

Тема 23 . Глобальна співдружність комп'ютерних мереж Інтернет.

Мета: Вивчити основні характеристики мережі Інтернет.

1. Загальна характеристика мережі Інтернет
2. Глобальна інформаційна служба WORLD WIDE WEB (WWW)
3. Захист інформації в Інтернет

1. Загальна характеристика мережі Інтернет

Інтернет почав розвиватись в 60-х роках у вигляді проекту американського уряду. Тоді були зв'язані між собою головні науково-дослідні центри країни. Так виникла мережа ARPAnet, яка складалась з 4-х вузлів. У 1971р.-15 вузлів, 1972р.-40. Почався розвиток інших мереж і з'явилась необхідність з'єднання різних мереж в одну. Так у 80-х роках виникає Інтернет.

Internet - саме масове та оперативне джерело інформації. Своє представництво, власну Web-сторінку в мережі має сьогодні практично кожна велика західна організація, фірма або компанія. В Internet розміщені «електронні» варіанти багатьох тисяч газет та журналів, через Мережу транслюють сотні радіостанцій та телекомпаній. Важко знайти будь-яку область людської діяльності, яка не була б представлена в Internet у всій своїй повноті сотнями і тисячами «сторінок». Інша популярна технологія отримання інформації - через так звані групи новин. Їх кількість наближається сьогодні до ста тисяч.

Internet - найбільше в світі джерело розваг. Ігри та музика, кіно та театр - всі види мистецтва і все це розмаїття величезної індустрії розваг представлено сьогодні в Internet. Ви можете зіграти гру з партнером, що знаходиться на іншому кінці планети, взяти новини про життя улюбленої рок-групи та прослухати останній їх диск, розгадати кросворд та отримати результат останнього футбольного матчу, зачитатися величезною колекцією анекдотів та стати колекціонером картин та багато чого іншого.

Internet - найбільш прогресивний засіб спілкування та комунікації. Щоденно користувачі Мережі відправляють один одному сотні мільйонів електронних послань - для багатьох з них Internet повністю замінив звичайну пошту. Мільйони людей щоденно знайомляться і спілкуються один з одним. Поки що порівняно мала кількість людей користується послугами Internet-телефонії та відеоконференцій. Однак ці технології спілкування стають все більш популярними.

Internet - найбільш сприятливий простір для бізнесу. Все більш популярною стає електронна торгівля, яка дозволяє користувачу здійснити покупку практично будь-якого товару в будь-якій точці планети. По Internet можна замовити та отримати нові програмні продукти, послати букет квітів улюбленій дівчині і навіть придбати автомобіль. Також взяти останні результати торгів на біржах всього світу, взяти про курс акцій тієї чи іншої

компанії та повернути з ними угоду. Для значних фірм та корпорацій Мережа стала ідеальним середовищем для проведення всеможливих операцій та розрахунків, бізнес-нарад в реальному часі. Але заробити в Internet може не тільки значна фірма, але й практично кожна людина, створивши свою сторінку.

Internet - ідеальний інструмент для реклами. Мережа дає будь-якій людині практично безкоштовну можливість повідомити багатомільйонну аудиторію про надавані послуги та продукцію. Internet зрівнює приватних осіб, фірми середньої ланки та значні корпорації: у всіх є однакові можливості для приваблення покупців. Але не потрібно платити тисячі і навіть мільйони доларів на мить реклами на телебаченні, не потрібно купувати полоси в газетах - ваша сторінка в Internet буде функціонувати цілодобово, без перерв.

Internet - це безмежний простір для творчості. З допомогою Мережі ви можете заявити про себе на весь світ, створивши особисту домашню сторінку.

Кожний комп'ютер під'єднаний до Internet, називається вузлом. Деякі вузли надають іншим вузлам програми та данні; вони називаються серверами. Інші комп'ютери, використовують інформацію, надавану сервером; вони називаються клієнтами. Системи, компоненти яких взаємодіють подібним чином, називаються системами клієнт/сервер. Клієнт-програма, або просто клієнт, - це програма з дружнім інтерфейсом, яка виконується на комп'ютері і має доступ до Internet-ресурсів. Коли клієнт-програмі потрібно отримати інформацію з Internet, вона звертається до програми-сервера. Програма-сервер, або просто сервер, повертає клієнт-програмі відповідь на її запит.

