, який є унікальним, можна будувати запити для валідації та верифікації конкретної електронної адреси за прикладом:

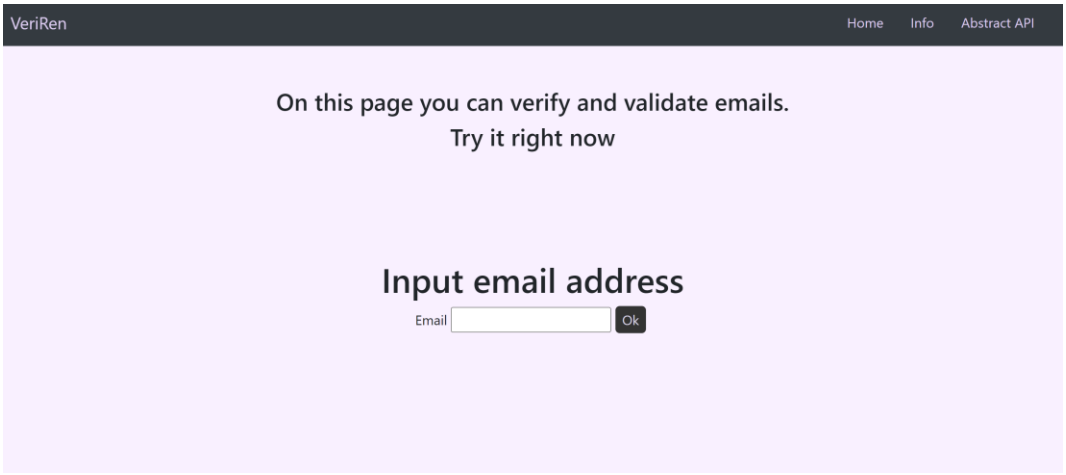
(Рис.13 Приклад запиту)

В результаті написано скрипт (Додаток 3), який бере значення з поля для введення електронної адреси, що бажає перевірити користувач, та формує запит, який складається з посилання прикладного інтерфейсу, ключа та значення (введена адреса). Після обробки такого запиту виводиться результат щодо статусу пошти. А саме оцінка прикладного інтерфейсу можливості доставки електронного листа. Можливі значення: DELIVERABLE, UNDELIVERABLE, RISKY і UNKNOWN [11], тобто доставка листа можлива, неможлива, ризикована та невідома відповідно. Якщо статус відправки невідомий, це означає що введена адреса має обліковий запис загального доступу (catchall). Це така адреса електронної пошти, яка збирає всю пошту, надіслану на доменне ім’я, а не на інші адреси електронної пошти, відомі серверу. Тому при помилковому введенні неможливо визначити чи відправлення листа відбулось на конкретну адресу,

чи на загальний домен. Також виводиться значення "Quality score", яке є десятковою оцінкою від 0,01 до 0,99 та відображає впевненість прикладного інтерфейсу в якості та доступності надісланого електронного листа.



(Рис. 14 Головна сторінка додатку)

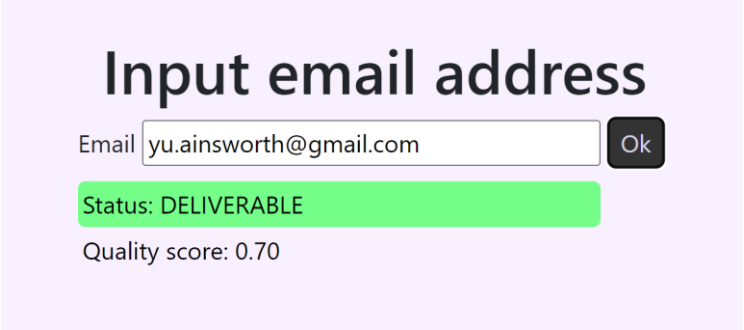


(Рис. 15 Сторінка додатку для перевірки)

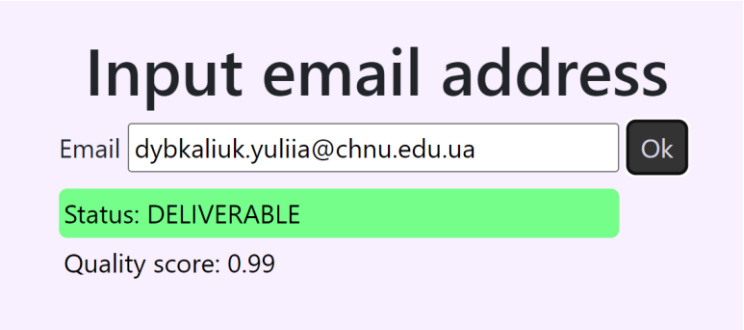
3.3 Приклади застосування розробленого додатку

Розглянемо застосування розробленого в роботі прикладного додатку для верифікації та валідації тестових електронних адрес. Будемо аналізувати значення "Quality score", що відображає впевненість в якості та доступності надісланого електронного листа.

