

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МИКОЛАЇВСЬКИЙ НАЦІОНАЛЬНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

Навчально–науковий інститут економіки та управління

Обліково–фінансовий факультет

Кафедра інформаційних систем і технологій



КОМП'ЮТЕРНІ МЕРЕЖІ

Методичні рекомендації

для здобувачів вищої освіти ступеня «бакалавр» 2 курсу напрямку

підготовки 6.030502 «Економічна кібернетика»

денної форми навчання

МИКОЛАЇВ

2017

УДК 004.7
К63

Друкується за рішенням науково-методичної комісії обліково-фінансового факультету Миколаївського національного аграрного університету від «13» квітня 2017 р., протокол № 11.

Укладач:

Ю. В. Волосюк – канд. техн. наук, доцент, завідувач кафедри інформаційних систем і технологій Миколаївського національного аграрного університету

Рецензенти:

І. П. Атаманюк – д-р техн. наук, професор, завідувач кафедри вищої та прикладної математики Миколаївського національного аграрного університету;

Д. М. Самойленко – канд. ф.-м. наук, доцент кафедри електрообладнання суден та інформаційної безпеки Національного університету кораблебудування імені адмірала Макарова.

ЗМІСТ

ВСТУП.....	3
ЗАГАЛЬНІ ВИМОГИ ДО ВИКОНАННЯ ПРАКТИЧНИХ РОБІТ	5
ПРАКТИЧНІ РОБОТИ.....	8
Практична робота №1. Основні поняття комп'ютерних мереж.....	8
Практична робота №2. Налагодження, використання та діагностика локальних комп'ютерних мереж.....	11
Практична робота №3. Організація підключення до Інтернету. Робота з файлами по протоколу FTP	15
Практична робота №4. Мережеві сніфери – TCPDump, Wireshark.....	27
Практична робота №5. Налаштування рівнів безпеки сучасних браузерів.	39
Практична робота №6. Використання облікових записів користувачів та груп для захисту від комп'ютерних вірусів на рівні операційної системи за допомогою реалізації політик безпеки з обмеженими правами доступу.....	46
Практична робота №7. Застосування криптографічних засобів захисту інформації.	49
Практична робота №8. Організація роботи в мережі Інтернет за допомогою додатку µTorrent. Робота з файлами по протоколу BitTorrent.....	56
КРИТЕРІЇ ОЦІНКИ ЗНАНЬ.....	69
РЕКОМЕНДОВАНА ЛІТЕРАТУРА	71

ВСТУП

Методичні рекомендації розроблені для студентів, які навчаються за напрямком підготовки 6.030502 «Економічна кібернетика» з навчальної дисципліни «Комп'ютерні мережі». Зазначена дисципліна згідно з освітньо-професійною програмою та навчальними планами підготовки бакалаврів належать до нормативної частини циклу дисциплін професійної і практичної підготовки.

Основним призначенням даного видання є: поглиблення теоретичних знань, отриманих студентами під час вивчення змістового модуля; набуття практичних навичок із налагодження та діагностики роботи засобів захисту інтелектуальних мережних пристроїв; набуття навичок дослідження процесів передачі даних у незахищених та захищених локальних мережах при використанні різних мережових технологій та протоколів, а також набуття навичок усунення вразливостей та протидії мережним атакам на кінцеві вузли та комунікаційні пристрої мереж.

Для проведення практичних робіт, залежно від можливостей навчальних лабораторій, передбачається два взаємодоповнюючих варіанти. Перший варіант – використання реального обладнання, другий – використання спеціалізованих програмних комплексів із комп'ютерної симуляції/емуляції роботи мережних пристроїв і вузлів та мереж у цілому. Такий підхід забезпечує набуття студентами комплексних знань та практичних навичок у сфері професійної діяльності.

Перевагою даних методичних рекомендацій є подача перед кожним із завдань на лабораторну роботу необхідних теоретичних відомостей, пов'язаних із вивченням досліджуваної технології чи протоколу захисту інформації. Методичні рекомендації містять достатньо деталізовану довідникову інформацію з питань налагодження та діагностики роботи засобів захисту мережних пристроїв, а також ознайомлюють студентів із готовими прикладами налагоджень пристроїв.

ЗАГАЛЬНІ ВИМОГИ ДО ВИКОНАННЯ ПРАКТИЧНИХ РОБІТ

Цикл практичних робіт із дисципліни «Комп'ютерні мережі» для студентів напряму підготовки 6.030502 «Економічна кібернетика» спрямований на поглиблення й закріплення теоретичних знань, набутих студентами під час лекційних занять.

У результаті виконання практичних робіт студент повинен отримати чітке уявлення про реалізацію теоретичних положень дисципліни на практиці.

Кожна практична робота складається з наступних складових:

- теми роботи;
- мети роботи;
- умови завдання, що містить опис задачі;
- покрокових інструкцій щодо виконання практичної роботи з певної тематики;
- завдань для самостійної роботи;
- контрольних питань, що дозволяють студенту підготуватися до захисту практичної роботи.

За результатами виконання кожної практичної роботи студенти складають звіт, який повинен містити:

- номер практичної роботи;
- тему практичної роботи;
- мету виконання практичної роботи;
- короткі теоретичні відомості щодо тематики виконуваної роботи;
- результати виконання завдань у вигляді скріншотів етапів виконання роботи, додатків;
- відповіді на питання, що наведені в практичній роботі;
- висновки.

Під час оформлення звіту необхідно дотримуватися таких вимог: звіт оформлюється на аркушах формату А4 з рамками (перша сто-рінка – з кутовим штампом форми 2, решта сторінок – форми 2а за ГОСТ 2.104-68 ЕСКД. Основные надписи). Штампи

заповнюються згідно з вимогами. Нумерація сторінок наскрізна в межах роботи. Поля для тексту: ліве – 25 мм, праве – 10 мм, верхнє 20 мм від краю аркуша, нижнє 10 мм від верхнього краю штампа. Текст роботи оформлюється шрифтом Times New Roman 12–14 розміру, міжрядковий інтервал 1 – 1,5. Абзацний відступ 5 символів. Тексти сценаріїв налагоджень, лістингів конфігураційних файлів та інших елементів рекомендується оформляти шрифтом Courier New, 10–12 розміру, міжрядковий інтервал 1. Рекомендується у текстах сценаріїв та лістингів видаляти інформацію, яка не є значущою для виконання завдання або роботи. Ілюстрації та таблиці повинні розміщуватися безпосередньо після тексту, де вони зустрічаються.

Ілюстрації (креслення, рисунки, схеми тощо) позначаються таким чином: «Рисунок № – Назва рисунка» (вирівнювання по центру, без абзацного відступу). Позначення ілюстрації виконується під ілюстрацією. Якщо кількість ілюстрацій значна і вони однотипні та невеликі за розміром, то їх рекомендується групувати в одну ілюстрацію, позначати літерами а), б) ... і підписувати їх як одну ілюстрацію.

Таблиці позначаються таким чином: «Таблиця № – Назва таблиці» (вирівнювання по лівому краю, без абзацного відступу). Їх нумерація здійснюється окремо і наскрізно у межах роботи. Позначення таблиці виконується над таблицею. Текст таблиць рекомендується оформляти шрифтом Times New Roman 12 розміру, міжрядковий інтервал 1. Якщо таблиця займає понад одну сторінку, то на другій і наступних сторінках ставиться позначення «Продовження табл. №», на останній сторінці ставиться позначення «Закінчення табл. №». Заголовок таблиці повторюється в усіх її частинах.

У тексті звіту можна використовувати переліки (списки в термінології текстових редакторів). Перед перерахуванням ставиться двокрапка. Перед кожною позицією переліку можна ставити тире, малу літеру українського алфавіту з дужкою, арабські цифри з дужкою. Елементи переліку пишуться з маленької літери,

наприкінці ставиться крапка з комою, для останнього елемента – крапка.

Відповіді на контрольні питання оформляються акуратно, чітким почерком, літерами достатнього для нормального сприйняття розміру. Їх оформлення слід починати з нового аркуша.

Слід звернути увагу на те, що контрольні питання, які наводяться після кожної лабораторної роботи, повинні бути ретельно відпрацьованими студентом самостійно з метою підготовки до контрольних заходів, таких як тестування та вирішення практичних завдань.

Виконана належним чином практична робота захищається шляхом співбесіди з викладачем. За результатами захисту викладач зараховує практичну роботу як виконану і виставляє відповідні бали.

ПРАКТИЧНІ РОБОТИ

ПРАКТИЧНА РОБОТА №1.

Тема: Основні поняття комп'ютерних мереж. Апаратні та програмні засоби побудови комп'ютерних мереж. Мережеві ресурси: мережеві файлові системи, принтери. Використання та створення мережевих ресурсів.

Мета роботи: ознайомити з основними принципами побудови програмних та апаратних засобів комп'ютерних мереж; ознайомити з поняттям мережевих ресурсів, навчити використовувати й створювати їх.

Теоретичні відомості

Локальна комп'ютерна мережа (ЛКМ) – комп'ютери, об'єднані за допомогою комунікаційного обладнання з метою обміну даними або спільного використання ресурсів комп'ютерної системи.

Топологія – просторова схема об'єднання вузлів мережі. Найбільшого поширення набули мережі з такою топологією: *шина (магістраль), зірка, кільце.*

Шинна топологія – це топологія, де мережеві вузли підключені до одного загального кабеля (шини).

Зірка – це топологія, де мережеві вузли підключаються безпосередньо до спеціального розподільного пристрою, що управляє обміном даними між вузлами мережі.

Кільце – це топологія, де мережеві вузли об'єднуються подібно до шинної топології, але сама шина замикається, утворюючи кільце.

Мережеві ресурси – об'єкти комп'ютерної системи (файли, папки, диски, принтери), які розміщені на віддалених комп'ютерах і можуть використовуватися іншими користувачами. Ресурсами мережі слугують диски, папки, файли, принтери.

Робоча станція – вузол мережі (комп'ютер), який використовує мережеві ресурси.

Сервер мережі — вузол мережі (досить потужний комп'ютер), який надає мережеві ресурси для спільного використання робочими станціями.

Мережева файлова система – набір засобів операційної системи для прозорого опрацювання папок, файлів, розміщених на віддалених мережевих вузлах.

Управління використанням мережевих ресурсів (*права доступу*) – правила використання мережевого ресурсу, читання, написання, перегляду тощо. Права доступу можуть встановлюватися для кожного ресурсу зокрема або для кожного зареєстрованого у мережі користувача.

Технологія виконання роботи.

1. Ознайомитися зі структурою мережі, яка функціонує у навчальному закладі:

- a. тип мережі (однорангова, з виділеним сервером);
- b. кількість і функціональне призначення сервера мережі;
- c. вказати тип мережевої операційної системи (сервера, робочої станції);
- d. визначити топологію комп'ютерної мережі;
- e. визначити тип обладнання, що використовується (тип кабелю, мережевий адаптер).

2. Користуючись "*Сетевым окружением*", визначити ресурси, які спільно використовуються (їх назви та призначення у локальній мережі) (табл. 1).

Таблиця 1

Ресурс	Мережева	Призначення

3. Визначити мережеві ресурси локальної мережі навчального класу.

4. Отримати перелік спільно використовуваних ресурсів для комп'ютера, що виконує функції сервера мережі.

5. Створити папку з назвою *Загальна*. Викликати вікно властивостей для створеної папки, визначити власника, встановлені права доступу до папки (табл. 2).

Таблиця 2

	Об'єкт	Права доступу
	Власник	

6. Змінити права доступу до папки так: а. власник має всі права на папку;
б. інші можуть тільки переглядати папку.

Завдання для самостійного виконання.

1. Запропонувати і обґрунтувати варіант побудови однорангової мережі з використанням витії пари для випадку об'єднання шести робочих місць, що знаходяться в одному кабінеті, та спільного використання принтера й файлів, що містяться на одному з комп'ютерів. Навести схему з'єднання, загальний перелік та кількість необхідного обладнання, вказати основні етапи побудови та налагодження мережі.
2. Вказати переваги й недоліки для мережі з виділеним сервером та для однорангової мережі.
3. Ознайомитися з іншими типами обладнання, яке не використовують у навчальному закладі (кабель, спосіб з'єднання).

Запитання для контролю.

1. Визначення комп'ютерної мережі (КМ).
2. Класифікація КМ за фізичним розташуванням (глобальні, регіональні, локальні мережі).
3. Поняття топології комп'ютерних мереж.
4. Класифікація комп'ютерних мереж за функціональним призначенням (з виділеним сервером, без виділеного сервера).
5. Обмін даними у комп'ютерній мережі. Поняття протоколу обміну даними.
6. Середовища обміну даними комп'ютерних мереж.
7. Пакетний принцип обміну даними.
8. Мережева операційна система: функції, склад та структура, призначення.
9. Програмне забезпечення мережевої операційної системи.
10. Апаратне забезпечення для побудови комп'ютерних мереж.
11. Вказати послідовність дій для використання файлової системи іншого комп'ютера.

ПРАКТИЧНА РОБОТА №2.

Тема. Налагодження, використання та діагностика локальних комп'ютерних мереж.

Мета роботи: набути навичок налагодження, діагностування локальної комп'ютерної мережі з використанням ОС Windows 7, 8, 10.

Теоретичні відомості.

IP-адреса – унікальна адреса для ідентифікації окремого вузла мережі. Прийнята в IP мережах адреса задається 32-бітним числом і розбита на чотири 8-бітних числа. У структурі IP-адреси міститься ідентифікатор мережі й унікальний ідентифікатора вузла. Наприклад: *192.168.1.12*.

Мережа – об'єднання мережевих вузлів за певною ознакою. Всі компютери однієї мережі мають у IP-адресі однакову мережеву частину. Наприклад, для мережевих вузлів *192.168.1.12*, *192.168.1.11*, *192.168.1.10* адреса мережі *192.168.1.0*.

Мережева маска – 32-розрядне число для визначення в IP-адресі отриманого пакета номера мережі й номера мережевого вузла. Як правило, мережева маска задається у вигляді *255.x.x.x*. Для наведених прикладів мережева маска буде такою: *255.255.255.0*.

Команди для роботи в мережі:

Hostname – команда дозволяє визначити ім'я (назву) комп'ютера в мережі.

Netstat – команда дозволяє отримати докладну інформацію про активні з'єднання (статистика протоколів і поточні TCP/IP мережні з'єднання). Можуть використовуватися параметри *-a* або *-n*. Синтаксис використання: **netstat** або **netstat параметр**.

Arp – команда дозволяє отримати доступ до таблиці протоколу ARP. Синтаксис використання: **arp -a**

Nslookup – команда проводить перетворення імені DNS в IP-адресу та навпаки.

Синтаксис використання: **nslookup назва вузла** або **nslookup адреса_вузла**.

Ping – команда для перевірки з'єднання з іншим вузлом мережі. Команда **ping** надсилає іншому вузлу запит-відгук на

основі протоколу Control Message Protocol ICMP. Після кожного посилання на екран виводиться повідомлення – відповідь-відгук. Команда *ping* призначена для аналізу й виявлення несправностей у мережах на основі протоколу TCP/IP, пов'язаних зі з'єднанням, визначенням імен.

Синтаксис використання: **ping** *назва вузла або _адреса_ вузла*.

Tracert – команда для визначення шляху до вузла призначення за допомогою надсилання відповіді-відгуку протоколу Control Message Protocol (ICMP). Виведений шлях є списком найближчих інтерфейсів, розміщених на шляху до вузла призначення.

Синтаксис використання: **tracert** *назва_вузла_або_адреса_вузла*. Наприклад: `tracert www.google.com`

Ipconfig – команда для відображення поточних параметрів Мережі TCP/IP. Виклик команди без параметрів виводить тільки IP-адресу, маска мережі – адресу основного шлюзу для кожного мережевого адаптера. Використавши параметр **all**, можна вивести докладну інформацію про налагодження мережевих інтерфейсів.

Синтаксис використання: **ipconfig**.

Net – набір команд для налагодження та управління мережевими з'єднаннями Microsoft. Команда містить параметри: *use, view, config, time* тощо. Докладна інформація про використання команди міститься у довідковій системі Windows.

Технологія виконання роботи.

1. Ознайомитись з правилами використання вказаних команд та заповнити таблицю 1.

Таблиця 1

Команда	Параметри команди	Призначення
hostname		
netstat		
	-a	
	-n	
arp	-a	
nslookup	IP	
	name	
ipconfig		
	all	
Net	use	
	view	

		send	
	ping		
	tracert		

- Визначити мережеву назву комп'ютера (hostname).
- Вказати значення поточних параметрів мережі, заповнити таблицю 2

Таблиця 2

Адреса мережі	Маска мережі	Адреса шлюзу	Адреса DNS сервера

- Визначити MAC-адреси робочої станції та 2-3 сусідніх робочих станцій.

Таблиця 3

№	TCP/IP-адреса робочої станції	MAC-адреса робочої станції
1		
2		
3		
4		

- Визначити діапазон адрес хостів локальної мережі класу, що використовуються за допомогою команди ping.

Таблиця 4

№	Мережеві адреси хостів
1	
2	
3	
4	
...	
12	

- Перевірити правильність роботи локального інтерфейсу (localhost 127.0.0.1), мережевого інтерфейсу.

- Надіслати повідомлення на сусідній комп'ютер, використовуючи команду *net* з параметром *send*.

Ознайомитися з використанням команди *net*. Записати призначення та кілька прикладів використання команди *net*.

Таблиця 5

№	Параметри команди net	Призначення
1	Use	
2	Send	
3	Print	
4	View	

Для отримання допомоги використовується команда `net help`:
net help use – вивести допомогу для команди *net use*.

8. Визначити доменне ім'я сервера локальної мережі.

9. Вказати основні етапи налагодження робочої станції для роботи у локальній мережі з використанням протоколу TCP/IP.

Завдання для самостійного виконання.

1. В офісі використовується локальна мережа з 10 робочих місць. Запропонувати варіант налагодження протоколу TCP/IP для випадку:

а. усі робочі місця мають вільно обмінюватися інформацією;

б. використовується поділ на 2 відділи (наприклад, редакційний відділ, бухгалтерія), яким заборонено обмінюватися інформацією.

2. Розглянути попереднє завдання для випадку використання протоколу NetBEUI.

3. Зробити аналіз відповідності моделі OSI/ISO протоколу TCP/IP.

4. Заповнити таблицю 6.

Таблиця 6

	Термін	Призначення
1	Протокол	
2	Шлюз	
3	Міст	
4	Сервер доменних імен DNS	
5	WINS	
6	NetBEUI	
7	Локальна мережа	
8	Адреса мережі	
9	Широкомовна адреса	
1	Адреса хосту	
1	Робоча група	

Запитання для контролю.

1. Протоколи локальних комп'ютерних мереж.
2. Адресація хостів у мережах MS Windows з використанням протоколу NetBEUI.
3. Адресація хостів у мережах з використанням протоколу TCP/IP.
4. Класифікація комп'ютерних мереж на основі протоколу TCP/IP.
5. Адреса хосту, мережева маска, широкомовна (broadcast) адреса, шлюз (gate).
6. Серверне програмне забезпечення.
7. Програмне забезпечення клієнта мережі.
8. Мережеві сервіси. Використання мережевих сервісів.
9. Сервери доменних імен (DNS).
10. Робоча група, домен у мережах операційних систем Windows.
11. Пояснити різницю термінів:
 - а) сервер – обчислювальна система;
 - б) сервер – програмне забезпечення (програма Apache Web-сервер).

ПРАКТИЧНА РОБОТА №3.

Тема: Організація підключення до Інтернету. Робота з файлами по протоколу FTP.

Мета роботи: Формування вмінь і навиків підключення до Інтернету та використання прикладного програмного забезпечення для завантаження файлів з Інтернету по протоколу FTP.

Теоретичні відомості

Загальні відомості про протокол FTP.

FTP розшифровується як “протокол передачі файлів” (File Transfer Protocol). Це один з базових протоколів Інтернету для обміну інформацією. На відміну від HTTP, який служить переважно для передачі web-текстів і зображень, FTP застосовується для обміну довільними файлами, переважно великого розміру. Окрім того, FTP є зручним для навігації по каталогах віддаленого комп'ютера і для доступу до розгалуженої

файлової структури. Доступ до файлів на віддаленому комп'ютері за протоколом FTP здійснюється за допомогою програм, що називаються FTP-клієнтами (в якості найпростішого FTP-клієнта можна використати www браузер, наприклад Chrome, Mozilla або Opera). Практично всі сучасні операційні системи містять FTP-клієнт для роботи по цьому протоколу.

Що таке FTP-сайт?