В Internet можна спілкуватися німецькою, французькою, російською мовами, навіть на суахілі. Але всі комп'ютери в мережі користуються мережними протоколами під назвою TCP/IP, - мовою, з допомогою якої комп'ютери спілкуються один з одним. Мовою TCP/IP можна спілкуватися не тільки з користувачами Windows 95, але і з користувачами, чий комп'ютер, в тому числі робочі станції UNIX та Makintosh, працюють під управлінням інших операційних систем. Протокол управління передачею (TCP) разом з протоколом Internet (IP) складають стандартну мову, з допомогою якої комп'ютери цієї глобальної мережі обмінюються інформацією.

Кожен комп'ютер, який підключений до Internet, має свою певну адресу - адресу IP, яка представляє собою велике число, розбите на чотири групи до трьох цифр в кожній.

Все це дуже добре для комп'ютера, але людина звикла мати справу із словами, а не з числами. Тому адресам Internet поставлені відповідні імена. Замість того, щоб запам'ятати одинадцятизначні числа ID-номерів Internet, достатньо запам'ятати: наприклад, що ім'я Web-сервера Internet - `www.msr.com`. За вірним переводом чисел в імена і навпаки слідкують спеціальні машини, які називаються серверами доменних імен.

Доменне ім'я складається з двох або більше слів, розділених крапками, по принципу: вузол.другий_рівень.перший_рівень. Домени першого рівня чітко визначені. Наприклад **com** або **uk**, вказують тип організації або країну, в якій ця організація знаходиться. Домени другого рівня визначають організацію. В

таблиці 1 описані домени першого рівня, які використовуються в Сполучених Штатах.

Таблиця

Доменні імена першого рівня

Ім'я	Тип організації
com	Комерційні організації
org	Різноманітні, в основному, не комерційні організації
net	Комп'ютери, які складають структуру Internet, та провайдери
edu	Університети та інші учбові заклади
gov	Урядові організації

Для передачі інформації глобальна мережа застосовує домени першого та другого рівнів. Доменне ім'я вузла використовується для передачі даних з комп'ютера на комп'ютер в межах локальної мережі.

Інтернет має великий набір служб та послуг:

- електронна пошта
- UseNet – служба новин
- WWW – “всесвітнє павутиння”
- TelNet – мережева програма, яка надає спосіб входу в систему та можливість роботи з іншого комп'ютера.
- FTP – протокол передачі файлів

2. Глобальна інформаційна служба WORLD WIDE WEB (WWW)

Internet неможливо уявити без глобальної інформаційної служби World Wide Web (www або просто Web). Сторінок інформації в www стільки, що перелічити їх практично неможливо по самих скромних оцінках, їх більше 50 мільйонів. Для перегляду Web-сторінок використовується програма Internet Explorer.

Що торкається змісту, то в Web можна знайти все: від неймовірних дурниць до відомостей першорядної важливості. Залежно від майстерності тієї людини, яка розробила Web-сторінки і наданих йому засобів, це може бути простий текст, набраний з використанням одного шрифту, або вражаюча презентація з текстом, графікою, звуками та анімацією. В іншому випадку Web відрізняється як від друкованого тексту, так і від телебачення наявністю гіпертекстових зв'язків (hypertext links), тобто засоби, які переносять на іншу Web-сторінку, зв'язану з даною, клацнувши мишею.

Що б не трапилося в світі, це напевне знайде своє відображення в Internet. Цією програмою користуються для пошуку відповідей на будь-які виникаючі запитання. Запитання можуть бути різноманітні, тобто від технічної підтримки комп'ютерів до банальних запитань про телебачення, а бувають випадки, коли Web виявляється буквально життєво необхідною.

Internet Explorer - кращий засіб перегляду Web-сторінок. З його допомогою можна зберігати данні, які відображаються на екрані, і потім використовувати їх в подальшому де завгодно.

- *Щоб зберегти Web-сторінку як файл, потрібно вибрати опцію **Файл, Сохранить как файл**. Якщо переглядати сторінку з допомогою Internet Explorer, потрібно вибрати формат HTML. Якщо потрібен лише текст, то треба зберегти сторінку в текстовому форматі. Але слід пам'ятати, що якщо на сторінці є графіка, кнопки або інші об'єкти, потрібно буде зберегти їх як окремі файли.*

- *Щоб скопіювати текст з Web-сторінки, необхідно виділити цей текст, натиснувши на виділеному фрагменті праву клавішу мишки і вибрати опцію **Копировать**. Тепер можна буде вставити цей текст в будь-який документ Windows, в тому числі і в створений в текстовому редакторі.*

- *Щоб скопіювати графічний об'єкт з Web-сторінки, на нього підвести курсор, клацнути правою клавішею мишки і вибрати опцію **Сохранить рисунок как**. Можна вказати нове ім'я і розміщення файла.*

- *Для роздрукування Web-сторінки просто клацнути мишкою по клавіші **Печать**.*

Internet Explorer резервує для своєї роботи дві спеціальні системні папки. Як правило, на них ніхто не звертає уваги, але в деяких випадках вони стають необхідними.

