# 5.1. Служби комунікацій

## Електронна пошта

Електронна пошта або E-mail - це комунікаційна технологія, що виконує функції передачі електронних повідомлень через мережу Інтернеті. За допомогою електронної пошти можна надсилати та отримувати повідомлення, відповідати на листи, додавати до листів різні файли, розсилати копії листів одночасно до кількох адресатів, пересилати отриманий лист за іншою адресою, використовувати замість адрес логічні імена, створювати кілька підрозділів поштової скриньки для різного роду кореспонденції.

Електронна пошта не вимагає одночасної присутності обох абонентів на різних кінцях лінії і може бути надіслана до кількох абонентів. Електронна пошта славиться швидкою доставкою, одержувач може використовувати отриману інформацію буквально за кілька секунд.

Втім, використання електронної пошти має певні проблеми, що пов’язані з поштовим спамом і можливістю перехоплення повідомлень зловмисниками. Електронна пошта не може гарантувати збереження приватних даних, тому, не слід вказувати в повідомленнях конфіденційних відомостей.

Для доставки листа необхідно знати електронну адресу одержувача. Адреса електронної пошти складається з імені користувача і домену поштового сервісу, на якому він зареєстрований, з'єднаних знаком @ («ет»). Наприклад, user@gmail.com - це адреса електронної пошти користувача user, зареєстрованого на сервісі Gmail. Адреса пишеться тільки латиницею, регістри літер в поштовій адресі не розрізняються. Якщо адресу написано невірно, то лист потрапить не до того адресату або повернеться до відправника із вказуванням причини повернення.

Електронний лист може складатися не лише з тексту, до тіла листа можна втілювати зображення та відформатовані об’єкти: таблиці, форми тощо. До листа можна прикріпляти файли різних форматів, за виключенням певних самовиконуваних форматів (наприклад, exe чи com) або тих, що мають ознаки макросів чи вірусів. В цьому випадку користувачеві буде видано повідомлення типу «Цей лист заблоковано через потенційно небезпечний вміст».

Для користування електронною поштою призначені спеціальні програми – поштові клієнти, що надають інтерфейс та засоби для отримання, створення та збереження електронних листів. Існує багато різних поштових клієнтів: одні з них є комерційними, інші знаходяться у вільному доступі.

Як правило, поштовий клієнт міститься в стандартному складі любої операційної системи, в Windows - це Windows Mail, в Mac OS — Apple Mail. Стандартні поштові клієнти містяться і в мобільних операційних системах, таких як iOS и Android. Існує багато інших поштових клієнтів, які можна завантажити та встановити самостійно, наприклад Opera Mail, Mozilla Thunderbird, The Bat! та інші. Поштові програми для персональних комп'ютерів використовують різні протоколи для прийому і надсилання пошти.

Іншим способом доступу до пошти є доступ через веб-інтерфейс поштового сервісу з будь-якого пристрою, що має під’єднання до Інтернету для використання пошти в браузері.

Деякі поштові сервіси мають тільки веб-версію свого клієнта. Такі сайти-портали, зазвичай, є багатофункціональними, і однією з їхніх послуг є надання безоплатної електронної скриньки для зареєстрованого користувача.

Електронна пошта може розглядатися як окремий випадок передачі файлів, але вона має ряд особливостей, незвичних для стандартних процедур пересилки файлів.

1. Відправник і одержувач майже завжди люди, а не машини. Це означає, що система електронної пошти складається з двох різних взаємопов'язаних частин: одна забезпечує взаємодію з людиною (наприклад, складання, редагування, читання повідомлень), інша - передачу повідомлень (наприклад, розсилання за списками, забезпечення передачі).
2. Поштові повідомлення представляють собою чітко структурований документ. В багатьох системах кожне надсилання супроводжується значною кількістю додаткових полів. Вони містять ім'я та адресу відправника, ім'я та адресу одержувача, дату і час надсилання листа, перелік осіб, до яких надіслано копію листа, рівень значимості, ступінь секретності.

### Функціонування електронної пошти

Робота електронної пошти ґрунтується на використанні електронних поштових скриньок. На шляху до адресата лист проходить кілька поштових відділень (вузлів). Процес поетапного визначення шляху просування листа називається маршрутизацією (routing).

