МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

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

Харків. Вид. ХНЕУ ім. С. Кузнеця, 2014

Затверджено на засіданні кафедри комп'ютерних систем і технологій.
Протокол № 4 від 06.12.2013 р.

Укладач Климнюк В. Є.

М54 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 ім. С. Кузнеця, 2014. – 60 с. (Укр. мов.)

Наведено методи, засоби та завдання для організації самостійного вивчення й поглиблення отриманих у рамках лекційного курсу, а також аудиторних лабораторних робіт компетентностей, знань, вмінь та навичок. Подано перелік необхідної для виконання завдань літератури і додатки, що містять довідкову інформацію.

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

Вступ

Навчальна дисципліна "Комп'ютерні мережі та захист інформації" є вибірковою і вивчається студентами напряму підготовки "Видавничо-поліграфічна справа" спеціалізації "Технології електронних мультимедійних видань" усіх форм навчання протягом шостого семестру навчання. Дисципліна потребує від студентів інтенсивної самостійної роботи над спеціальною літературою та програмним забезпеченням у час, вільний від обов'язкових навчальних занять. До методичних рекомендацій включені теми, які не розглядалися раніше в методичних рекомендаціях до лабораторних робіт [4].

Метою самостійної роботи є поглиблення знань, які було отримано на лекційних заняттях, та підтвердження і реалізація навичок, що були сформовані на лабораторних та практичних заняттях з дисципліни "Комп'ютерні мережі та захист інформації". Важливим завданням є формування компетентностей, що дозволяють студенту реалізовувати на практиці отримані знання.

Така робота потребує від студентів інтенсивної самостійної роботи над спеціальними інформаційними джерелами та інструментальними засобами, що дозволяють більш ефективно застосовувати сучасні автоматизовані системи проектування.

Студентам потрібно ознайомитись з конкретними реалізаціями мережних функцій та методами захисту інформації у різних операційних системах, провести пошук інформації в Інтернеті, а також додаткову роботу з налагодження мереж у комп'ютерних класах.

Основні види самостійної роботи, які запропоновані студентам з дисципліни:

вивчення лекційного матеріалу;

робота з вивчення рекомендованої літератури;

вивчення основних термінів та понять за темами дисципліни;

підготовка до лабораторних занять;

перевірка особистих знань за запитаннями для самостійного контролю та виконання контрольних завдань.

Для закріплення і перевірки набутих компетентностей під час самостійної роботи до кожної роботи пропонуються довідкові матеріали, практичні завдання і запитання для самодіагностики.

Змістовий модуль 1. Основи організації комп'ютерних мереж

Тема 1. Загальні відомості про комп'ютерні мережі

Самостійна робота № 1. Характеристика оптоволоконних ліній зв'язку

Мета роботи: отримання додаткових знань з найсучаснішими лініями зв'язку на основі оптоволокна.

У результаті виконання самостійної роботи у студента формуються **компетентності:** здатність самостійно вивчати нові технології, які підвищують ефективність комп'ютерних мереж.

Результатом виконання самостійної роботи є звіт з виконання завдання.

Завдання для самостійної роботи

1. Вивчити довідкові матеріали до самостійної роботи і вказану літературу.
2. Звести характеристики оптоволокна у компактну таблицю окремо для різних класів – одномодового оптоволокна, багатомодового волокна, та оптоволокна із ступінчастим профілем розподілу показників заломлення.
3. Знайти самостійно інформацію про ціни, характеристики та можливості переходу на оптоволоконну технологію у вашому місті, зокрема у Харкові.

Контрольні запитання для самодіагностики

1. Розкрити принцип дії оптоволокна для передачі сигналів.
2. Які типи оптоволокна ви знаєте? Чим вони відрізняються?
3. Які переваги оптоволоконних кабелів порівняно з дротовими ви знаєте?
4. Назвати основні характеристики оптоволокна з дальності і швидкості передачі інформації.
5. Перелічити недоліки оптоволоконної технології.
6. Які основні топології мереж створюються оптоволоконними кабелями?
7. Перелічити інші області застосування оптоволоконної технології.