Знаючи, як працює кеш диску в Internet Explorer, можна відрегулювати його таким способом, щоб Web-сторінки виводились на екран швидше.

*Щоб прискорити роботу Web, необхідно вибрати опцію **Вид, Параметры**, клацнути на кнопці **Другие**, потім - на кнопці **Настройка** на панелі **Временные файлы Internet**. Відкриється діалогове вікно малюнок 4.*

Існує дві стратегії прискорення доступу в Web.

* Якщо достатньо місця на жорсткому диску, можна задати більший об'єм кеш диску. Зрушивши важіль регулятора вправо, збільшиться об'єм дискового простору (в порівнянні з встановленими по замовчанню) - 2% від об'єму диску. Це дозволить Internet Explorer рідше очищати кеш для звільнення місця для нових сторінок.

* Встановити, щоб кеш перевірявся не так часто, або зовсім відключити перевірку. По замовчуванню в ході кожного відвідування Web-сторінки, Internet Explorer звертається до дати сторінки, щоб перевірити чи старша вона копії, яка знаходиться в кеші диску. Якщо сторінка в Internet новіша, то вона завантажується, в іншому випадку завантажується з кеша диску. При встановленому перемикачі **Никогда**, без перевірки буде завантажуватися сторінка із кеша.

Кожного разу, коли відвідувати Web-сторінку, Internet Explorer створює для неї ярлик в папці журналу (**History**). По замовчуванню кожен такий ярлик зберігається протягом 20 днів, а потім знищується. Припустимо, користувач на днях переглядав Web-сторінку, до якої хотів би повернутися знов. Якщо він не забув створити для цієї сторінки ярлик в папці **Избранное**, то це не буде важко. Для цього потрібно вибрати опцію **Вид, Параметры**, потім клацнути на

вкладинці **Переход**, потім на клавіші **Просмотр** на панелі **Журнал** в нижній частині діалогового вікна.

Забравши перевірку нових версій Web-сторінок виникає ризик користування застарілими даними, навіть не помічаючи цього. Щоб Internet Explorer представив в будь-якому випадку останні дані, необхідно клацнути на кнопці **Обновить**.

Internet просто насичена програмами. **FTP - сервери** - це центральні складові файлів, які використовують протоколи **FTP (File Transfer Protocol - протокол передачі файлів)** для обміну файлами з комп'ютерами. Одна з найбільш корисних колекцій програм (для користувачів Windows) знаходиться на Web-сторінці www.microsoft.com. За допомогою програми Internet Explorer все, що торкається роботи з FTP, відбувається автоматично. Для цього достатньо вказати і клацнути.

Іноді після натиснення мишки на посилання Internet Explorer замість Web-сторінки відкриває діалогове вікно. Звичайно це означає, що дане посилання вказує на файл, який не є Web-сторінкою. Перш ніж завантажити цей файл на жорсткий диск, необхідно подумати, чи достатньо надійне те місце. Якщо зберігати файл, для того щоб звернутися до нього пізніше, потрібно присвоїти йому ім'я і визначити шлях збереження.

В склад Internet може входити:

- **Нові версії** будь-яких програм, в тому числі Windows 95 та Internet Explorer.

- **Компоненти ActiveX** - це міні-програми, з допомогою яких інші програми зможуть виконувати з завантаженими файлами деякі спеціальні операції.

- **Умовно-безкоштовне програмне забезпечення (shareware programs)**. Це забезпечення відрізняється від основних програм, придбаних в магазині тим, що перед тим, як заплатити за таку програму гроші, можна з нею попрацювати і вирішити чи вона потрібна. Якщо дана програма сподобалася, то потрібно заплатити розробнику, якщо ж ні - просто знищити її з жорсткого диску.