Електронний лист скеровується з одного сервера до іншого сервера (поштові вузли або релеї), і в результаті доходить до поштового сервера одержувача. Пересиланням повідомлення опікуються спеціальні програми - поштові агенти (рис.1):

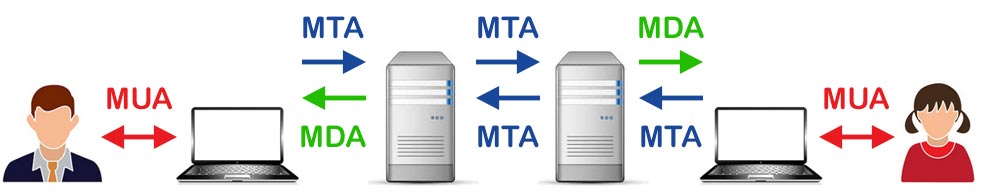


Рис.1. Задіяні поштові агенти для пересилання поштових повідомлень

* **MTA** (Mail Transfer Agent - агент пересилки пошти). Відповідає за пересилання пошти між поштовими серверами; як правило, перший MTA в ланцюжку отримує повідомлення від MUA, останній передає повідомлення до MDA.
* **MDA** (Mail Delivery Agent - агент доставки пошти). Відповідає за доставку пошти до кінцевого користувача.
* **MUA** (Mail User Agent - поштовий агент користувача). Програма, яка забезпечує користувацький інтерфейс, що відображає отримані листи і надає можливість відповідати, створювати, перескеровувати листи.

Повідомлення скеровується на поштовий сервер (MTA, тобто сервер електронної пошти), в завдання якого входить транспортування повідомлень до MTA одержувача. В Інтернеті MTA зв'язуються один з одним за допомогою протоколу SMTP, тому, вони називаються SMTP-серверами (або іноді серверами вихідної пошти) (рис.2).

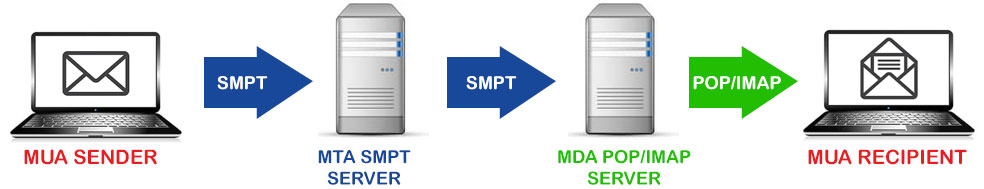


Рис.2. Порядок застосування протоколів під час пересилання повідомлень

MTA одержувача доставляє електронного листа на сервер вхідної пошти (MDA, тобто агент доставки електронної пошти), який зберігає лист в очікуванні його прийому користувачем. Сервери вхідної пошти отримали назви POP-сервери і IMAP-сервери, в залежності від використаного протоколу.

### Основні E-mail протоколи

Користувачі надсилають та отримують повідомлення за допомогою стандартизованих протоколів, які роблять це можливим під управлінням різних типів програмного забезпечення різних серверів, в тому числі в різних мережах.

* Протокол SMTP керує надсиланням та отриманням повідомлень.
* Протоколи POP3 і IMAP дозволяють отримувати і зберігати повідомлення протягом довшого часу.

**POP3 (Post Office Protocol 3)** - за допомогою POP3 протоколу листи вивантажуються в пристрій (наприклад комп'ютер або телефон) і видаляються з сервера. Головним недоліком є те, що за замовчуванням листи на сервері не зберігаються. Також, на сервері не зберігаються надіслані листи, їх можна побачити тільки на тому пристрої, з якого дані листи надіслано. Збереження вхідних листів на сервері та умови їх видалення можна окремо налаштувати в поштовому клієнті.

**IMAP (Internet Message Access Protocol)** - надає доступ до облікових записів електронної пошти на сервері, де їх можна зберігати без вивантаження на пристрій. Пошту можна читати з різних пристроїв і листи, що надіслані з одного пристрою, є доступними в папці «Надіслані» іншого пристрою. Це можливо у випадку, якщо папка «Надіслані» синхронізована на сервері.

При використанні протоколу IMAP листи завжди зберігаються на сервері. Зазвичай, щоночі робляться резервні копії поштових скриньок, тому, за необхідності листи можна завжди відновити. Відновлення з резервної копії є платною послугою і для отримання додаткової інформації слід звернутися в службу підтримки поштового сервісу.