Довідкові матеріали до самостійної роботи

Оптичне волокно – нитка з оптично прозорого матеріалу (скло, пластик), яка використовується для перенесення світла усередині себе за допомогою повного внутрішнього відзеркалення.

Волоконна оптика – розділ прикладної науки і машинобудування, що описує такі волокна. Кабелі на базі оптичних волокон використовуються у волоконно-оптичному зв'язку, що дозволяє передавати інформацію на великі відстані з більш високою швидкістю передачі даних, ніж в електронних засобах зв'язку.

Скляні оптичні волокна робляться з кварцового скла, але для далекого інфрачервоного діапазону можуть використовуватися інші матеріали, зокрема пластик. Як і кварцове скло, вони мають показник заломлення близько 1,5.

Волокно складається з сердечника, покриття що віддзеркалює, захисного лаку і буфера. Щоб утримати світловий сигнал всередині сердечника використовується оболонка, яка відіграє роль відбиваючого шару. У даному випадку йдеться про так зване повне внутрішнє відбиття світла від кордону двох речовин з різними коефіцієнтами заломлення (у скляної оболонки коефіцієнт заломлення значно нижче, ніж у центрального волокна). Оптичний кабель влаштований так, що всередині нього безліч оптичних волокон. Волокна від пошкодження захищає буфер (м'який захисний матеріал), який у свою чергу має жорстке покриття.

Металеве обплетення кабелю зазвичай відсутнє, так як екранування від зовнішніх електромагнітних перешкод тут не потрібне, однак іноді його все-таки застосовують для механічного захисту від навколишнього середовища (такий кабель іноді називають броньовим, він може об'єднувати під однією оболонкою кілька оптоволоконних кабелів).

На рис. 1 можна побачити структуру оптичного волокна.

Розмір сердечника для одномодового волокна складає 9 мкм, для багатомодового – 50 або 62,5 мкм. Найчастіше для багатомодового волокна використовують сердечники розміром 50 мкм. Зовнішній діаметр оболонки оптичного волокна зазвичай стандартний – 125 мкм. Оптоволокно маркується залежно від співвідношення розміру сердечника й оболонки.

Оптоволоконний кабель (він же волоконно-оптичний) – це принципово інший тип кабелю порівняно з іншими типами електричних або

мідних кабелів. Інформація по ньому передається не електричним сигналом, а світловим. Головний його елемент – це прозоре скловолокно, по якому світло проходить на величезні відстані з незначним ослабленням.

Рис. 1. **Структура оптичного волокна**

Оптоволоконний кабель володіє винятковими характеристиками по перешкодозахищеності та секретності переданої інформації. Ніякі зовнішні електромагнітні перешкоди в принципі не здатні спотворити світловий сигнал, а сам цей сигнал принципово не породжує зовнішніх електромагнітних випромінювань. Підключитися до цього типу кабелю для несанкціонованого прослуховування мережі практично неможливо, так як це вимагає порушення цілісності кабелю. Теоретично можлива смуга пропускання такого кабелю досягає величини 1012 Гц, що незрівнянно вище, ніж у будь-яких електричних кабелів. Вартість оптоволоконного кабелю постійно знижується і зараз приблизно дорівнює вартості тонкого коаксіального кабелю. Проте в даному випадку необхідне застосування спеціальних оптичних приймачів і передавачів, що перетворюють світлові сигнали в електричні і навпаки, що часом істотно збільшує вартість мережі в цілому.

Типова величина загасання сигналу в оптоволоконних кабелях на частотах, що використовуються в локальних мережах, становить близько

5 дБ/км, що приблизно відповідає показникам електричних кабелів на низьких частотах. Але у випадку оптоволоконного кабелю у процесі зростання частоти переданого сигналу загасання збільшується дуже незначно, і на великих частотах (особливо понад 200 МГц) його переваги перед електричним кабелем незаперечні, він просто не має конкурентів.