Більшість файлів, які завантажуються з Internet - саморозгортаємі. Один такий файл складається із декількох (іноді навіть сотні) файлів, стиснених в спеціальному форматі для того, щоб передача їх на будь-який комп'ютер проходила скоріше. Закінчивши завантаження файла, необхідно двічі клацнути на його піктограмі, для того, щоб витягти файли і записати їх на жорсткий диск комп'ютера. При цьому деякі саморозгортаємі файли завантажуються автоматично; для завантаження інших необхідно виконати подвійне натискання на піктограмі **Setup(Установка)**.

Одна із умовно-безкоштовних програм - **WinZip**. Це чудовий засіб роботи з файлами, стисненими з допомогою поширеної програми архівації в **Zip-форматі**. (Такі файли зустрічаються в Internet дуже часто). Копію цієї програми можна відшукати в www.winzip.com.

- В Internet можливо знайти сотні, навіть тисячі **шрифтів TrueType**.

- Деякі **графічні файли та файли з документами** записані в форматах, які потребують для перегляду файлів застосування спеціальних програм.

Наприклад, файли з розширенням PDF зберігаються в форматі Portable Document, і для їх читання або роздрукування потрібна програма Acrobat фірми Adobe.

При завантаженні будь-якого файла комп'ютер наражається на небезпеку зараження вірусом.

Одна із ознак надійності в Web - наявність **сертифіката** в тому місці, звідки проводиться завантаження. Якщо потрібний файл має подібний сертифікат, то проблем немає, але якщо потрібного сертифіката не існує, то виникає ризик. Ризик невеликий, якщо програма знайдена в достатньо відомому місці. Якщо файл знаходиться на Web- сторінці, яка мало відома - потрібно бути обережним.

До недавнього часу не було ніякої безпеки заразитися через Internet, якщо тільки не завантажувати звідти файли з програмами. На превеликий жаль, за останні декілька років ситуація змінилася. З'явилися віруси, здатні заразити невинні до цих часів файли даних - в першу чергу документи Microsoft Word. Внесення вірусу в систему може виникнути при завантаженні будь-якого файла з Internet. На щастя, щоб багаторазово знизити ризик, достатньо керуватися звичайним здоровим глуздом. Рекомендується завантажувати файли з тих місць Web, які належать відомим компаніям та особам. Найбільш надійні місця, в яких файли наділені сертифікатами. Якщо виникла потреба працювати з Microsoft Word або Excel, то слід задіяти їх антивірусні засоби. Для цього необхідно завантажити програму виявлення та знищення вірусів, або придбати комерційну антивірусну програму.

Де зберегти файл? Можна, звичайно, вибрати будь-яку папку, але краще спочатку розмістити піктограми нових файлів на робочому столі, тоді вони не загубляться. Пізніше їх можна буде перемістити в інше, більш безпечне місце.

Виходячи із швидкості передачі інформації для даної лінії зв'язку в мережі Internet і розміру файла, програма Internet Explorer розраховує оцінку тривалості завантаження. Проте, немає потреби чекати, поки завантаження закінчиться - в цей час можна займатися чимось іншим. Потрібно повернутися на Web-сторінку, з якої починалося завантаження інформації і клацнути на посилання або ввести адресу - подальша робота з Web не перерве завантаження.

Існує швидкий та простий спосіб слідкувати за завантаженням. Для цього потрібно згорнути вікно завантаження, на панелі задач з'явиться індикатор складу процесу завантаження, який, відображаючи процес завантажених даних, весь час буде в полі зору.

3. Захист інформації в Інтернет

Проблема безпеки інформації в період загальної інформатизації, широкого впровадження е-технологій – одне із найгостріших питань сьогодення.

У процесі роботи в Інтернет користувач стикається з такими проблемами безпеки передачі даних:

- перехоплення інформації – цілісність інформації зберігається, але її конфіденційність порушена;

- модифікація інформації – початкове повідомлення змінюється або повністю підмінюється іншим;
- підміна авторства інформації. Наприклад, хтось може послати листа від вашого імені, або сервер може прикинутися електронним магазином; приймати замовлення та номери кредитних карток, але ніяких товарів не висилати.

Тому, виділяються такі характеристики, що забезпечують безпеку системи:

1. Аутентифікація – це процес розпізнавання користувача системи і надання йому певних прав та повноважень.
2. Цілісність – стан даних, прав якому вони зберігають свій інформаційний зміст та однозначність інтерпретації в умовах різних дій. Наприклад, у разі передачі даних під цілісністю розуміють ідентичність відправленого та прийнятого.
3. Секретність – попередження несанкціонованого доступу до інформації.

