МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

Методичні рекомендації
до виконання лабораторних робіт
з навчальної дисципліни

"КОМП'ЮТЕРНІ МЕРЕЖІ ТА ЗАХИСТ ІНФОРМАЦІЇ"

для студентів напряму підготовки
6.051501 "Видавничо-поліграфічна справа"
всіх форм навчання

Харків. ХНЕУ ім. С. Кузнеця, 2016

Затверджено на засіданні кафедри комп'ютерних систем і технологій. Протокол № 7 від 01.12.2015 р.

Укладач В. Є. Климнюк

М 54 Методичні рекомендації до виконання лабораторних робіт з навчальної дисципліни "Комп'ютерні мережі та захист інформації" для студентів напряму підготовки 6.051501 "Видавничо-поліграфічна справа" усіх форм навчання / уклад. В. Є. Климнюк. – Харків : ХНЕУ ім. С. Кузнеця, 2016. – 64 с.

Запропоновано завдання, пов'язані з комп'ютерними мережами та захистом інформації. Наведено практичні рекомендації щодо створення локальних мереж різних типів та їх налагодження у середовищі *Windows*. Розглянуто питання оцінювання характеристик комп'ютерних мереж, що впливають на якість передачі мультимедійної інформації. Досліджено методи захисту інформації від несанкціонованого доступу, зокрема методи шифрування та застосування цифрового підпису.

Рекомендовано для студентів, викладачів і користувачів, які вивчають основи застосування комп'ютерних мереж і захисту інформації.

Вступ

Методичні рекомендації до виконання лабораторних робіт із навчальної дисципліни "Комп'ютерні мережі та захист інформації" забезпечують розвиток знань, навичок й удосконалювання мережних технологій у галузі мультимедіа та Інтернету. Лабораторний практикум доповнює і розвиває теоретичну підготовку студентів з мережних технологій.

Метою проведення лабораторних робіт є надання студентам практичних і методичних рекомендацій для застосування комп'ютерних мереж, зокрема глобальних та локальних у мультимедійних видавництвах.

У результаті проведення лабораторного практикуму студенти повинні вміти:

застосовувати комп'ютерні мережі для обміну інформацією та використання сумісних ресурсів;

призначати повноваження користувачам мережі забезпечувати розмежування їх доступу до ресурсу мережі;

створювати прості та однорангові локальні обчислювальні мережі, що складаються з двох і більш комп'ютерів і вибирати найбільш ефективне устаткування для монтажу мережі;

налаштовувати параметри мережі, використовуючи можливості операційних систем;

забезпечувати підключення локальної мережі до Інтернету;

застосовувати математичні методи для моделювання мереж різних технологій і оцінювати основні характеристики мережі, пропонувати заходи для підвищення якості обслуговування мережі;

забезпечувати захист інформації від несанкціонованого доступу методом шифрування та застосуванням цифрового підпису.

Усі роботи зі створювання локальних мереж проводяться у спеціалізованих лабораторіях кафедри комп'ютерних систем і технологій з використанням спеціалізованих програм, професійного обладнання та устаткування.

У процесі проведення лабораторних робіт студенти повинні виконати завдання і скласти звіт, у якому коротко описати свої дії, результати, висновки й відповісти на контрольні запитання.

Лабораторна робота 1
Створення простої мережі з двох персональних комп'ютерів

Мета роботи: отримати практичні навички в монтажу кабелю для мережі; навчитися проводити прості налаштування невеликої мережі і діагностувати неполадки мережі.

У результаті виконання лабораторної роботи у студента формуються **компетентності** з монтажу та діагностики простих локальних мереж.

Завдання

Монтаж кабелю типу "Вита пара" для з'єднання двох комп'ютерів

1. Створити робочі групи студентів із двох осіб, які сполучатимуть два сусідні комп'ютери.

2. Кожній групі виділяється відрізок кабелю завдовжки близько чотири метра і чотири роз'єми RJ-45 (два для роботи і два резервних).

3. Кожен член групи обробляє кабель, обжимає роз'єми RJ-45 спеціальними кліщами і готує кабель до монтажу мережі. Оброблення і обтискання кабелю слід проводити відповідно до Інструкції з оброблення кабелю.

Розводка кабелю для безпосереднього з'єднання двох комп'ютерів здійснюється відповідно до таблиці 1 прямої і зворотної розводки.

4. На системному блоці від'єднати підведені кабелі мережі лабораторії і підключити свій кабель одним кінцем до мережного адаптера однієї машини, а іншим – до мережного адаптера іншої.

Налаштування мережі

1. Зареєструватися як користувач із правами адміністратора або того, що належить до групи адміністраторів (імена і паролі уточнити в адміністратора навчальної лабораторії).

2. Переконатися, що мережні адаптери (мережні карти) підключені і працюють нормально: **Панель управления – Система – Свойства системы – Диспетчер устройств**. Вікно "Свойства системы" можна викликати поєднанням клавіш <Win + Break>. У розділі "Сетевые платы" двічі клікнути на значку мережного адаптера. На вкладці "Общие" вікна властивостей адаптера є інформація про загальний стан пристрою, його тип і розміщення. Переконайтеся, що пристрій працює нормально. Запишіть інформацію про мережний адаптер у звіт.

3. Перевірте, чи підсвічуються індикатори на мережних платах вашої пари комп'ютерів, це свідчить, що кабель обжатий правильно. Якщо індикатори не підсвічуються, то доведеться повторити операцію обтискання (п. 1.3).

4. Запишіть існуюче ім'я комп'ютера і робочої групи. Ця інформація буде потрібна в кінці заняття для відновлення початкового стану.

5. Установіть нове ім'я комп'ютера і робочої групи. Для цього необхідно відкрити вікно "Свойства системы", перейти на вкладку "Имя компьютера" і натиснути кнопку "Изменить".

Перевірка працездатності мережі

1. Відкрити папку "Сетевое окружение" і переконатися, що мережа складається з двох комп'ютерів – вашого і сусіднього. Визначити доступні мережні ресурси.

2. Проглянути склад робочої групи – вона повинна складатися з тих самих комп'ютерів: **Сетевое окружение – Группа сетевые задачи – Отобразить компьютеры рабочей группы**. Визначити, які доступні вам ресурси є на сусідніх комп'ютерах. Визначити доступні вам папки сусідніх комп'ютерів.

3. Установити права доступу на свої ресурси й обмінятися файлами з сусіднім комп'ютером.

4. Вивчити основні прийоми діагностики мережі з використанням утиліти *ping*.

Завершення роботи

1. Відновити мережу навчальної лабораторії (від'єднати свої кабелі і підключити до мережних адаптерів штатні кабелі).

2. Відновити імена комп'ютерів і робочих груп.

3. Відновити створені в ході роботи зайві папки і файли.

Загальні відомості

Таблиця 1

Нормальна і перехресна розводка жил кабелю для роз'єму RJ-45

(вигляд з боку контактів роз'єму)

Контакт	Нормальна розводка	Перехресна розводка
1	2	3
1	Біло-оранжевий	Біло-зелений
2	Оранжевий	Зелений

Закінчення табл. 1

1	2	3
3	Біло-зелений	Біло-оранжевий
4	Синій	Синій
5	Біло-синій	Біло-синій
6	Зелений	Оранжевий
7	Біло-коричневий	Біло-коричневий
8	Коричневий	Коричневий

Використання утиліти *ping* для діагностики мережі

Утиліта *ping* є засобом перевірки фізичного з'єднання комп'ютера з мережею. Під час увімкнення цієї програми *Windows* відправляє чотири невеликих пакети (з 32 байтів) управлінських повідомлень в Інтернет (ICMP) за вказаною адресою. Якщо комп'ютер, якому були адресовані пакети, дає відповідь, можна бути впевненим у тому, що ділянка мережі, що пов'язує два комп'ютери, є справною.

Більш детальніше можливості команди *ping* будуть досліджені у лабораторній роботі 3.

Для запуску команди *ping* необхідно:

1. Відкрити вікно командного режиму (**Пуск – Выполнить – cmd)**.

2. Ввести команду *ping имя_компьютера* (де *имя_компьютера* може бути ім'ям DNS або IP-адресою, наприклад 192.168.2.3).

IP-адресу комп'ютера можна дізнатися так: клацнути правої кнопкою мишки на значку свого з'єднання у вікні "Сетевые подключения", у вікні властивостей з'єднання вибрати компонент "Сетевые подключения)" і клацнути на кнопці "Свойства".

Якщо всі відправлені пакети повернулися з приблизно однаковим часом прийому-передачі, то з вашим підключенням усе гаразд.

Якщо ж усі пакети повертаються з повідомленням "Время ожидания истекло" (*Request timed out*), то, ймовірно, є проблема з підключенням вашого комп'ютера або із комп'ютером, з ким ви намагалися зв'язатися. Щоб переконатися, що з вашим комп'ютером усе гаразд, дайте команду *ping* для зв'язку зі своїм комп'ютером:

ping 127.0.0.1

або ping localhost

Це стандартні адреси зворотного зв'язку (повернення початкового відправлення комп'ютера). Якщо у відповідь буде отримано повідомлення

про помилку, то це означає, що неправильно налаштований протокол TCP/IP.

Контрольні запитання

1. Яке устаткування необхідне для прямого з'єднання двох комп'ютерів?
2. З якою метою скручуються провідники в кабелі "Вита пара"?
3. Назвіть засоби діагностики працездатності мережі.
4. Назвіть два способи визначення IP-адреси комп'ютера у мережі.
5. Для чого використовується IP-адрес 127.0.0.1?
6. Дайте характеристику статистичної інформації, що виводиться за командою *ping*.

Лабораторна робота 2
Створення одноранговоої локальної мережі з персональних комп'ютерів

Мета роботи: закріпити практичні навички в монтажі локальної мережі через комутатори; навчитися об'єднувати локальні мережі, проводити налаштування одноранговоої мережі, діагностувати неполадки мережі й отримувати доступ до ресурсів мережі.

У результаті виконання лабораторної роботи у студента формуються **компетентності** з монтажу та налаштування одноранговоих локальних мереж.

Завдання

Створення одноранговоої локальної мережі з використанням комутатора (*switch*)

1. У навчальній лабораторії створюється дві робочі групи студентів для монтажу автономних мереж (на кожну мережу призначити по одному адміністратору з числа студентів).
2. Кожній групі виділяються відрізки кабелю завдовжки близько чотири метри, роз'єми RJ-45 і комутатори (*switch*).
3. Розводка кабелю для з'єднання комп'ютерів у мережу через комутатор (*switch*) здійснюється відповідно до таблиці прямої або зворотної розводки (відповідно до табл. 1 лабораторної роботи 1).
4. На системному блоці від'єднати підведені кабелі мережі лабораторії і підключити свій кабель одним кінцем до мережного адаптера однієї машини, а іншим – до вільного порту комутатора (*switch*).

Налаштування мережі

1. Зареєструватися з правами адміністратора (імена і паролі уточнити в адміністратора навчальної лабораторії).

2. Переконатися, що мережні адаптери (мережні карти) підключені і працюють нормально.

3. Перевірити, чи підсвічується індикатор на мережній платі та індикатор на комутаторі, відповідний даному порту, що свідчить, що кабель правильно обжатий і приєднаний. Якщо індикатор не підсвічується, то доведеться перевірити правильність обтискання кабелю.

Примітка. У комутатора передбачений так званий час навчання, протягом якого заповнюється таблиця відповідності MAC-адрес комп'ютерів і номерів портів комутатора. Протягом цього часу індикатори на комутаторі можуть не підсвічуватися (1 – 2 хвилини).

4. Запишіть існуюче ім'я комп'ютера і робочої групи**.** Ця інформація необхідна для повернення комп'ютерних налаштувань початкового стану.

5. Призначте унікальні імена комп'ютерам групи та всій робочій групі.

6. Призначте IP-адреси комп'ютерам групи. Для цього на комп'ютері вибрати активне мережне підключення і правою кнопкою мишки викликати вікно **Свойства**. У вікні відкрити компонент *Протокол Интернет версия 4 (TCP/IPv4)* і IP-адреси для мереж класу С (з діапазону 192.168.0.0 – 192.168.255.0), наприклад, так 192.168.10. *, де 10 – адреса вашої локальної підмережі (робочої групи), * – будь-який унікальний номер з діапазону 1 – 255. У полі *Маска подсети* ввести маску для мереж класу С – 255.255.255.0. Решту полів залишити пустими, тому що шлюзи та сервери DNS у даному випадку непотрібні.

7. Збережіть всі зміни та перевантажте комп'ютер.

8. З'єднайте дві локальні підмережі в одну складену (загальну) мережу кабелем "Вита пара" через вільні порти комутатора.

9. Адміністратори мереж обумовлюють імена комп'ютерів і імена робочої групи загальної (складеної) мережі, а також IP-адреси "своїх" комп'ютерів. Перевірте, чи буде мережа працювати за умови різних імен робочої групи в різних підмережах, та що відбудеться, якщо в різних підмережах будуть комп'ютери з однаковими IP-адресами.

Перевірка працездатності мережі

1. Відкрийте папку "Сетевое окружение" і переконайтеся, що мережа складається із усіх комп'ютерів групи. Визначити доступні мережні ресурси.

2. Перегляньте склад робочої групи – вона повинна складатися з тих самих комп'ютерів. Визначте, які доступні вам ресурси є на сусідніх комп'ютерах. Визначте доступні вам папки сусідніх комп'ютерів.

3. Створіть декілька облікових записів за числом користувачів, на які ви хочете встановити права на використання ресурсів вашого комп'ютера (**Панель управления – Учетные записи пользователей**).

4. Установіть права доступу на свої ресурси та обміняйтеся файлами з сусіднім комп'ютером.

5. Застосуйте основні прийоми діагностики мережі з використанням утиліти ***ping***.

Загальні відомості

Одним зі способів з'єднання вузлів мережі є зіркоподібна топологія, яка утворюється у разі, коли кожен комп'ютер підключається безпосередньо до загального центрального пристрою, так званого концентратором. До функцій концентратора входить спрямування інформації, що передається комп'ютером до одного або решти комп'ютерів мережі. Концентратором може бути як універсальний комп'ютер, так і спеціалізований пристрій – комутатор (*switch*).

Мережі з використанням декількох концентраторів, ієрархічно сполучених між собою зв'язками типу зірки, називають ієрархічною зіркою, або деревом. У теперішній час дерево є найпоширенішою топологією зв'язків як у локальних, так і глобальних мережах.

За способом управління розрізняють мережі типу "Клієнт-сервер" і одноранговi мережі.

У ***одноранговій мережі*** всі комп'ютери рівні – мають один ранг. Будь-який комп'ютер може виступати як у ролі сервера, тобто надавати свої ресурси (файли, принтери) іншому комп'ютеру, так і в ролі клієнта, іншими словами – використовувати надані йому ресурси. Одноранговi мережі переважно поширені в домашніх мережах або невеликих офісах.

Коли мережа створена фізично (комп'ютери пов'язані за допомогою кабелю), потрібно налаштувати мережу програмно. Для цього необхідно, щоб на комп'ютерах були встановлені мережні операційні системи (*Linux, Windows NT, Windows (XP, 7, 8, 8.1, 10*).

Перевага одноранговової мережі – це її простота і дешевизна.

Мережі клієнт/сервер забезпечують вищий рівень продуктивності і безпеки.

На відміну від однорангової мережі, у мережі клієнт/сервер існує один або декілька головних комп'ютерів – серверів. Існують різні види серверів (залежно від послуг, що надаються ними): сервери баз даних, файлові сервери, сервери друку (друк-сервери), поштові сервери, web-сервери і т. д. Інші комп'ютери мережі називаються клієнтами, або робочими станціями (*workstations*).

Адресація в мережах

Кожен комп'ютер у мережі TCP/IP має три типи адрес:

локальна адреса вузла, що визначається технологією, за допомогою якої побудована окрема мережа, і до якої входить даний вузол. Для вузлів, що входять в локальні мережі, – це MAC-адреса (*Media Access Control* – управління доступом до середовища) мережного адаптера або порту маршрутизатора.

Формат MAC-адреси – 6 байт, визначений спеціальним стандартом. Його зазвичай записують у вигляді шести пар шістнадцяткових цифр, розділених тире або двокрапками, наприклад 11-A0-17-3D-BC-01;

доменне ім'я є символьне ім'я і слугує для зручності роботи користувачів. Символьні ідентифікатори мережних інтерфейсів у межах складеної мережі будуються за ієрархічною ознакою;

IP-адреса, що складається з чотирьох байт і призначається адміністратором мережі за певними правилами. IP-адреса складається з двох частин: номера мережі і номера вузла. Розподілення IP-адреси на поля номера мережі і номера вузла – гнучке, і межа між цими полями може встановлюватися довільно.

Перетворення адрес із одного вигляду в інший здійснюється за спеціальними допоміжними протоколами (правилами). Основу протоколу розділення адрес (ARP) складають ARP-таблиці відповідності фізичних (MAC) адрес і IP-адрес. Для встановлення відповідності IP-адрес і доменних імен у мережах TCP/IP використовується спеціальна система доменних імен (*Domain Name System*, DNS), що реалізовується за допомогою DNS-серверів.

Для характеристики масштабу мереж визначено п'ять класів: **A, B, C, D, E**. Три з них – **A, B, C** – використовуються для адресації мереж,

а два – **D, E** – мають спеціальне призначення. Для кожного класу мережних адрес визначено власне положення межі між номером мережі і номером вузла. Найбільш поширені мережі класу **C** – це, як правило, локальні мережі невеликих організацій. У адресах класу **C** під номер мережі відводиться три байти, а під номер вузла – один байт. Вони мають найменше максимальне число вузлів – $2^8 – 2 = 254$. До класу **C** належать всі адреси, старші три біти яких мають значення 110, – від 192.0.0 (11000000 00000000 00000000) до 223.255.255 (11011111 11111111 11111111).

Для більш гнучкого і раціонального використання адресного простору застосовується механізм масок. **Маска** – це число, що вживається у парі з IP-адресою, причому двійковий запис маски містить безперервну послідовність одиниць у тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Межа між послідовностями одиниць і нулів у масці відповідає межі між номером мережі і номером вузла в IP-адресі. Фактично, маска – це розмір мережі, тобто число адрес у мережі. Маску прийнято записувати в десятково-побайтному вигляді. Так, для всіх мереж класу **C** маска складає число 255.255.255.0.

Для автономного використання визначено декілька приватних адрес:

- у класі **A** – мережа 10.0.0.0;
- у класі **B** – діапазон із 16 номерів мереж 172.16.0.0 –172.31.0.0;
- у класі **C** – діапазон із 255 мереж – 192.168.0.0 – 192.168.255.0.

