УДК 004.7

КОМП'ЮТЕРНІ МЕРЕЖІ

Реут Є.С., здобувач вищої освіти *e-mail: reut11iunya@gmail.com*
Темніков Г.Є., старший викладач *e-mail:tegeev@ukr.net*
Таврійський державний агротехнологічний університет імені Дмитра Моторного

Актуальність та постановка проблеми. Сучасні комп'ютерні мережі є важливим елементом інформаційної інфраструктури, що забезпечує зв'язок, обмін даними та ефективну взаємодію між системами і користувачами. Актуальність цієї теми зумовлена стрімким розвитком цифрових технологій, зростанням обсягів інформації та потребою у забезпеченні безпечної та стабільної роботи мереж. Основними аспектами, які вивчаються у дослідженні, є типи комп'ютерних мереж, мережеві протоколи, безпека мереж, управління мережею, а також передача даних і стандарти мережевої взаємодії.

Наукова проблема полягає у потребі підвищення ефективності функціонування мереж шляхом покращення безпеки та протоколів передачі даних. Гіпотеза дослідження передбачає, що оптимізація мережевих протоколів і вдосконалення методів управління мережею дозволять підвищити стабільність та безпеку мереж. Новизна даного дослідження полягає у комплексному аналізі типів мереж та протоколів з акцентом на вдосконалення управління мережею і забезпечення її безпеки, що є важливим для ефективної експлуатації мережевих систем у різних сферах.

Основні матеріали дослідження. Спочатку розглянемо існуючи типи комп'ютерних мереж. Комп'ютерні мережі класифікуються за масштабом і призначенням, що дозволяє ефективно використовувати їх для різних потреб. Основними типами мереж є локальні (LAN), міські (MAN) та глобальні (WAN) (рис. 1).

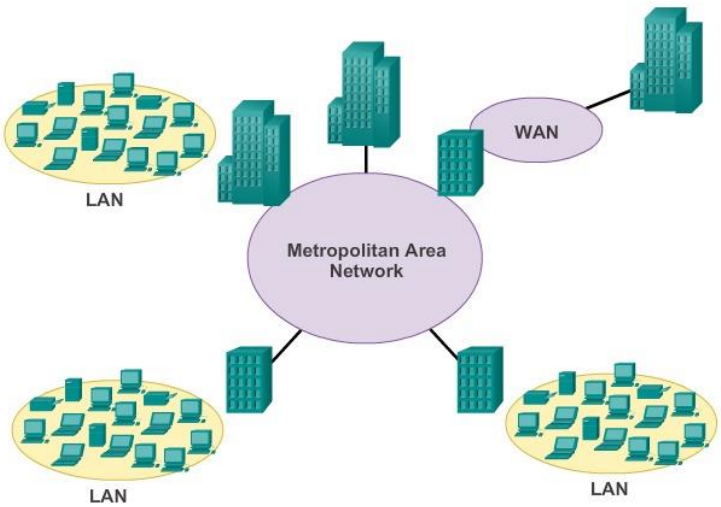

Рисунок 1 – Основні типи комп'ютерних мереж

А саме, мережі бувають:

1) *Локальні мережі* (LAN) – охоплюють невеликі географічні зони, такі як офіси, будівлі або групи будівель. Вони зазвичай використовуються для

підключення комп'ютерів у межах однієї організації або закладу. LAN характеризується високою швидкістю передачі даних і низькою затримкою. Основними технологіями, які застосовуються в локальних мережах, є Ethernet та Wi-Fi, що дозволяють забезпечити швидку та стабільну роботу. Такі мережі ідеально підходять для обміну інформацією, доступу до спільних ресурсів і роботи із серверними системами в межах одного підприємства.

2) Міські мережі (MAN) (Metropolitan Area Network) – обслуговують більші території, зазвичай місто або кілька населених пунктів. MAN поєднує кілька локальних мереж і забезпечує зв'язок між ними на більших відстанях. Такий тип мереж використовується для організацій з кількома офісами в різних районах міста, або для надання інтернет-послуг на міському рівні. MAN використовує технології оптоволоконних кабелів та бездротових з'єднань, що дозволяють передавати великі обсяги даних на високих швидкостях.