Приклад 1. Для початку протестуємо свої корпоративну та особисту електронні адреси.



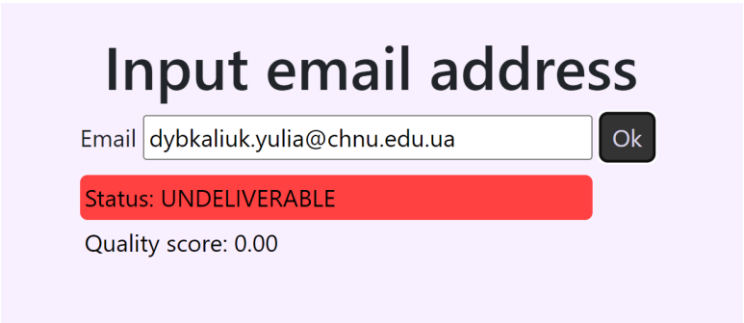
(Рис. 16 Перевірка особистої адреси)



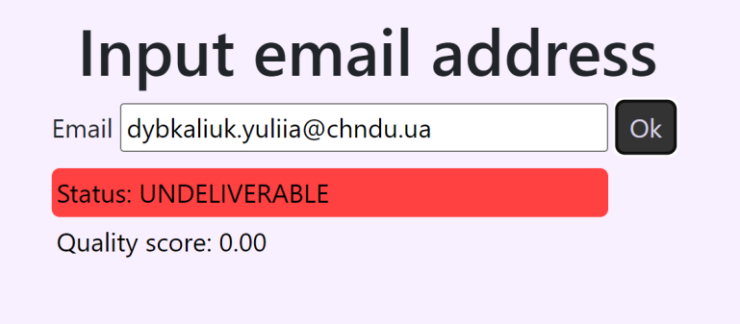
(Рис. 17 Перевірка корпоративної адреси)

При перевірці запропонованих електронних адрес можна побачити позитивний результат та досить високий показник якості відправленого листа.

Для наступного тестування зробимо спеціально помилки при написанні домену та самої адреси та запустимо розроблений додаток на тестування.



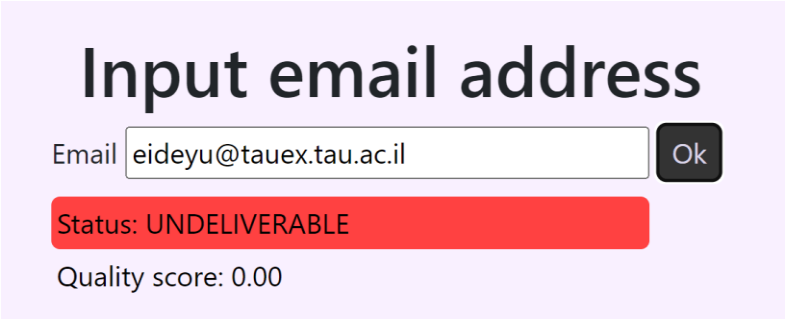
(Рис. 18 Помилка при введені адреси)



(Рис. 19 Помилка при введенні домену)

Як бачимо, очікувано отримали негативні результати.

Приклад 2. Для тестування розглядався наданий список адрес для розсилки до наукового семінару кафедри математичного моделювання присвяченому 85-річчю засновнику та багаторічному завідувачу кафедри професору Степану Дмитровичу Івасишену [19] (Семінар відбувся 10.12.2022). Переважна більшість адрес в результаті перевірки виявились валідними та мали оцінку більше за 0.65 що є хоршими результатами. Але виявилась одна не валідна адреса:



В той же час, під час семінару професор Ю.С. Єйдельман (Ізраїль) підєднався до семінару, використовуючи дану електронну адресу. Це пояснюється тим, що…….

Таким чином, використовуючи даний додаток можна перевірити електронні адреси перед розсиланням листів, щоб переконатись в якості списку адрес для поширення повідомлення та уникнення збільшенню показника відмов.

Висновки

У роботі розглянуто основні функції сервісу електронної пошти, його переваги та недоліки. Досліджено види спаму та описані рекомендації щодо його уникнення.

Детально розглянуто процес розсилки, його види та використання в рекламних кампаніях. Оскільки для ефективної розсилки потрібно контролювати якість списку електронних адрес, проаналізовано відомі інструменти для валідації та верифікації списків розсилки та їх прикладні інтерфейси.

Описано основні інструменти для розробки вебдодатку а саме: платформу Node.js, шаблонізатор EJS. Також детально розглянуто прикладний інтерфейс Abstract, який використовується для верифікації та валідації електронних адрес.