Ці адреси, виключені з безлічі централізовано розподілених адрес і складають величезний адресний простір, достатній для нумерації вузлів автономних мереж практично будь-яких розмірів.

Контрольні запитання

1. Яке устаткування необхідне для створення однорангової мережі?
2. Назвіть переваги і недоліки одноранговых мереж.
3. Поясніть принцип роботи комутатора у мережі.
4. Як налаштувати одноранговy мережу, використовуючи засоби операційної системи?
5. У чому полягає сутність розподіленого підходу встановлення відповідності між адресами різних типів?
6. У якому вигляді зазвичай записують MAC-адреси?

7. Для чого слугує доменне ім'я?

8. За якою схемою здійснюється перетворення адрес?

9. IP-адреса якого класу використовується для корпоративних мереж середнього розміру?

10. IP-адреса якого класу використовується в мережах невеликих організацій?

11. IP-адреса якого класу використовується під час організації крупної мережі загального користування?

12. До якого класу належить IP-адрес 198.105.80.130?

13. Що таке маска підмережі та як вона використовується під час адресації мережі?

Лабораторна робота 3

Дослідження команд для аналізу мережних підключень

Мета роботи: вивчити склад, призначення основних команд *Windows* для аналізу мережного підключення (*Arp, Ipconfig, Netstat, Ping, Tracert, Pathping*), а також вивчити можливості спеціальних сайтів із визначення характеристик мережі.

У результаті виконання лабораторної роботи у студента формуються компетентності зі застосування команд для аналізу мережних підключень і вибору оптимальних маршрутів для обміну мультимедійною інформацією.

Завдання

Перевірка загальних налаштувань підключення до Інтернету

Знаючи IP-адресу, можна отримати багато корисної та цікавої інформації.

1. Дізнатися, під якою IP-адресою вас бачать зовнішні користувачі (у випадку, коли у вас "сіра" адреса, це буде якась "біла" адреса постачальника) можна, наприклад, на Яндексі (http://internet.yandex.ru/). Крім того, також можна визначити багато корисної інформації щодо характеристик комп'ютера.

2. На сайті http://2ip.ru/geoip/ за IP-адресою можна визначити місцезнаходження абонента, а також отримати багато іншої цікавої інформації (рис. 1).

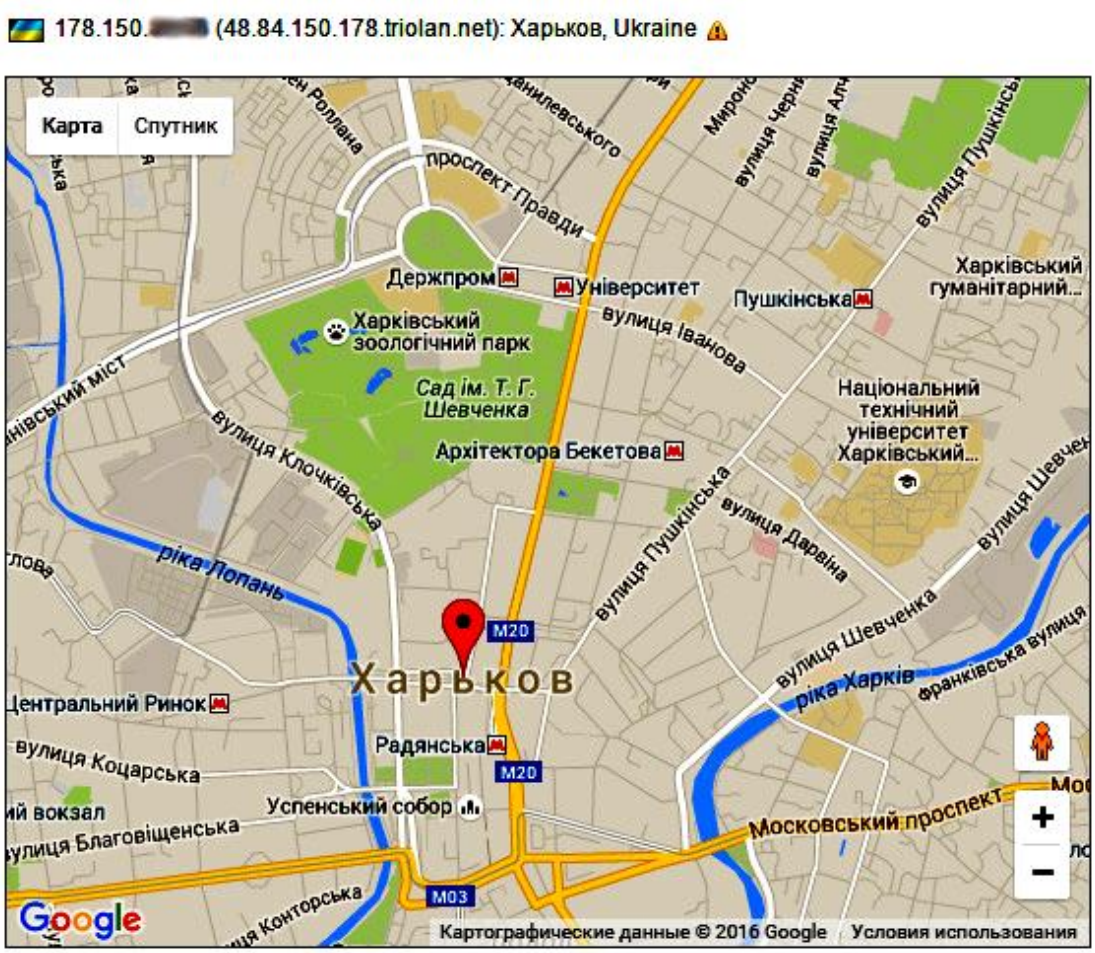


Рис. 1. **Місцезнаходження абонента на карті**

3. Перевірити швидкість свого підключення до Інтернету можна на багатьох інтерактивних сайтах, які вимірюють швидкість підключення, наприклад, http://www.speedtest.net/ru/.

Однак часто ця інформація є не достатньою, щоб діагностувати проблеми підключення. У цьому випадку можна використовувати команди операційної системи *Windows*.

Вивчення команд для аналізу мережного підключення

Робота виконується у вікні командного рядка, яке викликається командою **Пуск – Выполнить – cmd**.

Досліджувані команди: *Arp, Ipconfig, Netstat, Ping, Tracert, Pathping*

1. Послідовно вивчити довідки з указаних команд за допомогою довідкової системи *Windows* або загальних відомостей цієї роботи

2. Відпрацювати команду з параметрами, які виділені жирним шрифтом (під час підключення до Інтернету).

Загальні відомості

Команди аналізу та управління

ARP

Призначена для виведення та зміни записів в одній або кількох таблицях відповідності IP-адрес і фізичних адрес *Ethernet* або *Token Ring*. Для кожного мережного адаптера існує окрема таблиця. Команда *arp* без параметрів відображає довідку.

Синтаксис:

Arp -a

Показує поточні записи таблиці ARP для всіх інтерфейсів.

Arp -?

Відображає довідку у командному рядку.

Нотатки

IP-адреси записуються в точко-десятковій нотації.

Фізична адреса складається з шести байт, записується в шістнадцятковому записі і розділена дефісами (наприклад 00-AA-00-4F-2A-9C).

GETMAC

Показує MAC-адресу (фізичну адресу) мережної карти комп'ютера.

IPCONFIG – параметри TCP/IP

Відображає всі поточні мережі TCP/IP та оновлення параметрів DHCP і DNS. Коли команда викликається без параметрів, *ipconfig* відображає тільки IP-адресу, маску підмережі й основний шлюз для мережних адаптерів.

Синтаксис:

Ipconfig /all

Виводить повну конфігурацію TCP/IP для всіх адаптерів. Адаптери можуть становити інтерфейси, наприклад, установленої мережної карти або логічні інтерфейси, а саме – підключення віддаленого доступу.

Ipconfig /displaydns

Відображає вміст кеша розв'язання імен DNS клієнта, який містить елементи, попередньо завантажені з локального файла *Hosts*, а також останні записи отриманих ресурсів для запитів відповідності імен. Ця інформація використовується службою DNS клієнта для швидкого зіставлення імен без звернення до DNS-серверів.

Ipconfig /?

Відображає довідку у командному рядку.

NETSTAT – вивід з'єднань TCP

Відображає активні TCP-з'єднання, порти, які прослуховує комп'ютер, статистику *Ethernet*, таблиці IP-маршрутизації, статистику IPv4 (для протоколів IP, ICMP, TCP і UDP) і IPv6 (для протоколів IPv6, ICMPv6, TCP і UDP через протокол IPv6). Використовується без параметрів *netstat,* відображає активні TCP-з'єднання.

Синтаксис:

Netstat [-a] [-e] [-n] [-o] [-p протокол] [-r] [-s] [інтервал]

Параметри:

-a

Відображає всі активні TCP-з'єднання і всі порти TCP і UDP, які прослуховує комп'ютер.

-e

Відображає статистику *Ethernet*, наприклад кількість відправлених та отриманих байтів і пакетів. Цей параметр може комбінуватись з ключем s.

-n

Відображає активні TCP-з'єднання з відображенням адрес і номерів портів у числовому форматі без визначення простору імен.

-o

Відображає активні TCP-з'єднання і містить ідентифікатор процесу (PID) для кожного з'єднання.

-r

Відображає вміст таблиці маршрутизації IP.

-?

Відображає довідку у командному рядку.

PING – echo-запити

Надсилаючи повідомлення з *echo*-запитом, перевіряє рівень IP-підключення до іншого комп'ютера з підтримкою TCP/IP. Після передачі кожне повідомлення відображається з відповідним відгуком.

Ping – це основна TCP/IP-команда, яка використовується для виправлення проблем підключення, досяжності та розпізнавання імен. Команда *ping* без параметрів відображає довідку.

Синтаксис:

ping [-t] [-a] [-n кількість] [-l розмір] [-f] [-i TTL] [-v тип] [-r лічильник] [-s лічильник] [{-j список вузлів | -k список вузлів}] [-w інтервал] [ім'я кінцевого комп'ютера].

Параметри:

-t

Повідомлення з *echo*-запитом будуть йти до місця призначення, поки команду не буде перервано. Щоб перервати команду та відобразити статистику, необхідно натиснути клавіші CTRL + BREAK. Щоб перервати команду *ping* і вийти з неї, слід натиснути CTRL + C.

-a

Задає доменне ім'я за IP-адресою призначення. У разі успіху виводить відповідне ім'я хоста.

-n кількість

Визначає кількість повідомлень з *echo*-запитом, що надсилаються. За замовчуванням становить чотири.

-l розмір

Вказує довжину (у байтах) у полі даних відправлених повідомлень з *echo*-запитом. За замовчуванням використовується у 32 байтах. Максимальний розмір 65 527.

--w інтервал

Визначає час очікування у мілісекундах для отримання відгука, що відповідає повідомленню з *echo*-запитом. Якщо відгук не отримано в межах зазначеного інтервалу, виникає повідомлення про помилку "Превышен интервал ожидания для запроса". За замовчуванням інтервал дорівнює 4 000 (4 секунди).

Ім'я кінцевого комп'ютера

Установлює місце призначення, визначене IP-адресою, або назву віддаленого хоста.

-?

Відображає довідку у командному рядку.

TRACERT – визначає шлях до пункту призначення

Визначає шлях *echo*-запитів до місця призначення з поступовим збільшенням значень терміну життя TTL (*Time to Live*). Шлях – це список найближчих інтерфейсів маршрутизаторів на шляху між приймаючим

вузлом джерела і вузлом призначення. Використання без параметрів відображає допомогу.

Синтаксис:

TRACERT [-d] [-h макс_кількість_переходів] [-j список_вузлів] [-w інтервал] [Ім'я кінцевого комп'ютера]

Параметри:

-d

Запобігає команді, що намагається визначити IP-адреси з проміжних маршрутизаторів у відповідні символьні імена. Збільшує швидкість виведення результатів команди *tracert*.

-h макс_кількість_переходів

Установлює максимальну кількість переходів для пошуку кінцевого об'єкта. Значення за замовчуванням становить 30.

-w інтервал

Визначає час очікування у мілісекундах відгуку для відповідного *echo*-запиту. Якщо протягом зазначеного часу відгук не отримано, з'являється зірочка (*). Таймаут за замовчуванням становить 4 000 (4 секунди).

Ім'я кінцевого комп'ютера

Установлює точку призначення, яка вказана IP-адресою або назвою віддаленого хоста.

-?

Відображає довідку у командному рядку.

Нотатки

Для кожного проміжного вузла існує три спроби. Результат трасування містить адресу проміжних маршрутизаторів і час відгуку за кожною спробою у мілісекундах.

Кожен маршрутизатор на шляху зобов'язаний зменшити значення його TTL принаймні на одиницю. За своєю суттю TTL – це лічильник сайтів. Очікується, що за умови TTL = 0 маршрутизатор відправить повідомлення джерелу про закінчення терміну дії часу. Однак деякі маршрутизатори не надсилають повідомлення про закінчення терміну дії часу для пакетів із вичерпаним значенням TTL і є невидимими для команди *tracert*. У цьому випадку переходи відображаються кількома зірочками (*).

PATHPING – оцінювання втрат даних на проміжних вузлах

Надає інформацію про латентність мережі затримки і втрати на проміжних вузлах між джерелом і призначенням.

Команда *PathPing* протягом деякого періоду часу надсилає численні повідомлення з *echo*-запитом кожному маршрутизатору між вихідним та кінцевим розташуванням, а потім на основі пакетів, що повернулися з кожного маршрутизатора, обчислює результати. Оскільки *pathping* показує коефіцієнт втрати пакетів у будь-якому маршрутизаторі або підмережі, то можна визначити, які маршрутизатори або підмережі мають проблеми з мережею.

Використовується без параметрів команда *pathping* відображає довідку.

Синтаксис:

PathPing [-n] [-h макс_кількість_переходів] [-g список_вузлів] [-p період] [-q кількість запитів [-w інтервал] [-T] [-R] [Ім'я кінцевого комп'ютера]

Параметри:

-n

Запобігає команді, що намагається визначити IP-адреси з проміжних маршрутизаторів у відповідні символьні імена. Збільшує швидкість виведення результатів команди.

-h макс_кількість_переходів

Установлює максимальну кількість переходів на шляху, під час пошуку місця призначення. Значення за замовчуванням становить 30.

-g список_вузлів

Указує для *echo*-запитів використання параметра вільної маршрутизації у заголовку IP із набором проміжних точок, вказаний у списку комп'ютерів. Максимальна кількість адрес або імен зі списку дорівнює 9. Список адрес становить набір IP-адрес, які відокремлені пробілами.

-p період

Установлює час очікування між послідовними перевірками зв'язку (у мілісекундах). Типовим значенням є 250 мілісекунд (1/4 секунди).

-q кількість запитів

Визначає кількість повідомлень з *echo*-запитами для кожного маршрутизатора на шляху. За замовчуванням становить 100.

--w інтервал

Установлює час очікування для кожної відповіді (у мілісекундах). Типовим є 3 000 мілісекунд (3 секунди).

Ім'я кінцевого комп'ютера

Установлює точку призначення, яка вказана IP-адресою або назвою віддаленого хоста.

-?

Відображає довідку у командному рядку.

Нотатки

Параметри команди *PathPing* чутливі до регістру.

Для того, щоб уникнути перевантаження мережі, слід надіслати команди через досить великі інтервали часу.

Для мінімізації наслідків втрати пакетів не потрібно виконувати команду занадто часто.

Під час використання параметра **-p** пакети надсилаються до кожного проміжного вузла окремо. Таким чином, проміжок часу між двома пакетами, які передані одному вузлу, – це (період) х (кількість сайтів).

Після запуску команди *pathping* першим відображається шлях, такий, який виводиться командою *tracert*. Далі команда відобразить повідомлення про те, що вона буде зайнята протягом декількох хвилин (залежить від кількості переходів). За цей час збирається інформація з усіх всі маршрутизаторів і зв'язків між ними. Наприкінці цього періоду відображаються результати перевірки у вигляді таблиці, де:

RTT (Round Trip Time) – чистий час транспортування даних від відправника до вузла призначення та назад без урахування часу на підготовку відповіді вузлом призначення.

Оцінки втрат для сполучень, які задаються вертикальною рискою | у стовпці *Адрес,* показують перевантаження, яке викликає втрату пакетів, надісланих за маршрутом.

Контрольні запитання

1. Як визначити швидкість вашого Інтернету? Від чого вона залежить?
2. Як установити місцезнаходження вузла мережі за його IP-адресою?
3. Охарактеризуйте протокол ARP.
4. Як зіставити доменне ім'я вузла і його IP-адресу?
5. Як запустити вікно командного рядку?
6. Для чого слугує час життя пакетів TTL?
7. Що характеризує RTT?
8. Які основні параметри команди *ping* ви знаєте? Що вони характеризують?
9. Наведіть кілька засобів здобуття фізичної адреси мережної карти комп'ютера.
10. Яку статистику збирає команда *PathPing*?

Лабораторна робота 4
Дослідження можливостей віддаленого адміністрування

Мета роботи: отримати навички віддаленого адміністрування у локальних і глобальних мережах.

У результаті виконання лабораторної роботи у студента формуються компетентності з практичного застосування засобів віддаленого адміністрування для підвищення ефективності роботи мультимедійного видавництва.

Завдання 1

Налаштувати віддалене адміністрування у локальній мережі засобами ОС *Windows*

1. Студенти розподіляються на групи з двох користувачів.
2. За допомогою раніше оброблених кабелів кожна група відтворює свої локальні мережі з двох комп'ютерів, підключених напряму або через комутатор (лабораторна робота 1, 2). Ці два комп'ютера повинні входити до однієї робочої групи і знаходитися в одній підмережі.
3. Зареєструватися як користувач із правами адміністратора або того, що належить до групи адміністраторів (імена і паролі уточнити в адміністратора навчальної лабораторії).
4. Сформувати робочу групу і переконатись, що локальна мережа працює, є взаємний доступ до ресурсів комп'ютерів групи.
5. На комп'ютері 2 налаштувати віддалений доступ (див. загальні відомості) для користувачів створеної мережі.
6. На комп'ютері 1 налаштувати підключення до віддаленого робочого стола комп'ютера 2 (див. загальні відомості).
7. На комп'ютері 1 завантажити робочий стіл комп'ютера 1.
8. Попрацюйте на віддаленому робочому столі так само, як і за своїм – створіть будь-яку папку і задайте для неї права доступу, скопіюйте на комп'ютер і завантажте з віддаленого комп'ютера ресурси (папки, файли), запустіть різні додатки тощо.

Завдання 2

Налаштувати віддалене адміністрування через мережу Інтернет

Налаштувати віддалене адміністрування через глобальну мережу Інтернет можна за допомогою різних програм, наприклад, *TeamViewer,*

AnyDesk, LiteManager або як розширення *Удаленный рабочий стол Chrome* до браузера *Chrome*.