3) Глобальні мережі (WAN) (Wide Area Network) – охоплюють великі географічні області, що можуть включати країни або навіть континенти. WAN поєднує різні мережі на великі відстані, дозволяючи організаціям з багатьма офісами, розташованими в різних країнах, функціонувати як єдина мережа. Інтернет є найвідомішим прикладом глобальної мережі. Для WAN використовуються складні технології, такі як супутникові зв'язки, оптоволоконні кабелі та інші канали зв'язку, що забезпечують стабільну роботу і швидкий обмін інформацією на глобальному рівні.

Таким чином, кожен тип мережі має свої особливості та сфери застосування: локальні мережі – для обмежених географічних територій з високою швидкістю передачі, міські – для середніх відстаней і високої пропускної здатності, а глобальні – для з'єднання на великих відстанях, охоплюючи цілі країни чи континенти [1].

Мережеві протоколи.

Мережеві протоколи регулюють обмін даними між пристроями в мережі, забезпечуючи їхню взаємодію. Основними протоколами (табл. 1) є TCP/IP, UDP, HTTP, FTP та DNS [2].

Таблиця 1 – Поширені порти мережевих протоколів

Номер порту і протокол	**Опис**
8080/TCP	HTTP, застосовується проксі-серверами
3128/TCP	
443 / TCP, UDP	HTTP, за допомогою TLS або SSL
80 / TCP, UDP	HTTP
53 / TCP, UDP	DNS
30000-35000	FTP (пасивні порти)
21/TCP	FTP (для передачі команд)
20/TCP	FTP-data (для надсилання інформації по FTP)

TCP/IP (Transmission Control Protocol/Internet Protocol) — ключовий протокол для передачі даних в Інтернеті. TCP відповідає за розбиття даних на пакети та їхню надійну доставку, а IP — за маршрутизацію. Це основний протокол для надійної передачі даних (електронна пошта, веб-серфінг).

– UDP (User Datagram Protocol) — протокол для швидкої, але менш надійної передачі даних без перевірки на помилки. Використовується в додатках, де важлива швидкість, таких як онлайн-ігри та потокове відео.

– HTTP (Hypertext Transfer Protocol) — протокол для передачі гіпертексту, що використовується для взаємодії з веб-сайтами. HTTPS — захищена версія

протоколу з підтримкою шифрування.

– FTP (File Transfer Protocol) — протокол для передачі файлів між клієнтом і сервером. Використовується для завантаження та передавання великих файлів через мережу.

– DNS (Domain Name System) — перетворює доменні імена на IP-адреси, спрощуючи доступ до ресурсів Інтернету (рис. 2).

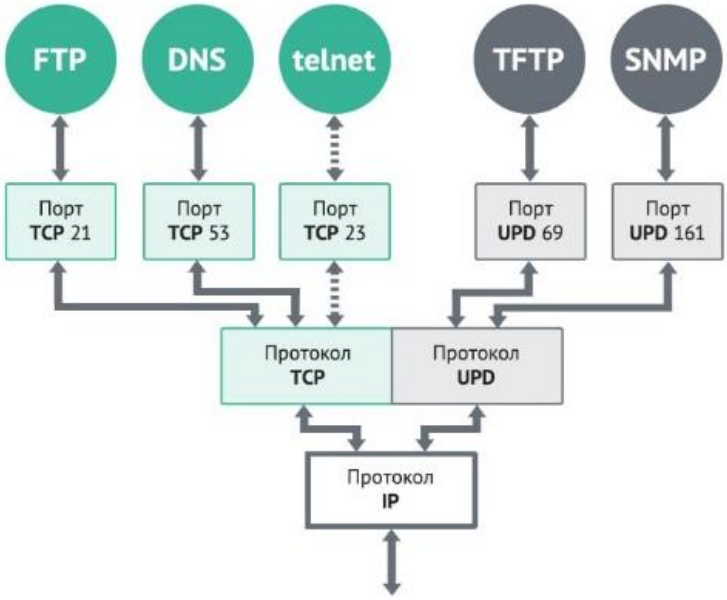

Рисунок 2 - Розподіл пакета даних IP за сервісами

Кожен з цих протоколів виконує специфічну функцію, забезпечуючи ефективну роботу мереж.