### Клієнтське програмне забезпечення

Використовуючи аналогію зі звичайною поштою, можна сказати, що MTA є своєрідними «поштовими відділеннями» (сортування пошти та доставка), в той час як MDA виконують роль поштових скриньок, які зберігають повідомлення, поки абонент не перевірить свою скриньку.

Щоб запобігти проникненню до пошти сторонніх осіб, MDA захищено іменем користувача (логін) і паролем. Витягування пошти здійснюється за допомогою програми MUA (клієнт електронної пошти).

* Якщо MUA встановлено на комп'ютері користувача, - це клієнт електронної пошти (такий як Mozilla Thunderbird, Microsoft Outlook, Opera Mail чи інші).
* Якщо ж в якості MUA виступає веб-інтерфейс, що використовується для взаємодії з сервером вхідної пошти, він називається веб-поштою.

## Безпека електронної пошти

Електронна пошта може бути вразливим сегментом роботи комп'ютера. Зазвичай, файли звичайних користувачів хакерів цікавлять мало, але нашкодити заради гри або з можливістю отримання вигоди - це ймовірно.

Доступ до чужої поштової скриньки може відкрити зловмиснику шлях до персональних даних його власника, включаючи електронні гаманці, та інші, цілком матеріальні ресурси. Отже, злам пошти — це ще й спроба стати власником чужої інформації та чужих грошей.

### Основні способи зламу електронної пошти.

#### Використання Трояна

Програма Троян насправді це щось більше за вірус. Це системний комплекс, який може серйозно пошкодити інформацію, що зберігається в пам'яті комп'ютера. Наприклад, він може її видалити або зашифрувати.

Зазвичай, Троян прикріплюється до електронного листа як ехе-файл, з яким потрібно зробити певні дії: завантажити, встановити тощо. У разі відкривання такого файлу, Троян поширюється на всі адреси, що прописані в адресній книзі електронної пошти. Таким чином, разом із отримувачем Трояна можуть постраждати його друзі та знайомі.

#### Віруси у текстових файлах та зображеннях

Ця категорія може класифікуватись як вірусна програма. Це може бути розсилка з різного роду змістом. Наприклад, лист з попередженням про те, що з'явився новий вірус і рекомендацією не відвідувати підозрілі веб-ресурси. Також пропонується це повідомлення надіслати до інших користувачів.

#### Лавинне розсилання (флуд)

Ситуація, коли зловмисник перевантажує систему, надсилаючи величезну кількість поштових повідомлень з метою паралізувати роботу поштового сервера. Без належного захисту, сервер буде змушений постійно відмовляти клієнтам в обслуговуванні, оскільки його локальний диск буде переповнений непотрібними повідомленнями. Система може припинити обслуговування і з іншої причини - через те, що всі її ресурси будуть витрачатися на обробку повідомлень, що надійшли.

Лавинне розсилання не є зламом поштової скриньки з метою отримання доступу до нього. Це швидше спосіб домогтися того, щоб поштова скринька була переповнена, і тому недоступна для отримання нових листів, які можуть бути дуже важливими для власника пошти. Якщо поштова скринька має весь зайнятий об'єм, то така пошта автоматично стає недоступною.

#### Спам

Зі збільшенням числа організацій, що пропонують свої послуги в інтернеті, мережею стало передаватися багато непотрібної рекламної та іншої інформації. Такі повідомлення, які називають спамом, зазвичай надсилаються до всіх учасників великих списків розсилки і потрапляють у поштові скриньки багатьох користувачів.

#### Шахрайство

До вірусного спаму можна віднести так звані «нігерійські листи», які набули масового поширення в Нігерії в середині 1980-х років звичайною поштою. У цих листах адвокат з Африки нібито розшукує спадкоємців померлого багатого родича. Користувач, звісно, потрапляє до категорії можливих спадкоємців. Йому пропонується перерахувати адвокату певну суму грошей у перспективі отримати «спадщину» як сплату податків, хабарі чиновникам, оформлення угод тощо.

Крім нігерійських листів, бувають пропозиції спробувати чарівний гаманець нібито з можливістю заробити за допомогою WebMoney.

#### Фішинг

Поштову скриньку може заблокувати адміністрація поштового сервісу. На додаткову поштову скриньку, вказану при реєстрації надходить повідомлення, що Вашу поштову скриньку заблоковано.