1. Завантажити на свої комп'ютери програму інсталяції однієї з указаних програм віддаленого адміністрування (папка *Удаленный доступ*, яку можна знайти на сайті ПНС з дисципліни "Комп'ютерні мережі та захист інформації"). Розширення *Удаленный рабочий стол Chrome* можна завантажити з сайта https://chrome.google.com/.

2. Самостійно встановити вибрану програму або розширення на свої комп'ютери.

3. Вивчити довідку з використання програм віддаленого адміністрування.

4. Розглянути можливості віддаленого адміністрування сусіднім комп'ютером за допомогою свого комп'ютера.

Загальні відомості

Програмні засоби віддаленого адміністрування дозволяють користувачеві управляти віддаленим комп'ютером як власним локальним (бачити інтерфейс, управляти мишкою, відкривати папки, запускати програми і т. д.).

Зазвичай користувач задає таке адміністрування для свого робочого комп'ютера, щоб з домашнього комп'ютера мати до нього доступ (скопіювати файл, відправити результати розрахунку до потрібної папки і багато чого іншого), не виходячи з дому.

Крім того, можна спілкуватись з партнерами, демонструвати їм макети видання, зразки дизайнерських рішень.

Великою перевагою віддаленого адміністрування є також можливість надавати поради або допомогу своїм колегам по роботі, проводити консультації, діагностику, моніторинг комп'ютера.

Усі засоби віддаленого адміністрування можна розподілити на ті, що застосовуються для комп'ютерів у локальних мережах і на ті, які застосовуються для комп'ютерів через глобальну мережу Інтернет.

Засоби віддаленого адміністрування у локальних мережах

Слід розглянути налаштування віддаленого робочого столу для двох комп'ютерів з ОС *Windows*, безпосередньо підключених один до одного.

Етап 1. На комп'ютері 2 налаштувати віддалений доступ.

За командою **Пуск – Панель управления – Система – Настройка удаленного доступа** на вкладці *Удаленный доступ* вікна *Свойства системы* (рис. 2) встановити перемикач *Разрешить подключаться*

только с компьютеров, на которых работает удаленный рабочий стол с проверкой подлинности на уровне сети.

Якщо з'явиться повідомлення, що комп'ютер налаштовано на перехід до режиму сну, то необхідно перейти за посиланням *Электропитание* і вибрати режим *Никогда* для відключення дисплея і переведення комп'ютера до режиму сну.

На вкладці *Удаленный доступ* натиснути кнопку *Выбрать пользователей* і додати необхідних користувачів. Якщо видалений доступ буде застосовувати тільки користувач цього комп'ютера, то ніяких додаткових користувачів можна не додавати.

Переконайтесь, що брандмауер *Windows* увімкнено. Для цього виконайте команду **Пуск – Панель управления – Брандмауэр Windows – Включение и отключение брандмауэра Windows**.

Закрити всі вікна і закінчити етап 1.

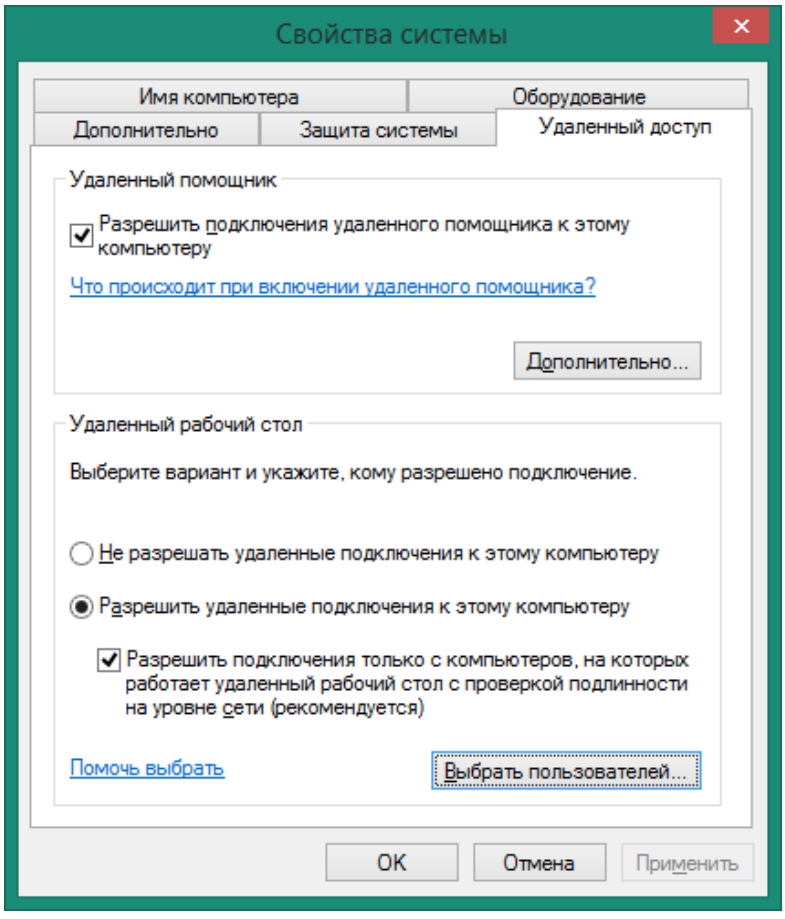


Рис. 2. **Вкладка *Удаленный доступ* вікна *Свойства системы***

Етап 2. На комп'ютері 1 налаштувати підключення до віддаленого робочого столу комп'ютера 2.

Виконайте команду **Пуск – Все программы – Стандартные – Подключение к удаленному рабочему столу** і задайте ім'я комп'ютера, до якого необхідно підключитися (у даному випадку – це ім'я комп'ютера 2), ім'я облікового запису і пароль, з якими було виконано вхід на комп'ютер 2.

Якщо з'явиться вікно з попередженням неможливості перевірки справжності віддаленого комп'ютера, то підтвердити підключення. Після цього відкриється вікно *Подключение к удаленному рабочему столу* (рис. 3).

Клацанням на кнопці *Показать параметры* додайте додаткові вкладки. На вкладці *Экран* вибрати розмір екрана віддаленого робочого столу та глибину кольору, на вкладці *Локальные ресурсы* можна вибрати режими відтворення звуку, включити аудіозапис із віддаленого робочого столу, можна налаштувати доступ до принтера, локального диска та інших пристроїв. Якість передачі даних регулюється на вкладці *Взаимодействие*.

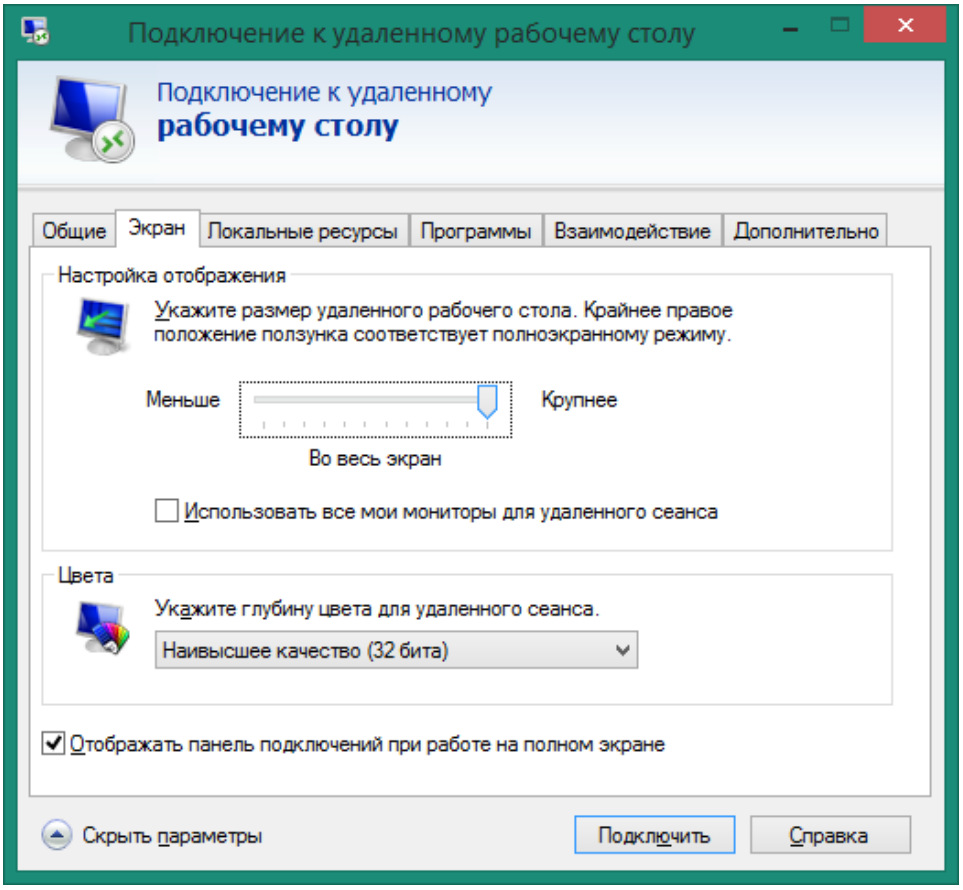


Рис. 3. **Підключення до віддаленого робочого столу**

Після клацання на кнопці *Подключить* на екрані комп'ютера 1 з'явиться робочий стіл комп'ютера 2, який доступний до роботи.

Завершення роботи з віддаленим робочим столом виконується вибором на ньому режиму *Завершение работы,* в якому вибрати команду **Завершение сеанса**.

Засоби віддаленого адміністрування у глобальних мережах

TeamViewer (http://www.teamviewer.com/ru/) – одна з найвідоміших програм, яка дозволяє налаштовувати віддалений доступ до домашнього комп'ютера, управляти робочим столом з різних платформ і пристроїв.

Установка програми

Програму не обов'язково встановлювати на комп'ютер, вона може бути просто запущена.

Режим роботи програми обирається у вікні установки після запуску виконавчого файла з розширенням *exe*. Під час повної установки програми копіюються необхідні файли. Після запуску програми з'являється вікно з довідковою інформацією. У центральній частині головного вікна (рис. 4) на вкладці *Удаленное управление* розташовані дві панелі *Разрешить управление* та *Управлять компьютером.*

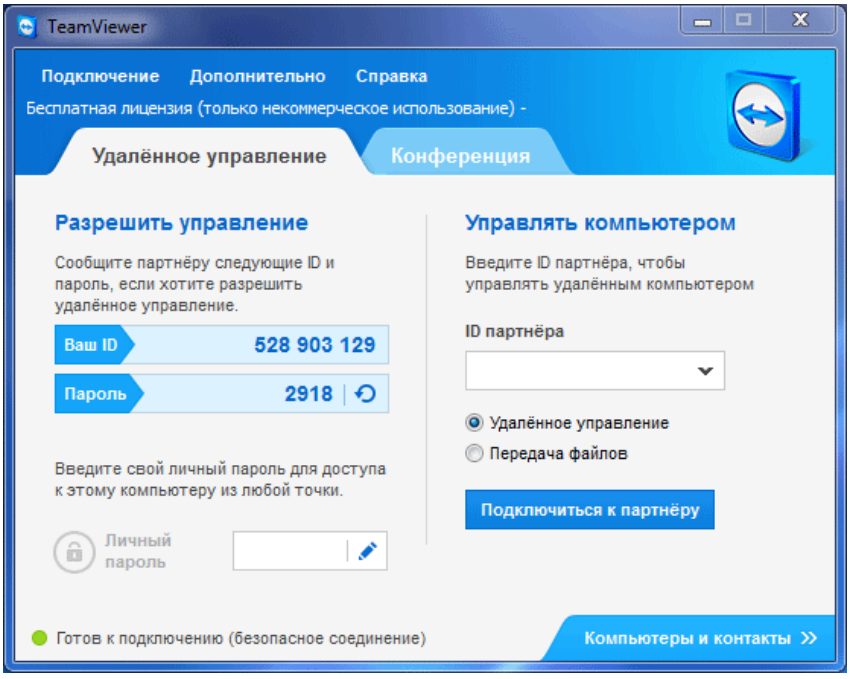


Рис. 4. **Головне вікно програми TeamViewer**

Після натиснення на кнопку *Компьютеры и контакты* і реєстрації у *TeamViewer* можна управляти комп'ютерами і контактами без необхідності запам'ятовувати ID і паролі.

Налаштування програми

Програма *TeamViewer* за замовчуванням уже налаштована і готова до використання.

Налаштувати програму під свої потреби можна за командою **Дополнительно – Опции.**

На вкладці *Основное* можна вибрати ім'я, налаштувати мережу, зв'язати комп'ютер із обліковим записом *TeamViewer*.

На вкладці *Безопасность* можна додати особистий пароль, а також правила підключення до свого комп'ютера.

На вкладці *Удаленное управление* змінюються налаштування зображення віддаленого комп'ютера, можна відключити шпалери на віддаленому комп'ютері за низької швидкості з'єднання.

Віддалене управління комп'ютером

Панель *Разрешить управление* слугує для виведення даних для віддаленого управління комп'ютером. Тут є інформація про ID даного комп'ютера у системі *TeamViewer*, а також пароль, який можна змінити (рис. 5).

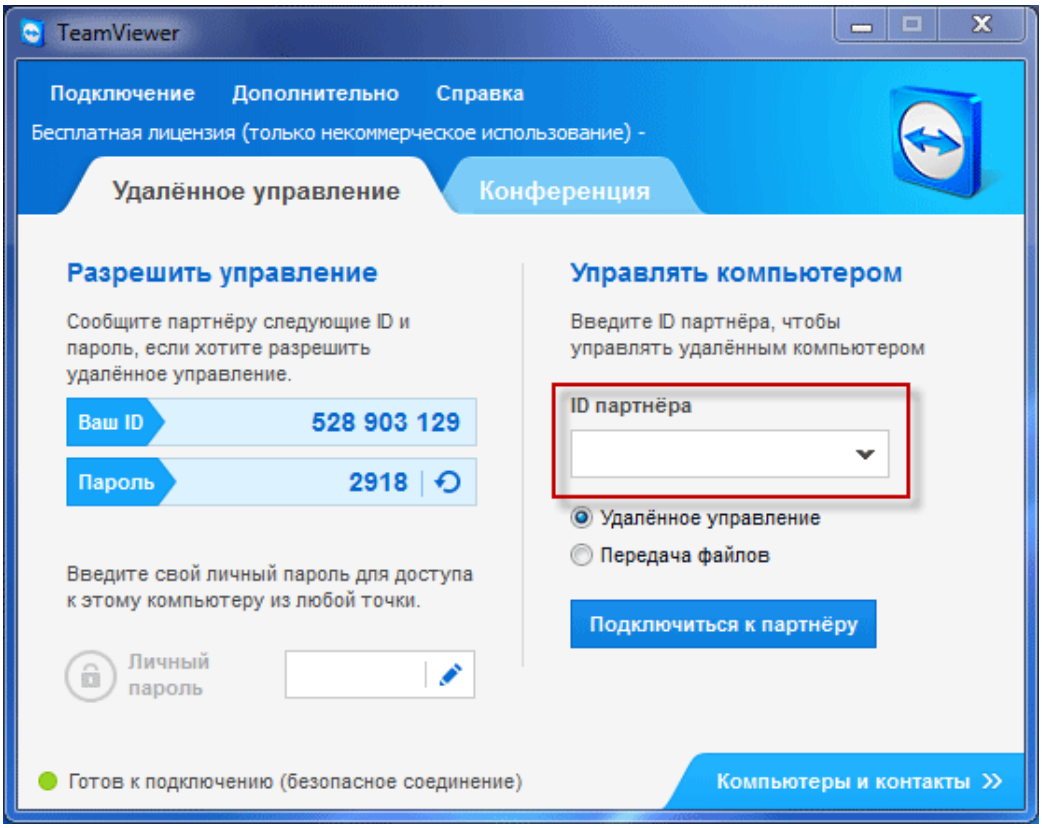


Рис. 5. **Управління комп'ютером**

Доступ до віддаленого комп'ютера

У головному вікні програми на панелі *Управлять компьютером* вводяться дані про інший комп'ютер – ID партнера, який разом із паролем необхідно отримати від користувача віддаленого комп'ютера. Необхідно вибрати режим *Удаленное управление* і підключитися до партнера.

Після введення одержаного пароля та натиснення на кнопку *Вход в систему* на екрані з'явиться робочий стіл віддаленого комп'ютера.

Зверху знаходиться панель інструментів, за допомогою якої можна управляти і налаштовувати програму, не заходячи безпосередньо до налаштування (рис. 6).

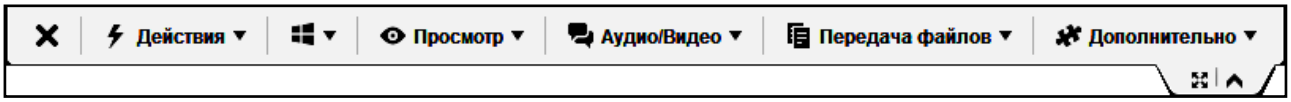


Рис. 6. **Панель інструментів**

Після підключення можна переходити до управління віддаленим комп'ютером – установлювати і видаляти програми, переглядати документи, здійснювати різні дії з налаштування ОС або програм.

Передача файлів у TeamViewer

Дуже корисною функцією є передача файлів із комп'ютера на комп'ютер. Для цього на панелі інструментів обрати *Передача файлов*, після чого відкриється вікно, розділене на два вікна. У лівому вікні розташовані файли локального комп'ютера, а в правому – віддаленого.

Після вибору файла чи папки, а також адреси, куди відправляти об'єкти, необхідно натиснути на кнопку *Отправить*.

Переміщувати файли можна також за допомогою *Хранилища файлов*. Відкрити *Хранилище файлов* можна за допомогою меню *Передача файлов* або з бокового вікна програми, натиснувши відповідний значок. Файли "перетягуються" з одного сховища в інше.

Тут розглянуті основні дії для віддаленого адміністрування. На цьому можливості програми не закінчуються, ще є функції спілкування, запису відео та інше. За необхідності розібратися з іншими функціями не важко.

Контрольні запитання

1. Назвіть переваги, які надає віддалене адміністрування.
2. Які методи віддаленого адміністрування ви знаєте?
3. Як підключитись до віддаленого робочого столу засобами *Windows*?
4. Які програми віддаленого адміністрування у глобальних мережах ви знаєте?
5. Як обмінюватись файлами з віддаленим робочим столом за допомогою програми *TeamViewer*?
6. Назвіть додаткові можливості програми *TeamViewer*.