FTP-сайт (або FTP-сервер) – це комп'ютер в мережі Інтернет, на якому запущена відповідна програма, що надає доступ до файлів і каталогів цього комп'ютера за протоколом FTP. FTP-сайт загального доступу (англійською anonymous FTP site) відрізняється від інших сайтів тим, що на ньому організовано спеціальне піддерево каталогів, доступ до якого надається будь-кому. Зазвичай на таких сайтах зберігають файли, актуальні для багатьох людей – безкоштовне програмне забезпечення, тексти, зображення, звукові файли і інше, тому такі сайти називають також FTP-архівами. Об'єм інформації, що надається сайтами загального доступу, величезний: тільки українські та російські сайти містять більше 100000 Гб.

Основна відмінність між FTP і HTTP-сайтом полягає в тому, що HTTP сайт – це фасад палацу, а FTP сайт – це прості складські приміщення. Також швидкість завантаження з FTP зазвичай є вищою, ніж завантаження за допомогою HTTP.

Більшість FTP-сайтів мають чіткий ліміт кількості одночасно підключених користувачів. У разі перевантаження сайту слід або зайти пізніше або спробувати знайти “дзеркало” сайту – інший сайт, що містить точну копію вмісту оригінального сайту. Такі зеркала, як правило, розміщуються в різних частинах світу, для економії міжконтинентального трафіку. Отже, якщо є можливість працювати з сайтом що знаходиться в Україні, то краще так і вчинити, адже це гарантує істотне збільшення швидкості роботи.

Інформація в FTP-архівах поділяється на три категорії:

захищена інформація, режим доступу до якої визнається її власником і надається за спеціальною угодою із споживачем. До цього виду ресурсів відносяться комерційні архіви, закриті національні та міжнародні некомерційні ресурси, приватна некомерційна інформація із спеціальними режимами доступу;

інформаційні ресурси обмеженого використання, до яких відносяться програми класу shareware. До даного класу можуть

входити ресурси обмеженого часу використання або обмеженого часу дії (тобто користувач може використовувати цю версію на свій страх і ризик, але ніхто не буде надавати йому підтримку);

вільно розповсюджені інформаційні ресурси або freeware. Якщо мова йде про програмне забезпечення, то до цих ресурсів відноситься все, що можна вільно отримати по мережі і використовувати без спеціальної реєстрації – це може бути документація, програми, та інше.

З вище перерахованих ресурсів найбільш цікавими, звичайно, є дві останні категорії, які, як правило, оформлюються у вигляді FTP-архівів.

Використання FTP

Як потрапити до FTP-сайту?

Адреси FTP-сайтів дуже схожі з адресами HTTP-сайтів з тією різницею, що замість `http://<адреса>` вказують `ftp://<адреса>`. Однак, ці адреси можуть і не збігатися, тобто можлива HTTP-адреса організації `http://company.com`, а її файли зберігаються за адресою `ftp://ftp.company.com`.

Деякі програми для роботи в Інтернеті самі намагаються визначити тип сервера, але краще самому явно вказати тип протоколу в адресі. Як і у випадку з HTTP-сайтами, FTP-сайти також можуть мати не символічну адресу, а числову, наприклад `ftp://196.17.33.10`.

Найчастіше для доступу до публічного відкритого FTP-сайту користувач по замовчуванню реєструється як анонімний (**anonymous**) і не має особливих прав доступу на віддаленому сервері. У відповідь на запит ідентифікації слід ввести свою поштову адресу (**e-mail**). Зазвичай достатньо ввести щось подібне на поштову адресу для допуску до ресурсів архіву, але бувають сервера, які перевіряють наявність такої адреси.

Як використовувати FTP?

FTP-сайт можна уявляти як додатковий жорсткий диск, з якого можна щось переписати або щось записати на нього. Але оскільки цей сайт є власністю іншої людини, то і дозволити вона Вам може не все. Для FTP-сайтів приватних організацій доступ буде, ймовірно, закритий, оскільки сайт може містити конфіденційну інформацію. На приватні FTP-архівах може бути відкрита лише частина даних. Запис даних на такі FTP може бути або заблокований або на них може бути виділена спеціальна

ділянка, куди записуються свої файли, які, в подальшому будуть перевірені адміністратором цього сайту і, якщо він визнає за потрібне, винесені ним в основний розділ.

Якщо користувач купив або безкоштовно отримав певне місце (наприклад, під власний сайт), то він може повністю контролювати дані, що знаходяться на його сайті. Проте в деяких організаціях, що пропонують безкоштовне місце під приватний сайт, можуть відбуватися перевірки допустимого вмісту і якщо те, що розміщено на сайті видасться модератору не допустимим, то до власника можуть бути застосовані санкції від попередження до повного відключення від даного сервера. В основному проблеми виникають у випадку розміщення нелегального ПО, програм для злому, файлів, що містять дані аморального або антисоціального характеру.

Навігація по FTP-сайту дуже подібна до навігації по жорсткому диску комп'ютера. Є папки, в яких містяться підпапки або файли. Для того, щоб полегшити навігацію на багатьох сайтах в папці містяться файли опису, наприклад 00index.txt, index.html.

Клієнти для роботи з FTP. FTP клієнти – найкраще з freeware.

FTP-клієнти давно перейшли з категорії спеціалізованих програм для веб-розробників в розряд загальнодоступних утиліт, без яких важко обійтися в повсякденній роботі в Інтернеті. Завантаження програм і об'ємних поновлень до комп'ютерних ігор з публічних FTP-серверів, не говорячи вже про доступ до численних локальних ресурсів в домашній мережі – це лише основна ділянка застосування даних програм.

FTP-клієнт в Total Commander.

Цей популярний файловий менеджер непогано працює як FTP-клієнт. Робота з FTP-сервером починається після створення з'єднання: кнопка «FTP Connect» на панелі програми, потім – кнопка «New connection», де задаються параметри майбутнього з'єднання: хост, логін, пароль, можна також задати віддалену папку сервера, яка відкриватиметься відразу після з'єднання і локальну папку, яка відкриється у сусідньому вікні, щоб без зволікань можна було почати працювати з файлами.

Файлова структура сервера після з'єднання відображається в одному з двох вікон програми. Робота за протоколом FTP для

користувача Total Commander практично не відрізняється від роботи з локальним диском: для видалення, перейменування файлів і папок використовуються ті ж команди і елементи інтерфейсу програми. Завантаження файлів на сервер і з сервера добре реалізовано через «F5 сору» як копіювання між локальною і віддаленою директоріями.

FTP-клієнт Total Commander дозволяє зберігати облікові записи FTP-серверів, відновлювати передачу або отримання файла при обриві зв'язку, створювати чергу завдань. Підтримується і передача даних між двома FTP-серверами безпосередньо, синхронізація директорій.

З недоліків цього клієнта слід зазначити невелику кількість ASCII-фільтрів за замовчуванням. Передача даних може відбуватися в двох форматах: двійковому (binary) і текстовому (ASCII). Більшість файлів (архіви, програми, малюнки і ін.) відносяться до двійкового типу, тому цей спосіб встановлено за замовчуванням. Режим текстової передачі даних включається, якщо тип файлу вказаний в списку ASCII-форматів. До серйозніших недоліків клієнта можна віднести також небезпечне зберігання паролів і відсутність в дистрибутиві підтримки захищених SSL-з'єднань.

FTP-клієнт Total Commander буде зручним для домашнього користувача. Не маючи потужних функцій по забезпеченню безпеки, він якісно реалізує решту можливостей FTP-клієнта, забезпечуючи все необхідне для роботи з файлами і папками віддаленого сервера і має найзручніший та інтуїтивно зрозуміліший інтерфейс серед подібних програм.

Trial-версія Total Commander доступна на www.ghisler.com.

SmartFTP 2.5.1006.48

Freeware: (тільки для некомерційного використання) Розробник: SmartSoft.



Сайт: www.smartftp.com Розмір: 4,32 МБ

Адреса для завантаження

www.smartftp.com/download

Переваги: могутній, зручний і функціональний FTP-клієнт

Недоліки: відсутній повноцінний планувальник.

SmartFTP мабуть можна назвати не просто кращим freeware FTP-клієнтом, а взагалі однією з найдовершеніших утиліт в своїй категорії. Цю програму розробники вирішили зробити безкоштовним для домашніх користувачів.

З безперечних переваг SmartFTP варто відзначити приємний і функціональний multi-tabbed-інтерфейс, зручну панель, де «складаються» в чергу всі завантаження, і навіть є можливість створення декількох вікон з вкладками. Останнє особливо сподобається власникам широкоформатних моніторів – класичний двохпанельний інтерфейс як у Total Commander, поза сумнівом, зручний, але три або навіть п'ять незалежних вікон ще зручніше, особливо якщо дозволяє екранний простір. SmartFTP підтримує SSL-протокол для передачі конфіденційної інформації, забезпечує прямий обмін файлами між двома FTP-серверами без проміжного завантаження даних на комп'ютер (протокол FXP), є дуже корисна функція URL Watcher для автоматичного «перехоплення» FTP-посилань з буфера обміну і т.п.

При паралельній роботі з «швидким» і «повільним» FTP-сервером часто виникає ситуація, коли один з них як би «перетягує» всю пропускну спроможність каналу на себе, в результаті чого передача даних з іншого сервера взагалі припиняється. Тому SmartFTP дає змогу вручну виставити обмеження швидкості для кожного з FTP-з'єднань, внаслідок чого і канал стане використовуватися по максимуму, і обидва файли будуть завантажуватися з однаковим пріоритетом. Не забуто і віддалене редагування/перегляд різних типів файлів, детальні налаштування завантажень у чергах, детальний опис з'єднання, аналог папки *Избранное* для зберігання посилань на найчастіше відвідувані FTP-ресурси і т.д. З нечисленних недоліків програми варто відзначити лише відсутність повноцінного планувальника та деколи докучливе віконце з нагадуванням «ви використовуєте цю програму вже n-й день», яке з'являється кожного разу при старті SmartFTP.

AceFTP 3.80.3

Freeware (тільки для некомерційного використання)

Розробник: Visicom Media

Сайт: software.visicommedia.com/

Розмір: 5,08 МБ

Адреса для завантаження:

software.visicommedia.com/en/download

Переваги: непогана функціональність

Недоліки: банер, нав'язливі нагадування про купівлю Pro-версії, незадовільна робота з чергами



Як і багато інших freeware-утиліт, AceFTP Free є обмеженою версією платної AceFTP Pro, що, зрештою, не заважає їй справно виконувати свої функції. Вона підтримує прямий обмін файлами між двома FTP-серверами, має multi-tabbed-інтерфейс, дозволяє створювати скрипти для автоматизації серії рутинних дій і т.д. Присутньою є опція передпроглядання зображень прямо з сервера, хоча, користі від цього мало. Програма все одно завантажить малюнок на локальний комп'ютер і лише потім відкриє його у вбудованому переглядачі, тому жодних переваг ані у трафіку, ані у часі не буде. Реалізовано підтримку drag'and'drop – дана функція вже стає стандартом для сучасних FTP-клієнтів. Інтерфейс програми є функціональним – все максимально просто і навіть аскетично, хіба що великий банер у верхній частині екрану псує картину. Є претензії і до управління чергою завантажень та вивантажень, точніше, до її повної відсутності.

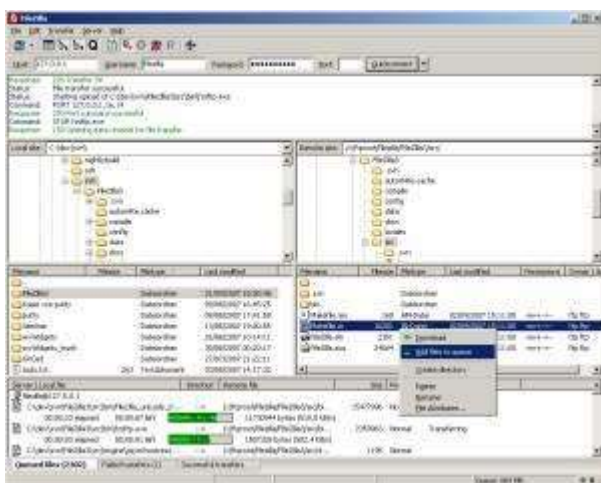
FileZilla 3.03

Freeware (тільки для некомерційного використання)

Розробник: Tim Kosse

Сайт: filezilla-project.org

Розмір: 2,6 МБ



Адреса для завантаження: project.org/download.php?type=client

Переваги: простий і зручний в роботі FTP-клієнт, не переобтяжений зайвими функціями.

Недоліки: кожен FTP-сеанс відкривається в окремому вікні.

Мультиплатформний open source FTP-клієнт у версії 3.3 став серйозним конкурентом для багатьох комерційних аналогів. Так, в новій FileZilla з'явилася підтримка drag'and'drop, опція обмеження за швидкостями download/upload, покращено регулювання черг, зменшено ресурсоемність програми і т.д. В усьому іншому – це класичний двохпанельний FTP-клієнт, простий і не переобтяжений зайвими функціями. Роботу з FTP-серверами FileZilla забезпечує на дуже високому рівні – зручний менеджер хостів, потужна система фільтрів для «відсікання» непотрібних файлів і каталогів на сервері, а також показ прихованих файлів на хості. Нажаль, присутня не ідеальна взаємодія програми з перевантаженим FTP-сервером або з сервером у разі поганого з'єднання. При цьому зв'язок з хостом часто обривається а завантажені на сервер файли іноді виявляються пошкодженими.

Пасивне і активне FTP-з'єднання

Існує два режими з'єднання з FTP-сервером – **активний** (active) і **пасивний** (passive). При роботі за протоколом FTP між клієнтом і сервером встановлюється два з'єднання – керуюче (по ньому йдуть команди) і з'єднання передачі даних (по ньому передаються файли). Керуюче з'єднання є однаковим для активного і пасивного режиму. Клієнт ініціює TCP-з'єднання з динамічного порту (1024-65535) до порту номер 21 на FTP-сервері і говорить "Привіт! Я хочу підключитися до тебе. Ось моє ім'я і мій пароль". Подальші дії залежать від того, який режим FTP (активний або пасивний) вибрано.

В активному режимі, коли клієнт говорить "Привіт!" він також повідомляє серверу номер порту (з динамічного діапазону 1024-65535) для того, щоб сервер міг підключитися до клієнта для встановлення з'єднання з метою передачі даних. FTP-сервер підключається до заданого номера порту клієнта, використовуючи з свого боку номер TCP-порту 20 для передачі даних.

В пасивному режимі, після того, як клієнт сказав "Привіт!", сервер повідомляє клієнтові номер TCP-порту (з динамічного

діапазону 1024-65535), до якого можна підключитися для встановлення з'єднання з метою передачі даних.

Головна відмінність між активним режимом FTP і пасивним режимом FTP – це сторона, яка відкриває з'єднання для передачі даних. В активному режимі, клієнт повинен прийняти з'єднання від FTP-сервера. У пасивному режимі, клієнт завжди ініціює з'єднання. Пасивний режим призначений для з'єднання через firewall. Якщо робота в Інтернеті відбувається через домашню локальну мережу або через локальну мережу підприємства, зазвичай для захисту мережі адміністратори використовують певний firewall. При роботі по FTP через firewall можна отримати помилку вигляду "425 Can't build data connection: Connection refused" або подібну. Це означає, що потрібно змінити налаштування FTP-програми так, щоб вона примусово використовувала пасивний режим FTP для з'єднання з FTP сервером.

Пошук файлів на FTP

Іноді, відомо точне або приблизне ім'я файлу, але де його можна вивантажити не відомо. Тоді слід пошукати цей файл на FTP. Для цього існують спеціалізовані пошукові машини, такі як <http://ftp-poisk.kiev.ua> – файловий пошук столиці, <http://filesearch.ru>. У полі пошуку слід ввести відоме ім'я файлу чи його частину, вибрати тип файлу і натиснути "Пошук". Інше зробить пошукова машина.

Перелік корисних FTP-сайтів

<ftp://kinodata.kiev.ua> <ftp://univ.kiev.ua>

<ftp://ftp.basilka.ru>

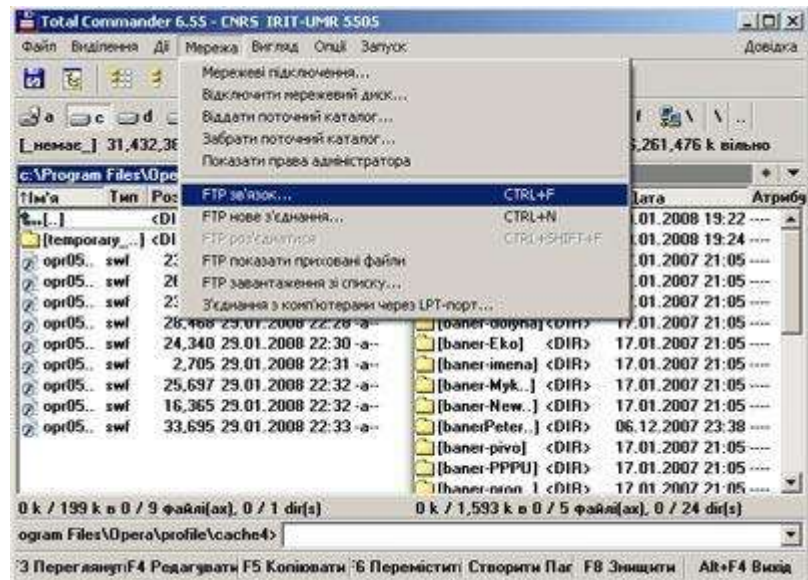
<ftp://matrix.farlep.net> [yakimus.kiev.ua](ftp://yakimus.kiev.ua)

<ftp://matrix.farlep.net> <ftp://maff.org.ua>

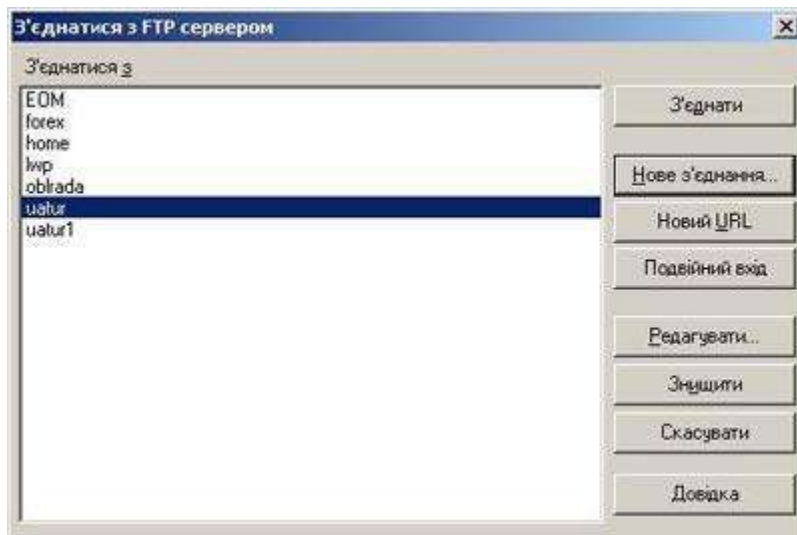
<ftp://ftp.frigate.kiev.ua> <ftp://ftp.lviv.farlep.net>

Налаштування Total Commander

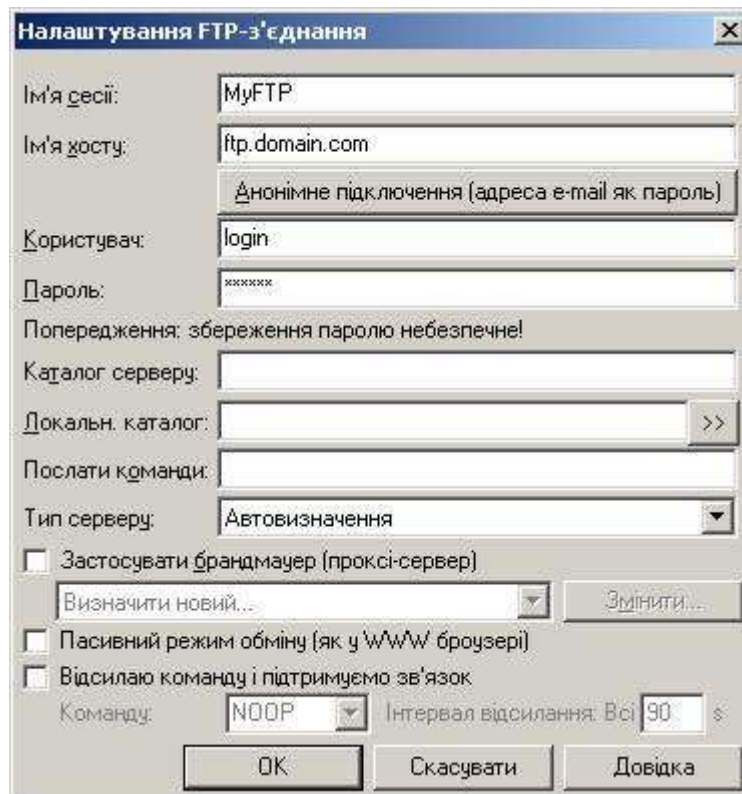
Після отримання інформації з реквізитами доступу до хостинг-акаунту можна створювати FTP-з'єднання з сервером. Виклик FTP-клієнта в програмах Total Commander / Windows Commander здійснюється за допомогою комбінації клавіш CTRL+F, або через меню **Net** (Мережа) | **FTP Connect** (FTP зв'язок).