Основне застосування оптичні волокна знаходять як середовища передачі на волоконно-оптичних телекомунікаційних мережах різних рівнів: від міжконтинентальних магістралей до домашніх комп'ютерних мереж. Застосування оптичних волокон для ліній зв'язку обумовлено тим, що оптичне волокно забезпечує високу захищеність від несанкціонованого доступу, низьке загасання сигналу під час передачі інформації на великі відстані та можливість оперувати з надзвичайно високими швидкостями передачі. Вже у 2006 р. була досягнута швидкість модуляції 111 ГГц [2; 3], у той час як швидкості 10 і 40 Гбіт/с стали вже стандартними швидкостями передачі по одному каналу оптичного волокна. При цьому кожне волокно, використовуючи технологію спектрального ущільнення каналів, може передавати до декількох сотень каналів одночасно, забезпечуючи загальну швидкість передачі інформації, що обчислюється Терабітами за секунду. Так, у 2003 р. була досягнута швидкість 10,72 Тбіт/с [4], а у 2012 – 20 Тбіт/с.

У ході експериментів максимальна дальність передачі склала 3 200 кілометрів на швидкості 1 Тбіт/с.

Виділяють декілька класів оптоволокон за особливостями структури і принципом дії:

одномодові оптоволокна;

багатомодові оптоволокна;

оптоволокна з градієнтним показником заломлення;

оптоволокна із ступінчастим профілем розподілу показників заломлення.

Через фізичні властивості оптоволокна необхідні спеціальні методи для їх з'єднання з обладнанням. Оптоволокна є базою для різних типів кабелів (рис. 2), залежно від того, де вони будуть використовуватися.

Ємність оптичного кабелю визначається кількістю волокон, яких може бути в одному кабелі 48 і більше. Таким чином, при монтажі ВОЛЗ, у більшості випадків, досить прокласти 1 оптичний кабель потрібної ємності.

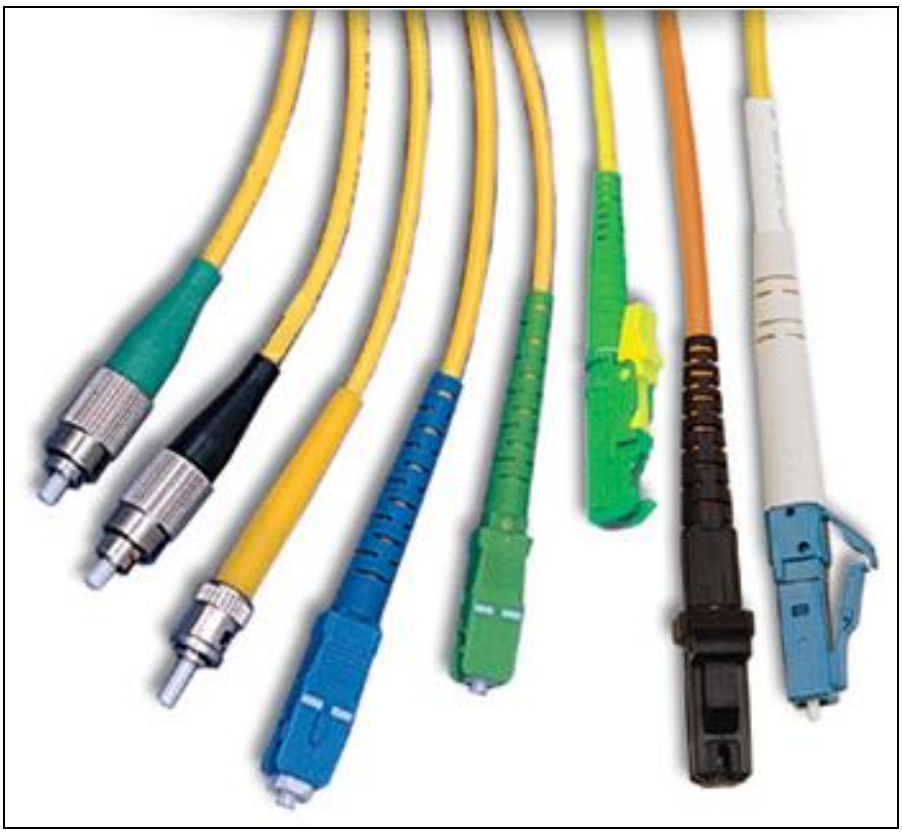

Рис. 2. **Кабелі на основі оптоволокна**

Мережа утворюється за допомогою оптоволоконних модемів – пристроїв, які забезпечують передачу і прийом потоку з оптичного волокна. Оптоволоконні модеми встановлюються на розподільних вузлах і об'єднуються оптоволоконним кабелем. Максимальна відстань між модемами становить близько 140 км, але більшість з них добиває тільки на 100 км. Але при цьому використовуються підсилювачі для якісної передачі сигналу.

