# 4.1. 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 славиться швидкою доставкою, одержувач може використовувати отриману інформацію буквально за кілька секунд.

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.

Існує кілька можливих причин, з яких електронний лист не може бути доставлено одержувачу.

* Неправильна адреса електронної пошти. Варто перевірити правильність написання адреси електронної пошти та переконатися, що немає помилок або інших помилок.
* Якщо поштова скринька в отримувача переповнена лист може бути відхилено та повернено відправнику.
* Поштовий сервер одержувача може виявити шкідливі вкладення листа. У таких випадках лист може бути повністю відхилений.
* Лист може бути відфільтрований поштовими фільтрами спаму на стороні отримувача. Якщо лист містить ознаки спаму або його відправник є підозрілим, він може бути автоматично переміщений до папки "спам" або видалено.
* Тимчасові проблеми з мережею або сервером можуть статися як на стороні відправника, так і на стороні отримувача.
* Отримувач може мати налаштування, які блокують листи від певних відправників або доменів. Якщо відправник перебуває у блокуванні, лист не буде доставлений.
* Некоректні параметри DNS поштового сервера можуть перешкоджати доставці листів.

Якщо лист не доставлено, рекомендується перевірити правильність адреси одержувача, перевірити папку "спам" або дізнатися причину проблеми з доставкою в оператора поштового сервера.

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 (файли .js). В цьому випадку користувачеві буде видано повідомлення типу «Цей лист заблоковано через потенційно небезпечний вміст».

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.

### Поштові клієнти

Для користування електронною поштою призначені спеціальні програми – поштові клієнти, що надають інтерфейс та засоби для отримання, створення та збереження електронних листів. Поштові клієнти використовують різні протоколи для прийому і надсилання пошти.

* 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.
* Спеціалізовані поштові клієнти, які можна завантажити та встановити самостійно на конкретний пристрій, наприклад Opera Mail, Mozilla Thunderbird, The Bat! та інші.
* Поштові клієнти з веб-інтерфейсом надають доступ до поштового сервісу з будь-якого пристрою. 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. Наприклад Ukr.net, I.ua, Meta.ua.

### Функціонування електронної пошти

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

Робота електронної пошти ґрунтується на використанні електронних поштових скриньок, де відправник і отримувач 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).

На шляху до адресата лист проходить кілька поштових відділень (вузлів). Електронний лист скеровується з одного сервера до іншого сервера (поштові вузли), і в результаті доходить до поштового сервера одержувача. Пересиланням повідомлення опікуються спеціальні програми - поштові агенти (рис.1):

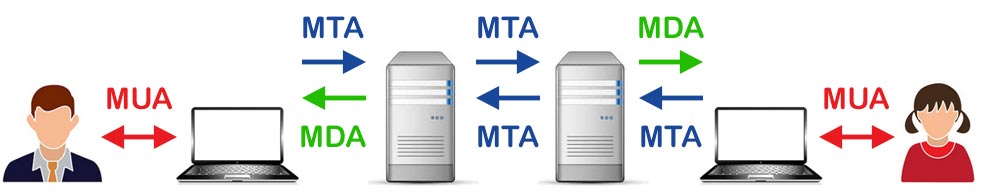


Рис.1. Задіяні поштові агенти для пересилання поштових повідомлень

* **MUA** (Mail User Agent - поштовий агент користувача). Програма, яка забезпечує користувацький інтерфейс, що відображає отримані листи і надає можливість відповідати, створювати, перескеровувати листи.
* **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.

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).

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 (рис.2).

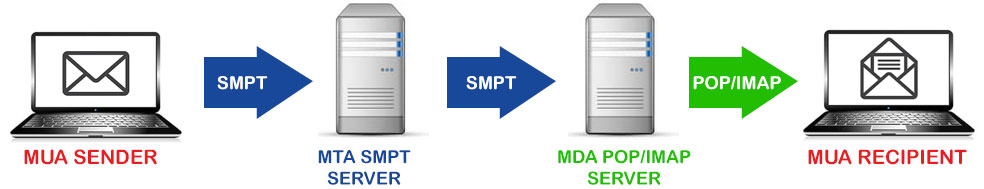


Рис.2. Порядок застосування протоколів під час пересилання повідомлень

### Основні поштові протоколи

Користувачі надсилають та отримують повідомлення за допомогою стандартних протоколів.

**SMTP (Simple Mail Transfer Protocol)** – це стандартний протокол, який є важливим стандартом для електронної пошти та забезпечує надійну доставку повідомлень між поштовими серверами.