У відповідному вікні натискаємо кнопку «**New connection**» (Нове з'єднання):



У вікні, що з'явиться, заповнюються поля відповідно до наданої інформації:



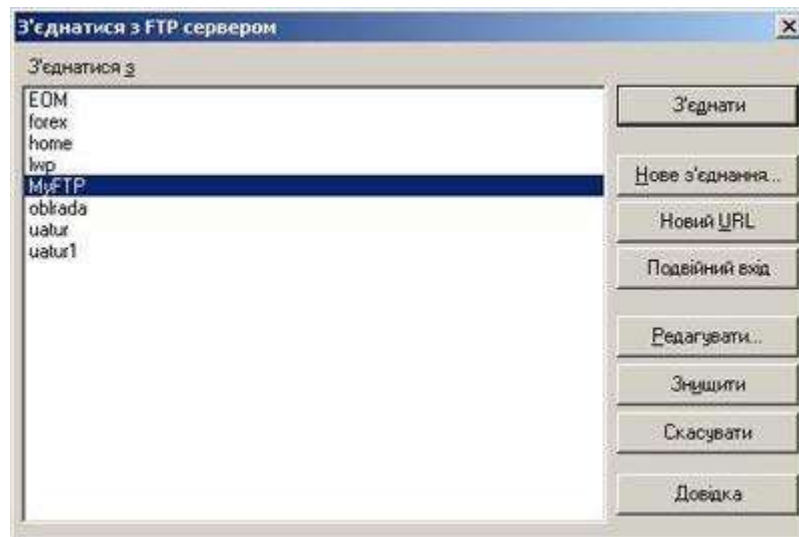
Session (Ім'я сесії) – назва з'єднання для відображення у вікні з'єднань

Host name (Ім'я хосту) – адреса FTP-сервера, наприклад, «<ftp.univ.kiev.ua>» **User name** (Користувач) – системний користувач, наприклад, «login» **Password** (Пароль) – системний пароль.

Ім'я користувача і пароль найчастіше задають за допомогою кнопки «Анонімне підключення», зазначаючи при цьому можливий e-mail.

При роботі через проксі-сервер, або у разі коли FTP-клієнт успішно проходить авторизацію, але видає порожній перелік файлів, слід в обов'язковому порядку вказати пасивний режим з'єднання – відзначити пункт «**Use passive mode for transfers (like a WWW browser)**» (Пасивний режим обміну (як у WWW браузері)). При потребі адреса проксі-сервера вводиться після встановлення відповідного прапорця та натиснення кнопки «Змінити». При цьому вказується спосіб з'єднання «HTTP-проксі з підтримкою FTP», а номер порта після адреси проксі-сервера відмежовується від неї двокрапкою.

Після заповнення форм натискають серію «ОК», в результаті чого у списку з'єднань з'являється нове з'єднання:



Для встановлення з'єднання з сервером натискають кнопку «**Connect**» (З'єднати). Після успішного з'єднання вміст обраного FTP-сервера відобразиться в активній панелі.

Технологія виконання роботи.

1. Віднайдіть в Інтернеті на одному з популярних сайтів пісню або архів пісні у форматі zip чи rar Вашого улюбленого виконавця. Образ екрану з результатами пошуку збережіть у файлі *Screen.doc*. Завантажте у Вашу папку одну з останніх пісень обраного виконавця, засікши при цьому час завантаження.

2. Самостійно чи за допомогою пошукового ftp-вказівника (наприклад <http://www.filesearch.ru/>) віднайдіть ftp-сервер та папку на ньому з піснями чи архівами музичних файлів Вашого виконавця. Образ екрану з результатами пошуку збережіть у файлі *Screen.doc*. Перейдіть в цю папку за допомогою Провідника. Завантажте у Вашу папку ще один архів пісні обраного виконавця з розміром, близьким до попереднього завантаженого файла, засікши при цьому час завантаження.

3. Завантажте ftp-клієнт з двома панелями вмісту, наприклад Total Commander. Створіть у ньому підключення до обраного ftp-сервера з правами анонімного користувача (логін: *anonymus*, пароль: *guest*) у **пасивному режимі**. Під'єднайтеся до цього сервера. Образи екранів з параметрами з'єднання та результатом підключення збережіть у файлі *Screen.doc*. Завантажте у Вашу папку ще одну пісню чи архів пісні обраного виконавця з розміром, близьким до попереднього завантаженого файла, засікши при цьому час завантаження.

4. Оцініть переваги та недоліки кожного з трьох використаних способів завантаження.

Запитання для контролю.

1. У чому переваги передачі файлів по протоколу ftp?
2. Як під'єднатися до ftp-сервера з правами анонімного користувача?
3. Які параметри по замовчуванню використовує ftp-клієнт?
4. Чим відрізняється пасивне ftp-з'єднання від активного?
5. Як зберегти параметри з'єднання з ftp-сервером у диспетчері з двома панелями вмісту? Як встановити таке з'єднання через проксі-сервер?

ПРАКТИЧНА РОБОТА №4.

Тема: Мережеві сніфери – TCPDump, Wireshark.

Мета роботи: Ознайомитися і навчитися працювати з такими мережевими сніферами, як TCPDump та Wireshark. Освоєння аналізаторів мережного трафіку, отримання навичок написання фільтрів для аналізаторів та ознайомлення зі стеком мережеских протоколів.

Теоретичні відомості

Аналізатор трафіку, або сніфер (від англ. To sniff – нюхати) – мережевий аналізатор трафіку, програма або програмно-апаратний пристрій, призначений для перехоплення і подальшого аналізу, або тільки аналізу мережевого трафіку, призначеного для інших вузлів. Сніфер може аналізувати тільки те, що проходить через його мережеву карту. Всередині одного сегмента мережі Ethernet усі пакети розсилаються всім машинам, через це можливе перехоплювати чужу інформацію. Використання комутаторів (switch, switch-hub) і їх грамотна конфігурація вже є захистом від прослуховування. Між сегментами інформація передається через комутатори. Комутація пакетів – форма передачі, при якій дані, розбиті на окремі пакети, можуть пересилатися з вихідного пункту в пункт призначення різними маршрутами. Так що як-що хтось в

іншому сегменті посилає всередині нього будь-які пакети, то у ваш сегмент комутатор ці дані не відправить.

Перехоплення трафіку може здійснюватися:

а. Звичайним "прослуховуванням" мережевого інтерфейсу (метод ефективний при використанні в сегменті концентраторів (хабів) замість комутаторів (світчей), в іншому випадку метод малоефективний, оскільки на сніфер потрапляють лише окремі фрейми);

б. Підключенням сніфера в розрив каналу;

в. Відгалуженням (програмним або апаратним) трафіку і спрямуванням його копії на сніфер;

г. Через аналіз побічних електромагнітних випромінювань і відновлення таким чином трафіку, що прослуховується;

д. Через атаку на каналному (MAC-spoofing) або мережевому рівні (IP-spoofing), що приводить до перенаправлення трафіку жертви або всього трафіку сегменту на сніфер з подальшим поверненням трафіку в належну адресу.

На початку 1990-х широко застосовувався хакерами для захоплення корис-тувальницьких логінів і паролів, які в ряді мережевих протоколів передаються в незашифрованому або слабозашифрованому вигляді. Широке поширення хабів дозволяло захоплювати трафік без великих зусиль у великих сегментах мережі практично без ризику бути виявленим.

Сніфери застосовуються як в позитивних, так і в деструктивних цілях. Аналіз пройшов через сніфер трафіку дозволяє:

а. Виявити паразитний, вірусний і закільцьований трафік, наявність якого збільшує завантаження мережного устаткування і каналів зв'язку (сніфери тут малоефективні; як правило, для цих цілей використовують збір різноманітної статистики серверами і активним мережним устаткуванням і її подальший аналіз).

б. Виявити в мережі шкідливе і несанкціоноване ПЗ, наприклад, мережеві сканери, флудери, троянські програми, клієнти пірінгових мереж та інші (це зазвичай роблять за допомогою спеціалізованих сніфер моніторів мережної активності).

в. Перехопити будь-який незашифрований (а деколи і зашифрований) трафік користувача з метою отримання паролів і іншої інформації.

г. Локалізувати несправність мережі або помилку конфігурації мережних агентів (для цієї мети сніфери часто застосовуються системними адміністраторами)

Далі розповімо докладніше про конкретних представників сніфферів.

tcpdump

tcpdump (від TCP і англ. dump – звалище, скидати) – утиліта UNIX, дозволяє перехоплювати і аналізувати мережевий трафік, що проходить через комп'ю-тер, на якому запущена дана програма. Для виконання програми потрібна наявність прав суперкористувача і пря-мий доступ до пристрою.

Основні призначення tcpdump:

– налагодження мережевих додатків

– налагодження мережі і мережної конфігурації в цілому

TcpDump – сніффер, що найбільш часто використовується під *nix системи. Ви можете знайти його в будь-якому з останніх дистрибутивів тієї операційної системи, яку ви використовуєте.

Опції командного рядка:

```
TcpDump [ -adeflnNOpqStvx ] [ -c count ] [ -F file ] [ -i interface ] [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ] [ expression ]
```

Параметр використання:

-a Дозволяє конвертувати мережеві і широкомовні адреси в імена;

-c Вихід після обробки count пакетів;

-d Виводить вміст пакету у зрозумілому людині вигляді;

-dd Виводить вміст пакету як фрагмент Cі-програми;

-ddd Виводить вміст пакету в десятковому вигляді;

-e Виводить заголовки канального рівня в кожній новій рядку;

-f Виводить адреси віддалених і локального хостів без перетворення в імена;

-F Використовувати file з описом параметрів фільтрації (дода-ткові вирази в командному рядку ігноруються) ;

-i Використовувати інтерфейс interface для трасування. Якщо не визначений, tcpdump знаходить активний мережевий ін-терфейс з найменшим номером (виключаючи loopback) ;

- l Використовує буферизований вивід на stdout. Корисним може виявитися конструкція вигляду "tcpdump-l | tee dat" or "tcpdump-l > dat & tail-f dat";
- n Не перетворювати адреси (тобто, адресу хоста, номер порту і т.п.) в імена;
- N Не друкувати доменне ім'я в імені хоста. Тобто, якщо використаний даний прапорець, tcpdump надрукує "nic" замість "nic.ddn.mil";
- O Не запускати оптимізатор пакетів;
- p Не переводити мережевий інтерфейс в "promiscuous mode";
- q Виводить інформацію в скороченому вигляді;
- r Читає пакети з файлу file (які створені за допомогою опції-w). Якщо ви хочете використовувати в якості введення консоль, то file це "-"
- s Видає snaplen байт кожного пакета (в SunOS'овсокому NIT мінімальна кількість 96). 68 байт достатньо для протоколів IP, ICMP, TCP і UDP, проте обрізає інформацію з більш ви-соких рівнів, скажімо, DNS і NFS пакетів;
- T Примусова інтерпретація пакетів по типу type відповідних масці "expression". На даний момент відомі наступні типи: rps (Remote Procedure Call), rtp (Real-Time Applications protocol), rtcp (Real-Time Applications control protocol), vat (Visual Audio Tool), і wb (distributed White Board) ;
- S Виводить абсолютний номер TCP-пакету;
- t Не виводить час в кожному рядку;
- tt Виводить неформатований час в кожному рядку;
- v Детальний вивід. Наприклад, час життя пакетів та тип сервісу;
- vv Більш детальний вивід. Наприклад, вивід додаткових полів NFS reply packets;
- w Записує raw-пакети в file, які ви зможете надалі розшифрувати з використанням опції -r. Якщо ви хочете використовувати в якості виводу консоль, то file це "-"
- x Виводить кожен пакет в шістнадцятковому вигляді (без заголовка). На вивід буде відправлено snaplen байт

Приклади:

Якщо tcpdump запустити без параметрів, він буде виводити інформацію про всі мережеві пакети. За допомогою параметра -i можна вказати мережевий інтерфейс, з якого слід приймати дані:

```
# tcpdump -i eth2
```

Щоб дізнатися отримані або відправлені пакети від певного хоста, необхідно його ім'я або IP-адресу вказати після ключового слова host:

```
# tcpdump host nameofserver
```

Щоб дізнатися про пакети якими обмінюються nameofserverA та nameofserverB: # tcpdump host nameofserverA and nameofserverB
Для відстеження тільки вихідних пакетів від якогось вузла потрібно вказати на-ступне:

```
# tcpdump src host nameofserver
```

Тільки вхідні пакети:

```
# tcpdump dst host nameofserver
```

Порт відправника і порт одержувача відповідно: # tcpdump dst port 80

```
# tcpdump src port 22
```

Щоб відстежувати один з протоколів TCP, UDP, ICMP, його назву слід вказати в команді. Використання операторів and (&&), or (||) і not (!) Дозволяє задавати фільтри будь-якої складності. Приклад фільтра, що відслідковує тільки UDP-пакети, що приходять з зовнішньої мережі:

```
# tcpdump udp and not src net localnet
```

Приклади використання tcpdump як фільтра:

Видача всіх вхідних та вихідних пакетів від sundown:

```
#tcpdump host sundown
```

Видача трафіку між helios і одним з двох hot або ace: #tcpdump host helios and \ (hot or ace \)

Видача всіх пакетов між ace та іншими хостами, виключаючи helios: #tcpdump ip host ace and not helios

Видача трафіку між машиною і машиною, що знаходиться в Berkeley: #tcpdump net ucb-ether

Видача ftp трафіку через шлюз snup:

```
#tcpdump gateway snup and (port ftp or ftp-data)'
```

Видача трафіку машинам, що не належать локальній мережі (якщо ваша машина – шлюз в іншу мережу, tcpdump не зможе видати трафік вашої локальної мережі).

```
#tcpdump ip and not net localnet
```

Видача старт і стоп пакетів (SYN і FIN пакети), які не належать до локальної ме-режі.

```
#tcpdump 'tcp[13] & 3!= 0 and not src and dst net localnet'
```

Видача IP пакетів довжиною більше 576 байт, переданих через шлюз snup: #tcpdump 'gateway snup and ip[2:2] > 576'

Видача IP broadcast або multicast пакетів, які не посилаються через Ethernet broadcast або multicast:

```
#tcpdump 'ether[0] & 1 = 0 and ip[16] >= 224'
```

Видача всіх ICMP пакетів, які не є запитами-відлуннями / відповідями (тобто, не ping пакети):

```
#tcpdump 'icmp[0]!= 8 and icmp[0]!= 0" Wireshark
```

Wireshark (раніше – Ethereal) – програма-аналізатор трафіку для комп'ютер-них мереж Ethernet і деяких інших. Має графічний користувальницький інтерфейс. У червні 2006 року проект був перейменований в Wireshark через проблеми з торговою маркою.

Функціональність, яку надає Wireshark, дуже схожа з можливостями про-грами tcpdump, проте Wireshark має графічний користувальницький інтерфейс і набагато більше можливостей із сортування і фільтрації інформації. Програма до-зволяє користувачеві переглядати весь проходить по мережі трафік в режимі реа-льного часу, переводячи мережну карту в нерозбірливий режим (англ. promiscuous mode).

Існують версії для більшості типів UNIX, в тому числі Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, а також для Windows.

Wireshark – це додаток, який «знає» структуру самих різних мережевих про-токолів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня. Оскільки для захоплення пакетів використовується pcap, існує можливість захоплення даних тільки з тих мереж, які підтримуються цією бібліотекою. Тим не менш, Wireshark уміє працювати з безліччю форматів вхідних даних, відповідно, можна відкривати файли даних, захоплених іншими програмами, що розширює можливості захоплення.

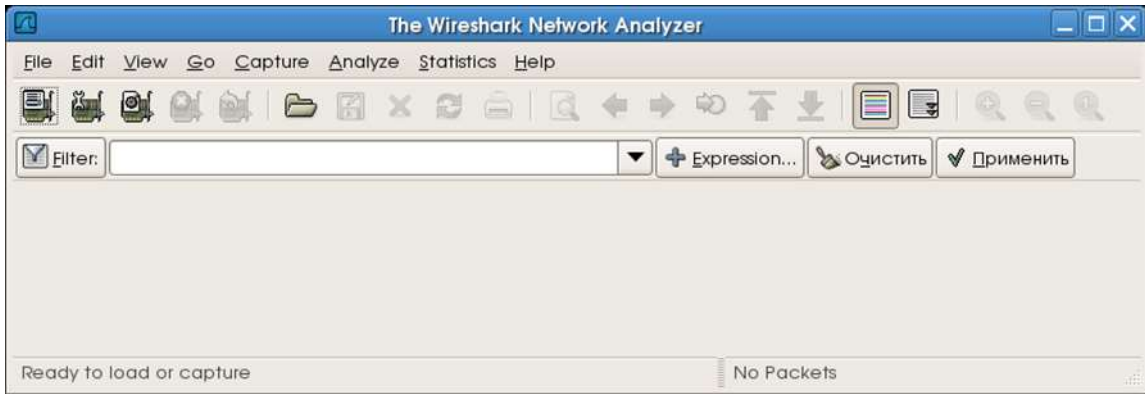


Рисунок 4.1 – Головне вікно програми

Захоплення пакетів:

Всі опції захоплення пакетів доступні через меню Capture 1. Вибір інтерфейсу(Capture/Interfaces).



Рисунок 4.2 – Вибір інтерфейсу

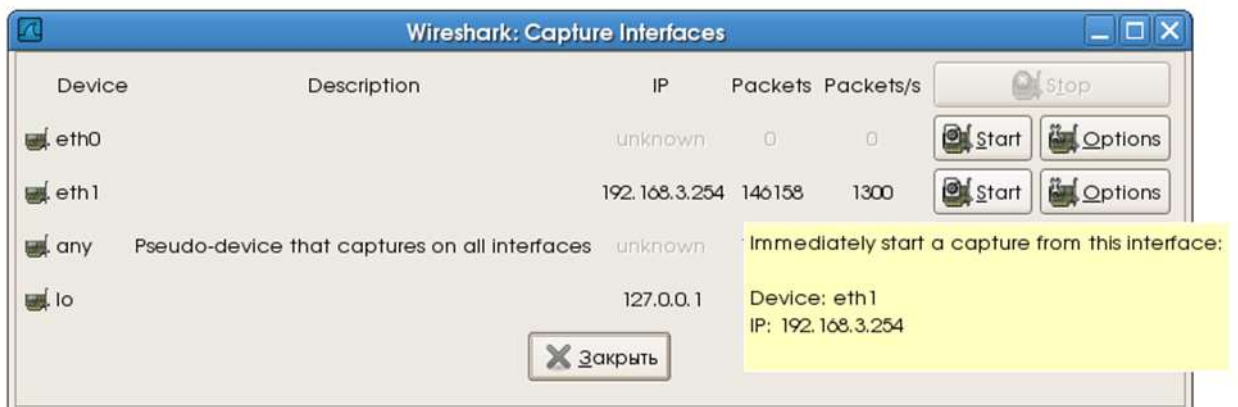


Рисунок 4.3 – Вікно процесу.

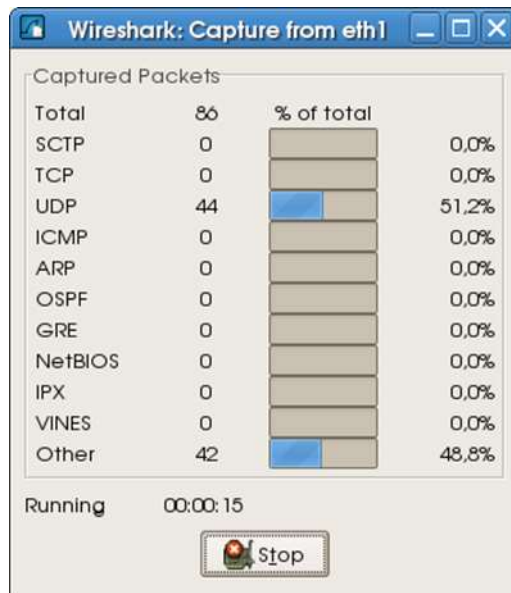


Рисунок 4.4 – Вікно процесу

3. Зупинка захоплення і завантаження результатів.