Лабораторна робота 5
Дослідження протоколів прикладного рівня. Пошук інформації в Інтернеті

Мета роботи: вивчити основні можливості програм-браузерів (*Internet Explorer, Google Chrome* та ін.) з питань завантаження, перегляду і збереження web-сторінок. Навчитися здійснювати пошук необхідної інформації в Інтернеті з використанням пошукових серверів мережі.

У результаті виконання лабораторної роботи у студента формуються компетентності і застосування різних браузерів щодо пошуку необхідної інформації та її збереження на комп'ютері для подальшого використання.

Завдання

Вивчення сервісу WWW (переглядання web-сторінок)

1. Запустити програму *Internet Explorer* (або будь-який інший браузер) будь-яким зручним способом. Вивчити структуру вікна браузера, ознайомитися з довідковою системою і налаштуванням програми.
2. Змінити налаштування браузера. Зробити домашньою сторінку, вказану викладачем, www.meta-ukraine.com або http://meta.ua. Переконатися, що під час повторного запуску браузера завантажується вказана сторінка.
3. Відключити завантаження об'єктів мультимедіа (малюнки, анімації та ін.), порівняти час завантаження одних і тих самих сторінок із відключеним і включеним режимом завантаження об'єктів мультимедіа.
4. Навчитися управляти режимом переглядання web-сторінок:

на весь екран;

із включеними і відключеними панелями;

із правильно підібраним кодуванням символів.

5. Вивчити прийоми переміщення web-сторінками, вказаними викладачем*:

увівши в поле адреси вікна браузера необхідну адресу URL;

використовуючи список у полі адреси;

використовуючи панель "Ссылки";

використовуючи записи в Журналі;

обравши зі списку в папці "Избранное";

переміщаючись раніше завантаженими сторінками за допомогою кнопок "Вперед" і "Назад".

* **Рекомендовані сайти**

Пошуковий сервер – https://www.google.com.

Українські пошукові сервери – meta-ukraine.com або http://meta.ua.

Російські пошукові сервери – https://ya.ru; www.rambler.ru.

Урядові сервери – www.kmu.gov.ua; www.rada.gov.ua; www.ukrstat.gov.ua.

Про Харків – all.kharkov.ua; inkkharkov.com; gorod.kharkov.ua; social.kharkov.ua; kharkov-mobil.narod.ru.

Про ХНЕУ ім. С. Кузнеця – www.hneu.edu.ua.

Вакансії, резюме, дошка оголошень – join.com.ua.

Погода в Харкові ("Гисметео–Россия") **–** www.gismeteo.ru/towns/34300.htm.

Погода в Харкові (CNN–США) – http://weather.cnn.com/weather/forecast.jsp?locCode=UKHA.

6. Прослідкувати, як змінюється URL-адреса сторінок у рядку стану під час установки покажчика мишки на різних посиланнях.

7. Відкрити нове робоче вікно браузера й одночасно завантажити декілька різних сторінок. Слід мати на увазі, що швидкість завантаження сторінок у цьому разі знижується і не потрібно завантажувати більше трьох-чотирьох сторінок одночасно.

8. Навчитися використовувати сторінки, що зацікавили:

використовуючи папку "Избранное" – ознайомитися із структурою папки та її налаштуванням, навчитися створювати, перейменовувати і вилучати папки, групувати, перейменовувати і вилучати сторінки;

використовуючи панель "Ссылки" для сторінок, які часто використовуються.

9. Зберегти відкриту сторінку на диску в різних режимах:

тільки текст;

web-сторінку в повному обсязі;

окремо малюнки.

10. Навчитися переглядати збережену на диску інформацію в автономному режимі.

11. Використовувати текстові фрагменти з web-сторінок, наприклад, вставити деякі з них у документ *Word*.

Пошук даних у мережі Інтернет

1. Дослідити можливості будь-якого пошукового сервера (*Google*, *Яндекс*, *Rambler*):

вивчити зовнішній вигляд, налаштування, засоби пошуку і допомоги, каталоги;

вивчити довідку зі складання запитів;

із використанням каталогів провести направлений пошук інформації, заданої викладачем.

Увага! Під час перегляду знайдених у ході пошуку сторінок доцільно відключити завантаження зображень та анімацію. За необхідності їх можна буде завантажити додатково.

Примітка. Приклади каталогів: *мультимедіа, електронні видання, мистецтво, література, комп'ютери, комп'ютерні мережі, захист інформації, програми*.

Виконати контекстний пошук за ключовими словами, зберегти знайдені сторінки для подальшого використання.

Примітка. Приклади ключових слів: *хост, Вікіпедія, VPN, Wi-Fi, RSS, ipv6.* Список ключових слів може бути уточнений викладачем.

2. Визначити статистику застосування різних браузерів. Який із них є найбільш популярним? Яким браузером користуєтесь ви?

3. Ознайомитися зі змістом сторінки *www.meta-ukraine.com*: зовнішній вигляд, налаштування, засоби пошуку і допомоги, каталоги. Вивчити довідку зі складання запитів.

4. Виконати контекстний пошук (2 – 3-х різних пошукових систем) за ключовими словами (тими ж, що використовувались раніше), порівняти результати пошуку.

5. Створити запит на пошук інформації про одне з українських поліграфічних підприємств із використанням різних синтаксичних конструкцій на *www.google.com* і одній з мета-пошукових систем, порівняти і прокоментувати результати.

6. Скласти для вибраних пошукових засобів запит, спрямований на різні частини документа (*url, назва* і т. д.).

7 Зібрати інформацію про одне з українських поліграфічних підприємств: *власники, керівництво, перелік робіт, проекти, фінансовий звіт* і т. д.

8. Зберегти отриману інформацію на локальний диск.

9. У списку періодичних видань знайти харківський журнал "Бізнес-Інформ". Дізнатися про структуру журналу, хто є засновником, видавцем журналу.

Google Trends

1. Ознайомитись з мережною послугою *Google Trends* пошукової системи *Google*, де статистика надається від різних регіонів до міст.

Ця послуга може бути дуже корисною для обґрунтування актуальності тих чи інших проблем під час написання статей, курсових та дипломних робіт.

2. Визначити статистику для запитів із п. 2.1.

3. Підготовити статистику за своїми власними запитами.

Контрольні запитання

1. Дайте характеристику сервісу WWW як єдиного інформаційного простору.

2. Для яких цілей слугують гіперпосилання і як ними користуватися?

3. Включіть режим переглядання сторінок без завантаження зображень. Як під час цього дозавантажити який-небудь малюнок?

4. Як змінити кодування для перегляду web-сторінок?

5. Назвіть повну структуру адреси URL.

6. Які частини URL можна не враховувати під час задавання адреси?

7. Назвіть декілька способів завантаження web-сторінок під час використання браузерів.

8. Помістіть посилання на домашню сторінку в папку "Избранное", прогляньте вміст папки і знайдіть збережену сторінку.

9. Як знайти у журналі останню з відвіданих сторінок?

10. Як зберегти web-сторінку у файлі і відкрити її у другому вікні для перегляду з файла?

11. Як зберегти який-небудь малюнок з web-сторінки і проглянути його в графічному редакторі?

12. Що таке пошукова машина?

13. Назвіть відомі вам пошукові сервери.

14. Чим відрізняються контекстний і направлений пошук інформації?

15. Як знайти документ, якщо відома частина його URL?

16. Як знайти документ за допомогою пошукового сервера *www.meta-ukraine.com* за словом у його заголовку?

17. Що робити, якщо за запитом отримано дуже багато документів?

18. У чому відмінність запитів "Вузи України", Вузи України, Вузи + України, Вузи – України?

19. Де здійснюватиме пошук ключових слів *www.altavista.com* під час використання таких конструкцій:

title: *дизайн;

url:design;

host:*.ua.

Лабораторна робота 6

Оцінювання характеристик затримок пакетів у мережі

Мета роботи: навчитися будувати гістограми затримок пакетів і оцінювати основні характеристики затримок у реальних мережах.

У результаті виконання лабораторної роботи у студента формуються компетентності з оцінювання характеристик затримок пакетів у мережі методами натурного випробовування.

Завдання

Оцінити якість мережі для передачі мультимедійної інформації в реальному режимі часу. Для цього кожен студент оцінює характеристики затримок пакетів у мережі, підключившись до одного з вибраних сайтів Інтернету.

Налаштувати вікно командного рядка для збереження 500 рядків інформації

1. Відкрити вікно командного рядка **Пуск – Выполнить – cmd**;

2. Клацнути на іконку в лівій частині заголовка вікна і вибрати пункт меню *Свойства.*

3. На вкладці *Общие* у секції *Редактирование* встановити прапорець *Выделение мышью*.

4. На вкладці *Расположение* встановити розмір буфера обміну більш ніж 500, наприклад 600.

Запуск 500 пакетів за адресою вибраного сайта, наприклад *rambler.ru*

У вікні командного рядка виконати команду ***ping rambler.ru –n 500.***

Копіювання даних

1. Після відправки і прийому пакетів виділити мишкою у вікні командного рядка стовпець даних із часом затримки – усі 500 рядків (рис. 7).

2. Скопіювати дані в буфер обміну натисненням на клавішу *Enter***.**

Підготовка даних для оброблення в *Excel*

1. Зафіксувати результати роботи команди *ping* (*min*, *max* і середнє значення затримок, а також відсоток втрат пакетів).

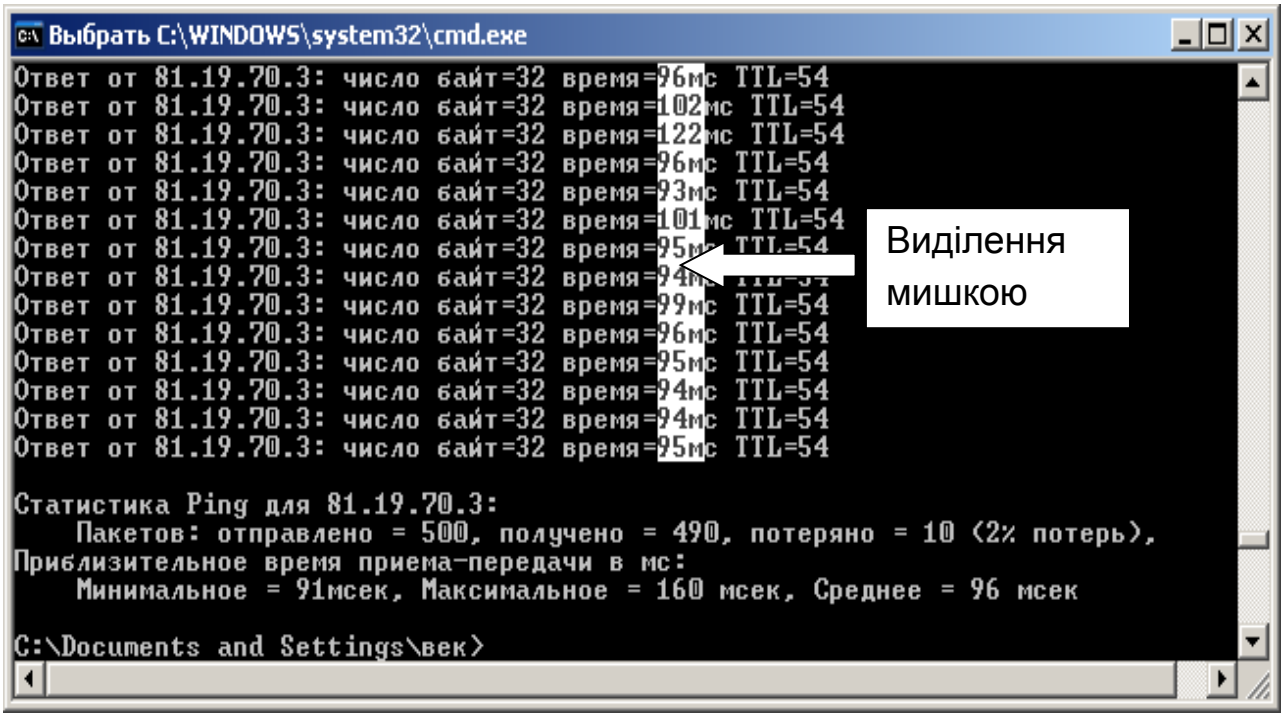


Рис. 7. **Виділення даних у вікні командного рядка**

2. Скопіювати значення масиву (500 рядків) із буфера обміну в стовпець на листі *Excel*.

3. Відредагувати отримані значення – можливо, доведеться видалити букву "м", що залишилася через неспівпадання розрядності величини затримки і видалити (зі зрушенням вгору) порожні рядки (там, де були відбракування через перевищення часу очікування). Визначити кількість даних, що залишилися (за допомогою номерів рядків, у даному випадку – 490). Подумайте, як спростити цю роботу (рис. 8).

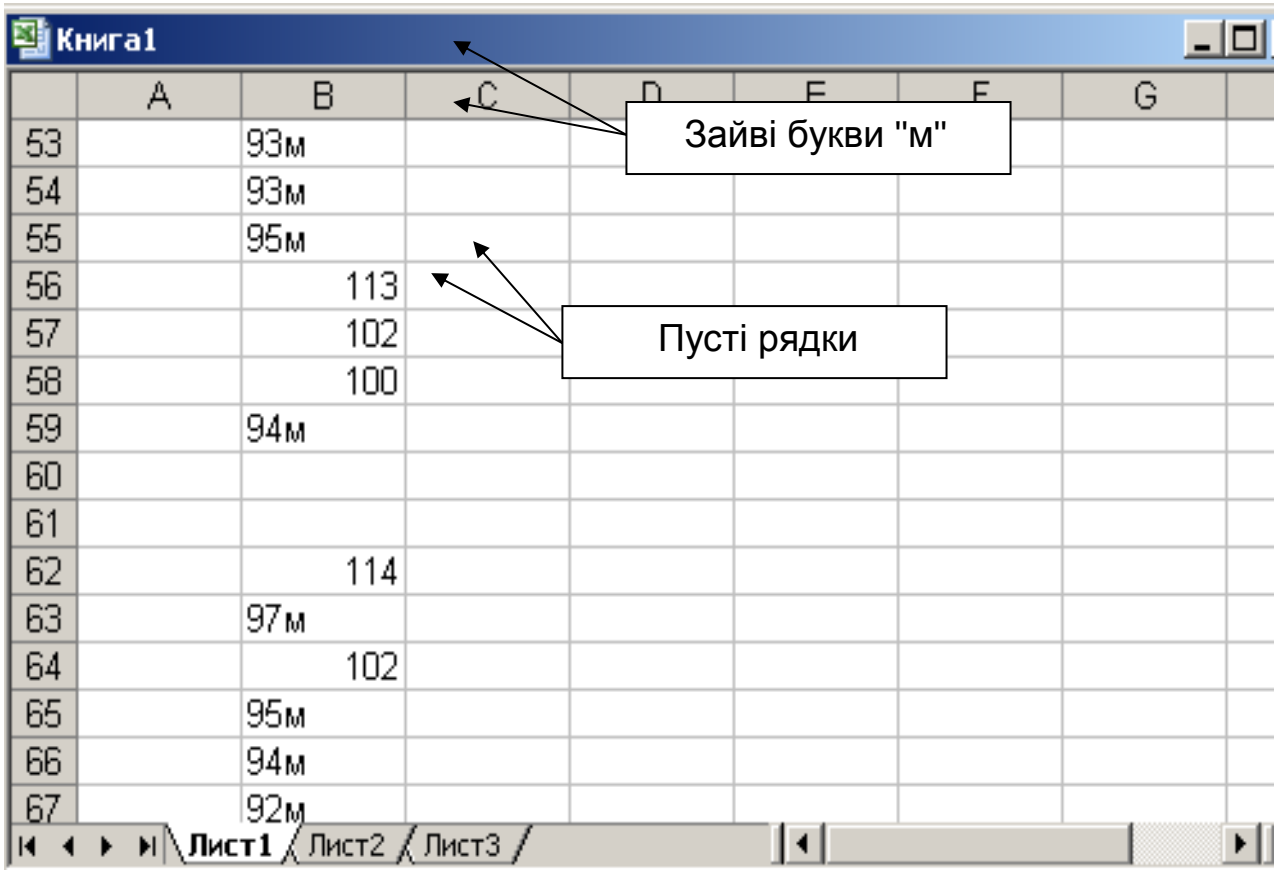
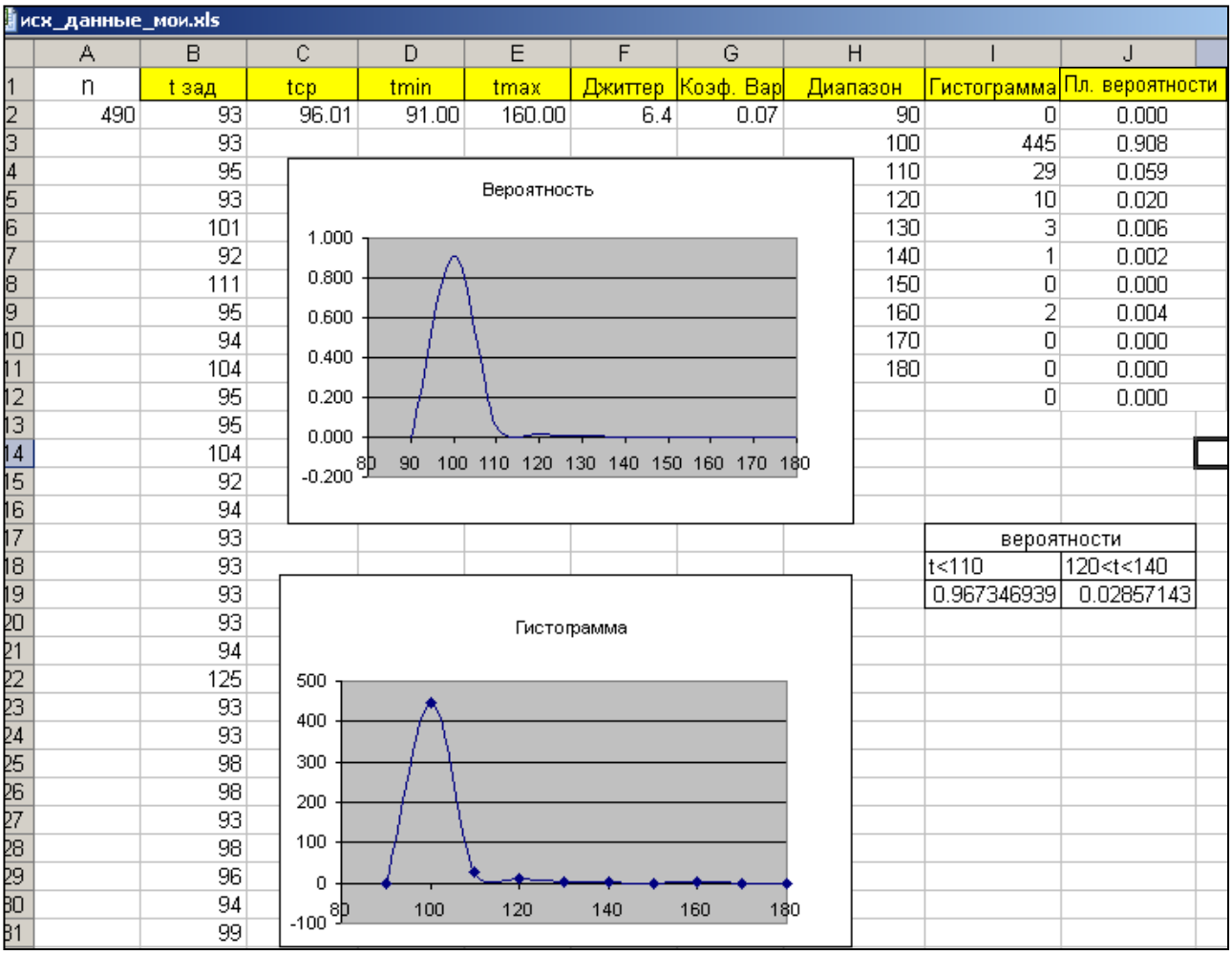


Рис. 8. **Корекція даних у вікні *Excel***

Оброблення даних у *Excel*

1. Розрахувати за отриманими відкоректованими даними *min*, *max*, середнє значення затримок, джиттер, коефіцієнт варіації і порівняти з отриманими результатами після виконання команди *ping*.