Такі листи від адміністрації поштового сервісу можуть бути справжніми, а можуть бути фішинговими (підробленими), наприклад, з метою отримання пароля для доступу до пошти. У цьому випадку краще самостійно звернутися до служби підтримки поштової служби та уточнити у них, чи надсилали вони такий лист або це фішинг (підробка). Справжні адміністрації ніколи не вимагають і не просять надіслати пароль до поштової скриньки.

#### Витік конфіденційної інформації

Перш ніж лист потрапить до одержувача, він проходить через багато непідконтрольних користувачеві систем. Якщо важливе повідомлення не є зашифрованим, зловмисники можуть перехопити та прочитати його у будь-якій точці маршруту пересилання.

### Засоби захисту електронної пошти

Для захисту від лавинної розсилки та спаму слід правильно налаштувати сервер електронної пошти. Більшість поштових програм передбачають засоби захисту від таких атак. Крім того, можна звернутися до провайдера інтернету з проханням надати додатковий захист від таких атак.

Додаткові заходи захисту, які необхідно вжити, залежать від необхідного рівня конфіденційності та засобів захисту, передбачених у додатках електронної пошти. Наприклад, чи достатньо буде застосувати конфіденційність лише щодо вмісту електронного повідомлення? Або потрібно зробити конфіденційною всю інформацію, що стосується електронної пошти, включаючи IP-адреси відправника та одержувача?

У деяких поштових клієнтах передбачені вбудовані засоби захисту, яких може бути достатньо для потреб користувача. Наприклад, Lotus Notes Domino містить вбудовані функції захисту, які дозволяють, зокрема, шифрувати весь документ або його окремі поля.

Під час шифрування електронних листів Lotus Notes Domino створює унікальні особисті та спільні ключі для кожного користувача. Своїм особистим ключем відправник зашифровує повідомлення, і його зможуть прочитати лише користувачі, які мають спільний ключ. Таким чином, для того, щоб інші користувачі могли розшифровувати ваші повідомлення, їм потрібно надіслати особистий ключ. Якщо отримувач отримує зашифрований лист, Lotus Notes Domino розшифровує його за допомогою загального ключа відправника.

Відомості про ці функції шифрування Notes наведено в електронній довідковій системі програми.

Організувати безпечну передачу конфіденційної інформації по відкритих мережах за допомогою електронної пошти можна в різний спосіб.

Якщо поштовий сервер підтримує протокол SSL (Secure Sockets Layer), за допомогою SSL можна створити захищений сеанс між сервером і клієнтами електронної пошти. SSL підтримує необов'язкову ідентифікацію клієнта, якщо програма клієнта передбачає таку ідентифікацію. Оскільки шифрується весь сеанс, SSL гарантує цілісність даних під час їх передачі.

Інший спосіб полягає у застосуванні віртуальної приватної мережі (VPN). У системі можна настроїти різні з'єднання VPN, у тому числі з'єднання з віддаленими клієнтами. У разі застосування VPN шифрується весь потік між кінцевими точками з'єднання, що гарантує як конфіденційність, так і цілісність даних, що передаються.

## Популярні поштові сервіси в Україні

### GMail (<https://gmail.com>)

Cервіс GMail з'явився на ринку в 2004 році, сьогодні кількість його користувачів у всьому світі вище за мільярд і підтримка більше 80 мов.

Gmail має лаконічний інтерфейс, де більша частина головного екрану відводиться під листи. Сервіс має неймовірно багатий функціонал: повідомлення автоматично розподіляються за категоріями, спам-фільтр дуже надійний і не пропускає нічого зайвого.

Інтерфейс GMail універсальний і дозволяє працювати з будь-якими поштовими акаунтами, що підтримують стандарти IMAP або POP. За замовчуванням кожен користувач отримує 15 Гб місця в поштовій скриньці. Такий обсяг є загальним для всього Google-акаунту, а тому використовується і іншими сервісами, таких як Google Photo або Google Drive.

У Google також є платна бізнес-версія GMail, що входить до пакету G-Suite. Це більш професійний продукт, який дозволяє створювати і використовувати адреси з унікальними доменними іменами, (на зразок yourname@yourcompany.tld).

Заводячи пошту на GMail, користувач підписується на весь пакет послуг Google. Акаунт Gmail - це доступ до всіх програм і сервісів Google.