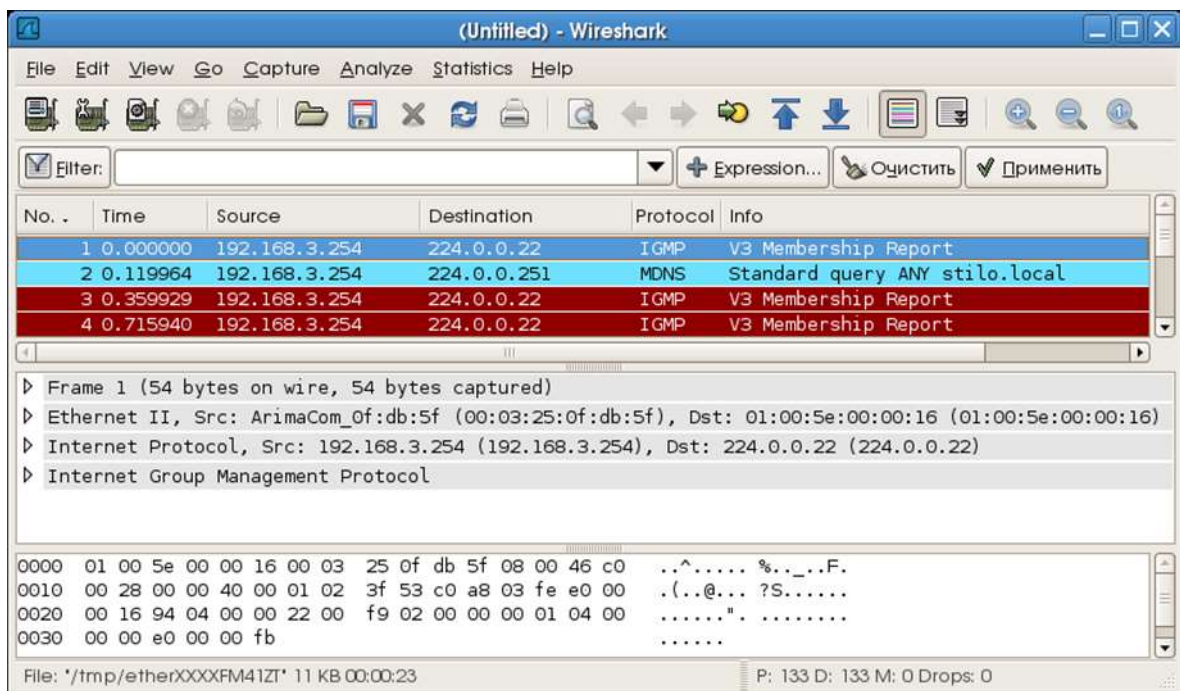


Рисунок 4.5 – Статистика

Типові звіти про використання мережі доступні через меню Statistics. Нижче наведені приклади відображення різних звітів.

1. Вибір звіту (Statistics):

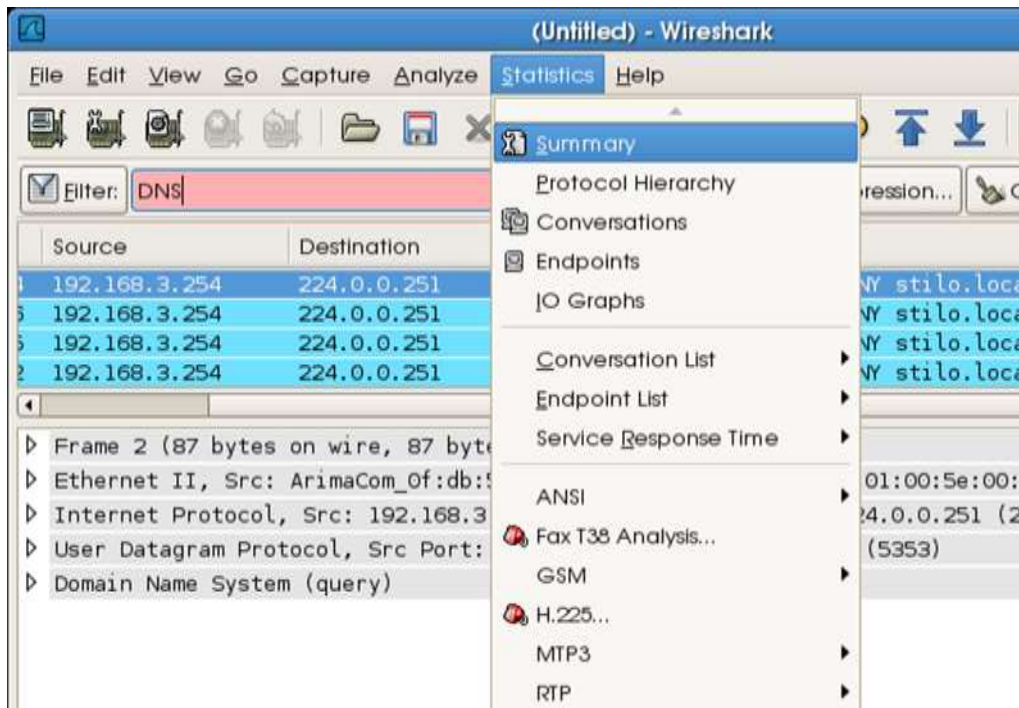


Рисунок 4.6 – Вибір звіту

2. Загальна статистика (меню Statistics/Summary).
3. Статистика по протоколам (меню Statistics/Protocol Hierarchy).

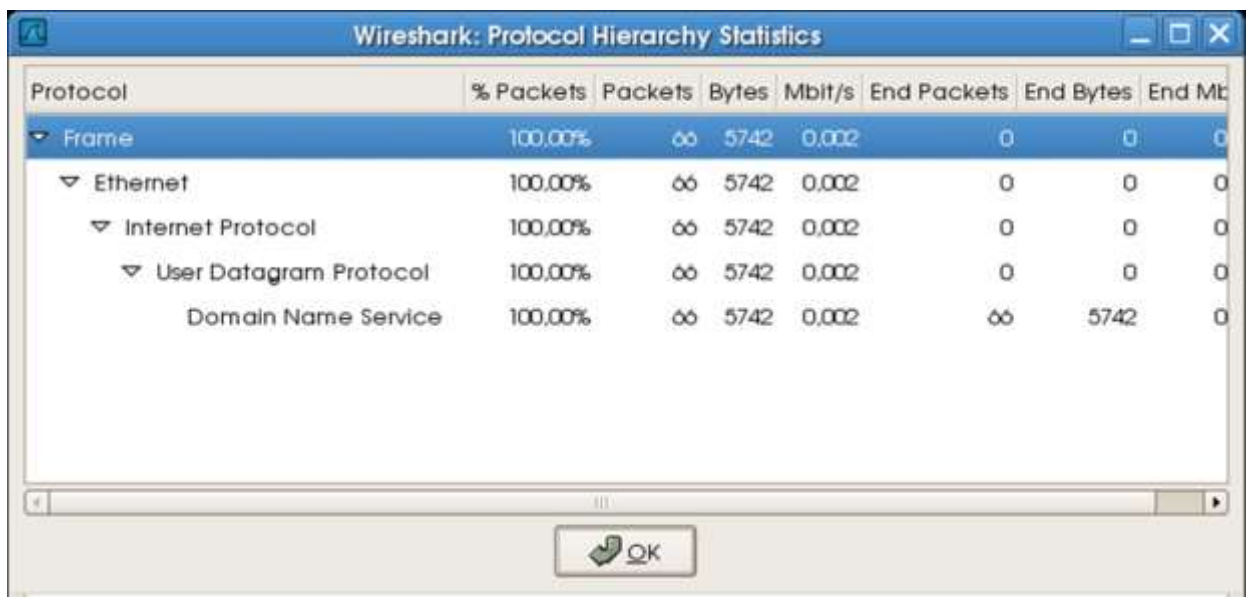



Рисунок 4.7 – Статистика по протоколам

4. Статистика по інтерфейсам (меню Statistics/Endpoints/Ethernet)



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
AirmaCom_0f:db:5f	9537	1393831	8521	1317229	1016	76602
AsustekC_ad:92:fa	1930	863951	851	70679	1049	793272
AsustekC_ad:93:51	279	23922	100	12366	129	11556
CompaqCo_29:58:a2	83	5970	53	3705	30	2265
CompaqCo_d2:bf:5b	41	3066	23	1788	18	1278
3Com_21:77:c7	26	3532	16	2211	11	1321
01:00:5e:00:00:fb	3660	318420	0	0	3660	318420
01:00:5e:00:00:16	3701	199854	0	0	3701	199854
Broadcast	29	3410	0	0	29	3410

Рисунок 4.8 – Статистика по інтерфейсам

Технологія виконання роботи.

Завдання 1. утиліта *tcpdump*

Розгляньте приклад докладно. Ваше завдання навчитися при його допомозі працювати з утилітою використовуючи фільтри.

Утиліта *tcpdump* призначена для аналізу мережевого трафіку і входить в поставку всіх POSIX систем. Ця утиліта виводить заголовки пакетів, які відповідають заданим критеріям, на мережевому інтерфейсі, перекладеному попередньо в режим прийому всіх пакетів (*promiscuous mode*). Критерії задаються у формі логічного виразу, наприклад:

```
root@kid>tcpdump -i ed1 -v -X -e host kid.stu and host ics-76-3.stu tcpdump: listening on ed1
```

Дана команда виводить на екран дамп пакетів між хостами *kid.stu* і *ics-76-3.stu* на інтерфейсі *ed1* хоста *kid.stu* в режимі розширеного виводу (*-v*) з печаткою вмісту пакету (*-X*).

Логічні вирази для критеріїв необхідні для того, щоб із загального мережевого трафіку виділити тільки ті пакети, що нас цікавлять. Синтаксис логічних виразів включає наступні ключові слова:

host – IP адреса або DNS

імя хосту *net* – адреса

мережі, наприклад

net 192.168.7, net 192.168.7.0 mask 255.255.255.224

port – номер порту (має сенс для протоколів TCP и UDP)

proto – тип протоколу. Можливі типи: ether, fddi, tr, ip, ip6, arp, rarp, decnet, lat, sca, mopr, mopr, iso, esis, isis, icmp, icmp6, tcp and udp. Наприклад, tcpdump tcp port 80

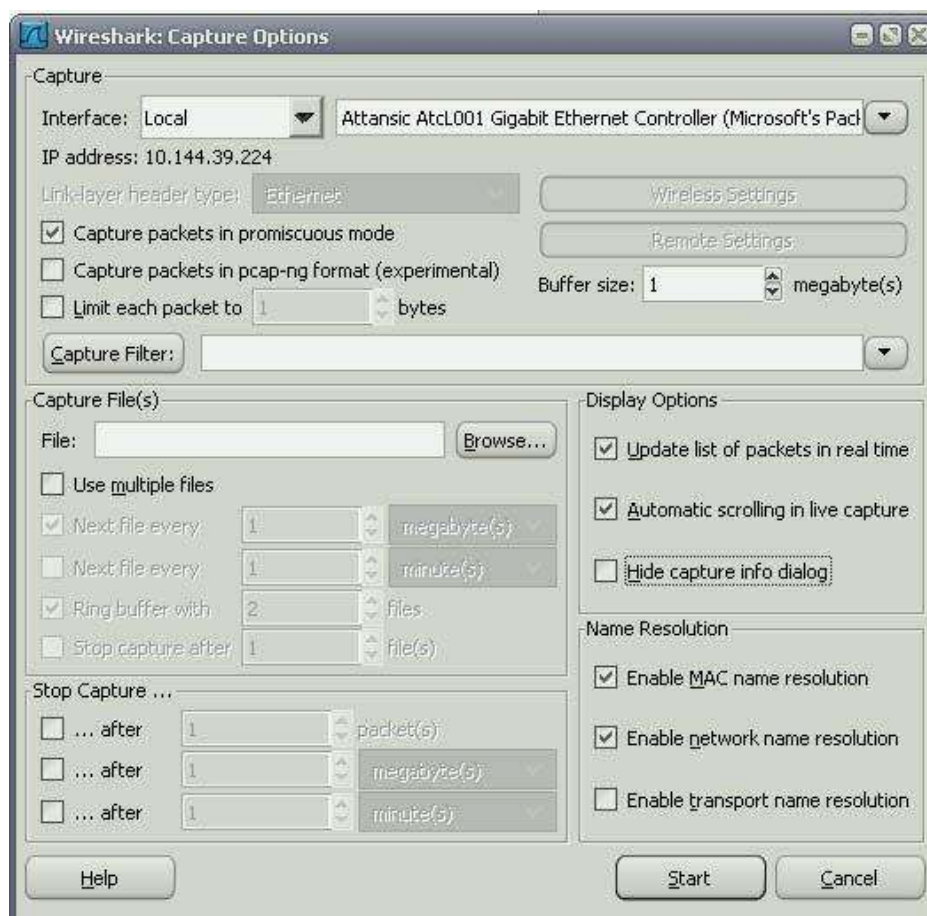
dir – напрямок, можливі значення – src або dst . Наприклад, tcpdump src host kid.stu.

Крім того, можна використовувати адресу несучою мережі Ethernet:

```
tcpdump ether dst  
00:02:44:5b:ee:9b або IP  
мережа:  
tcpdump net src 192.168.7.0/27
```

Завдання 2. Програма Wiresharks

- а. Налаштування параметрів захоплення мережевого трафіку. Встановіть параметри у відповідності до рисунку:



Наступні опції мають бути активовані:

- Capture packets in promiscuous mode.
- Update list of packets in real time
- Automatic scrolling in live capture
- Enable MAC name resolution
- Enable network name resolution

В якості інтерфейсу, використаного для захоплення трафіку вибрати фізичний (не віртуальний) адаптер і встановити тип адаптера Local.

б. Налаштування фільтрації виведення по протоколах DNS і HTTP.

Для налаштування фільтрації необхідно ввести в поле фільтра вираз: "dns || http". Далі натисніть кнопку Apply.

в. Запустіть оновлення антивірусу на даному комп'ютері (наприклад – avast) г. Зупиніть захоплення трафіку, натиснувши Capture > Stop.

д. Проаналізуйте трафік, захоплений програмою.

Знайдіть серед PDU, захоплених в списку DNS-запит (query) і DNS-відповідь (query response).

Подивившись вміст DNS-запиту і DNS-відповіді з'ясувати і записати в звіт наступну інформацію:

DNS ім'я сервера оновлень антивірусу.

Будь-які 5 мережевих адрес сервера оновлень.

Далі серед PDU, захоплених програмою знайдіть HTTP-запит (HTTP GET). Подивившись вміст PDU з'ясувати і записати в звіт наступну інформацію:

Мережний адресу сервера оновлень.

е. Вивчивши вміст DNS-запиту, HTTP-запит і DNS-відповіді з'ясувати і записати в звіт наступну інформацію:

MAC-адресу комп'ютера. MAC-адреса шлюзу.

IP-адресу проксі-сервера DNS ім'я проксі-сервера.

Протокол транспортного рівня, який використовує сервіс DNS. Протокол транспортного рівня, який використовує протокол HTTP.

ж. Збережіть захоплений трафік, натиснувши File> Save As.

Запитання для контролю.

1. У чому головна відмінність між tcpdump і Wireshark?
2. Два хоста обмінюються пакетами між собою, як за допомогою утиліти tcpdump можна подивитися їх трафік?
3. Що буде, якщо в поле фільтра після сеансу захоплення мережевого трафіку Wireshark ввести «ftp || ftp-data»?
4. Яким чином можна подивитися статистику по протоколам після аналогічно-го сеансу Wireshark?
5. Чи можна за допомогою Wireshark перехопити паролі або текстові повідомлення, призначені іншому користувачеві? Що для цього потрібно?

ПРАКТИЧНА РОБОТА №5.

Тема: Налаштування рівнів безпеки сучасних браузерів.

Мета роботи: Формування вмінь і навиків налаштування рівнів безпеки сучасних браузерів – Chrome, IE, Mozilla Firefox, Opera та ін. для обмеження впливу людського фактору на інформаційну безпеку. Порівняння рівня безпеки сучасних браузерів.

Теоретичні відомості

Фішинг – це технологія онлайн-шахрайства, яка використовується зловмисниками для отримання особистої інформації користувачів.

Існує кілька тактик виманювання інформації, зокрема повідомлення електронної пошти та веб-сайти, які використовують підроблені відомі та надійні бренди. Типовою фішинг-махінацією є використання оманливих повідомлень, які виглядають як повідомлення від відомих компаній або веб-сайтів, наприклад, банків, емітентів кредитних карток, благодійних організації або з сайтів організацій, що займаються електронною комерцією.

Cookie – це невелика порція текстової інформації, яку сервер передає браузеру. Коли користувач звертається до сервера (набирає його адресу в рядку браузера), сервер може зчитувати інформацію, що міститься в cookies, і на підставі її аналізу здійснювати які-небудь дії. Наприклад, у випадку авторизованого доступу до чогось через веб, у cookies зберігаються логін і пароль протягом


сесії, що дає можливість користувачу не вводити їх знову при запитах кожного документа, захищеного паролем.

SSL (Secure Sockets Layer – рівень захищених сокетів) – протокол рівня передачі даних, який пропонує захищений канал передачі даних між клієнтом і сервером з використанням аутентифікації, цифрових підписів і шифрування. Для шифрування/дешифрування трафіку використовується ключ (сертифікат), отриманий клієнтом від сервера.

В основі технології SSL лежать спеціально розроблені криптографічні алгоритми, що використовують поняття публічного і приватного ключів. Таким чином SSL-сертифікат – це комбінація спеціальним чином згенерованого приватного і публічного ключів, виписана на певне доменне ім'я, програму або IP-адресу. Публічний і приватний ключі є звичайними текстовими файлами, що містять табульований набір символів. Протокол SSL гарантує безпечне з'єднання між сервером і браузером користувача. При використанні каналу, захищеного SSL-сертифікатом, інформація передається в закодованому вигляді по протоколу HTTPS, і розшифрувати її можна тільки за допомогою спеціального ключа, який відомий тільки власнику сертифіката і довіреному Центру сертифікації, який видав даний SSL-сертифікат. Використання SSL дозволяє вирішити наступні завдання:

- забезпечення цілісності інформації (гарантія того, що дані не були змінені в процесі передачі);
- підтвердження дійсності сторін, що беруть участь в обміні інформацією (у діалозі);
- гарантування безпеки передачі даних (дані передаються по мережі в зашифрованому вигляді).

Технологія виконання роботи.

1. Відкрийте браузер Google Chrome.
2. Відкрийте меню Chrome  на панелі інструментів браузера.
3. Виберіть у ньому пункт **Налаштування**.
4. Самостійно встановіть українську мову інтерфейсу та при потребі перезавантажте браузер і знову ввійдіть на сторінку налаштувань.

Налаштування параметрів безпеки Google Chrome

5. При наявності натисніть посилання Показати розширені налаштування.
6. Перегляньте список налаштувань, які можна змінювати в Google Chrome.

Захист від фішингу та шкідливих програм

7. Переконайтеся, що у розділі Конфіденційність прапорець Активувати захист від фішингу та шкідливих програм встановлений по замовчуванню. Коли цей прапорець встановлений, Google Chrome показує попередження, якщо відкривається сайт, який підозрюється в фішингу або поширенні зловмисних програм.

Налаштування та сертифікати SSL

8. У розділі HTTPS/SSL натисніть кнопку Керування сертифікатами та перегляньте різновиди та дані встановлених сертифікатів. Для чого вони використовуються?
9. Самостійно поверніться до сторінки налаштувань Google Chrome.

Налаштування веб-вмісту сторінок

10. У розділі Конфіденційність натисніть кнопку Налаштування вмісту.
11. У вікні, що з'явиться (рис. 5.1) натисніть кнопку Усі файли cookie та дані із сайтів..., щоб відкрити діалогове вікно Файли cookie та дані із сайтів (рис. 5.2).



Рис. 5.1. – Вікно налаштування вмісту сторінок Google Chrome

12. Самостійно видаліть файли cookie від сайтів, які не заслуговують на вашу довіру. Якщо необхідно швидко видалити всі файли cookie, то натисніть кнопку Видалити все.