2. Для побудови 10-смугової гістограми на вільному місці листа *Excel* підготувати діапазон із 10 початкових значень (рядків) для гістограми в межах від *min* до *max* значення часу затримки пакетів (у даному випадку отриманий діапазон рядків від 90 мс до 180 мс із кроком 10 мс (рис. 9).



	A	B	C	D	E	F	G	H	I	J
1	n	t зад	tcp	tmin	tmax	Джиттер	Коэф. Вар	Диапазон	Гистограмма	Пл. вероятности
2	490	93	96.01	91.00	160.00	6.4	0.07	90	0	0.000
3		93						100	445	0.908
4		95						110	29	0.059
5		93						120	10	0.020
6		101						130	3	0.006
7		92						140	1	0.002
8		111						150	0	0.000
9		95						160	2	0.004
10		94						170	0	0.000
11		104						180	0	0.000
12		95							0	0.000
13		95								
14		104								
15		92								
16		94								
17		93								
18		93								
19		93								
20		93								
21		94								
22		125								
23		93								
24		93								
25		98								
26		98								
27		93								
28		98								
29		96								
30		94								
31		99								

вероятности	
t<110	120<t<140
0.967346939	0.02857143

Рис. 9. **Оброблення даних у *Excel***

3. Поряд із першою коміркою діапазону (справа) увести функцію ЧАСТОТА() з аргументами:

діапазон затримок (масив із 490 значень);

діапазон з **10 + 1** початкового значення для гістограми.

Після введення функції у комірці з формулою буде **0**.

4. Виділити стовпець (з назвою *Гістограма*) з **10 + 1** комірок, починаючи з комірки з формулою, натиснути **F2**, а потім **Ctrl + Shift + Enter**. У всіх комірках з'являться числа вимірювань, що потрапили у відповідний діапазон.

5. За даними *Діапазону* і *Частоти* побудуйте точковий графік гістограми (див. рис. 9).

Оцінювання вірогідних характеристик

1. Поряд зі стовпцем *Гістограма* побудуйте стовпець значень щільності розподілу затримок (розділіть кожне значення гістограми на

максимальне число вимірювань 490). Дайте назву отриманому діапазону значень із 10 рядків як *Пл. вірогідності.*

2. Використовуючи функцію ВЕРОЯТНОСТЬ(), оцінити вірогідність того, що затримка не перевищуватиме задану величину або вірогідність того, що затримка лежатиме в заданих межах (див. рис. 9).

Зробити висновки про можливість застосування цій мережі для передачі мультимедійної інформації.

Загальні відомості

У даний час комп'ютерні мережі все частіше використовують для розповсюдження мультимедійної інформації та інтерактивного спілкування користувачів (IPTV, IP-телефонія, відеоконференції, ігри), трансляції важливих політичних, спортивно-масових та інших значущих подій.

Передача такої інформації відрізняється від звичайних сервісів з передачі файлів і web-сервісів тим, що вона відбувається в реальному масштабі часу і дуже чутлива до затримок, до неї неможливо застосувати такі відомі способи корекції, як повторна передача спотворених і втрачених пакетів.

У цьому випадку якість інформації напряму залежить від якості комп'ютерних мереж, якими вона передається.

Основними чинниками, що впливають на якість інтерактивної мультимедійної інформації, що передається в мережах, є час затримки, джиттер і втрати пакетів.

Час затримки помітно впливає на дуплексну телефонну розмову. Повна затримка стає помітною, коли вона перевищує 250 мс. Під час перевищення цього порога підтримувати дуплексну розмову важко – голоси абонентів накладаються один на одного. Двобічна затримка більше ніж 500 мс робить телефонні розмови практично неможливими. Для довідки: типова затримка під час розмови через геостаціонарний супутник – 150 – 500 мс. Затримка має фіксовану і змінну складові. Наприклад, фіксована затримка визначається відстанню, тоді як змінна залежить від змінних мережних умов.

Джиттером у мережних технологіях називають відхилення від середньої затримки проходження пакетів. Термін "джиттер" є прикладом мережного жаргону: математики називають цю величину *стандартним відхиленням*. Затримка може бути різною для кожного пакета, внаслідок

чого, відправлені через однаковий інтервал, вони прибувають нерівномірно, або і не в початковій послідовності. Щоб прибрати істотне спотворення звуку або мерехтіння відео на приймальному вузлі необхідний буфер компенсації джиттера. Він затримує пакети, що надходять, щоб передавати їх пристрою декомпресії із заданим фіксованим інтервалом, а також виявляє будь-які помилки. Проте буфер компенсації вносить вельми значущу затримку (до 80 мс).

Втрата пакетів не повинна перевищувати величину 5 %, у цьому випадку програми корекції забезпечують прийнятну якість звуку.

Усі розглянуті параметри в мережах із комутацією пакетів залежать від безлічі чинників і мають випадковий характер, тому для їх оцінювання необхідно застосовувати *статистичні методи.* Статистичні характеристики виявляють закономірності в поведінці мережі, які виявляються тільки на тривалих періодах часу. Тому для отримання стійких результатів потрібно спостерігати поведінку мережі принаймні протягом хвилин, а краще – декількох годин.

Для того, щоб отримати статистичні характеристики мережі необхідно виміряти затримку кожного пакета, зберегти отримані результати і провести їх оброблення.

Основним інструментом статистики є так звана гістограма розподілу оцінюваної величини.

Для того, щоб отримати гістограму розподілу, необхідно розбити весь діапазон можливих затримок на декілька інтервалів і підрахувати, скільки пакетів із послідовності вимірювань потрапило до кожного інтервалу.

Гістограма затримок дає гарне уявлення про продуктивність мережі. За нею можна виявити, які рівні затримок вірогідніші, а які менш вірогідніші. Чим більший період часу, протягом якого збираються дані для побудови гістограми, тим із вищим ступенем вірогідності можна передбачити поведінку мережі в майбутньому.

Середнє значення затримки (D) обчислюється як сума всіх затримок d_i, що ділиться на кількість усіх вимірювань N:

$$D = \sum_i \frac{d_i}{N}.$$

Джиттер (J) є середнім відхиленням кожної окремої затримки від середнього значення затримки:

$$J = \frac{\sum_i (d_i - D)^2}{N - 1}.$$

Коефіцієнт варіації – це безрозмірна величина, яка дорівнює відношенню джиттера до середнього значення затримки:

$$CV = J / D.$$

Ідеальний рівномірний потік даних завжди матиме нульове значення коефіцієнта варіації. Коефіцієнт варіації, що дорівнює одиниці, означає дуже важкий для мережі пульсуючий трафік (затримки розподілені за пуассонівським законом).

Як характеристика втрати пакетів використовується частка втрачених пакетів (L). Вона дорівнює відношенню кількості втрачених пакетів (*NL*) до загальної кількості переданих пакетів (N):

$$L = NL / N.$$

Під час збільшення кількості інтервалів і часу спостереження буде отримана безперервна функція, яка називається *щільністю розподілу затримки пакета*. Вірогідність того, що значення випадкової величини опиниться в певному діапазоні, дорівнює визначеному інтегралу щільності розподілу випадкової величини від нижньої до верхньої межі даного діапазону. Таким чином може бути обчислене вірогідне значення затримки пакета.

Для отримання вказаних характеристик можна розробити спеціальне програмне забезпечення або використовувати відомі методи, засновані на використанні комплексу доступних програм, кожна з яких реалізує частину загального завдання.

Системна команда *ping* запускається з командного рядка *Windows* і забезпечує формування та надсилання за заданою IP-адресою будь-якої кількості пакетів довільної тривалості, розрахунок середньої, макси-

мальної і мінімальної затримки пакетів, а також відсоток втрачених пакетів. На жаль, за допомогою цієї команди неможливо оцінити величину джиттера і коефіцієнта варіації, оскільки у ході запуску з командного рядка *Windows* результати затримки кожного пакета не зберігаються.

Спочатку необхідно налаштувати вікно командного рядка *Windows* так, щоб у ньому помістилося набагато більше початкової інформації – до 5 000 рядків замість 250 за замовчуванням. Після накопичення у вікні необхідної кількості рядків із окремими затримками пакетів, рядки можна виділити, скопіювати у вигляді масиву і передати в програму оброблення, наприклад *Excel*.

У програмі *Excel* пропонується використовувати статистичну функцію *СТАНДОТКЛОН()*, за допомогою якої можна розрахувати джиттер, функцію *ЧАСТОТА()*, за допомогою якої можна отримати дані для побудови гістограми.

Для оцінювання вірогідності того, що затримка не перевищуватиме задану величину або вірогідність того, що затримка лежатиме в заданих межах, можна використовувати статистичну функцію *ВЕРОЯТНОСТЬ()*.

Контрольні запитання

1. Чим характеризується продуктивність мереж?
2. Чому для аналізу затримок пакетів у мережі необхідно використовувати статистичні методи?
3. Назвіть основні характеристики випадкової величини.
4. Що таке джиттер?
5. Що таке максимальна затримка?
6. Що показує час реакції мережі?
7. Назвіть характеристики швидкості передачі даних.
8. Назвіть основні способи використання альтернативних маршрутів у мережі.
9. Назвіть основні методи підвищення надійності роботи мережі.
10. Які класи додатків за чутливістю до затримок пакетів ви знаєте?
11. До якого класу за чутливістю до затримок пакетів належать додатки, що управляють друкарським технологічним процесом?
12. До якого класу за чутливістю до затримок пакетів належить електронна пошта?

Лабораторна робота 7
Розроблення і дослідження математичної моделі локальної мережі

Мета роботи: навчитися використовувати математичний апарат теорії черг (СМО) для оцінювання характеристик локальних мереж.

У результаті виконання лабораторної роботи у студента формуються компетентності з оцінювання характеристик затримок пакетів у мережі методами математичного моделювання.

Характеристика мережі

Комп'ютери мультимедійного видавництва потрібно об'єднати в локальну мережу зі швидкістю передачі даних 10 Мбіт/с. Обмін між комп'ютерами здійснюватиметься за протоколом TCP/IP, тобто всі повідомлення, що передаються, будуть розподілені на пакети певної довжини $L_п$ (у байтах).

Черговий пакет передається в мережу за протоколом *Ethernet 10Base-T* через фіксований інтервал часу ($t_ф$ = 9,6 мкс) після видачі попереднього.

Час оброблення пакета $T_{обр}$ комутувальним пристроєм дорівнює тривалості пакета $T_п$ плюс фіксована затримка на оброблення пакета – $t_о$.

Завдання

Визначити характеристики мережі відповідно до заданого варіанта для випадків:

1. У комутувального пристрою немає буферної пам'яті (система з відмовами).

2. Комутувальні пристрої володіють нескінченно великою місткістю буферної пам'яті для збереження пакетів у черзі (система без втрат).

3. Комутувальні пристрої володіють заданою місткістю буферної пам'яті для збереження пакетів у черзі *m*.

Розрахунки вести в припущенні, що вхідний потік – пуассонівський з інтенсивністю надходження заявок (пакетів) дорівненій λ = 1 / T заявок на секунду, де T – інтервал між пакетами у мережі.

Час обслуговування одного пакета комутувальним пристроєм – випадкова величина з пуассонівською щільністю розподілу. Інтенсивність обслуговування $\mu = 1 / T_{обр}$.

Варіанти завдань наведені у табл. 2.

Таблиця 2

Варіанти завдань

№ варіанта	Довжина пакета $L_п$, байти	$t_{о,\ мкс}$	m1	m2
1	72	5	100	1 000
2	72	10	200	3 000
3	200	4	100	5 000
4	200	10	50	100
5	600	5	200	1 500
6	750	6	50	5 000
7	750	3	60	1 000
8	1 000	10	70	2 500
9	1 200	8	10	500
10	1 200	5	100	4 000
11	1 526	6	60	3 000
12	1 526	8	100	2 000

Рекомендації щодо проведення роботи

1. Оцінки розрахувати з використанням мови програмування C# або з використанням табличного процесора *Excel*.

2. Спочатку розрахуйте значення T – інтервал між пакетами у мережі за заданою швидкістю 10 Мбіт/с, і заданими величинами – довжина пакета $L_п$, (у байтах) і $t_ф$, (у мкс), маючи на увазі, що за швидкістю 10 Мбіт/с 1 біт інформації передається за 0,1 мкс.

3. Знаючи T, розрахуйте максимально можливе значення λ.

4. Задайте діапазон зміни λ від мінімального до максимально можливого з певним кроком (для подальшої побудови графіка буде потрібно приблизно 12 – 15 значень).

5. Використовуючи ті самі дані (п. 2), розрахуйте тривалість пакета $T_п$ і час обслуговування одного пакету комутувальним пристроєм $T_{обр}$ з урахуванням заданої фіксованої затримки $t_о$.

5. Знаючи $T_{обр}$, розрахуйте значення μ і ρ.

6. Усі початкові дані і розрахункові величини зведіть у таблицю (зразок наведено у файлі *Результати.xls*).

7. Побудуйте графіки залежності середніх часів очікування пакетів у черзі і в системі (комутувальному пристрої), особливо звертаючи увагу на режим перевантаження (ρ ≈ 1, але не дорівнює одиниці і не перевищуюче одиницю).

Проведення дослідження

Для систем із обмеженою місткістю буферної пам'яті

Визначити за умови заданого (чималого) значення λ, якою має бути місткість буферної пам'яті, щоб забезпечити вірогідність відмови передачі пакета на рівні: а) не більше ніж 10^{-6}; б) 10^{-9}.

Для цієї мети використати функцію *Excel – Подбор параметра*.

Для систем із необмеженою місткістю буферної пам'яті

Визначити для заданої місткості буферної пам'яті, за якої інтенсивності надходження пакетів до мережі їх середня затримка в системі не перевищить: а) 0,1 мс; б) 0,3 мс.

Для цього також використати функцію *Excel – Подбор параметра*.

Перевірити правильність розрахунків.

Для систем із обмеженою місткістю буферної пам'яті за чималим m > 1 000, характеристики повинні співпадати з характеристиками систем з необмеженою чергою.

Для систем із обмеженою місткістю буферної пам'яті за $m = 0$ характеристики повинні співпадати з характеристиками систем із відмовами.

Загальні відомості

Ознайомлення з моделлю M/M/1

Існує гілка прикладної математики, предметом якої є процеси утворення черг – теорія черг, або теорія систем масового обслуговування (СМО).

На рис. 10 показана найбільш проста модель теорії черг, відома під назвою M/M/1, де: 1 – один обслуговуючий пристрій, M – марківське або пуассонівське розподілення інтервалів надходження заявок (пакетів) і значень часу обслуговування цієї заявки (просування пакета через комутувальний пристрій).

Основними елементами моделі є:

вхідний потік абстрактних заявок (пакетів) на обслуговування;

буфер;

обслуговувальний пристрій, наприклад комутатор (*switch*);

вихідний потік обслужених заявок.

Заявки надходять до входу буфера у випадкові моменти часу. Якщо у момент надходження заявки буфер порожній і обслуговуючий пристрій вільний, то заявка відразу ж передається в цей пристрій для обслуговування. Обслуговування ж триває невизначений час (відповідає середньому часу просування пакета процесором комутатора з вхідного буфера до вихідного каналу – довжина пакета + час на оброблення << довжини пакета).

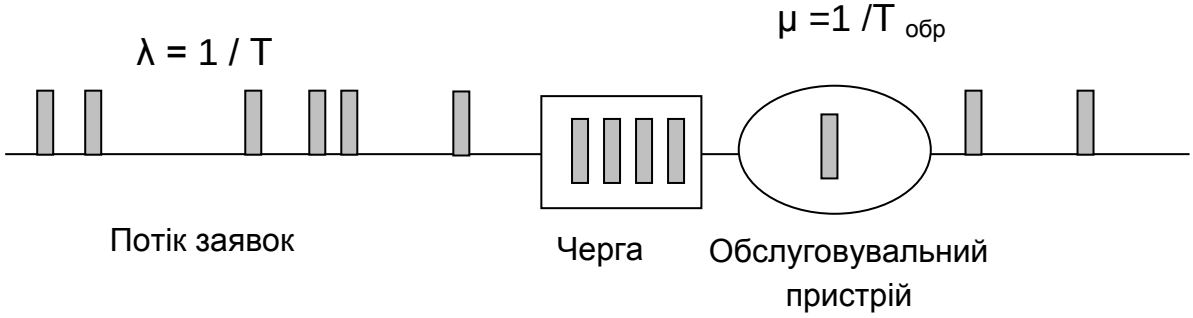


Рис. 10. **Модель M/M/1**

Якщо у момент надходження заявки буфер порожній, але обслуговувальний пристрій зайнятий обслуговуванням заявки, що надійшла раніше, то заявка чекає у буфері. Як тільки обслуговувальний пристрій завершує обслуговування чергової заявки, вона передається на вихід, а прилад обирає наступну заявку (якщо буфер не порожній). Якщо заявка застає буфер не порожнім, то вона стає в чергу і чекає обслуговування.

Заявки, що виходять з обслуговувального пристрою, утворюють вихідний потік.

Буфер може бути нескінченним, і тоді заявки ніколи не втрачаються через те, що вичерпана місткість буфера – *система без втрат*.

Місткість буфера може мати кінцеве значення *m*, тоді можливі втрати заявок.