Результатом проведеної роботи є розроблений веб-додаток VeriRen використовуючи платформу Node.js та Abstract API. Даний додаток дозволяє легко здійснити процес перевірки електронних адрес для власного списку розсилки.

Список літератури

1. Закон України про електронні документи та електронний документообіг [Електронний ресурс] — https://zakon.rada.gov.ua/laws/show/851-15#Text
2. Gmail від Google [Електронний ресурс] — https://www.google.com/gmail/about/
3. Outlook [Електронний ресурс] — https://outlook.live.com/owa/
4. AOL [Електронний ресурс] — https://help.aol.com/products/aol-mail
5. Yahoo! [Електронний ресурс] — https://www.yahoo.com/
6. iCloud [Електронний ресурс] — https://support.apple.com/guide/icloud/welcome/1.0/icloud
7. Стаття про м’які та жорсткі відмови [Електронний ресурс] — https://snov.io/knowledgebase/ua/what-are-hard-and-soft-email-bounces-ua/
8. Визначення "спаму" [Електронний ресурс] — https://www.templetons.com/brad/spamterm.html
9. Email Spam Surged [Електронний ресурс] — https://www.hipaajournal.com/email-spam-surged-2016-65-emails-spam-8676/
10. Database Decay Simulation [Електронний ресурс] — https://www.hubspot.com/database-decay?_ga=2.250582277.2096535637.1564061950-651819347.1554889946
11. Документація Abstract API [Електронний ресурс] — https://www.abstractapi.com/
12. Документація Hunter [Електронний ресурс] — https://hunter.io/
13. Документація Captain Verify [Електронний ресурс] — https://captainverify.com/
14. Документація MailBoxLayer [Електронний ресурс] — https://mailboxlayer.com/

15. Документація Email Hippo [Електронний ресурс] — https://tools.emailhippo.com/

16. Node.js in Action Mike Cantelon, Marc Harter, T.J. Holowaychuk, and Nathan Rajlich (книга)

17. Платформа Node.js [Електронний ресурс] — https://nodejs.org/en/

18. Шаблонізатор EJS [Електронний ресурс] — https://ejs.co/

19. https://mail.google.com/mail/u/0/?zx=hvoi1staw25p#inbox/FMfcgzGrbRTLtldRhpCmgcvhXfpvBWxM

Додаток 1
package.json

```
{
  "name": "verivali",
  "version": "1.0.0",
  "description": "app for validation and verification email addresses",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "keywords": [],
  "author": "Yuliia Dybkaliuk",
  "license": "ISC",
  "devDependencies": {
    "nodemon": "^2.0.20"
  },
  "dependencies": {
    "axios": "^1.2.0",
    "ejs": "^3.1.8",
    "express": "^4.18.2",
    "path": "^0.12.7"
  }
}
```

Додаток 2
Index.js

```
const express = require('express');
const path = require("path");
const app = express();
const port = 3001;
const axios = require('axios');

const API_KEY = '05510f59609f4b4ca7851343c5b0aeaf';

app.set("view engine", "ejs")

app.use(express.static(__dirname + '/public'));

app.get("/", (req, res) => {
   res.render("pages/welcome", {title: 'Welcome'});
});

app.get("/info", (req, res) => {
   res.render("pages/info", {title: 'Info'});
});

app.get("/index", (req, res) => {
   res.render("pages/index", {title: 'VeriRen'});
})



app.listen(port, () => {
   console.log(`Server has been started on port ${port}...`);
});
```

Додаток 3
Script checkMail

```
<script>
  const API_KEY = '05510f59609f4b4ca7851343c5b0aeaf'
  function loadXMLDoc() {
    let xhttp = new XMLHttpRequest();
    xhttp.onreadystatechange = function() {
      if (this.readyState == 4 && this.status == 200) {
        //console.log(xhttp.responseText)
        let myObj = JSON.parse(this.responseText);
        //console.log(myObj.deliverability);
        if (myObj.deliverability == "DELIVERABLE"){
          document.getElementsByClassName("result_item")[0].style.backgroundColor="#75FF8AFF";
        }
        if (myObj.deliverability == "UNDELIVERABLE"){
          document.getElementsByClassName("result_item")[0].style.backgroundColor="#FF4141FF";
        }
        if (myObj.deliverability == "RISKY"){
          document.getElementsByClassName("result_item")[0].style.backgroundColor="#B370FFFF";
        }

        document.getElementById("result").innerHTML = "Status: " + myObj.deliverability;
        document.getElementById("score").innerHTML = "Quality score: " + myObj.quality_score;
      }
    };
    let email = document.getElementById('email').value
    let url = "https://emailvalidation.abstractapi.com/v1/?api_key=" + API_KEY + "&email=" + email

    xhttp.open("GET", url, true);
    xhttp.send();
  }
</script>
```