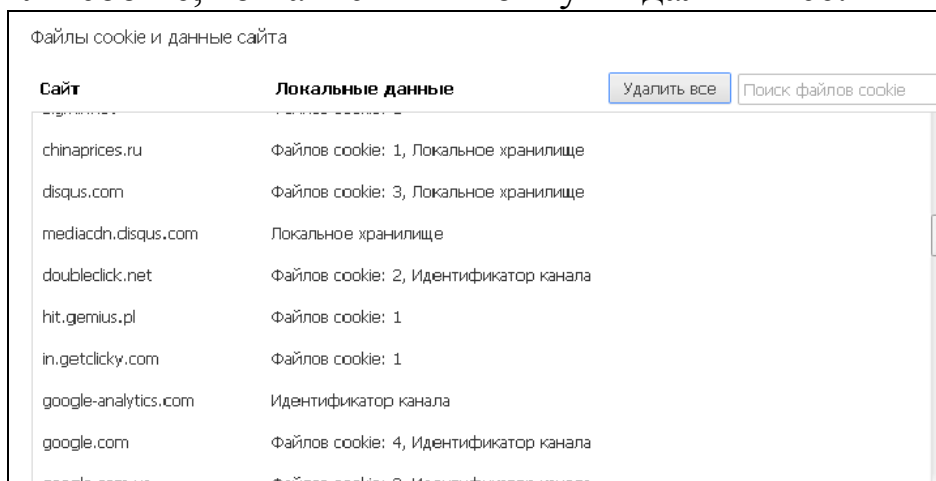



Рис. 5.2. – Діалогове вікно Файли cookie та дані із сайтів

13. Щоб браузер Google Chrome автоматично видаляв файли cookie при закритті усіх вікон, у діалоговому вікні Налаштування вмісту встановіть прапорець Зберігати локальні дані лише до закриття веб-оглядача. Якщо ж необхідно заблокувати всі файли cookie, виберіть Не дозволяти сайтам зберігати дані. При блокуванні файлу cookie в адресному рядку відображається .
14. Для задання винятків з правил обробки cookie-файлів натисніть кнопку Керувати винятками. У вікні, яке відкриється, введіть ім'я домену, для якого потрібно встановити виняток (ваш улюблений сайт). Щоб створити виключення для всього домену, вставте перед його ім'ям [*.] (рис. 5.3). Для задання домену також можна вказати його IP-адресу, IPv6-адресу або URL.

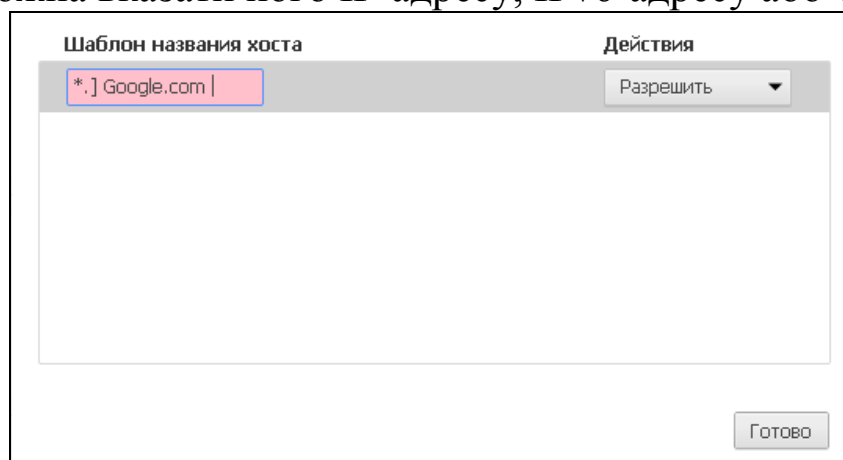


Рис. 5.3. – Вікно формування винятків

15. За допомогою меню Поведінка дозвольте обраному сайту створювати файли cookie (при виборі ж параметра Очищати під час виходу файли cookie видалятимуться, як тільки ви закриєте браузер).
16. Самостійно дослідіть інші налаштування вмісту сторінки браузера Google Chrome.
17. Закрийте Google Chrome.

Налаштування параметрів безпеки браузера Internet Explorer

18. Завантажте браузер Internet Explorer (надалі – ІЕ).
19. Для перевірки можливості блокування окремого вузла виконайте наступні дії:
 - 19.1. В головному меню оберіть підпункт Сервіс – Властивості оглядача;
 - 19.2. У вікні, що з'явиться, перейдіть на вкладку Конфіденційність (рис. 4) та натисніть кнопку Вузли;

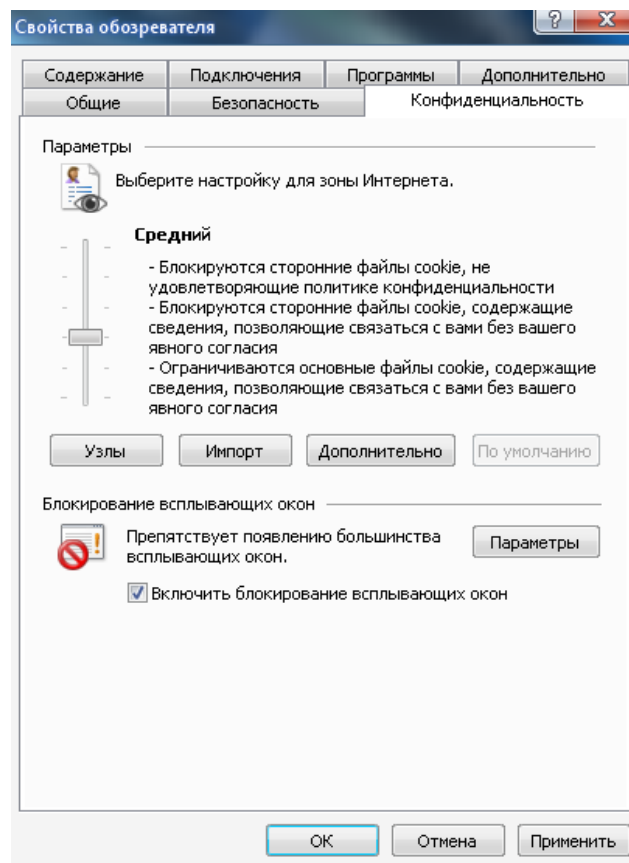


Рис. 5.4. – Налаштування параметрів конфіденційності в ІЕ

- 19.3. У виведеному вікні в рядку для задання адреси введіть адресу сайту *www.ukr.net*, і натисніть кнопку Блокувати;

19.4. Зайдіть на сайт *www.ukr.net* та спробуйте відкрити на ньому вашу поштову скриньку. Що при цьому відбувається?

19.5. Самостійно видаліть вузол *www.ukr.net* зі списку заблокованих вузлів та спробуйте знову зайти на цьому вузлі у вашу поштову скриньку. Чи вдалося це зробити?

В домашніх умовах:

20. В ІЕ самостійно перейдіть у вікно Властивості оглядача та активізуйте у ньому вкладку Безпека.

21. Відмітьте піктограму Інтернет і у групі Рівень безпеки для цієї зони натисніть кнопку Інший (рис. 5).

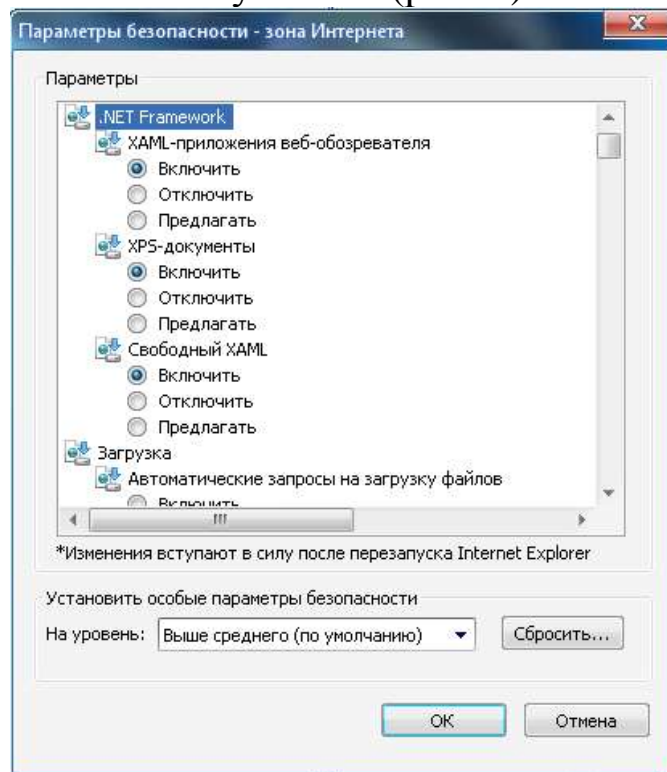


Рис. 5.5. – Налаштування параметрів безпеки в ІЕ

22. У розділі Параметри перегляньте налаштування параметрів безпеки, самостійно забезпечте завантаження файлів на основі вмісту, а не розширення та блокування спливаючих вікон і натисніть кнопку ОК.

23. Для підвищення загального рівня безпеки і захисту комп'ютера від будь-яких несанкціонованих завантажень, використайте можливість занесення небезпечних сайтів у зону Обмежені вузли. Для перевірки цієї можливості виконайте наступні дії:

23.1. Самостійно поверніться у вікно Властивості оглядача;

23.2. На вкладці Безпека відмітьте посилання Обмежені вузли;

23.3. Натисніть кнопку **Вузли**, в рядку для задання адреси введіть *comr.usoz.net* та натисніть кнопку **Додати** (рис. 5.6);

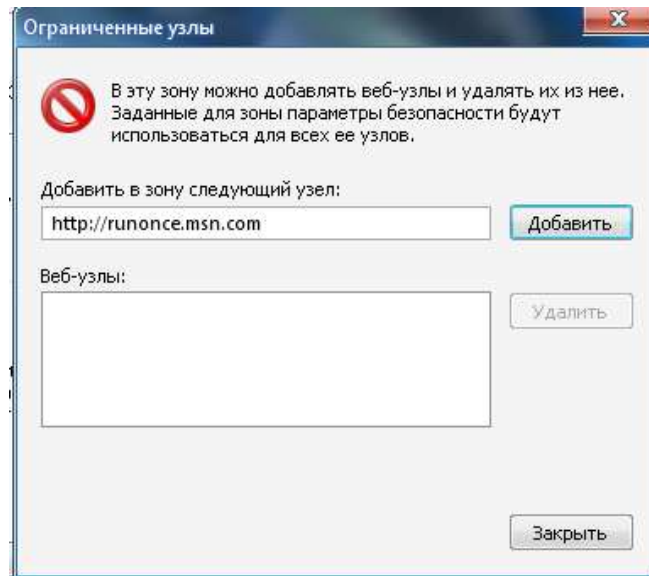


Рис. 5.6. – Вікно формування списку заборонених вузлів

23.4. Почергово закрийте вікна **Обмежені вузли** та **Властивості оглядача** з збереженням внесених змін;

23.5. Спробуйте завантажити сторінку *comr.usoz.net*. Що при цьому відбувається?

23.6. Самостійно видаліть вузол *comr.usoz.net* зі списку обмежених вузлів та забезпечте відображення цієї сторінки у вікні оглядача.

Запитання для контролю.

1. Які можливості налаштування безпеки має Google Chrome?
2. Як вимкнути потенційно вразливі компоненти браузера?
3. Що таке файли cookies? Навіщо їх видаляють?
4. Налаштування яких параметрів вмісту сторінки можливо у браузері Google Chrome?
5. Як в ІЕ заблокувати окремі вузли? Навіщо це робити?
6. Як в ІЕ віднести окремих вузол до переліку обмежених? Навіщо це робити?
7. Який з сучасних браузерів захищений найкраще на Вашу думку? Обґрунтуйте свою позицію.

ПРАКТИЧНА РОБОТА №6.

Тема: Використання облікових записів користувачів та груп для захисту від комп'ютерних вірусів на рівні операційної системи за допомогою реалізації політик безпеки з обмеженими правами доступу.

Мета роботи: Формування вмінь і навиків надання обмеженого доступу до окремих папок та кореневого диску флеш-носіїв засобами операційної системи. Закріплення знань файлової структури, вмінь і навиків створення та переміщення файлів і папок.

Теоретичні відомості

На сьогодні більшість комп'ютерних вірусів, вражаючи флеш-носії, намагаються вразити чи створити вражені файли насамперед у кореневій папці, адже саме з неї відбувається старт автоматичного завантаження програм і початковий перегляд вмісту. Для захисту від таких дій засобами операційної системи доцільно створити власну папку на флеш-носії для збереження папок і файлів, а в кореневу папку заборонити внесення змін, що й буде зроблено під час виконання лабораторної роботи.

Загальні вказівки до виконання роботи

Виконувати лабораторну роботу слід на власному ПК з правами доступу адміністратора. Інструкції до виконання роботи апробовані в ОС Windows 7, в інших ОС аналогічні засоби реалізації завдань мають бути віднайдені виконавцем самостійно. Виконуючи перенесення даних та форматування дисків слід бути максимально уважним, адже викладач дисципліни відповідальності за збереження ваших даних не несе.

Технологія виконання роботи.

Підготовчий етап заняття. Актуалізація знань.

1. Перед тим як виконувати описані нижче дії необхідно зберегти інформацію із вашого flash носія у іншому місці, так як вся інформація з нього буде видалена.
2. Для того, щоб всі дії можна було виконати потрібно зайти у систему під користувачем із правами адміністратора, яким не являється користувач з іменем "student".

Організація захисту від запису в кореневу папку флеш-носія

1. Відкрити "Пуск" і вибрати "Мой компьютер".
2. Для відображення можливостей доступу у вікні "Сервис" – "Свойства папки" перейти на закладку "Вид", зняти прапорець "Использовать простой общий доступ к файлам (рекомендуется)" та зберегти внесені зміни.
3. У вікні "Мой компьютер" викликати контекстне меню flash диску і вибрати команду "Свойства".
4. Вікно "Свойства: Съемный диск":
 1. Відкрити закладку "Оборудование".
 2. У списку "Все диски" вибрати свій flash носій.
 3. Натиснути кнопку "Свойства".
5. Вікно "Свойства":
 1. Відкрити закладку "Политика".
 2. Встановити перемикач "Оптимизировать для выполнения".
 3. Натиснути кнопку "ОК".
6. У вікні "Свойства: Съемный диск" натиснути кнопку "ОК".
7. У вікні "Мой компьютер" викликати контекстне меню flash диску і вибрати команду "Форматировать...".
8. Вікно "Формат Съемный диск":
 1. У розгорнутому списку "Файловая система" вибрати пункт "NTFS".
 2. Натиснути кнопку "Начать".
9. У вікні попередження "Формат Съемный диск" натиснути кнопку "ОК".
10. Чекаємо завершення форматування...
11. У вікні "Форматирование Съемный диск" натиснути кнопку "ОК".
12. У вікні "Формат Съемный диск" натиснути кнопку "Закрыть".
13. Зайти у кореневий каталог flash диску.
14. У головному меню вікна перейти до "Файл" – "Создать" – "Папку".
15. Ввести назву папки "data" де *data* – це ваше прізвище, введене латинськими лвтерами, і натиснути "Enter" на клавіатурі.
16. У контекстному меню папки "data" вибрати команду "Свойства".

17. Вікно "Свойства: data":
 1. Відкрити закладку "Безопасность".
 2. Натиснути кнопку "Добавить...".
18. Вікно "Выбор: Пользователи или Группы":
 1. Натиснути кнопку "Дополнительно...", "Поиск".
 2. У сформованій знизу вікна таблиці вибрати рядок в колонці "Имя (RDN)" якого записане слово "Все", а комірка колонки "В папке" порожня.
 3. Натиснути кнопку "ОК".
19. Вікно "Свойства: data" (зкладка "Безопасность"):
 1. Для таблиці "Разрешения для Все" встановити прапорець на перетині рядка "Полный доступ" і стовпця "Разрешить".
 2. Натиснути кнопку "Применить" і "ОК".
20. У вікні провідника для flash диску на панелі інструментів натиснути кнопку "Назад".
21. У вікні "Мой компьютер" викликати контекстне меню flash диску і вибрати команду "Свойства".
22. Вікно "Свойства: Съемный диск":
 1. Відкрити закладку "Безопасность".
 2. У списку "Группы или пользователи" вибрати рядок "Все".
 3. Для таблиці "Разрешения для Все" встановити прапорці "Список содержимого папки" і "Чтение" у стовпці "Разрешить" та прапорець "Запись" у стовпці "Запретить".
 4. Натиснути кнопку "Применить".
23. У вікні "Безопасность" натиснути кнопку "Да".
24. У вікні "Свойства: Съемный диск" натиснути кнопку "ОК".

Завершальний етап заняття

1. Перенесіть збережені раніше дані у створену папку на флеш-носії.
2. Спробуйте здійснити копіювання довільного файлу у кореневий диск флеш-носія. Чи вдалося це зробити? Чому?
3. Створіть електронний лист з відповідями на контрольні запитання у своїй поштовій скриньці на сайті gmail.com. Тему листа сформуєте за шаблоном *<група>_<номер лабораторної>_<прізвище ім'я>*, наприклад:

ЕК21_ЛР6_Величко Володимир. Надішліть створений лист на адресу volosyuk@mna.edu.ua.

Запитання для контролю.

1. Чому для флеш-носіїв доцільно заборонити запис у кореневий диск?
2. Навіщо форматувати флеш-носій перед заборонаю запису у кореневий диск? Яка файлова система при цьому має використовуватися?
3. Як заборонити запис даних в окрему папку засобами ОС?
4. Параметри доступу для якої групи користувачів встановлюються для заборони запису даних в окрему папку засобами ОС? Чому?
5. Чому, забороняючи запис в кореневу папку, не потрібно поширювати ці параметри на вкладені об'єкти?

ПРАКТИЧНА РОБОТА №7.

Тема: Застосування криптографічних засобів захисту інформації. Формування пар відкритих та закритих ключів для реалізації асиметричного шифрування.

Мета роботи: Формування вмінь і навиків організації криптографічного захисту інформації. Отримання знань методів і способів асиметричного шифрування та навиків використання відповідного програмного забезпечення. Закріплення знань файлової структури, вмінь і навиків використання можливостей диспетчерів файлів та поштових систем для пересилання фалів іншим користувачам.

Теоретичні відомості

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, які можуть бути реалізовані за допомогою обчислювальних засобів. Відомо більш десятка перевірених алгоритмів шифрування, які, при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу. Широко використовуються такі алгоритми шифрування як Twofish, IDEA, RC4, DES, та ін.

У багатьох країнах прийняті національні стандарти шифрування. У 2001 році в США прийнятий стандарт симетричного шифрування AES на основі алгоритму Rijndael з довжиною ключа 128, 192 і 256 біт. Алгоритм AES прийшов на зміну колишньому алгоритмові DES, який тепер рекомендовано використовувати тільки в режимі Triple-DES (3DES).

Тривалий час під криптографією розумілось лише шифрування – процес перетворення звичайної інформації (відкритого тексту) в незрозумілий набір знаків (тобто, шифротекст). Дешифрування – це обернений процес відтворення інформації із шифротексту. Шифром називається пара алгоритмів шифрування/дешифрування. Дія шифру керується як алгоритмами, так і, в кожному випадку, ключем. Ключ – це секретний параметр (в ідеалі, відомий лише двом сторонам) для однозначного шифрування/дешифрування повідомлень. Ключі дуже важливі, оскільки без змінних ключів алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків.

До алгоритмів симетричного шифрування належать способи шифрування, в яких і відправник, і отримувач повідомлення мають однаковий ключ (або дин ключ легко обчислюється з іншого). Ці алгоритми шифрування були єдиними загально відомими до липня 1976.

На відміну від симетричних, асиметричні алгоритми шифрування використовують пару споріднених ключів – відкритий та секретний. При цьому, не зважаючи на пов'язаність відкритого та секретного ключа в парі, обчислення секретного ключа на основі відкритого вважається технічно неможливим.

PGP (англ. Pretty Good Privacy) – комп'ютерна програма, що дозволяє виконувати операції шифрування (кодування) і цифрового підпису повідомлень, файлів і іншої інформації, представленої в електронному вигляді. Її першу версію розробив Філіп Циммерман у 1991 році.

PGP має безліч реалізацій, сумісних між собою і рядом інших програм (GNUPG, Filecrypt і ін.) завдяки стандарту OPENPGP (RFC 4880), які мають різний набір функціональних можливостей. Існують реалізації PGP для всіх найпоширеніших операційних систем. Окрім вільно поширюваних, є комерційні реалізації.

Користувач PGP створює ключову пару: відкритий і закритий ключ. При генерації ключів задаються їх власник (ім'я і адреса

електронної пошти), тип ключа, довжина ключа і термін його дії. PGP підтримує три типи ключів RSA v4, RSA legacy (v3) і Diffiehellman / dss (Elgamal в термінології GNUPG).