Теорія черг дозволяє оцінити для цієї моделі середню довжину черги і середній час очікування заявки в черзі залежно від характеристик вхідного потоку і часу обслуговування.

Будемо вважати, що відомий середній час між надходженнями заявок T. Це означає, що інтенсивність надходження заявок, яка традиційно позначається в теорії черг символом *λ* дорівнює:

$$\lambda = 1/T \text{ заявок за секунду.}$$

Випадковий процес надходження заявок описується в цій моделі функцією розподілу інтервалів між надходженнями заявок. Для спрощення отримання компактних аналітичних результатів зазвичай уважають, що ці інтервали описуються так званим марківським розподілом (інша назва – пуассонівський). Середнє відхилення інтервалів у цьому разі також дорівнює T, тому стандартне відхилення дорівнює T / T = 1. Вхідний потік є істотно пульсуючим.

Також будемо вважати, що середній час обслуговування заявки дорівнює $T_{обр}$. Це означає, що обслуговувальний прилад здатний просувати заявки на вихід із інтенсивністю $\mu = 1 / T_{обр}$.

Знову ж таки для отримання аналітичного результату вважають, що час обслуговування – це випадкова величина з пуассонівською щільністю розподілу.

Прийняття таких припущень у *системах без утрат* (з необмеженою чергою) дає простий результат для:

середнього часу очікування заявки в черзі:

$$t_{ож} = \rho \frac{T_{обр}}{1 - \rho};$$

середнього часу перебування у системі:

$$t_{сист} = \frac{1}{\mu(1 - \rho)};$$

середньої кількості заявок, що знаходяться в черзі:

$$r = \frac{\rho^2}{1 - \rho};$$

відносної пропускної спроможності:

$$q = 1;$$

абсолютної пропускної спроможності:

$$A = 1;$$

вірогідності відмови:

$$P_{отк} = 0.$$

Через параметр ρ позначено відношення λ / μ – коефіцієнт використання обслуговувального приладу (інтерфейсу комутатора, процесора комутатора, каналу або середовища, що розділяється).

Параметр ρ відіграє ключову роль в утворенні черги. Якщо значення ρ близьке до нуля, то і середній час очікування дуже близький до нуля.

Чим ближчі середні значення інтервалів між пакетами до середнього часу обслуговування, тим складніше обслуговувальному пристрою справлятися з навантаженням.

Черга створюється на тих проміжках, на яких інтенсивність надходження пакетів набагато перевищує інтенсивність обслуговування. Перевантаження ресурсів може призвести до повної деградації мережі, коли, не дивлячись на те, що мережа передає пакети, корисна швидкість передачі даних дорівнює нулю. Це відбувається в тому випадку, якщо затримки доставки всіх пакетів перевищують деякий поріг, і пакети відкидаються вузлом призначення як застарілі. Якщо ж протоколи, що працюють у мережі, використовують надійні процедури передачі даних на основі квитування і повторної передачі загублених пакетів, то процес перевантаження наростатиме лавиноподібно.

Якщо місткість буфера мережі кінцева і дорівнює m, тоді можливі втрати заявок. Теорія черг і в цьому випадку дає достатньо прості формули для розрахунку тимчасових характеристик мережі за тих самих допущеннях.

Середній час очікування заявки в черзі:

$$t_{ож} = \frac{r}{\lambda}.$$

Середній час перебування в системі:

$$t_{сист} = t_{ож} + \frac{q}{\mu}.$$

Середнє число заявок, що знаходяться в черзі:

$$r = \frac{\rho^2\ 1 - \rho^m(m + 1 - m\rho)}{1 - \rho^{m+2}\ (1 - \rho)}.$$

Відносна пропускна спроможність:

$$q = 1 - \rho^{m+1} p_0.$$

Абсолютна пропускна спроможність:

$$A = \lambda q.$$

Вірогідність відмови:

$$P_{отк} = \rho^{m+1} p_0,$$

де p_0 – вірогідність того, що обслуговувальний пристрій вільний:

$$p_0 = \frac{1 - \rho}{1 - \rho^{m+2}}.$$

Далі наведені співвідношення для систем із відмовами, у яких немає буфера, і заявка, що надійшла прийшла під час обслуговування, і яка буде відкинута, – *нетерплячі заявки:*

відносна пропускна спроможність:

$$q = p_0;$$

абсолютна пропускна спроможність:

$$A = \lambda q;$$

вірогідність відмови:

$$P_{отк} = 1 - q,$$

де $p_0 = \frac{\mu}{\lambda + \mu}$.

Контрольні запитання

1. Назвіть характеристики мереж, які можна оцінити за допомогою теорії масового обслуговування?
2. Що означають букви ММ у моделі М/М/1?

3. Який параметр визначається за допомогою формули:

$$r = \frac{\rho^2\ 1 - \rho^m(m + 1 - m\rho)}{1 - \rho^{m+2}\ (1 - \rho)}.$$

4. Що таке абсолютна пропускна спроможність?

5. Які заходи необхідно вжити для запобігання перевантаженням мережі?

Лабораторна робота 8
Створення бездротової локальної мережі

Мета роботи: отримати теоретичні знання та практичні навички із застосування технологій бездротових комп'ютерних мереж.

У результаті виконання лабораторної роботи у студента формуються компетентності з налаштування бездротової локальної мережі між декількома пристроями – ПК, ноутбуками, планшетами, смартфонами тощо.

Завдання 1

Бездротова мережа між двома комп'ютерами

Робота виконується із застосуванням ноутбуків із Wi-Fi. Студенти розподіляються на групи з двох користувачів зі своїми ноутбуками.

1. Переконатися, що режим Wi-Fi увімкнено на обох ноутбуках.
2. Створити точку доступу на одному з комп'ютерів групи – встановити на ньому програмний (віртуальний) Wi-Fi-адаптер. Комп'ютер після цього буде виконувати функції Wi-Fi-роутера.
3. Створити нову Wi-Fi-мережу – точку доступу.
4. Налаштувати запуск створеної мережі та її зупинення за допомогою *bat*-файлів.
5. Підключити ноутбуки один до одного через їх IP-адреси або через мережне оточення (у цьому випадку комп'ютери повинні знаходитися в одній робочій групі) й отримати доступ до їх ресурсів (папок і файлів).
6. Підключити другий комп'ютер (ноутбук, планшет, смартфон) до Інтернету через створену мережу.

Завдання 2

Бездротова локальна мережа з декількох комп'ютерів

Розподілити студентів на дві групи для створення двох локальних мереж.

1. Визначити робочі групи і підключити ноутбуки до однієї з робочих груп.

2. Переконатися, що режим Wi-Fi увімкнено на всіх комп'ютерах мережі.

3. Налаштувати головні комп'ютери для підключення до мережі і відкриття загального доступу до файлів.

4. Налаштувати інші комп'ютери для підключення до своєї мережі і перевірити можливість роботи з доступними ресурсами мережі.

5. Підключити комп'ютери до Інтернету через головний комп'ютер мережі.

Загальні відомості

1. Бездротова мережа Wi-Fi між двома комп'ютерами

Щоб створити локальну бездротову Wi-Fi-мережу між двома комп'ютерами з можливістю виходу в Інтернет через один з них, який підключений до Інтернету через кабель, необхідно виконати ряд етапів.

Етап 1 – створення віртуального мережного адаптера на ноутбуці, який транслюватиме бездротову мережу та Інтернет, тобто ноутбук буде виконувати роль Wi-Fi-роутера.

Для цього необхідно виконати команду *cmd* з правами адміністратора.

У вікні командного режиму набрати вручну, або, що набагато простіше і точніше, скопіювати рядок:

netsh wlan set hostednetwork mode=allow ssid=МояСеть key=87654321 keyUsage=persistent,

де *ssid* – ідентифікатор створюваної мережі з ім'ям *МояСеть* (якщо в імені є пробіли, то ім'я береться у лапки – *"Моя сеть"*, а значення *key* – це пароль для підключення, від 8 до 63 символів у кодуванні ASCII. У даному прикладі пароль 87 654 321.

Мережа створена, але знаходиться у неактивному стані.

Для активації (старту) створеної бездротової мережі знову запустити вікно командного режиму *cmd* з правами адміністратора, в якому вводиться такий рядок: *netsh wlan start hostednetwork*.

Для того, щоб за необхідності зупинити мережу, необхідно виконати команду: *netsh wlan stop hostednetwork*.

Усі ці команди краще оформити у вигляді *bat*-файлів для швидкого запуску за необхідністю, наприклад, start_bat і stop_bat.

Bat-файл, або пакетний файл – звичайний текстовий файл з розширенням **.bat*, що містить послідовність команд, призначених для виконання командним інтерпретатором. У розглянутому прикладі *bat*-файли містять по одному зазначеному рядку. Запускаються *bat*-файли клацанням мишки.

Після запуску мережі її можна визначити за допомогою будь-якого Wi-Fi-пристрою (ноутбука, планшетного комп'ютера, смартфона і т. д.). Наприклад, зайшовши в меню пошуку та підключення мереж смартфона на *OS Android* (**Настройка – Сеть – Настройка Wi-Fi – Включить Wi-Fi – Сети Wi-Fi**) можна виявити мережу *MS Virtual Wi-Fi*. Підключитися до мережі можна, натиснувши кнопку *Подключение* у списку доступних мереж і ввівши пароль, який був заданий під час створення мережі. У даному випадку це 87 654 321.

Бездротова програмна точка доступу (*SoftAP*) з парольним захистом створена і готова до використання.

Етап 2 – налаштування доступу до Інтернету за допомогою створеної програмної точки доступу на базі ноутбука, тобто потрібно зробити відкритим доступ кабельного мережного адаптера на ноутбуці.

Для цього відкрити вікно *Центр управления сетями и общим доступом*, яке доступне на панелі управління або після клацання мишки на значку *Сеть* на панелі задач. У вікні перейти за посиланням *Изменение параметров адаптера* і знайти мережний (кабельний) адаптер. Натисненням правої кнопки мишки на значку адаптера викликати вікно *Свойства*. На вкладці *Доступ* позначити прапорцем режим *Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера*. Крім цього, необхідно вказати, якому конкретно адаптеру відкритий доступ до мережі в меню, що з'являється нижче рядка *Подключение домашней сети*. Тут треба вказати щойно створену віртуальну мережу (*Беспроводное сетевое соединение 2*).

Після натиснення кнопки *ОК* для збереження параметрів мережа повинна відразу почати роздавати Інтернет без перезавантаження – створена мережа візуально на панелі задач повинна бути з доступом до Інтернету.

Важливо: запускати створену мережу необхідно після кожного перезапуску операційної системи *Windows*, що доводить доцільність створення двох *bat*-файлів на запуск і зупинку віртуального Wi-Fi-адаптера з ярликами на робочому столі для максимальної зручності.

Слід мати на увазі, що точка доступу створена програмно, і таким чином мережа буде працювати повільніше, ніж мережа з адаптером у вигляді реального пристрою.

2. Бездротова локальна мережа Wi-Fi

Налаштування головного комп'ютера мережі

Головний комп'ютер мережі – це комп'ютер або ноутбук, підключений до Інтернету і який виступає як Інтернет-шлюз. На цьому комп'ютері буде створено Wi-Fi-з'єднання.

Нехай всі комп'ютери мережі забезпечені Wi-Fi-адаптерами, а головний комп'ютер мережі вже підключений до Інтернету. Необхідно створити робочу групу, до якої увійдуть комп'ютери Wi-Fi-мережі. Кожен комп'ютер мережі повинен мати унікальне ім'я і входити до складу однієї і тієї ж робочої групи.

Варто нагадати, що ім'я робочої групи і комп'ютера можна змінити, клацнувши правою кнопкою мишки на значку *Компьютер*, вибравши меню *Свойства* і перейшовши за посиланням *Дополнительные параметры системы*.

Після зміни імені комп'ютера і робочої групи необхідно перезавантажити комп'ютер.

На головному комп'ютері включити Wi-Fi-адаптер, далі для створення бездротової мережі необхідно відкрити вікно *Центр управления сетями и общим доступом*, яке доступне з панелі управління або після клацання правою кнопкою мишки на значку *Сеть* на панелі задач.

У вікні *Центр управления сетями и общим доступом* перейти за посиланням *Управление беспроводными сетями.* У вікні *Управление беспроводными сетями* (рис. 11) клікнути на кнопці *Добавить* і створити бездротову мережу. У вікні *Подключение к беспроводной сети вручную* перейти за посиланням *Создать сеть "компьютер – компьютер".*

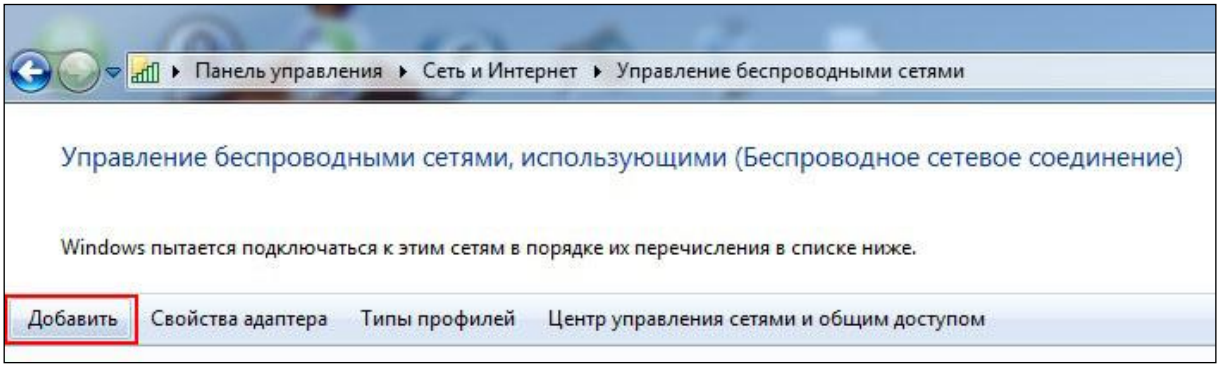


Рис. 11. **Управління бездротовими мережами**

Уважно ознайомитись з визначенням *"мережа "комп'ютер – комп'ютер""* і обмеженнями на її використання (рис. 12) і натиснути кнопку *Далее*.

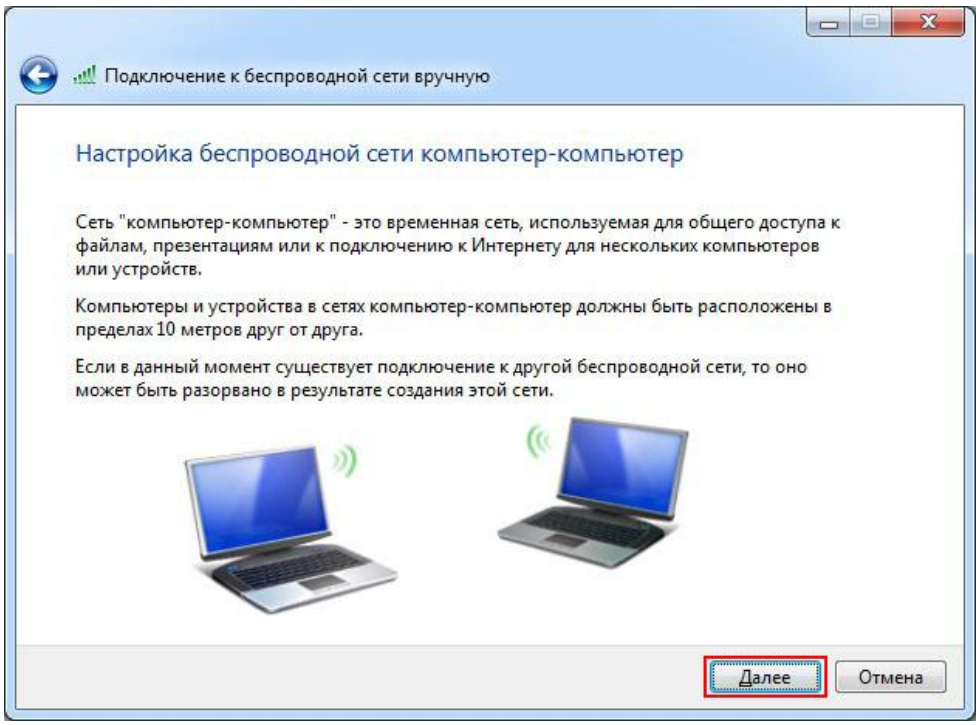


Рис. 12. **Бездротова *мережа "комп'ютер – комп'ютер"***

У полі *Имя сети:* задати довільне ім'я мережі (рис. 13).

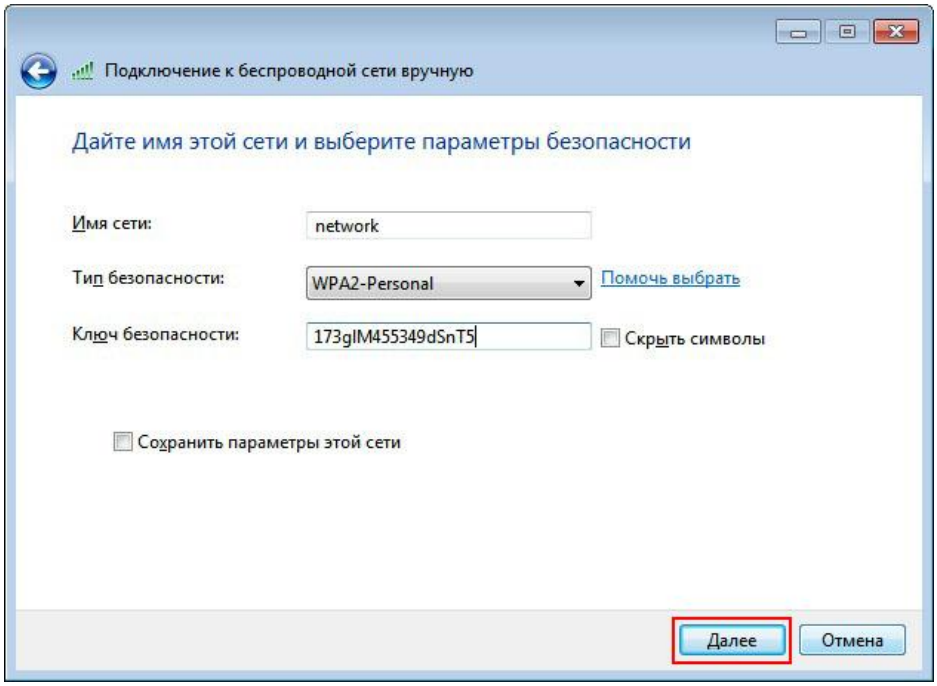


Рис. 13. **Підключення до бездротової мережі**

У полі *Тип безопасности:* вибрати *WPA2-Personal* (для ОС *Windows XP* обрати *WEP*).