Безпека в Gmail на дуже високому рівні. При будь-якій підозрі в тому, що пошту використовує не власник, сервіс надсилає повідомлення і просить підтвердження. З огляду на тісний зв'язок акаунту зі всіма сервісами Google, це цілком адекватні запобіжні заходи. Для максимальної безпеки бажано увімкнути двохфакторну аутентифікацію і налаштувати додаткову скриньку для відновлення паролю.

### UKR.net Пошта (<https://mail.ukr.net/>)

Український портал Ukr.net має зручний і комфортний поштовий сервіс. Безкоштовна, швидка пошта Ukr.net має багато переваг перед аналогічними ресурсами.

* Можливість надсилати великі за обсягом листи (до 1,5 ГБ).
* Скриньку надійно захищено від спаму та вірусів.
* Безкоштовний віртуальний e-Disk, з об'ємом пам'яті 4 Гб. Можна безстроково зберігати різні файли в надійно захищеному сховищі.
* Інтерфейс сервісу доступний українською, російською та англійською.
* Можливість надсилати листи з іншої адреси, тим самим, не залишаючи поштову скриньку.
* Наявність мобільного додатку для телефонів.
* Широкий вибір смайликів, які роблять листування набагато цікавіше.

На сервісі зареєстровано понад 6 мільйонів поштових скриньок, тому пошта Ukr.net утримує лідируючі позиції в Україні. Для початківців присутні спеціальні підказки в кожному розділі, щоб користуватися всіма запропонованими функціями і зручностями.

### I.UA (<https://mail.i.ua/>)

Поштовий сервіс від порталу I.UA має простий і зручний інтерфейс трьома мовами: українською, російською або англійською.

* Можливість пересилати файли до загальним розміром до 8Гб. Файли розміром до 20Мб можуть пересилатися разом з листом. Файли розміром від 20 Мб завантажуються на сервер I.UA, а одержувачеві приходить посилання на його швидке вивантаження.
* Захист від вірусів і спаму. Наявність власної антивірусної системи, системи «Карантин» та антиспам системи, яку можна навчати.
* Великий розмір поштової скриньки, після реєстрації - 1Гб, при активному використанні об'єм автоматично збільшується.
* Автоматичне збирання пошти з інших скриньок, зручне сортування листів, наявність автовідповідача та пере адресації на інші адреси
* Для підвищення безпеки є можливість активувати автоматичне ведення журналу, в якому фіксуються всі заходи на поштовий акаунт. Можна обмежити доступ до скриньки тільки із заданих IP адрес.
* Наявний мобільний додаток для телефонів. Отримання повідомлення про нові листи за допомогою SMS та сповіщень на комп’ютері.
* Корисні дрібниці: вивантаження великого числа прикріплених до листа файлів одним архівом; швидке додавання прикріплених до листа зображень у фотоальбоми на I.UA; форматування тексту листа; зручна робота з контактами.

### <МЕТА> - Україна (<https://webmail.meta.ua/>)

Пошта МЕТА.ua надає широкі можливості з обробки поштових повідомлень, гнучкий, зручний користувацький інтерфейс. Легке налаштування функцій, перевірка повідомлень на наявність вірусів, максимально можливе розмежування справжніх листів від спаму. Після реєстрації в МетаПаспорті автоматично створюється поштова скринька.

* Обсяг безкоштовної поштової скриньки - 0,1 Гб з можливістю збільшення не частіше ніж раз на місяць.
* Інтерфейс сервісу доступний українською, російською та англійською.
* Мобільний додаток відсутній.
* Збір пошти з інших скриньок можливий не частіше ніж через 3 години, і не більше 200 листів за раз (повідомлення більше 30 МБ не будуть прийняті).
* Пошта передається по незахищеному з'єднанню і тому неналежний захист акаунту.

## Популярні поштові клієнти

Поштові програми для комп'ютера дозволяють більш гнучке користування електронною кореспонденцією. Фільтри, правила, ярлики і багато іншого, а головне - доступ офлайн, до того, що було завантажено раніше.

### Mozilla Thunderbird (<https://www.thunderbird.net/uk/>)

Поштовий клієнт Mozilla Thunderbird є багатофункціональним інструментом від Mozilla.

* Підтримка будь-якої кількості акаунтів.
* Можливість розширення за рахунок плагінів.
* Обмежені можливості календаря.

Поштовий клієнт від Mozilla працює зі сторонніми плагінами, що дозволяє істотно розширити можливості програми. Окрім читання і надсилання листів, Thunderbird без плагінів дозволяє читати RSS канали.