Для забезпечення секретності інформації застосовується криптографія (шифрування), що дозволяє трансформувати дані у зашифровану форму, з якої вибрати початкову інформацію можна тільки за наявності ключа. Шифрування ґрунтується на двох поняттях: алгоритм та ключ. Алгоритм – це спосіб кодування початкового тексту. Закодоване послання може бути переглянуте тільки за допомогою ключа. Крім того, можна використовувати один алгоритм з різними ключами для відправлення повідомлень різним адресатам. Таким чином, безпека системи шифрування залежить від ключа, а не від секретності алгоритму. Багато існуючих алгоритмів – загальновідомі.

Кількість можливих ключів для даного алгоритму залежить від числа бітів у ключі. Наприклад, 4-бітний ключ допускає 16 (2^4) комбінацій ключів, 128-бітний – 2^{128} . Подальший розвиток комп'ютерної техніки призводить до підвищення її продуктивності й, тим самим, до можливості перебору комбінацій ключів. Тому системам забезпечення безпеки доводиться використовувати все довші ключі, що призводить до збільшення часу на шифрування. Існує дві схеми шифрування: симетричне та асиметричне (шифрування з відкритим ключем).

Симетричне шифрування передбачає, що відправник та отримувач володіють одним ключем (секретним). При такому виді шифрування використовуються ключі невеликої довжини, що дозволяє швидко розшифровувати великі обсяги даних. Недоліки симетричного шифрування: відправнику та отримувачу складно таємно від інших вибрати ключ; для кожного адресата необхідно зберігати окремий секретний ключ; неможливо гарантувати безпеку відправника, тому що два користувача володіють одним ключем.

Шифрування з відкритим ключем передбачає існування двох різних ключів. За допомогою одного з них повідомлення шифрується, а за допомогою другого – розшифрується. Недоліком цього методу шифрування є необхідність використання більш довгих ключів, що вимагає потужніших ресурсів для організації процесу шифрування.

Навіть якщо послання зашифроване, існує можливість модифікації початкового повідомлення або його підміни. Одним із шляхів вирішення цієї проблеми є передача відправником отримувачу стислого змісту повідомлення (контрольної суми).

Алгоритм розрахунку контрольних сум розроблені таким чином, щоб вони були унікальним для кожного повідомлення. Але виникає проблема передачі контрольних сум включають до електронного підпису.

Електронні підписи створюються шифруванням контрольної суми та додаткової інформації за допомогою особистого ключа відправника. Для захисту від перехоплення та повторного використання підпис містить унікальне число – порядковий номер.

Аутентифікація – це один з найважливіших компонентів організації захисту інформації у мережі. Під час отримання запиту на використання ресурсу від імені користувача сервер передає управління серверу аутентифікації. Після отримання позитивної відповіді від сервера аутентифікації, користувачеві надається ресурс, що запитується.

Одним із методів аутентифікації є використання стандартних паролів. Недолік цього методу – можливість перехоплення пароля. Тому частіше використовуються одноразові паролі. Для генерації паролів застосовуються як програмні (наприклад), так і апаратні генератори, які являють собою пристрої, що вставляються у слот комп'ютера.

Для захисту корпоративних інформаційних мереж застосовується брандмауери.

Брандмауер – це система, що дозволяє поділити мережу на декілька частин та реалізувати набір правил, які визначають умови проходження пакетів з однієї частини в іншу. Частіше ця межа проводиться між локальною мережею підприємства та Інтернет. Брандмауер може бути реалізований як апаратними, так і програмними засобами. Всі брандмауери можна поділити на такі типи:

- пакетні фільтри, які виконують фільтрацію IP-пакетів засобами маршрутизаторів фільтрації;
- сервери прикладного рівня, які блокують доступ до певних сервісів у мережі.

Питання для самоконтролю:

- 1.Що таке мережа Інтернет?
- 2.Які комп'ютери називаються серверами і клієнтами Інтернету?
- 3.Що таке протокол TCP/IP і для чого він призначений ?
- 4.Які послуги звичайно надає провайдер Інтернету?
- 5.Назвіть основні інформаційні ресурси Інтернету.
- 6.Що таке режим обміну on-line і off-line?
- 7.Який принцип адресації прийнято в Інтернеті?
- 8.Що таке IP-адреса?
- 9.Опишіть принцип побудови доменних імен.
- 10.Наведіть приклади імен серверів.