У полі *Ключ безопасности:* ввести пароль. Пароль повинен складатися від 8 до 63 знаків (для *WEP* пароль від 5 до 13 знаків). Натиснути кнопку *Далее*. У вікні, яке з'явилося (рис. 14), включити режим *Включить общий доступ к подключению Интернет* і закрити вікно. На цьому налаштування головного комп'ютера закінчується.

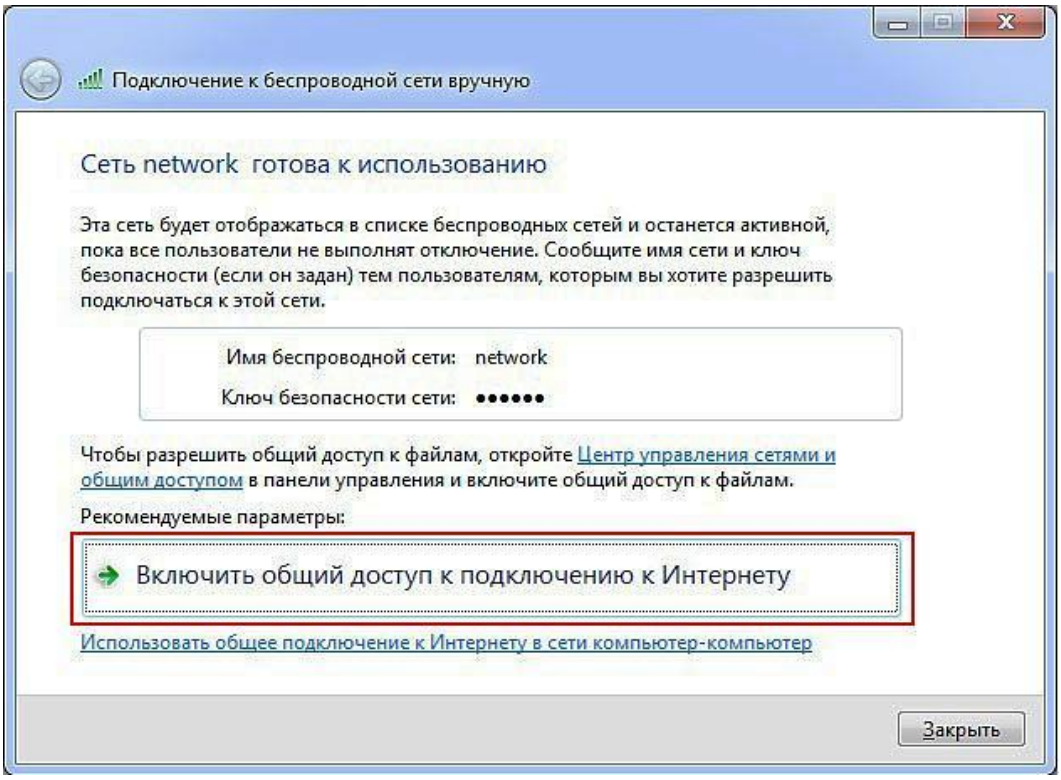


Рис. 14. **Підключення загального доступу**

Налаштування інших комп'ютерів у мережі

Інші комп'ютери мережі – це комп'ютери або ноутбуки, підключенні до Wi-Fi-мережі, створеної на головному комп'ютері, які мають доступ до Інтернету через цей комп'ютер.

На кожному комп'ютері налаштувати ім'я робочої групи і комп'ютера так само, як і для головного комп'ютера.

На кожному комп'ютері мережі включити Wi-Fi-адаптери, відкрити вікно *Центр управления сетями и общим доступом*, перейти за посиланням *Подключиться к сети* і вибрати бездротову мережу для підключення (рис. 15).

У вікні *Центр управления сетями и общим доступом* перейти за посиланням *Изменение параметров адаптера*.

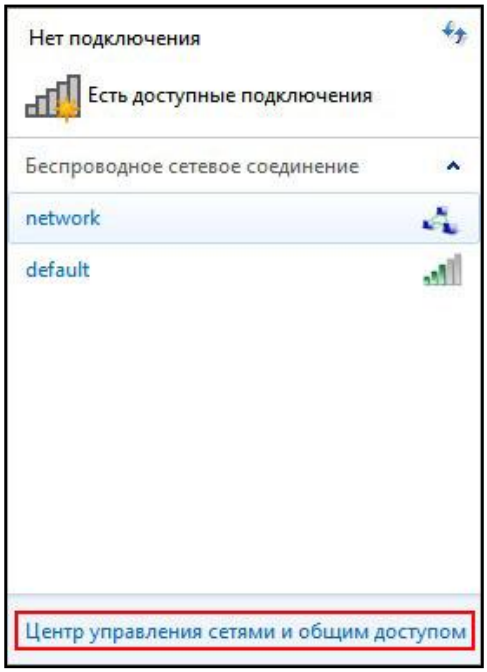


Рис. 15. **Вибір бездротової мережі для підключення**

Клікнувши правою кнопкою мишки на значку бездротового мережного адаптера, вибрати пункт *Свойства*. У вікні, що відкрилося, вибрати пункт *Протокол Интернета версии 4 (TCP/IPv4)* і змінити його властивості.

Відзначити пункт *Использовать следующий IP-адрес*.

У полі *IP-адрес:* призначити IP-адресу бездротовому адаптеру. IP-адреса має бути унікальною і з тієї ж підмережі, що IP-адреса бездротового адаптера головного комп'ютера. У мережі не повинно бути пристроїв з однаковими IP-адресами. Через те, що на головному комп'ютері бездротовому адаптерові Wi-Fi присвоєна IP-адреса 192.168.10.1, то на інших комп'ютерах мережі IP-адреси повинні бути такими: 192.168.10.2, 192.168.10.3 і т. д.

У полі *Маска подсети:* вказати значення 255.255.255.0.

У полі *Основной шлюз:* вказати IP-адресу головного комп'ютера – 192.168.10.1.

У полі *Предпочитаемый DNS-сервер:* вказати IP-адресу бажаного *DNS*-сервера провайдера.

У полі *Альтернативный DNS-сервер:* вказати IP-адресу альтернативного *DNS*-сервера провайдера.

Адреси *DNS*-серверів можна дізнатись у провайдера. У даному прикладі вказані адреси 109.86.2.2 і 109.86.2.21 відповідно. Підтвердити налаштування і закрити вікно, натиснувши кнопку *ОК*.

Для підключення комп'ютера до бездротової мережі слід клікнути на значку мережного з'єднання, а потім двічі на створеній мережі. Увести пароль (ключ безпеки) і натиснути кнопку *ОК*.

Контрольні запитання

1. Назвіть особливості передачі інформації в бездротових мережах.
2. Назвіть типи бездротових мереж за їх розміром.
3. Які існують схеми підключення до Інтернету через стаціонарний супутник? Чи можливі такі схеми через середньоорбітальні супутники?
4. Як можна бездротово підключитися до Інтернету без супутника?
5. Які типи сучасних *WLAN* ви знаєте?
6. Назвіть режими доступу до середовища у мережі Wi-Fi.
7. Назвіть різновиди стандарту 802.11.
8. Назвіть основні схеми підключення вузлів до бездротової мережі Wi-Fi.
9. Яка структура бездротової мережі *WiMAX*?
10. Як працюють пікомережі *Bluetooth*?

Лабораторна робота 9
Дослідження програмних методів захисту мультимедійної інформації

Мета роботи: освоїти практичні навички із застосування програмних засобів захисту інформації.

У результаті виконання лабораторної роботи у студентів формуються компетентності з практичного застосування захисту засобами *Microsoft Office* та спеціальними програмними засобами.

Результатом виконання самостійної роботи є практичне застосування програми *Gpg4win* для шифрування файлів і цифрового підпису, а також застосування цифрових підписів у документах *Microsoft Office.*

Завдання 1

Створювання ключів

1. Установити на комп'ютері вільно розповсюджену програму *Gpg4win* (див. загальні відомості).
2. Створити власну пару ключів (закритий та відкритий).
3. Додати (імпортувати) відкритий (*public*) ключ викладача до списку сертифікатів. Відкритий ключ викладача може бути пересланий

електронною поштою або знаходитися в указаній викладачем папці, наприклад *КС і З*/*Лабораторна робота 9/Ключ викладача*. Ознайомитись зі структурою відкритого ключа.

4. Надіслати (експортувати) свій власний відкритий ключ викладачеві електронною поштою у вигляді вкладеного файла.

Завдання 2

Шифрування і підписання документів

1. Створити у редакторі *MS Word* документ із коротким звітом про виконану роботу (звіт може включати ілюстрації). Зберегти звіт у файлі.

2. Зашифрувати файл, використовуючи для цього свій закритий ключ і відкритий ключ викладача.

3. Відправити цей файл електронною поштою викладачу.

Завдання 3

Розшифрування документів і перевірка цифрових підписів

1. Знайти в указаній папці згідно з вашим варіантом або переслany вам електронною поштою зашифрований та підписаний закритим ключем викладача мультимедійній файл. Це може бути текстовий, графічний або GIF-анімаційний файл.

2. Розшифрувати файл і переконатись, що він дійсно дійшов від викладача і не був модифікований.

3. Закінчити звіт із лабораторної роботи, підписати файл цифровим підписом, використовуючи для цього свій закритий ключ і відкритий ключ викладача.

4. Відправити викладачеві звіт і файл цифрового підпису.

Увага! Після підписання файла не можна робити ніяких змін у цих файлах. Підпис не буде дійсним!

Завдання 4

Захист інформації засобами *Microsoft Office*

До будь-яких документів *Microsoft Office* можна додавати невидимий та додатково видимий цифровий підпис, який гарантує недоторканність документа та підтверджує авторство. Для більш надійного захисту особливо важливих документів необхідно придбати сертифікати за окрему плату у спеціалізованих незалежних центрах сертифікації. Для

менш важливих документів можна скористатись автопідтверджувальним власним сертифікатом.

Далі розглянуто дії для цифрового підписання документів *Microsoft Office 2013*. У других версіях можливі незначні зміни.

1. Створити автопідтверджувальний сертифікат можна в управлінні сертифікатами шифрування файлів комп'ютера. Для цього на комп'ютері включити *Пошук* і знайти *Управление сертификатами шифрования файлов*. За допомогою майстра створити новий сертифікат.

2. Створити будь-який документ *Microsoft Office* і захистити документ *невидимим цифровим підписом* за командою **Файл – Сведения-Защита документа – Добавить цифровую подпись**.

3. Додати до документа рядок *видимого підпису* за командою **Вставка – Текст – Строка подписи** і ввести необхідні параметри.

4. Підписати документ подвійним кліканням на зображені підпису, активізувати процес підписання і підписати документ видимим підписом. Якщо попередньо не було створено невидимого цифрового підпису, то на даному етапі він також буде створений. Зверніть увагу на те, що після підписання видимим або невидимим підписом документ не можна редагувати, інакше цифровий підпис буде видалений.

5. На нижньому рядку документа праворуч від вибору мови перевірки правопису знайти позначку *Этот документ содержит подписи.* Клікнувши на неї, відкрити вікно *Подписи.* У контекстному меню рядка підпису можна дізнатися інформацію про того, хто підписав документ.

6. Відправити документ разом зі звітом викладачеві.

Загальні відомості

У роботі розглядаються методи захисту мультимедійної інформації від несанкціонованого доступу і модифікації, зокрема метод несиметричного шифрування із *відкритим* (публічним) і *закритим* (секретним, приватним) ключами.

Одним із найкращих інструментів для несиметричного шифрування файлів і пошти є безкоштовна програма *Gpg4win*. Крім шифрування програма забезпечує цифровий криптографічний підпис, що дозволяє гарантувати, що файл надійшов саме від власника ключа і не був змінений третьою особою.

Пакет *Gpg4win* складається з таких компонентів:

GnuPG – ядро програми, яке виконує всі операції шифрування й створення цифрових підписів;

Kleopatra – менеджер ключів шифрування;

GPA – альтернативний менеджер ключів;

GpgOL – плагін для 32-бітних версій *Microsoft Outlook 2003/2007/ 2010/2013*;

GpgEX – плагін для провідника *Windows*, який додає дії з шифрування до контекстного меню файлів і папок;

Документація Gpg4win (англійською та німецькою мовами).

Установлення програми Gpg4win

Установлення *Gpg4win* не відрізняється від установлення більшості програм. На одному з етапів необхідно вибрати, які компоненти з описаних установлювати (рис. 16). Доцільно вибрати всі.

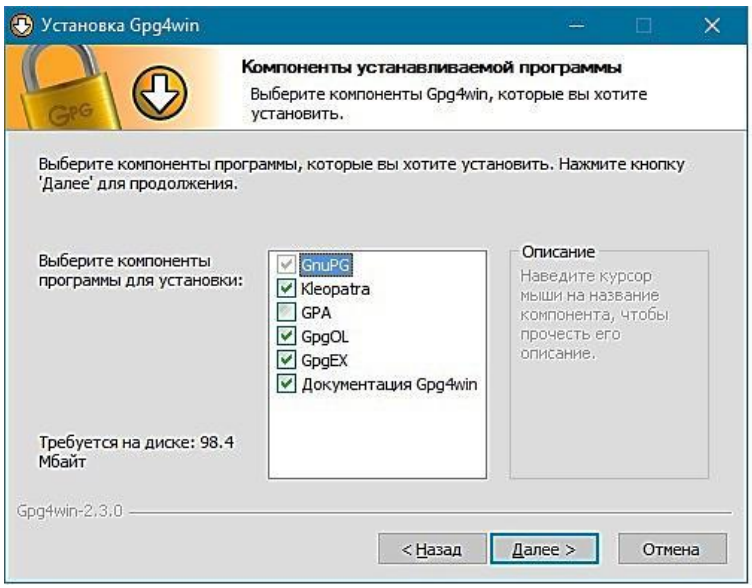


Рис. 16. **Вибір компонентів програми *Gpg4win***

Також потрібно буде вказати шлях для установлення (рекомендується залишити значення за замовчуванням) та указати, які ярлики створювати.

Після установлення можна приступати до застосування *Gpg4win*.

Створення ключів

На початку роботи з програмою *Gpg4win* необхідно створити пару ключів. Відкритий ключ необхідно передати своєму абоненту, з яким потрібно обмінюватись зашифрованими файлами та повідомленнями. Ваш абонент також повинен створити свою пару ключів і надіслати вам свій відкритий ключ.

Увага! Обмінюватись з будь-якими своїми закритими ключами не можна.

Створення ключів розглянемо на прикладі менеджера ключів *Kleopatra*. Такими ж можливостями володіє й альтернативний менеджер ключів *GPA*.

Запустити менеджер ключів *Kleopatra* (рис. 17).

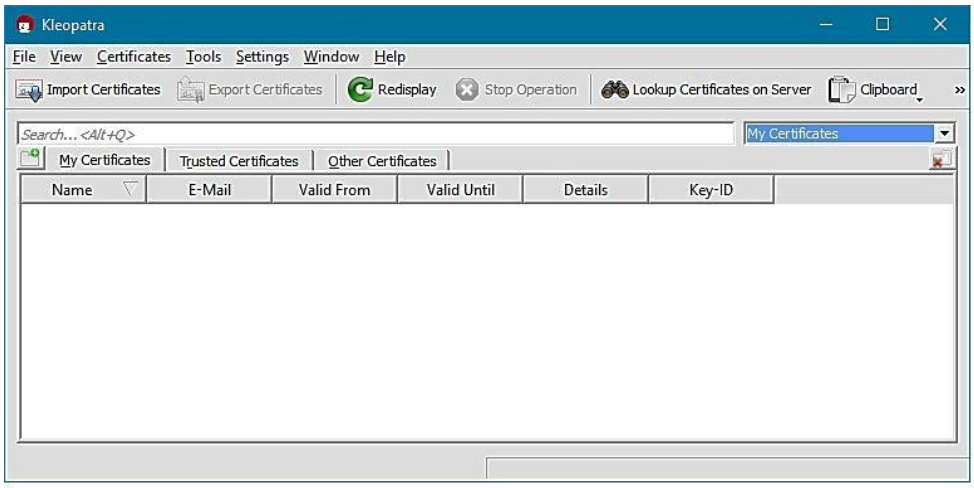


Рис. 17. **Менеджер ключів *Kleopatra***

Виконати команду **File – New Certificate…** й у вікні, яке з'явиться, вибрати стандарт ключів *OpenPGP* (рис. 18).

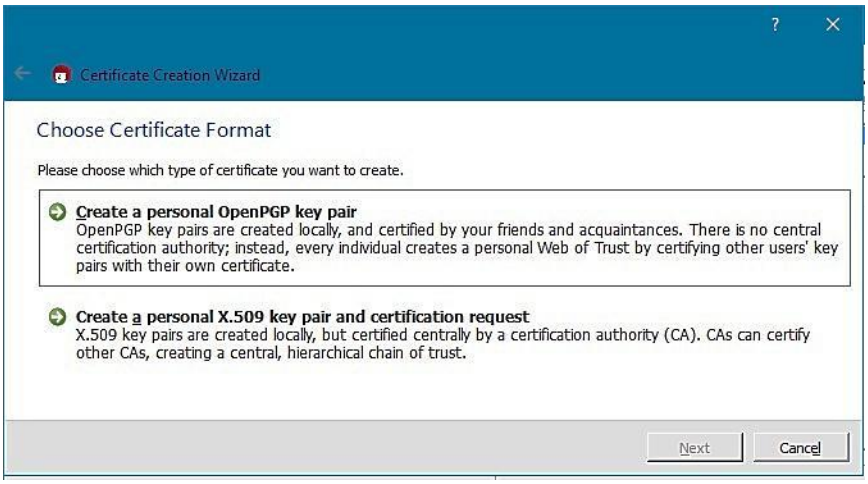


Рис. 18. **Вибір стандарту ключів**

Далі у новому вікні (рис. 19) заповнити форму з інформацією щодо власника ключа.

За допомогою кнопки *Advanced Settings*… можна вибрати технічні параметри ключів – алгоритм (*RSA* або *DSA*), за яким створюються ключі, розрядність ключів, а також для яких операцій призначені ключі – для *шифрування (Encryption)*, *підпису (Sign)*, *сертифікації (Certification)*

або *аутентифікації (Authentication)*. Тут можна вказати термін дії пари ключів, після закінчення якого необхідно змінити ключі. Рекомендується залишити все за замовчуванням.