Для ключів RSA legacy довжина ключа може складати від 1024 до 2048 біт, а для Diffie-hellman/dss і RSA – від 1024 до 4096. Ключі RSA legacy містять одну ключову пару, а ключі Diffie-hellman/dss і RSA можуть містити один головний ключ і додаткові ключі для шифрування. При цьому ключ електронного підпису в ключах Diffie-hellman/dss завжди має розмір 1024. Термін дії для кожного з типів ключів може бути визначений як необмежений або до конкретної дати. Для захисту ключового контейнера використовується секретна фраза. Ключі RSA legacy (v3) для шифрування зараз не використовуються і виведені із стандарту OPENPGP.

Електронний цифровий підпис формується шляхом підпису дайджеста (хеш-значення) повідомлення (файлу) закритим ключем відправника (автора). Для формування дайджеста можуть використовуватися алгоритми Md5, Sha-1, Ripemd-160, Sha-256, Sha-384, Sha-512. У нових версіях PGP підтримка Md5 здійснюється для збереження сумісності з ранніми версіями. Для підпису використовуються алгоритми RSA або DSA (залежно від типу ключа).

Шифрування здійснюється з використанням одного з п'яти симетричних алгоритмів (AES, Cast5, TRIPLEDES, IDEA, Twofish) на сеансовому ключі. Сеансовий ключ генерується з використанням криптографічного стійкого генератора псевдовипадкових чисел. Сеансовий ключ зашифровується відкритим ключем одержувача з використанням алгоритмів RSA або Elgamal (залежно від типу ключа одержувача).

Для отримання практичних навичок шифрування інформації використаємо саме програму PGP, головна перевага якої – простота використання.

Технологія виконання роботи.

Віднайдіть ваш файл з описом різновиду апаратного засобу захисту чи зламу захисту та скопіюйте його в буфер обміну.

Створіть нову папку для організації криптографічного захисту та вставте в неї скопійований файл.

Для генерації та використання ключів встановіть програму PGP 8.0 (для ОС до Windows XP) чи PGP Desktop 10 (для Windows 7, 8, 10).

Створення пари відкритого і закритого ключів для шифрування повідомлень.

Для завантаження програми генерації ключів віднайдіть та виберіть у меню Пуск операційної системи в групі PGP посилання PGPkeys для Windows XP (чи PGP Desktop для Windows 7).

З метою створення власної пари відкритого і закритого ключів оберіть в меню Keys для Windows XP (рис. 6.1) чи в меню File для Windows 7 (після активації розділу PGP Keys (рис. 6.2)) пункт New key.



Рис. 6.1. – Меню **Keys** програми адміністрування ключів **PGPkeys**

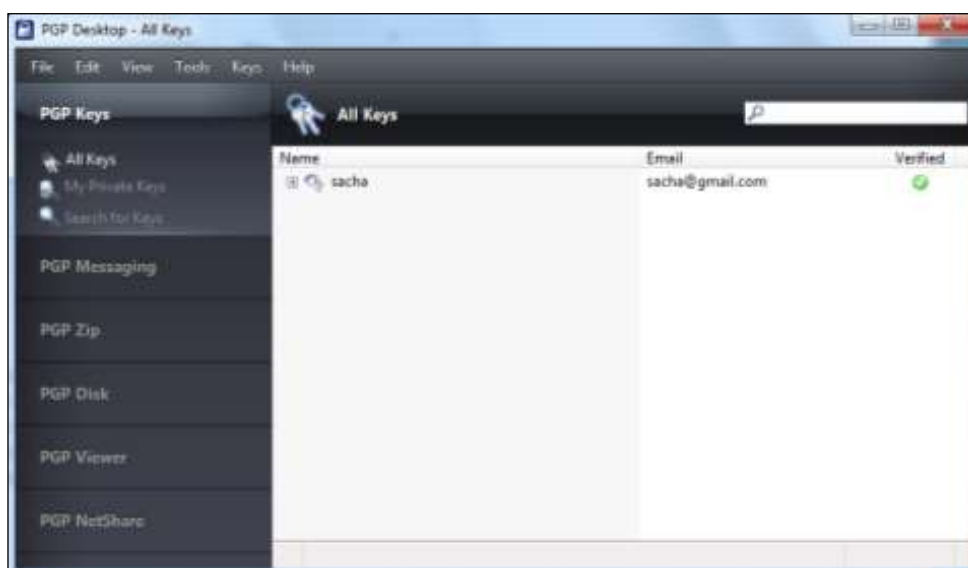


Рис. 6.2. – Розділ **PGP Keys** програми **PGP Desktop**

На першому кроці майстра створення ключів введіть латинськими літерами своє прізвище, ім'я та адресу електронної пошти (рис. 6.3).

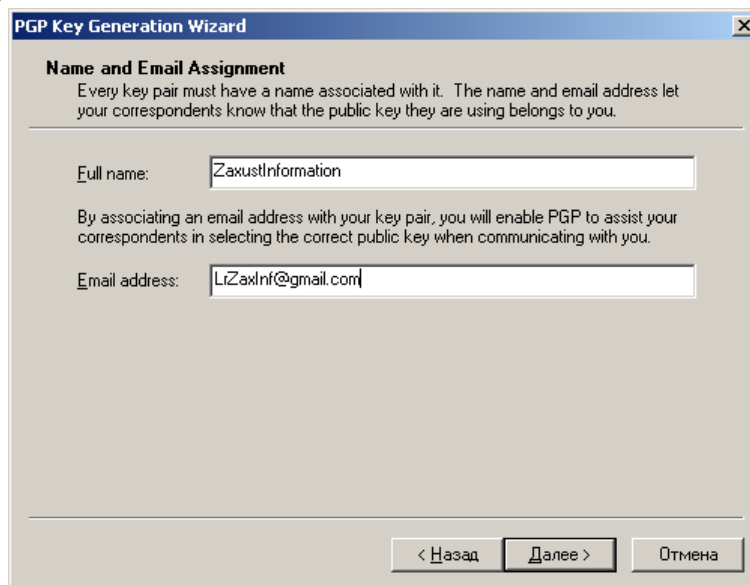


Рис. 6.3. – Вікно першого кроку майстра створення нової пари ключів

Для забезпечення використання пари ключів лише вами на другому кроці цього майстра латинськими літерами вкажіть та підтвердіть ключову фразу, знявши попередньо прапорець **Hide Typing** (рис. 6.4).

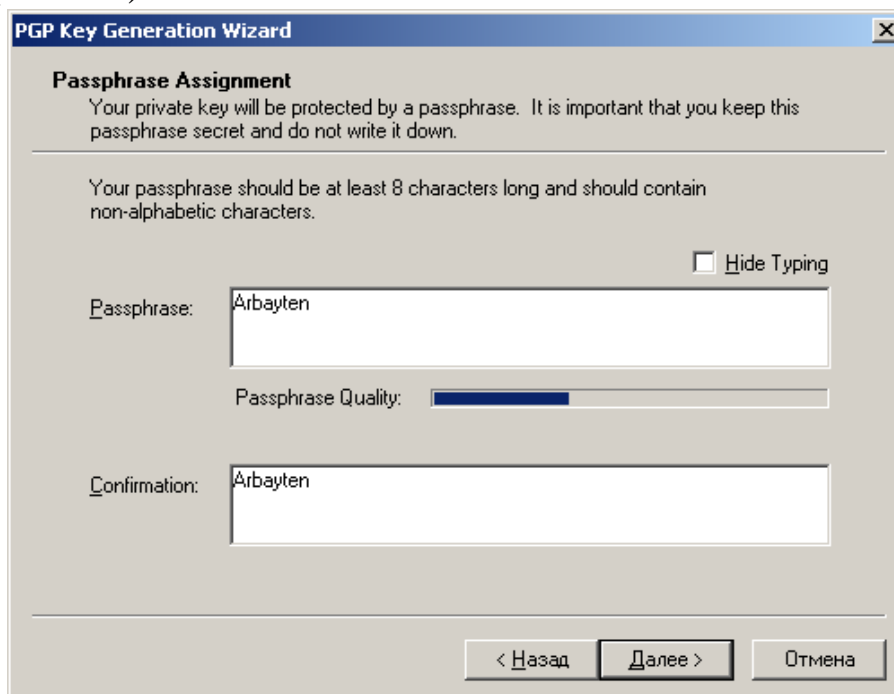


Рис. 6.4. – Вікно другого кроку майстра створення нової пари ключів

Самостійно завершіть створення нової пари ключів.

Віднайдіть в головному меню програми чи в контекстному меню ключа можливість вибору ключа по замовчуванню та активації/деактивації ключа.

Використання пари відкритого і закритого ключів для передачі зашифрованих повідомлень.

Використовуючи пункт головного меню програми **Keys – Export** (рис. 1) чи **File – Export** (рис. 6.2), створіть файл з вашим відкритим ключем. Перешліть його електронною поштою двом обраним вашим однокласникам.

З метою організації передачі зашифрованих повідомлень вашим однокласникам перенесіть з отриманих вами листів їх відкриті ключі в папку для організації криптографічного захисту.

Використовуючи пункт головного меню програми **Keys – Import** (рис. 1) чи **File – Import** (рис. 2), перенесіть відкриті ключі однокласників в програму адміністрування ключів.

Для передачі зашифрованих повідомлень однокласникам, **які надіслали вам свої відкриті ключі**, віднайдіть та виберіть у меню **Пуск** операційної системи посилання **PGPmail** чи активізуйте розділ **PGP Zip** у програмі **PGP Desktop** (рис. 6.5).

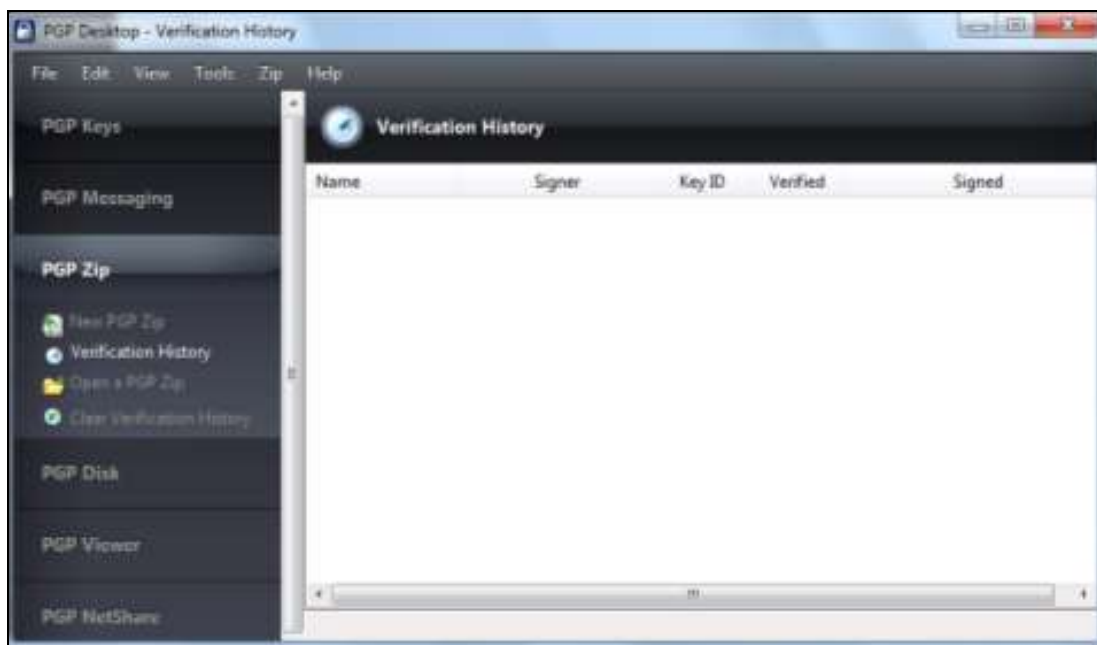


Рис. 6.5. – Розділ **PGP Zip** програми **PGP Desktop**

З метою шифрування вашого файлу з описом різновиду апаратного засобу захисту чи зламу захисту для створення зашифрованого файлу кожному з вибраних однокласників послідовно декілька разів виконайте такі дії:

3.1. В ОС Windows XP натисніть на панелі інструментів програми **PGPmail** (рис. 6.6) другу кнопку зліва чи в ОС Windows 7 оберіть посилання **New PGP Zip** (рис. 6.5);



Рис. 6.6. – Панель елементів програми шифрування/розшифрування **PGPmail**

3.2. На першому кроці завантаженого майстра оберіть файл для шифрування;

3.3. На другому кроці майстра у вікні вибору ключів шифрування **оберіть відкритий ключ однокористувача, якому бажаєте передати повідомлення** (рис. 6.7);

3.4. На наступних кроках майстра введіть назву для зашифрованого файлу та самостійно завершіть його створення.

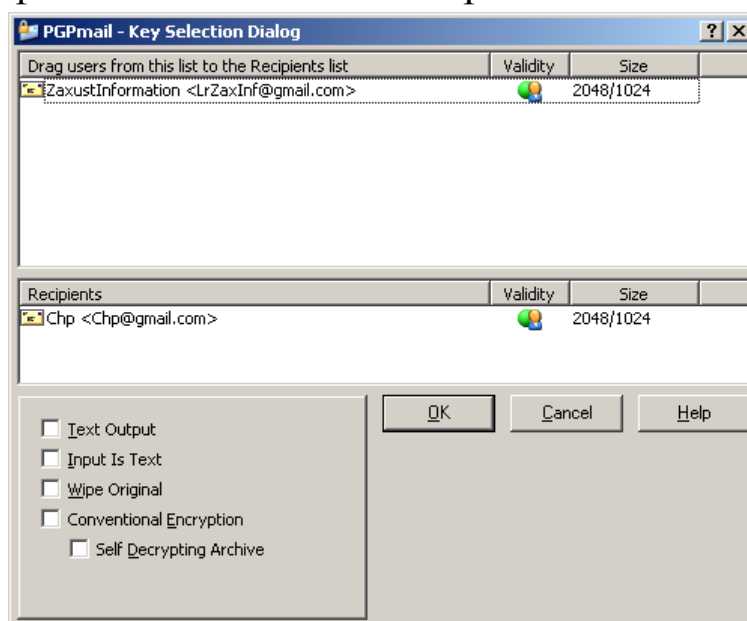


Рис. 6.7. – Вікно вибору ключів шифрування програми **PGPmail**

Перешліть електронною поштою зашифровані файли двом обраним вашим однокористувачам, відповідними **відкритими ключами яких ви користувалися для шифрування**.

Після отримання від однокористувачів файлів, **зашифрованих вашим ключем**, розшифруйте їх, натиснувши в ОС Windows XP на панелі інструментів програми **PGPmail** (рис. 6.5) п'яту кнопку зліва чи в ОС Windows 7 оберіть посилання **Open a PGP Zip** в програмі

PGP Desktop (рис. 6.5) або у контекстному меню зашифрованого файла.

4. Самостійно створіть привітання однокласнику з нагоди приходу весни, зашифруйте та надішліть його адресату електронною поштою. Розшифруйте надіслані вам привітання.

5. Створіть електронний лист з формулюваннями та відповідями на контрольні запитання у своїй поштовій скриньці на сайті gmail.com. Приєднайте до цього листа архів з наявних у вас відкритих ключів та довільний отриманий зашифрований і відповідний розшифрований документ. Тему листа сформууйте за шаблоном *<група>_<номер лабораторної>_<прізвище ім'я>*, наприклад: *EK51_LP10_Величко Володимир*. Надішліть створений лист на адресу volosyuk@mnau.edu.ua.

Запитання для контролю.

1. Чому для шифрування даних на сьогодні крім обраних алгоритмів найчастіше використовуються ключі?
2. Які алгоритми шифрування називаються симетричними, а які – асиметричними, які відкритими, а які – закритими?
3. Яке призначення відкритих ключів?
4. Де і навіщо зберігаються закриті ключі?
5. Як і навіщо використовується ключова фраза, задана при формуванні ключа?
6. Що необхідно встановити і отримати на комп'ютері для стандартизованої передачі зашифрованих повідомлень?
7. Чому розмір зашифрованих файлів може бути меншим від вхідного файла?

ПРАКТИЧНА РОБОТА №7.

Тема: Організація роботи в мережі Інтернет за допомогою додатку µTorrent. Робота з файлами по протоколу BitTorrent.

Мета роботи: Формування вмінь і навиків підключення до Інтернету та використання прикладного програмного забезпечення для завантаження файлів з Інтернету по протоколу BitTorrent. Закріплення вмінь і навиків використання глобальної мережі. Актуалізація знань, вмінь і навичок використання можливостей операційної системи для роботи з файловою структурою.

Теоретичні відомості

BitTorrent (скорочено BT) – це протокол, що дозволяє швидко і ефективно завантажувати файли. Це пірінговий протокол, який означає, що завантаження та роздача здійснюються від інших користувачів, що завантажили цей файл. BitTorrent часто використовується для роздачі дуже великих або популярних файлів, оскільки роздача файлів користувачам, таким же як ми, з використанням BitTorrent зручніше, швидше і ефективніше.

µTorrent – це клієнт BitTorrent, тому він використовує протокол BitTorrent, так само, як користувач використовує протокол HTTP. Як і у випадку з браузерами, які бувають різними, BitTorrent клієнти також бувають різними, і програма µTorrent – найпопулярніший клієнт.

Для переходу на веб-сайт і для завантаження вмісту з цього сайту вам потрібен URL, наприклад www.google.com, таким же чином, для завантаження необхідного вмісту через BitTorrent вам буде потрібно “торрент файл” – невеликий файл, в якому міститься інформація, необхідна для BitTorrent клієнта. Торрент файли зазвичай беруть на веб-сайті торрентів. Багато сайтів пропонують використовувати торренти в якості способу завантаження файлів. Наприклад, програму OpenOffice.org, безкоштовну альтернативу Microsoft Office, можна завантажити через BitTorrent. Інші сайти, такі як legaltorrents.com, пропонують торренти для різних файлів – ці сайти служать своєрідним сховищем торрентів, і ці торренти часто завантажуються на сайт різними користувачами. Такі сайти називають індексами торрентів.

Після отримання торрент-файлу вам потрібно завантажити його в µTorrent. Це можна зробити декількома способами.

Виберіть, відкрити його або завантажити при завантаженні в браузері.

Відкрийте файл торрента, двічі клацнувши його або перетягнувши у вікно µTorrent.

Роздача – це процес, при якому відкритий BitTorrent клієнт після завершення завантаження продовжує розсилати частини файлу (роздача файлу відбувається і при закачуванні, проте краще продовжити роздачу файлу навіть після завершення завантаження). Більшість даних, які ви завантажуйте, ви отримуєте з роздач, тому зробіть такий жест іншим користувачам. Це не потребує великих

зусиль – µTorrent буде продовжувати роздачу до видалення торрента (клацніть торрент правою кнопкою і натисніть Видалити). На практиці зазвичай роздачу продовжують до досягнення коефіцієнта відсилання до завантаження як мінімум 1.00.

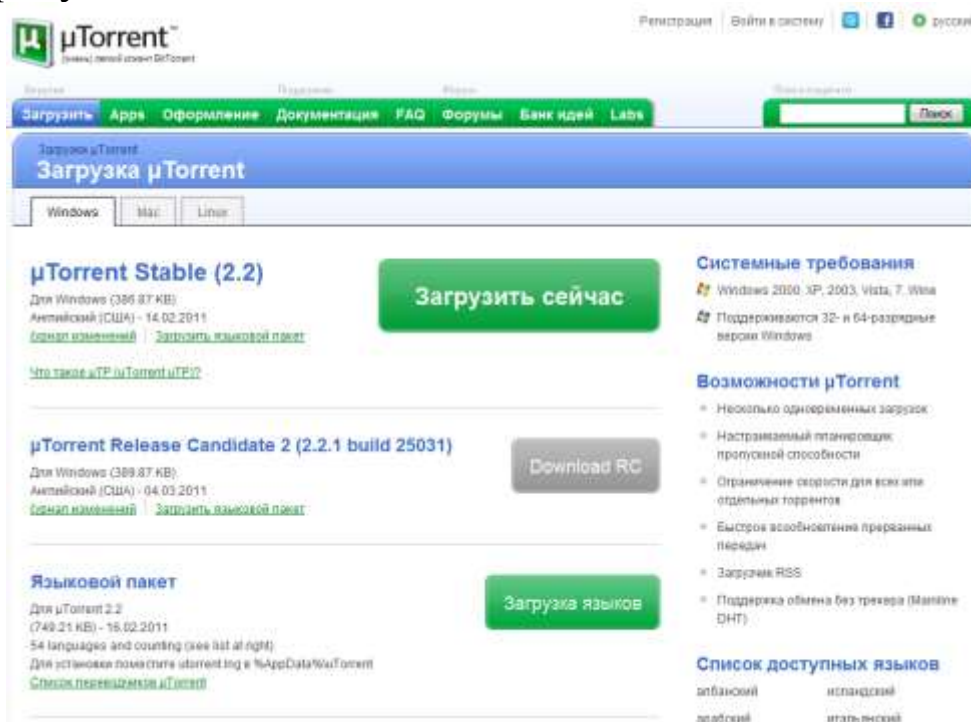
Більшість людей використовують пошукові машини, такі як Google, для знаходження файлу, при пошуку до запиту додають "торрент". BitTorrent можна використовувати для завантаження файлів будь-якого типу. BitTorrent – це просто метод розповсюдження вмісту (як і веб-браузер) і не використовує ніяких технологій, які дозволяли б розпізнавати ліцензійний і піратський контент. Пам'ятайте, що при використанні µTorrent ваша IP адреса буде доступний всім, що дозволить ідентифікувати ваш комп'ютер в мережі Інтернет. Дотримуйтесь законодавства своєї країни щодо захисту авторських прав.