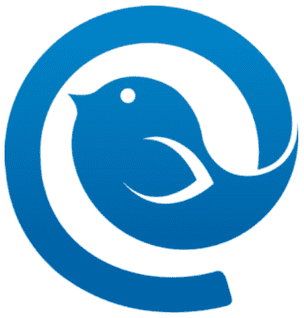
Налаштувати клієнт доволі просто, більшість корисних функцій вже встановлено за замовчуванням.

### eM Client (<https://www.emclient.com/>)

Головний конкурент Thunderbird на ринку безкоштовних поштових клієнтів. Серед корисних переваг - проста міграція з інших поштових програм і розумний перекладач.

* Прості інструменти міграції.
* Вбудований чат, перекладач.
* Підтримує лише два акаунти.

Історія eM Client налічує вже 10 років, і він вважається кращим поштовим клієнтом для Windows. eM Client дозволяє легко і швидко перенести свої повідомлення з Gmail, Exchange, iCloud і Outlook.com, має вбудований пошук, календар і адресну книгу. Вбудований чат підтримує роботу зі сторонніми месенджерами, наприклад, Jabber або Google Chat.

З додаткових можливостей - відтерміноване надсилання повідомлень і шифрування.

### Mailbird Lite (<https://www.getmailbird.com/ru/>)

Поштовий клієнт з широкими соціальними можливостями

* Інтеграція з соціальними сервісами.
* Легке встановлення.
* Підтримує тільки один акаунт.

Mailbird Lite - це платформа для комунікацій, що розширює можливості програми для ведення розкладів, чатів, синхронізації файлів і командної роботи. До пошті можна додати Facebook акаунт, WhatsApp, Календар Google, безкоштовний менеджер завдань Moo.do і додаток Asana для колективної роботи.

У безкоштовної версії є певні обмеження, наприклад не підтримується попередній перегляд вкладених до листів файлів до їх відкривання.

### The Bat! (<https://www.ritlabs.com/ru/products/thebat/>)

Головними завданнями The Bat! є збереження конфіденційності листування, зручність і економія часу при роботі з поштою.

The Bat! це умовно-безкоштовний поштовий клієнт для операційних систем Microsoft Windows. Він комплексно захищає інформацію, в тому числі шифруванням даних користувача на твердому диску і шифруванням трафіку за допомогою протоколів SSL/TLS.

The Bat! забезпечує таємницю листування, оскільки працює без використання глобальних постачальників послуг електронної пошти та веб-інтерфейсу. Листи зберігаються на комп'ютері користувача, а не в хмарних сховищах, де можуть бути доступні стороннім особам. The Bat! дозволяє працювати з необмеженою кількістю поштових скриньок, обробляти і зберігати необмежену кількість листів.

## Контрольні питання

1. Перелічити причини, з яких причин електронного листа не можна надіслати? Чому?
2. Які програми-агенти призначені для керування надсиланням та прийманням електронних листів, їх функції?
3. Навести перелік поштових протоколів. В чому полягає їх відмінність?
4. Які принципові відмінності є між протоколами POP3 і IMAP?
5. Перелічіть основні способи зламу електронної пошти.
6. Які небезпеки створює лавинне розсилання повідомлень на пошту?
7. Перелічіть заходи захисту електронної пошти
8. Яким чином віруси можуть попасти з електронної пошти?
9. Проаналізувати можливості поштового серверу Gmail
10. В яких випадках встановлюють спеціалізований поштовий клієнт?

## Використані джерела

1. Електронна пошта Email <https://zvondozvon.ru/tehnologii/kompyuternye-seti/email>
2. Протоколи електронної пошти <https://coderlessons.com/tutorials/akademicheskii/internet-tekhnologii/protokoly-elektronnoi-pochty-2>
3. Поштовий клієнт - <https://sendpulse.ua/ru/support/glossary/email-client>
4. Поштовий сервер <https://itelon.ru/blog/pochtovyy-server/>
5. SMTP-протокол <https://selectel.ru/blog/smtp-protocol/>
6. Поштовий сервер Gmail - <https://gmail.com>
7. Налаштування Gmail для користувачів - <https://support.google.com/a/answer/173555?hl=ru>
8. Кращі поштові клієнти - <https://pcgramota.ru/best-email-clients/>