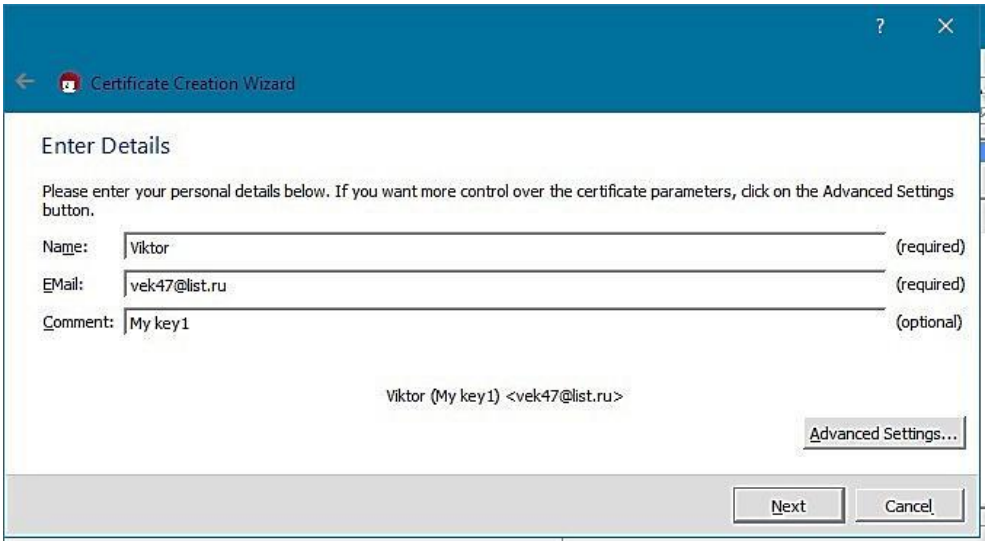


Рис. 19. **Інформація щодо власника ключа**

У наступному вікні (рис. 20) показані всі деталі ключів, які створюються.

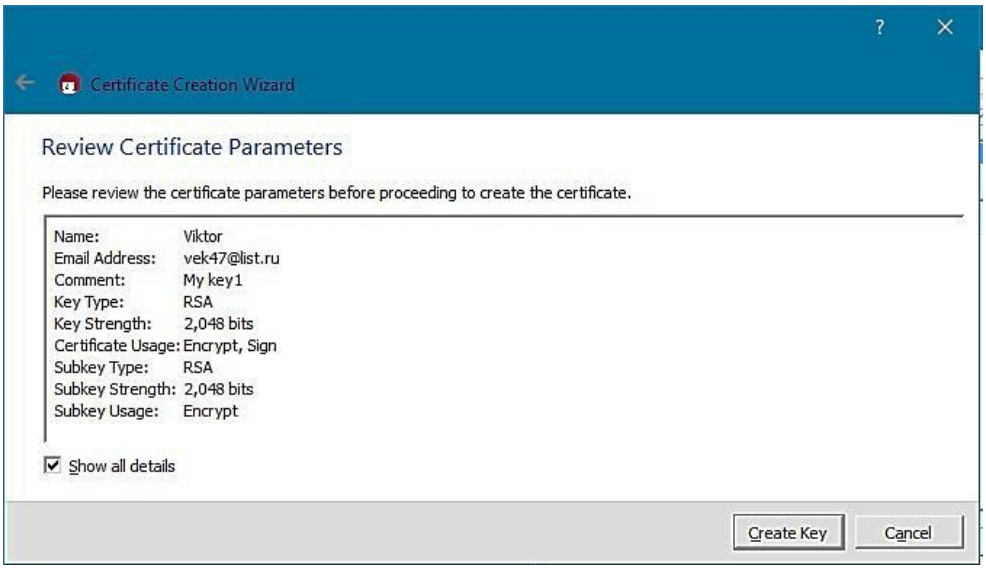


Рис. 20. **Параметри ключа**

Якщо все влаштовує, то натиснути на кнопку *Generate Key (генерувати ключ)*. З'явиться вікно, в якому необхідно ввести парольну фразу для шифрування закритого ключа. Він потрібен для того, щоб тільки власник мав доступ до закритого ключа і, відповідно, до зашифрованих даних. Крім того, пароль може захистити ключ, якщо він буде викрадений.

У наступному вікні можна створити резервну копію ключів, зберегти її у файлі, відправити електронною поштою відкритий ключ. Натиснувши на кнопку *Finish,* з'явиться вікно *Kleopatra* зі створеною парою ключів (рис. 21).

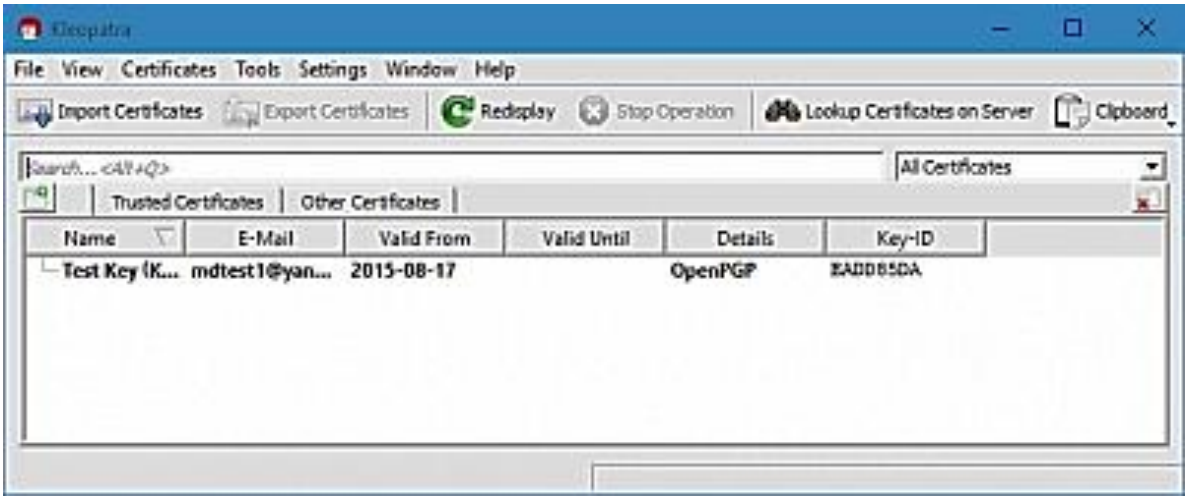


Рис. 21. **Створені ключі**

Обмін ключами

Якщо абонент створив на своєму комп'ютері свою пару ключів за таким самим алгоритмом, то можна з ним обмінятися відкритими ключами і ввести їх до списку своїх ключів.

Відправлення (експорт) свого відкритого ключа відбувається за командою ***File – Export Certificates***. Програма запропонує зберегти його як звичайний текстовий файл із розширенням *.asc*. Після збереження можна переглянути вміст файла. Далі файл відправляється абоненту електронною поштою або будь-яким іншим засобом.

Додавання надісланого відкритого ключа абонента до списку своїх ключів відбувається за командою ***File – Import Certificates*** і обранням файла із розширенням *asc*, який надіслав абонент. Буде виведено повідомлення про те, що ключ імпортовано і в списку ключів *Kleopatra* з'явиться відкритий ключ абонента (рис. 22).

Подвійним кліканням на ньому можна проглянути інформацію про цей ключ.

Шифрування файлів

Відбувається за командою ***File – Sign/Encrypt Files*** **(Файл – Підписати/Зашифрувати)** або вибором із контекстного меню фала команди **Подписать и Зашифровать**.

Рис. 22. **Відкритий ключ абонента імпортовано**

У вікні, що з'явиться, необхідно обрати необхідні дії з файлом – *Sign and Encrypt (Підписати і Зашифрувати), Encrypt (Зашифрувати), Sign (Підписати)*.

Якщо прапорець *Text Output (ASCII amor)* установлено, то у результаті шифрування буде створено не бінарний файл із розширенням *.gpg*, а текстовий файл із розширенням *.asc*, який можна переглянути і вставити у текст електронного листа. На етапі засвоєння програми *gpg4win*, доцільно встановлювати цей прапорець.

Якщо вибрані дії *Підписати і Зашифрувати* або *Зашифрувати*, то у верхній частині наступного вікна (рис. 23) необхідно виділити ключі абонентів (один або декілька), для яких призначені *зашифрований* або *зашифрований і підписаний файл*.

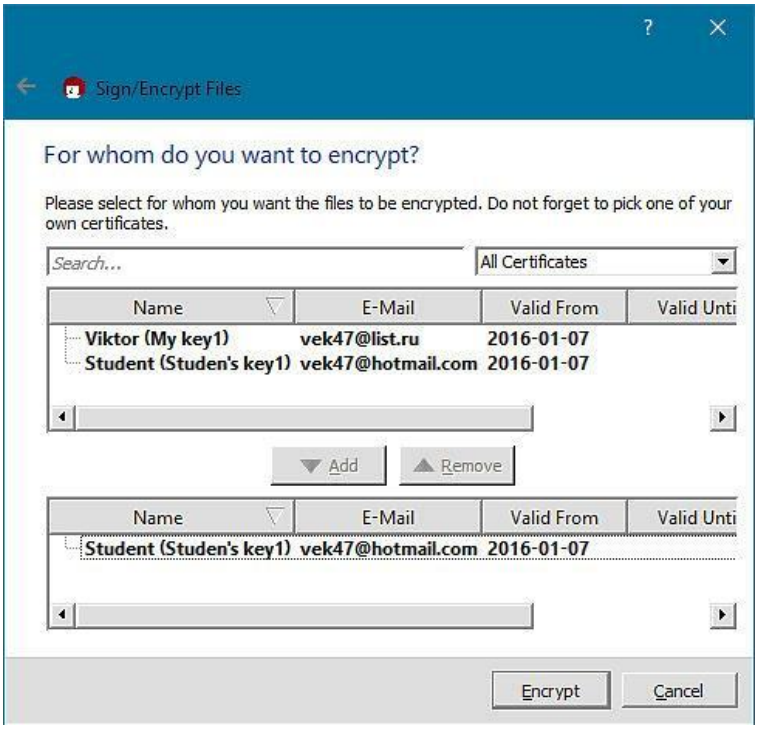


Рис. 23. **Підготовка до розшифрування файла**

Обрані ключі додати у нижню частину вікна (кнопка *Add*). Результатом обраних дій буде зашифрований файл із розширенням *.gpg* або *.asc*, який необхідно вислати тим абонентам, відкритті ключі яких додавались до *шифрування* або *шифрування і підписання*. Наприклад, результатом шифрування файла *Договір.doc* буде файл *Договір.doc.gpg* або *Договір.doc.asc* залежно від обраного режиму прапорця *Text Output (ASCII amor)* у попередньому вікні.

Якщо необхідно лише підписати файл без шифрування, то з'явиться вікно іншої форми, де всі параметри можна залишити за замовчуванням. У цьому разі буде сформований додатковий зашифрований файл підпису з розширенням *Договір.doc.sig*, який разом із незашифрованим файлом-оригіналом *Договір.doc* необхідно надіслати всім зацікавленим абонентам, у яких є відкритий ключ відправника файлів.

Розшифрування файлів і перевірка підпису

Відбувається за командою ***File – Decrypt/Verify Files*** **(Файл – Розшифрувати/Перевірити)** або вибором із контекстного меню файла команди **Расшифровать и проверить**.

Після обрання папки для розшифрованих файлів і натиснення на кнопку *Decrypt/Verify* необхідно підтвердити особу одержувача введенням парольної фрази до свого ключа. Результат розшифрування і перевірки підпису відображається у спеціальному вікні (рис. 24), а розшифрований файл з'являється у вибраній папці.

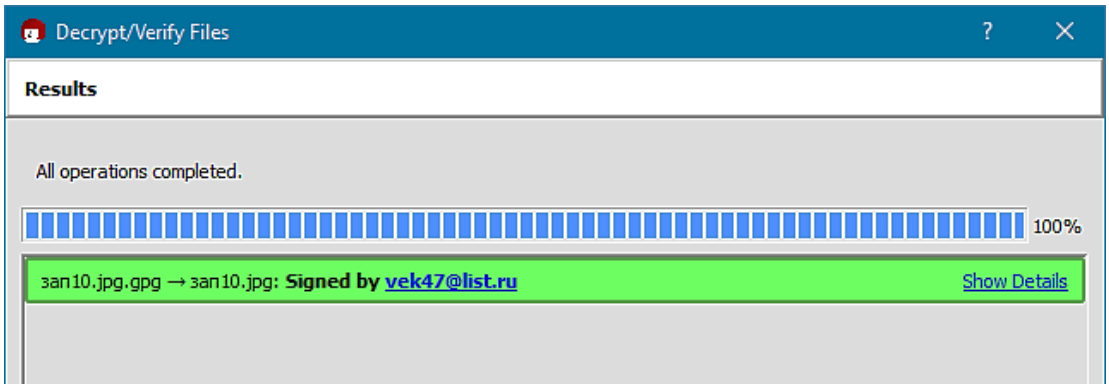


Рис. 24. **Результати розшифрування і перевірки цифрового підпису незміненого файла**

Якщо файл або його цифровий підпис було змінено, то прийнято вважати, що файл скомпроментовано і в цьому випадку з'явиться вікно з відповідним повідомленням (рис. 25).

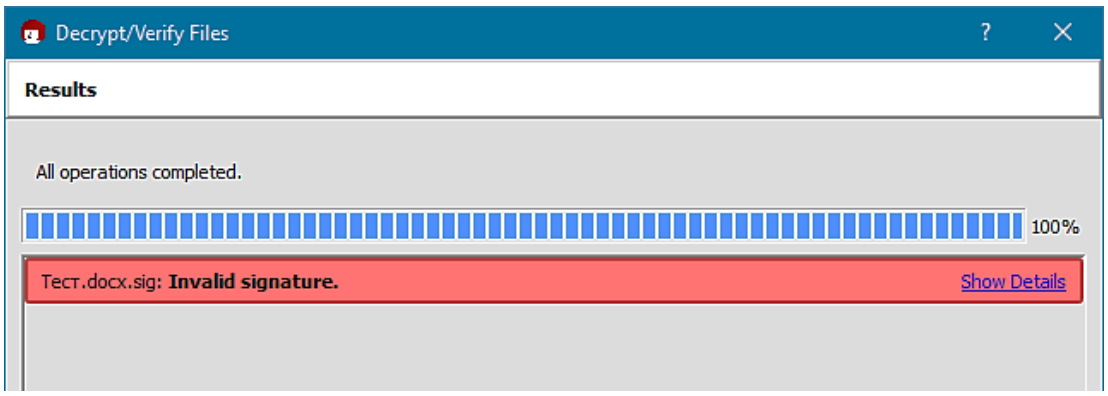


Рис. 25. **Результати розшифрування і перевірки цифрового підпису модифікованого файла або цифрового підпису**

Під час підтвердження тільки підписаних, але не зашифрованих файлів, необхідно, щоб були доступні обидва файли – файл підпису і файл оригіналу. Якщо вони знаходяться в одній папці, то програма сама знаходить необхідний файл оригіналу і після натиснення на кнопку *Decrypt/Verify* підтверджує або не підтверджує його цілісність. Якщо файли знаходяться в різних папках, то у вікні *Signed data* необхідно спочатку вказати шлях до файла оригіналу.

Контрольні запитання

1. Які методи захисту інформації ви знаєте?
2. Назвіть ситуації, коли необхідно застосовувати засоби шифрування інформації в мультимедійному видавництві.
3. Чому фізичний захист не може гарантувати безпеку?
4. У чому відмінність симетричних і несиметричних алгоритмів шифрування?
5. Що буде, якщо зробити спробу відредагувати підписаний документ?
6. Назвіть основні помилки під час вибору паролів.
7. Що таке сертифікат і як можна його здобути?
8. Яку кримінальну відповідальність визначають закони України за комп'ютерні злочини?
9. Що таке цифровий підпис?
10. Чи захищає цифровий підпис від несанкціонованого доступу чи модифікації?
11. Назвіть можливості програми *Gpg4win*.

Рекомендована література

1. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима. – М. : Изд. BHV, 2001. – 320 с.

2. Климнюк В. Є. Комп'ютерні мережі та захист інформації : конспект лекцій. Ч. 1 / В. Є. Климнюк, В. М. Гіковатий. – Х. : Вид. ХНЕУ, 2008. – 96 с.

3. Климнюк В. Є. Комп'ютерні мережі та захист інформації : конспект лекцій / В. Є. Климнюк. – Х. : Вид. ХНЕУ, 2011. – 129 с.

4. Колисниченко Д. Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание / Д. Н. Колисниченко. – 2-е изд., перераб. и доп. – СПб. : Наука и техника, 2006. – 448 с.

5. Методичні рекомендації до самостійної роботи з навчальної дисципліни "Комп'ютерні мережі та захист інформації" для студентів напряму підготовки 6.051501 "Видавничо-поліграфічна справа" всіх форм навчання / укл. В. Є. Климнюк. – Х. : Вид. ХНЕУ, 2014. – 60 с.

6. Олифер В. Г. Компьютерные сети. Принципы, технологи, протоколы : учебник для вузов / В. Г. Олифер, Н. Г. Олифер. – 3-е изд. – СПб. : [б. и.], 2006. – 958 с.

7. Таненбаум Э. Компьютерные сети / Э. Таненбаум ; пер. с англ. – 4-е изд. – СПб. : Питер, 2006. – 991 с.

8. Захист сайтів та їх безпека [Електронний ресурс]. – Режим доступу : www.bug.kpi.ua.

9. Как подключить компьютер к компьютеру – по сети, по WiFi и через USB [Электронный ресурс]. – Режим доступа : http://nastroisam.ru/kompyuter-k-kompyuteru.

10. Портал Безпека [Електронний ресурс]. – Режим доступу : www.bezpeka.com.

11. Шифрование с помощью GnuPG для пользователей [Электронный ресурс]. – Режим доступа : http://jenyay.net/blog/2012/01/04/shifrovanie-s-pomoshhyu-gnupg-dlya-polzovatelejj/.

НАВЧАЛЬНЕ ВИДАННЯ

Методичні рекомендації до виконання лабораторних робіт з навчальної дисципліни "КОМП'ЮТЕРНІ МЕРЕЖІ ТА ЗАХИСТ ІНФОРМАЦІЇ"

для студентів напряму підготовки 6.051501 "Видавничо-поліграфічна справа" всіх форм навчання

Укладач **Климнюк** Віктор Євгенович

Відповідальний за випуск *О. І. Пушкар*

Редактор *В. В. Міхно*

Коректор *В. О. Бутенко*

План 2016 р. Поз. № 99.
Підп. до друку 19.07.2016 р. Формат 60×90 1/16. Папір офсетний. Друк цифровий.
Ум. друк. арк. 4,0 Обл.-вид. арк. 5,0. Тираж 40 пр. Зам. № 127.

Видавець і виготівник – ХНЕУ ім. С. Кузнеця, 61166, м. Харків, просп. Науки, 9-А

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру ***ДК № 4853 від 20.02.2015 р.***