Безпека мереж. Безпека мереж є критично важливим аспектом забезпечення стабільної та надійної роботи комп'ютерних систем. Вона охоплює різноманітні технології, методи і протоколи, спрямовані на захист даних і ресурсів від несанкціонованого доступу, кібератак та інших загроз. Основними компонентами безпеки мереж є шифрування, аутентифікація, брандмауери, системи виявлення вторгнень та резервне копіювання даних.

Шифрування даних – це процес перетворення інформації в закодований вигляд, який можна прочитати лише за наявності відповідного ключа. Шифрування захищає конфіденційність даних під час передачі через мережу, що є особливо важливим для фінансових і особистих даних.

Аутентифікація є процесом перевірки особи або системи, що намагається отримати доступ до мережі. Використання багатофакторної аутентифікації, що поєднує кілька методів перевірки (наприклад, пароль і смс-код), значно підвищує рівень захисту.

Брандмауери – це мережеві пристрої або програмні рішення, які контролюють вхідний і вихідний трафік, запобігаючи несанкціонованому доступу до мережі. Вони можуть фільтрувати трафік за різними критеріями, такими як IP-адреси, порти та протоколи.

Системи виявлення вторгнень (IDS) моніторять мережевий трафік на предмет підозрілої активності, виявляючи потенційні загрози та атаки. IDS можуть бути як активними, так і пасивними, надаючи адміністраторам інформацію для реагування на загрози.

Резервне копіювання даних є важливим елементом безпеки, що дозволяє відновити інформацію у разі її втрати внаслідок кібератаки або технічних збоїв. Регулярне резервне копіювання гарантує, що важливі дані не будуть втрачені.

Загалом, безпека мереж є багатогранним поняттям, що включає в себе технології, процеси та найкращі практики, які разом забезпечують захист інформації і ресурсів від численних загроз у цифровому світі.

Управління мережею.

Управління мережею – це процес моніторингу, контролю та оптимізації роботи комп'ютерних мереж, що забезпечує їхню ефективність, стабільність і безпеку. Воно охоплює ряд важливих аспектів, таких як *моніторинг мережі, управління трафіком, конфігурація пристроїв, виявлення та усунення збоїв і оптимізація продуктивності.* А саме:

– *Моніторинг мережі* – це постійне відстеження стану мережі та її компонентів, що дозволяє виявляти проблеми на ранніх стадіях. Використання спеціалізованих інструментів моніторингу дає змогу адміністраторам отримувати інформацію про завантаженість мережі, затримки, втрати пакетів та інші критично важливі показники (рис. 3).