Технологія виконання роботи.

1. Установка клієнта µTorrent

Для початку треба завантажити клієнт. Скачувати клієнт треба тільки з офіційного сайту µTorrent: <http://www.utorrent.com/intl/ru/>. Заходимо на офіційний сайт у розділ Download і викачуємо клієнт.

Натискаємо на посилання Download Now і зберігаємо клієнт на жорсткий диск. Тепер можна створити папку з якої ви будете надалі запускати клієнт і помістити туди завантажений дистрибутив.



2. Українізація клієнта

Є можливість українізувати клієнт, для цього знову заходимо в розділ Download офіційного сайту і завантажуюємо файл української мови.

Ви повинні завантажити файл utorrent.lng. Якщо з якихось причин не закачується, то завжди є можливість завантажити його з офіційного форуму, де постійно ведеться робота над помилками як клієнта, так і перекладу.

Тепер файл перекладу можна помістити в папку куди ви перемістили utorrent.exe і перезапустити клієнт, якщо він вже завантажений. Після перезавантаження клієнт буде русифікований, але, якщо цього не сталося, то треба зайти в Options – Preferences – General і в пункті Language вибрати Russian і перезапустити клієнт.

Языковой пакет

Для µTorrent 2.2

(749.21 KB) - 16.02.2011

54 languages and counting (see list at right)

Для установки поместите utorrent.lng в %AppData%\uTorrent

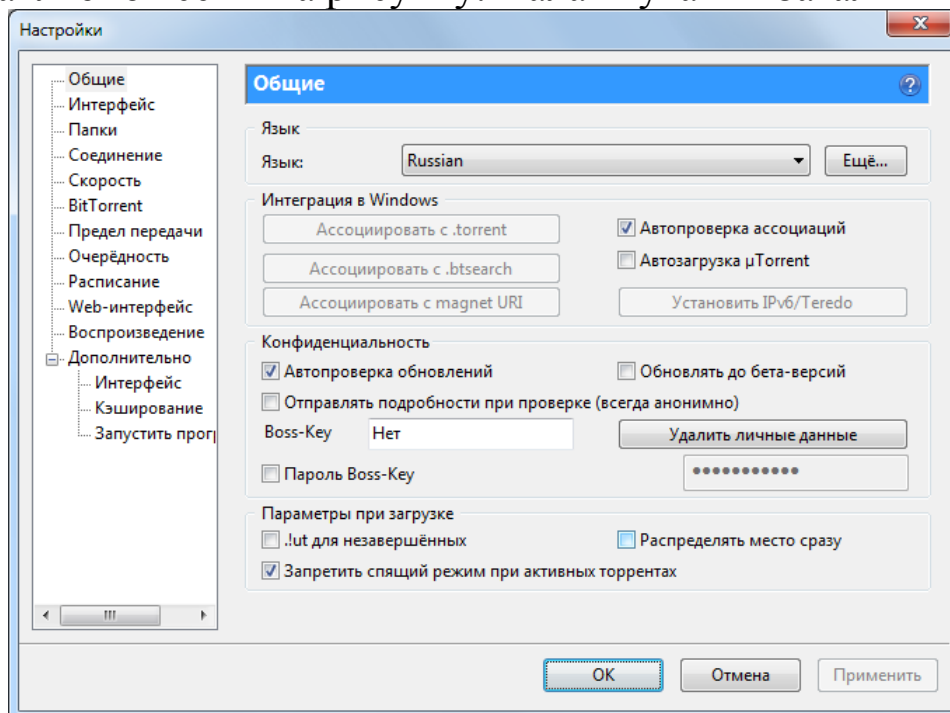
[Список переводчиков µTorrent](#)

Загрузка языков

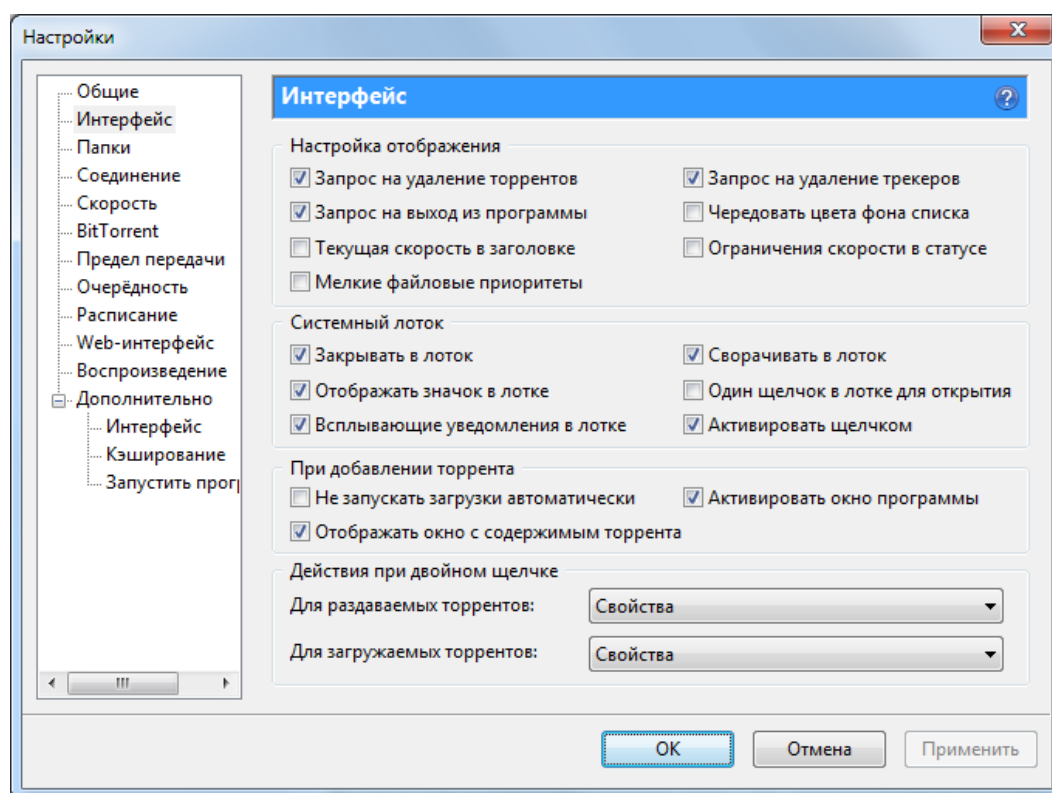
3. Налаштування клієнта

3.1. Загальні

Виставляємо все як на рисунку. Налаштування Загальні готові.



3.2. Інтерфейс налаштовуємо на відповідній закладці як показано на рисунку.

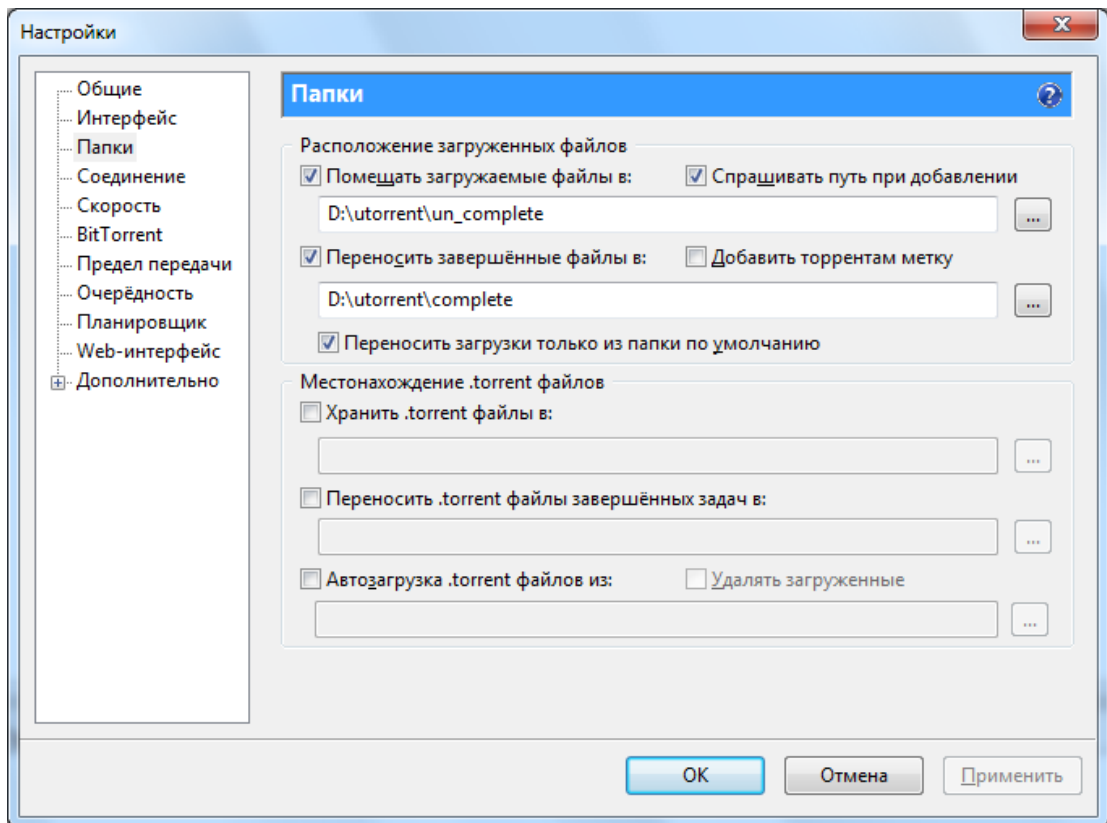


3.3. Папки

Дивимось рисунок і налаштовуємо папки для завантаження (імена для папок можете задати свої).

Поміщати завантаження в – служить для позначення місця зберігання ще не докачати, тимчасових файлів.

Переносити завершені файли в – це місцезнаходження для вже закачаних файлів.

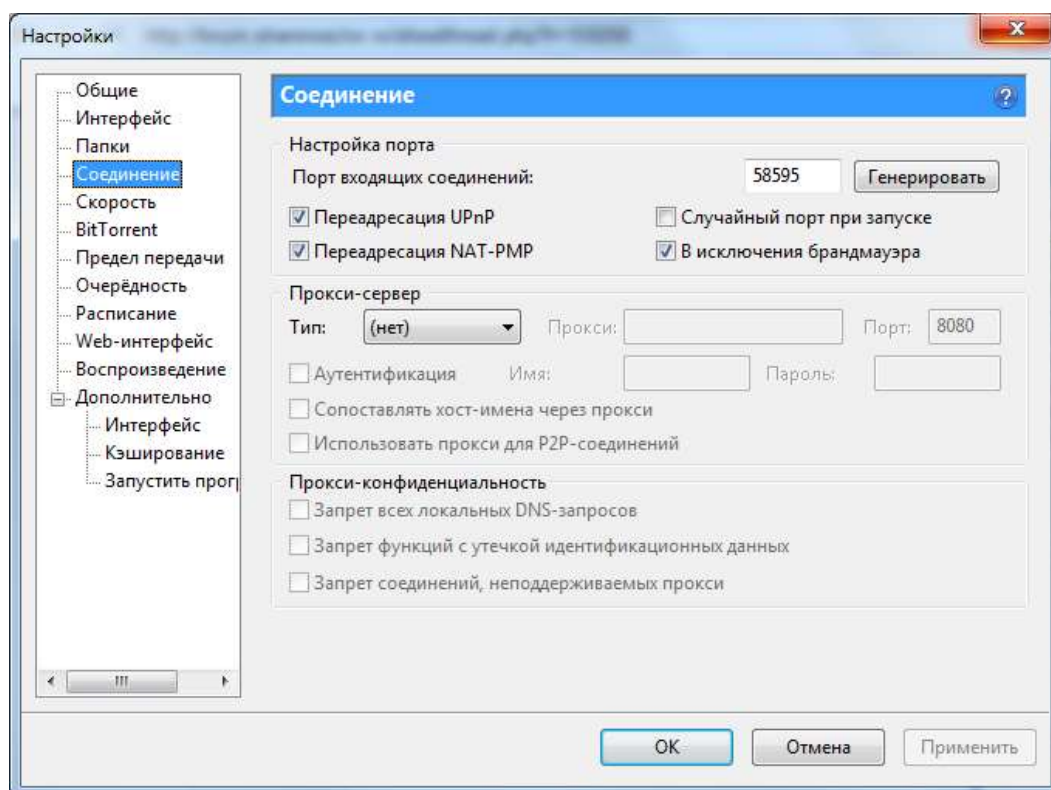


3.4. З'єднання

Переадресація UPnP та Переадресація NAT-PMP потрібно залишити, якщо ви використовуєте роутер і він підтримує технологію UPnP.

Випадковий порт при запуску – кожного разу при запуску клієнта номер порту буде генеруватися (змінюватися) автоматично. Якщо ви використовуєте роутер, то краще не включати цю функцію, оскільки щоразу доведеться прокидати порти заново.

У виключення брандмауера – залиште, якщо ви використовуєте стандартний фаєрвол Windows, тому що, якщо цього не зробити, то кожен раз при запуску клієнта в журналі буде виникати помилка: Error opening Windows firewall: 0x80070005 Відмовлено в доступі.



3.5. Швидкість

1) У цьому розділі установки залежать від вашого з'єднання (прийом і віддача), яке надає ваш провайдер.

2) Установки виробляються в кіло байтах, а провайдер вказують свої тарифи в кіло бітах (1 кіло байт = 8 кіло біт), тому для того щоб правильно налаштувати з'єднання, треба вашу швидкість (прийом та віддачу) поділити на 8. Наприклад, в моєму випадку (як на скріншоті) налаштоване з'єднання за тарифом 2560/512 (2560 - завантаження / прийом, тобто швидкість до вас; 512 - віддача, тобто швидкість від вас).

$$2560/8 = 320 \quad 2560 / 8 = 320$$

$$512/8 = 64 \quad 512 / 8 = 64$$

3) Максимально можливу швидкість віддачі та прийому краще не виставляти, тому що це може негативно вплинути як на за качаку, так і на віддачу контенту. Оптимально виставити 80% від максимальної швидкості вашого каналу. Як у моєму прикладі (дивися скріншот та пункт 2).

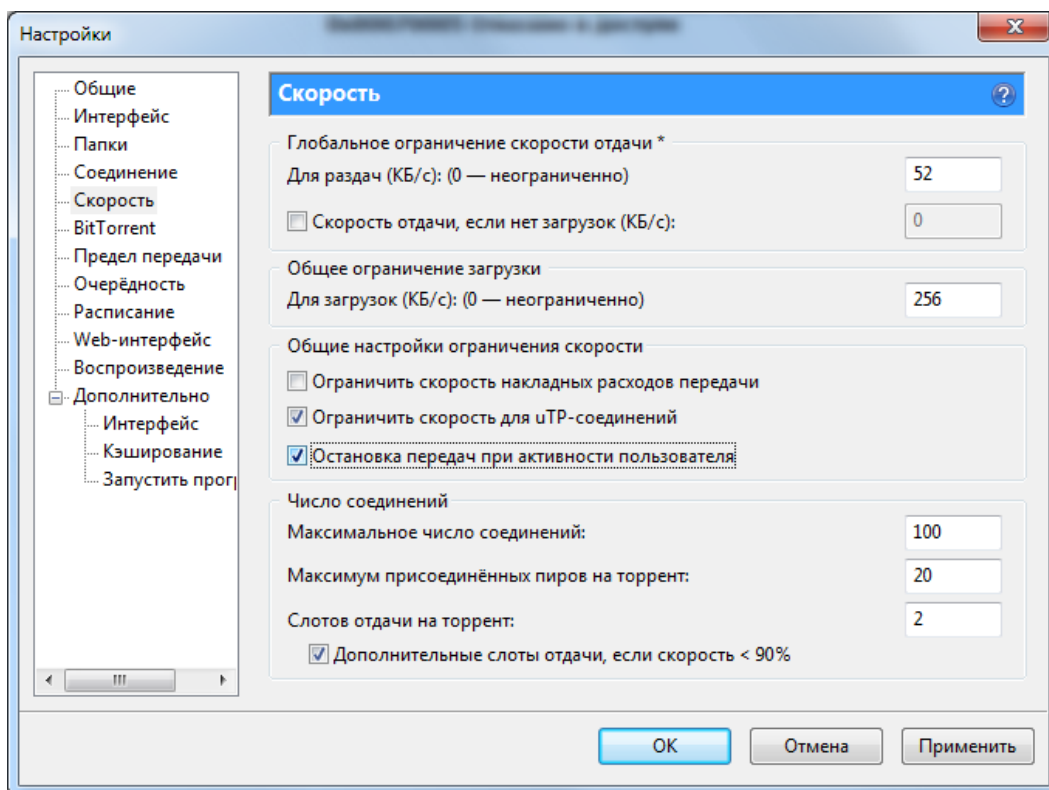
$$320 * 0.8 = 256 \quad 320 * 0.8 = 256$$

$64 * 0.8 = 51,2$ (я виставив 52, т. як в поле можна ввести тільки цифру).

Максимальна кількість з'єднань – зазвичай 50-100 цілком достатньо.

Максимум приєднаних пірів на один торрент – так само досить виставити в районі 10-20.

Кількість слотів роздачі на торрент – можна виставити в районі 2-4.



3.6. BitTorrent

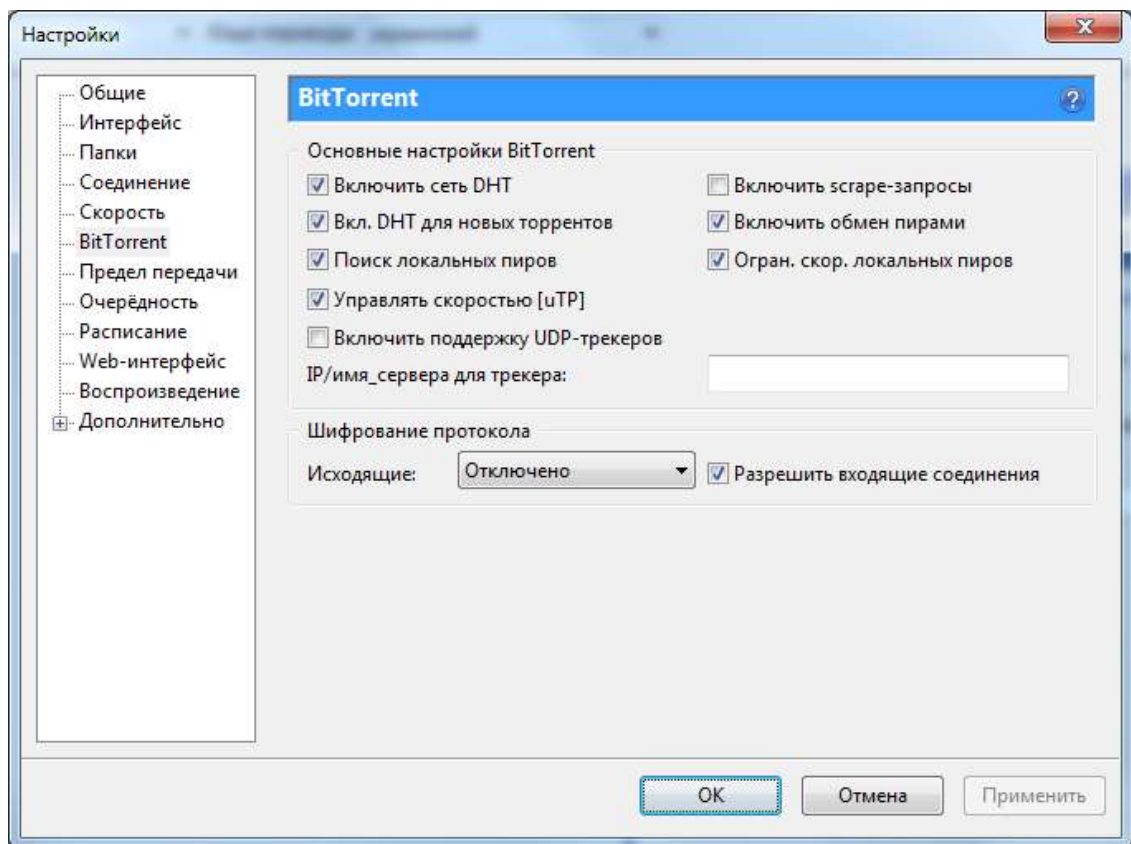
Включити мережу DHT і DHT для нових торрентів – дозволяє клієнту знаходити джерела роздачі і охочих скачати поза трекера.