Протокол SMTP забезпечує механізм надсилання пошти від клієнта (наприклад, поштового клієнта) до поштового сервера. Клієнт встановлює з'єднання з сервером та передає лист для доставки. SMTP дозволяє поштовим серверам надсилати листи один одному.

SMTP підтримує різні методи аутентифікації, які дозволяють клієнтам проходити автентифікацію перед надсиланням листів. Це допомагає запобігти несанкціонованому надсиланню листів і підвищує безпеку процесу. Якщо лист не може бути доставлений з будь-якої причини, SMTP повертає звіт про помилку відправнику, щоб він міг вжити відповідних заходів.

**POP3 (Post Office Protocol 3)** - за допомогою POP3 протоколу листи вивантажуються на пристрій (наприклад комп'ютер або телефон) і видаляються з сервера. Головним недоліком є те, що за замовченням 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

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.

Доступ до чужої поштової скриньки може відкрити зловмиснику шлях до персональних даних його власника, включаючи електронні гаманці, та інші, цілком матеріальні ресурси.

#### Основні загрози, з якими стикаються електронні листи:

**Спам** – це небажані повідомлення, які можуть містити рекламу, шахрайські схеми, віруси чи інші шкідливі посилання. Спам засмічує поштову скриньку та є потенційною загрозою для безпеки, оскільки деякі повідомлення можуть містити шкідливі вкладення або посилання на фішингові сайти.

**Фішинг** - це вид шахрайства, при якому зловмисники видають себе за довірені організації або особи з метою отримання особистих даних, таких як паролі, номери кредитних карток або соціальні номери. Фішингові листи можуть виглядати автентично та можуть містити посилання на фальшиві веб-сайти, де зловмисники можуть збирати особисту інформацію.

Електронна пошта може містити **шкідливі програми**, такі як віруси, трояни або шпигунське програмне забезпечення. Ці програми можуть бути вкладені в листи або маскуватись під безпечні файли. Відкриваючи шкідливі вкладення або переходячи за шкідливими посиланнями, користувач може піддати свою систему ризику зараження та порушення безпеки даних.

* **Програма Троян** - 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** - 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.

Зловмисники можуть використовувати **методи соціальної інженерії**, щоб переконати користувачів розкрити особисту інформацію чи виконати шкідливі дії. Наприклад, вони можуть надіслати електронний лист, вдавши з себе представника банку або іншої довіреної організації, і попросити користувача надати свої облікові дані.

Деякі поштові клієнти та сервери можуть мати **вразливості**, які можуть бути використані зловмисниками для вторгнення в систему або перехоплення електронної пошти. Це може призвести до несанкціонованого доступу до конфіденційних даних або використання поштового сервера для масового розсилання спаму.

#### Для захисту електронної пошти рекомендується:

* Використовувати надійні антивірусні програми та програми захисту від спаму.
* Наявність захищеного з'єднання (HTTPS) при вході до своєї пошти або введення
* Складні та унікальні паролі для облікового запису електронної пошти. Пароль має бути досить довгим і містити комбінацію літер, цифр та спеціальних символів. Уникати використання паролів, що легко вгадуються, таких як дати народження або прості послідовності.
* Двофакторна аутентифікація (2FA) для облікового запису електронної пошти. Це додає додатковий рівень безпеки, вимагаючи другий фактор підтвердження, наприклад, одноразовий код, надісланий на мобільний телефон після введення паролю.
* Оновлення програмного забезпечення поштового клієнта та операційної системи. Оновлення часто містять виправлення вразливостей безпеки, які допомагають захистити від відомих загроз.
* Обережність при відкриванні вкладень або переході за посиланнями у листах. Якщо немає впевненості у його справжності, краще не відкривати. Те саме стосується і посилань - перевіряти URL-адресу перед тим, як перейти по ньому. Не розкривати особисту інформацію або облікові дані у відповідь на електронні запити, якщо немає впевненості у автентичності відправника.
* За можливістю використовувати шифрування для електронної пошти. Шифрування допомагає захистити листи від несанкціонованого доступу. Можена використовувати шифрування на основі сертифікатів (наприклад, S/MIME) або використовувати end-to-end шифрування за допомогою інструментів, подібних до PGP (Pretty Good Privacy).
* Обережність під час використання відкритих Wi-Fi для доступу до електронної пошти. Такі мережі можуть бути небезпечними і зловмисники можуть перехоплювати інформацію. Використовувати віртуальну приватну мережу (VPN), щоб забезпечити шифрування та безпеку інтернет-з'єднання.

Прийняття цих заходів безпеки допоможе зміцнити захист електронної пошти та запобігти багатьом поширеним загрозам.

## 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/>