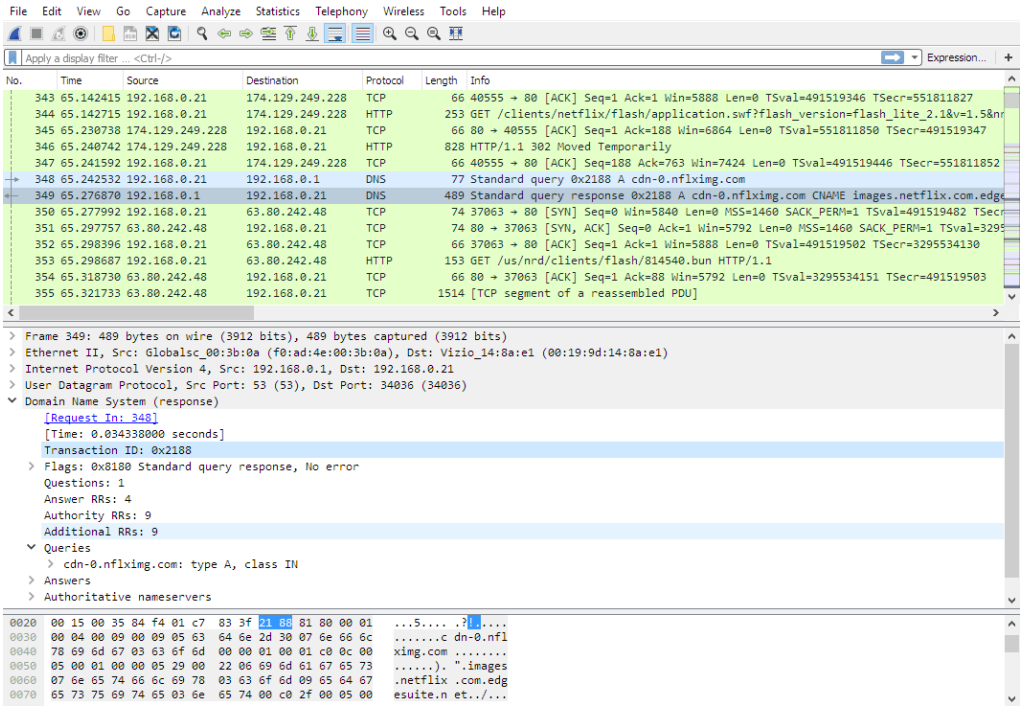

Рисунок 3 – ПЗ для моніторінгу мереж «WireShark»

– *Управління трафіком* полягає в контролі й оптимізації потоку даних у мережі. Це може включати пріоритизацію трафіку для критично важливих застосунків або обмеження використання ресурсів для менш важливих. Технології, такі як QoS (Quality of Service), допомагають забезпечити стабільну роботу мережі в умовах великого навантаження.
– *Конфігурація пристроїв* охоплює налаштування маршрутизаторів, комутаторів, брандмауерів та інших мережевих компонентів. Правильна конфігурація є ключовою для забезпечення безпеки і продуктивності мережі.
– *Виявлення та усунення збоїв* є критично важливими для підтримки безперервності роботи мережі. Системи виявлення збоїв автоматично моніторять стан мережі і сповіщають адміністратора про проблеми, що виникають, що дозволяє швидко реагувати на ситуації, які можуть призвести до перерви в обслуговуванні.

– *Оптимізація продуктивності мережі передбачає використання аналітики* даних і звітності для виявлення вузьких місць і можливостей для

покращення. Застосування методів, таких як балансування навантаження, може допомогти рівномірно розподілити трафік між кількома серверами або мережевими шляхами.

Управління мережею є критично важливим елементом для підтримки стабільності, продуктивності та безпеки комп'ютерних мереж. Воно дозволяє організаціям максимально використовувати свої мережеві ресурси і забезпечувати безперервний доступ до необхідних послуг і інформації [3].

Передача даних.

Передача даних – це процес обміну інформацією між пристроями в комп'ютерних мережах. Основні аспекти цього процесу включають швидкість передачі, пропускну здатність, затримку та надійність. А саме:

– Швидкість передачі даних вимірюється в бітах на секунду (bps) і визначає, як швидко інформація може бути передана. Наприклад, волоконно-оптичні мережі забезпечують вищу швидкість, ніж мідні кабелі.

– Пропускна здатність – це максимальна кількість даних, яка може бути передана за певний проміжок часу, що важливо для мереж з великими обсягами трафіку.

– Затримка – час, необхідний для доставки пакету даних від відправника до одержувача. Висока затримка може негативно вплинути на такі сервіси, як відеоконференції та онлайн-ігри.

– Надійність передачі даних визначає, наскільки точно та повно інформація доходить до адресата. Протоколи, як-от TCP, забезпечують виявлення помилок і повторну передачу даних, тоді як UDP надає перевагу швидкості.

Методи *кодування та модуляції* використовуються для перетворення даних у сигнали, що дозволяють їх передачу через різні середовища. В цілому, ефективність передачі даних є критично важливою для швидкості та якості обслуговування в комп'ютерних мережах [4].

Інтерпретація даних.

Інтерпретація даних – це процес аналізу та осмислення інформації, отриманої в результаті передачі або збору даних. Вона включає в себе *обробку, візуалізацію та аналіз* даних для отримання корисних висновків.

– *Обробка даних* передбачає очищення, трансформацію та підготовку інформації до аналізу. Це може включати видалення помилок, нормалізацію даних або об'єднання різних джерел інформації.

– *Візуалізація* даних – це використання графіків, діаграм та інших візуальних засобів для представлення інформації. Вона допомагає спростити сприйняття складних наборів даних і виявити тренди чи аномалії.

– *Аналіз даних* включає в себе статистичні методи та алгоритми для виявлення закономірностей, тенденцій і зв'язків у даних. Це може бути корисно для прийняття обґрунтованих рішень у бізнесі, науці чи інших сферах.