Пошук локальних пірів – дозволяє знаходити охочих скачати або віддати в локальній мережі вашого провайдера. Перед тим як включати краще порадитися на форумі вашого провайдера, тому що можна отримати бан, за так званий флуд трафік.

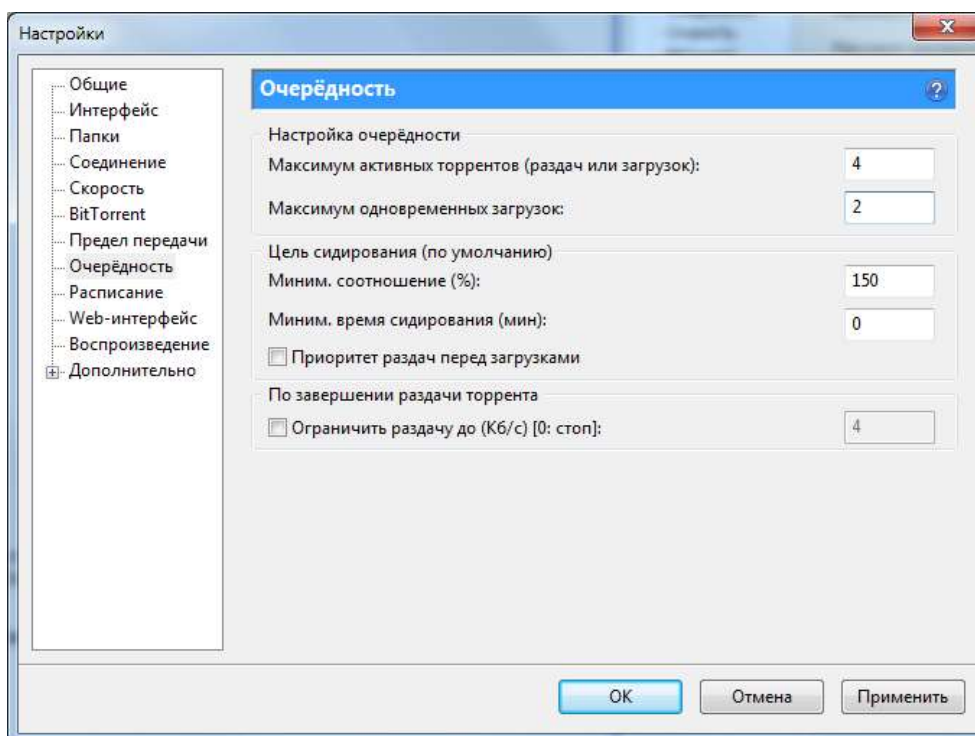
Scrape-запити трекера – потрібна для того, щоб клієнт додатково опитував трекер на предмет точної кількості сидів і бенкетів на роздачі. Сильно навантажує трекер і багато трекери відключають цю функцію.

Обмін між пірами – дуже корисна функція, дозволяє знаходити інших учасників обміну без безпосереднього опитування трекера.

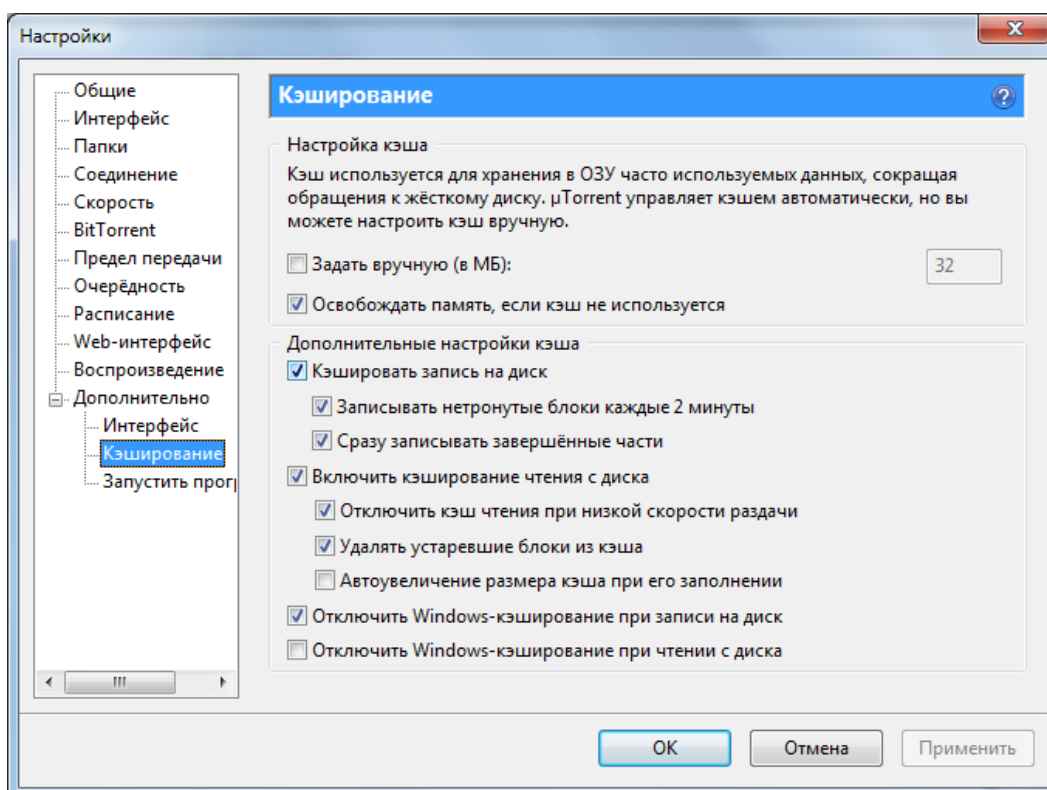
Ліміт швидкості локальних пірів – за замовчуванням uTorrent вважає, що провайдер надає в локальну мережу велику швидкість, ніж у зовнішню, і загальні обмеження на скачування і віддачу не повинні поширюватися на локальних пірів. Якщо ви згодні з цим – галочку зніміть. Але тоді локальні піри можуть забити ваш канал повністю, і вас можуть бути проблеми з провайдерів, тобто флуд трафік.



3.7. Черговість налаштовуємо на відповідній закладці як показано на рисунку.



3.8. Додатково-Кешування налаштовуємо на відповідній закладці як показано на рисунку



4. У вікні додатку **µTorrent** послідовно забезпечте відображення наступних колонок: Назва, Розмір, Залишилось, Готово, Статус, Швидкість зачачки, До кінця залишилось. Для цього:

4.1. Для відображення необхідних колонок необхідно натиснути праву клавіші на назві будь-якої колонки та відмітити необхідні позиції.

4.2. Для сортування стовпців необхідно натиснути ліву клавішу га потрібному стовпці та перемістити його у необхідне положення.

Завантаження торрент файлу у додатку **µTorrent**

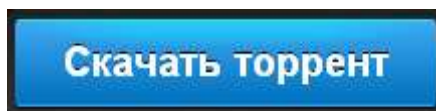
1. Знайдіть в мережі Інтернет торрент файл з вашим улюбленим фільмом для цього:

1.1. Відкриваємо будь-який браузер та заходимо на сайт торрент трекер, наприклад <http://www.torrentino.com/>

1.2. У рядку пошуку вводимо назву фільму і дивимося на результати.

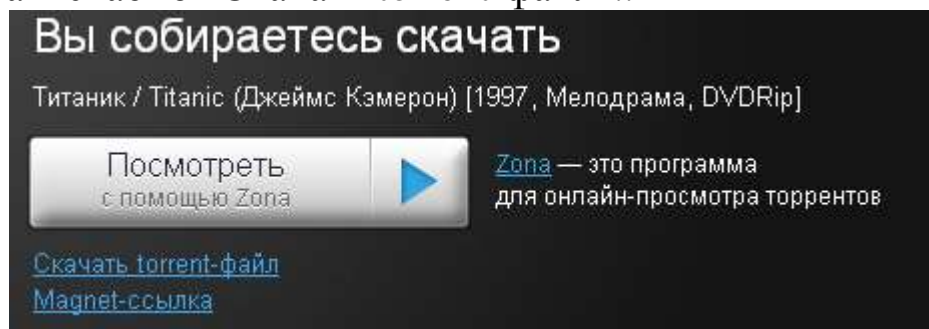


1.3. Натискаємо на відповідний торрент і натискаємо "Скачати торрент":

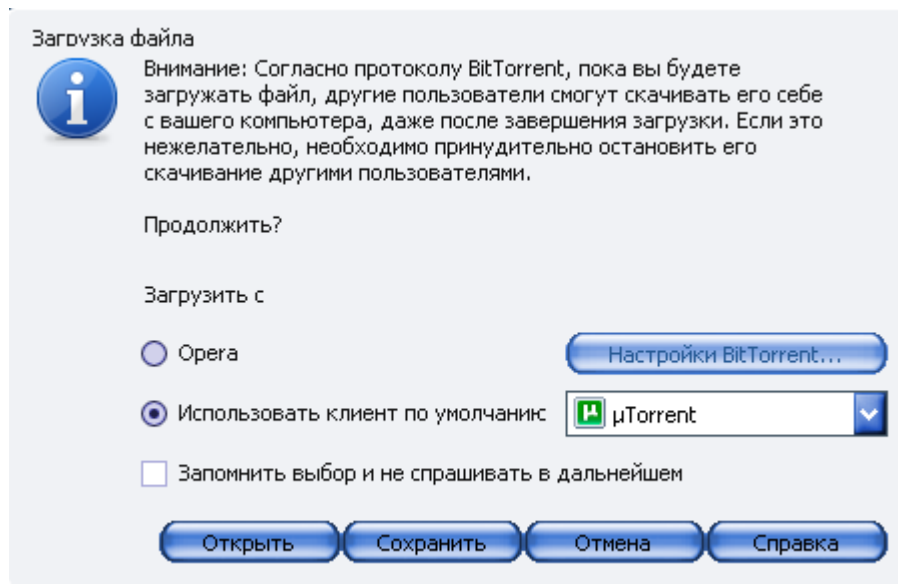


2. Завантаження торренту

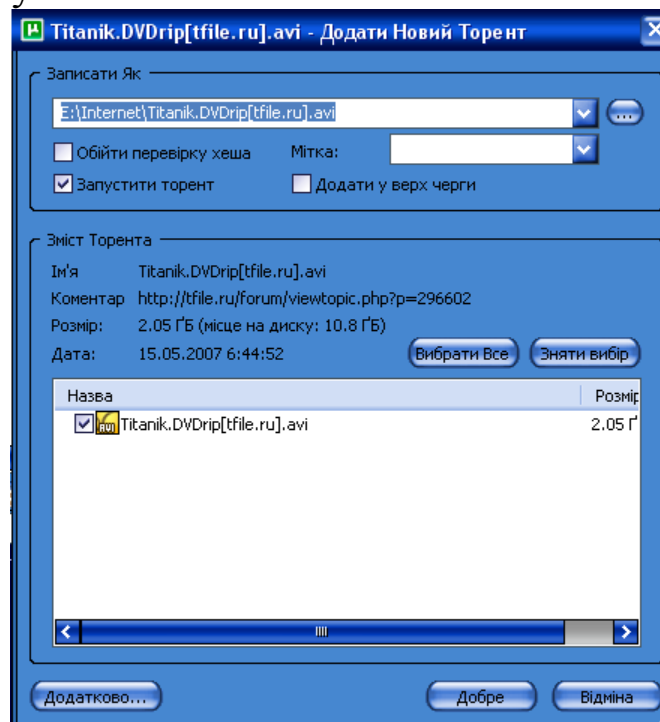
2.1. Натискаємо "Скачать torrent-файл"..



2.2. У відповідному віконці, що з'явилося, натискаємо "Использовать клиент по умолчанию" uTorrent:



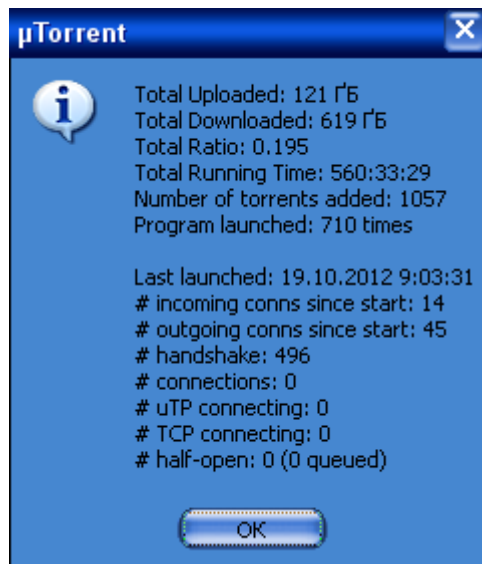
2.3. Далі можна побачити вміст торрента і вибрати місце для зберігання файлу:



Після чого почнетесь завантаження, коли ви побачите слово "роздається" на синьому фоні означає ваш файл завантажений і тепер він роздається іншим людям, ви можете скасувати роздачу по вашому розсуду натиснувши на стоп..

3. Самостійно визначіть швидкість та час завантаження.

4. Перегляньте статистику µTorrent, за весь період роботи додатку (розмір завантажених та відданих даних, рейтинг, час роботи та кількість торрентів), для цього виконайте команду головного меню «Допомога» – «Показати статистику».



Завершальний етап заняття. Повторення вивченого матеріалу.

1. Знайдіть в мережі Інтернет торрент файл з вашим улюбленим серіалом. Скопіюйте його образ вікна у звіт по лабораторній роботі.

2. В процесі завантаження торренту збережіть його у вигляді окремого файлу на диску.

3. Відкрийте збережений файл у додатку uTorrent та виберіть для скачування 1, 3, 5 серії. Скопіюйте образ вікна вибору та образ вікна процесу скачування у звіт по лабораторній роботі.

4. Перейдіть на закладку «Файли» та перевірте правильність завантаження.

5. Створіть електронний лист з відповідями на контрольні запитання у своїй поштовій скриньці на сайті *gmail.com*. Приєднайте до цього листа документ з скопійованими образами вікон. Тему листа сформууйте за шаблоном *<група>_<номер лабораторної>_<прізвище ім'я>*, наприклад: *EK21_LP7_Величко Володимир*. Надішліть створений лист на адресу *volosyuk@mnau.edu.ua*

Запитання для контролю.

1. Який протокол відповідає за передачу торрент-файлів? Які ще протоколи передачі Ви знаєте?
2. Для чого використовується додаток uTorrent?
3. Як встановити мову інтерфейсу uTorrent?

4. Де можна вказати шлях по замовчуванню, який використовується для збереження файлів, що завантажуються?
5. Яким чином можна обмежити швидкість віддачі торренту?
6. Назвіть перелік сайтів торрент трекерів, які Ви знаєте?
7. Яке розширення мають торрент-файли?
8. Назвіть переваги передачі файлів через протокол BitTorrent?
9. Де можна подивитися статистику роботи додатку μ Torrent?

Критерії оцінки знань.

Контроль знань і умінь студентів (поточний і підсумковий) з навчальної дисципліни «Комп'ютерні мережі» здійснюють згідно з кредитно-модульною системою організації навчального процесу.

Поточний – під час виконання практичних робіт, індивідуальних завдань (описових робіт, написання рефератів). Контроль за засвоєнням певного модуля (модульний контроль) проводять у вигляді тестового контролю знань із змістового модуля навчальної дисципліни.

Підсумковий – включає залік.

Навчальна дисципліна «Комп'ютерні мережі» складається з 2-х модулів. Кожен модуль оцінюється в умовних балах пропорційно обсягу часу, відведеному на засвоєння матеріалу цього модуля. Максимально можлива кількість умовних балів за навчальні заняття студента становить 100%.

Студент може збільшити свій рейтинг за навчальну роботу на величину додаткового рейтингу ($R_{др}$), визначену лектором. Навчальну роботу вводять за рішенням кафедри під час виконання робіт, що не передбачені навчальним планом, але сприяють підвищенню кваліфікації студентів із навчальної дисципліни (доповідь на студентській конференції, здобуття призового місця на II-му етапі всеукраїнської олімпіади, виготовлення макетів, підготовку наочних посібників тощо). Рейтинг із додаткової роботи ($R_{др}$) може становити до 10 балів. $R_{др}$ додається до $R_{нр}$ (рейтинг з навчальної роботи).

Рейтинг штрафний ($R_{штр}$) віднімається від $R_{нр}$ і може становити до 5 балів. $R_{штр}$ визначає лектор і вводять за рішенням кафедри для студентів, які невчасно засвоїли матеріал модуля, не дотримувалися графіка роботи, пропускали заняття тощо.

Для допуску до атестації (заліку) студенту необхідно набрати не менше 50% балів від рейтингу з навчальної роботи R_{нр}. Це означає, що в цілому студенту необхідно виконати такий мінімум робіт:

- виконати всі заплановані практичні завдання (лабораторні роботи, розрахункові завдання, домашні завдання, контрольні роботи);

Рейтинг з атестації R_{ат} включає рейтинг з заліку R_{іс} і визначається кількістю балів, отриманих студентом на атестації з дисципліни і передбачених робочим навчальним планом.

Студенти, які протягом семестру набрали необхідну кількість балів (не менше 60% від розрахункового рейтингу дисципліни, тобто 60 балів), мають можливість:

- не складаючи залік отримати залік – автоматично, відповідно до набраної за семестр кількості балів;
- складати залік з метою підвищення рейтингу з дисципліни.

Критерії оцінки виконання навчальних завдань є одним з основних способів перевірки знань, умінь і навичок студентів з дисципліни «Комп'ютерні мережі». При оцінці завдань за основу слід брати повноту і правильність їх виконання. Необхідно враховувати наступні навички і вміння студентів (студент вміє):

- диференціювати, інтегрувати та уніфікувати отримані знання;
- викладати матеріал логічно й послідовно;
- користуватися додатковою літературою.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Буров Є. В. Комп'ютерні мережі: Підручник. – Львів: “Магнолія плюс”, 2006. – 264 с.
2. Буров Є. Комп'ютерні мережі. 2-ге оновлене і доповн. вид. – Львів: БаК, 2003. – 584 с.
3. Дж. Бони. Руководство по Cisco IOS / Бони Дж. – СПб.: Питер; М.: Издательство „Русская Редакция”, 2008. – 784 с.
4. Кулаков Ю. О. Комп'ютерні мережі / Ю. О. Кулаков, І. А. Жуков. – К.: Вид-во Нац. авіац. ун-ту "НАУ-друк", 2009. – 392 с.
5. Одом Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101; акад. изд. / пер. с англ. Уэн-делл Одом. – М. : ООО “Вильямс”, 2015. – 896 с.
6. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. – 4-е изд. / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2012. – 944 с. 8. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. – 5-е изд. / В. Г. Олифер, Н. А. Олифер. – СПб. : Питер, 2016. – 992 с.
7. Таненбаум Э. Компьютерные сети. 5-е изд. / Э. Таненбаум , Д. Уэзеролл – СПб. : Питер, 2012. – 960 с.
8. Филимонов А. Ю. Построение мультисервисных сетей Ethernet / А. Ю. Филимонов. – СПб. : БХВ-Петербург, 2007. – 592 с.

Навчальне видання

Комп'ютерні мережі
Методичні рекомендації

Укладач: **Волосюк** Юрій Вікторович

Формат 60x84 1/16 Ум. друк. арк. 2,6.
Тираж 30 прим. Зам. №_____

Надруковано у видавничому відділі
Миколаївського національного аграрного університету.
54020 м. Миколаїв, вул. Георгія Гонгадзе, 9

Свідоцтво суб'єкта видавничої справи ДК № 4490 від 20.02.2013 р.