Загалом, інтерпретація даних є важливим етапом у використанні інформації для досягнення цілей і покращення процесів у різних галузях [5].

Висновки. Управління комп'ютерними мережами охоплює важливі аспекти, такі як безпека, передача даних, управління та інтерпретація інформації. Безпека мереж захищає дані від несанкціонованого доступу через шифрування, аутентифікацію та брандмауери. Передача даних визначає швидкість і надійність обміну інформацією між пристроями, впливаючи на користувацький досвід.

Управління мережею забезпечує моніторинг і оптимізацію ресурсів, виявляючи та усуваючи збої, тоді як інтерпретація даних дозволяє отримувати цінні висновки з аналізу інформації. Інтеграція всіх цих елементів є ключем до стабільності, безпеки та продуктивності комп'ютерних мереж у сучасному цифровому середовищі.

Список використаних джерел:

1. Чим відрізняються LAN, MAN і WAN: особливості 3 типів мереж. URL: e-server.com.ua (дата звернення: 11.12.2024)
2. Типи мережевих протоколів і їх призначення: HTTP, IP, SSH, FTP, POP3, MAC. URL: deltahost.ua (дата звернення: 11.12.2024)
3. Основи комп'ютерних мереж. Городецька І.О. URL: deltahost.ua (дата звернення: 11.12.2024)
4. Комп'ютерні мережі. Горобець А.О. URL: pdf.lib.vntu.edu.ua (дата звернення: 11.12.2024)
5. Мережі: курс лекцій. Хміль Р.Р., Русскін В.В. URL: repository.khpa.edu.ua (дата звернення: 11.12.2024)

УДК 681.3

ПРОФІЛЬ АНДРАГОГА В СИСТЕМІ ІНФОРМАЦІЙНОЇ ПІДТРИМКИ НАВЧАННЯ ДОРОСЛИХ

Рогушина Ю.В.[1], к.ф.-м.н. e-*mail: ladamandraka2010@gmail.com*
Гладун А.Я.[2], к.т.н. *e-mail: glanat@yahoo.com*
Прийма С.М.[3], д.пед.н. *e-mail: pryima.serhii@tsatu.edu.ua*
Аніщенко О.В.[4], д.пед.н. *e-mail: anishchenko_olena@gmail.com*
[1]*Інститут програмних систем НАН України, Інститут цифровізації освіти НАПН України*
[2]*Міжнародний науково-навчальний центр інформаційних технологій та систем НАН та МОН України*
[3]*Таврійський державний агротехнологічний університет імені Дмитра Моторного*
[4]*Інститут педагогічної освіти і освіти дорослих імені Івана Зязюна НАПН України*

Актуальність та постановка проблеми. Відмітною ознакою сучасного освітнього простору є його персоніфікованість, яка забезпечується, зокрема, шляхом проєктування та впровадження *індивідуальних освітніх траєкторій* (ІОТ) [1]. Це може сприяти розвитку суб'єктності як здобувачів освіти, так й андрагогів шляхом створення індивідуальних умов роботи за гнучким навчальним графіком на основі семантичних технологій у структурі екосистеми освіти дорослих, важливим суб'єктом якої є андрагог з притаманними йому характеристиками. *Профіль андрагога* є однією з важливих умов побудови ІОТ, яка дозволяє знаходити найбільш ефективні поєднання "андрагог – здобувач освіти". Саме для дорослих здобувачів освіти, які досить чітко уявляють свій освітній поступ, принципово важливо, щоб їх навчальну діяльність скеровувала особа, яка має більш глибокі знання в тих підрозділах *предметної області* (ПрО), в яких здобувачі планують працювати і в яких вони самі не мають достатнього досвіду. Особливості взаємодії здобувача освіти з андрагогом полягають, зокрема, в тому, що сам здобувач не тільки є активним суб'єктом створення ІОТ, але й, що більш характерно саме для дорослих, увиразнює не тільки свої освітні потреби та можливості, але й різноманітні аспекти комунікації, психологічної сумісності тощо. З огляду на зазначене вище, наявність додаткових відомостей про андрагога є одним із чинників забезпечення ефективності освітнього процесу.