Переваги оптоволоконних модемів перед дротяними полягають у більш високій пропускній здатності, більшій дальності передачі сигналу, підвищеній захищеності даних, стійкості до перешкод і стрибків напруги. Дальність передачі даних між модемами залежить від типу джерела світла і типу волокна.

Оптоволоконні модеми (рис. 3), як і решта модемів, можуть випускатися в декількох виконаннях: настільному, портативному і стійковому. Настільні оптоволоконні модеми мають окремий корпус і блок живлення. Приєднуються до комп'ютера за допомогою кабелю, що з'єднує комутаційний порт пристрою та порт ПК. Настільні модеми сумісні з будь-якими комп'ютерами або термінальними пристроями.

Рис. 3. **Оптоволоконні модеми**

Застосовують оптоволоконний кабель тільки в мережах з топологією "зірка" і "кільце". Ніяких проблем узгодження і заземлення в даному випадку не існує. Кабель забезпечує ідеальну гальванічну розв'язку комп'ютерів мережі. У майбутньому цей тип кабелю, ймовірно, витіснить електричні кабелі всіх типів або, у всякому разі, сильно потіснить їх. Запаси міді на планеті виснажуються, а сировини для виробництва скла більш ніж достатньо.

Недоліки оптоволоконної технології зв'язку

Оптоволоконний кабель має і деякі недоліки. Найголовніший з них – висока складність монтажу (у процесі установки роз'ємів необхідна мікронна точність, від точності відколу скловолокна і ступеня його полірування сильно залежить загасання в роз'ємі). Для установки роз'ємів застосовують зварювання або склеювання за допомогою спеціального гелю, що має такий же коефіцієнт заломлення світла, що і скловолокно. У кожному разі для цього потрібна висока кваліфікація персоналу і спеціальні інструменти. Тому найчастіше оптоволоконний кабель продається у вигляді заздалегідь нарізаних шматків різної довжини, на обох кінцях яких вже встановлені роз'єми потрібного типу.

Хоча оптоволоконні кабелі і допускають розгалуження сигналів (для цього випускаються спеціальні розгалужувачі на 2 – 8 каналів), як правило, їх використовують для передачі. Адже будь-яке розгалуження неминуче сильно послаблює світловий сигнал, і якщо розгалужень буде багато, то світло може просто не дійти до кінця мережі.

Оптоволоконний кабель менш міцний, ніж електричний, і менш гнучкий (типова величина допустимого радіуса вигину становить близько 10 – 20 см). Чутливий він і до іонізуючих випромінювань, через які знижується прозорість скловолокна, тобто збільшується загасання сигналу. Чутливий він також до різких перепадів температури, в результаті яких скловолокно може тріснути. В даний час випускаються оптичні кабелі з радіаційно стійкого скла (коштують вони, звичайно, дорожче).

Оптоволоконні кабелі чутливі також до механічних впливів (удари, ультразвук) – так званий мікрофонний ефект. Для його зменшення використовують м'які звукопоглинальні оболонки.

Необхідно також відзначити й інші області застосування оптоволоконних технологій.

Оптичні волокна широко використовуються для освітлення. Вони використовуються як світлопроводи в медичних та інших цілях, де яскраве світло необхідно доставити у важкодоступну зону. У деяких будівлях оптичні волокна направляють сонячне світло з даху в якунебудь частину будівлі. Волоконно-оптичне світло може використовуватися в декоративних цілях, включаючи комерційну рекламу, мистецтво і штучні різдвяні ялинки.

Оптичне волокно також використовується для формування зображення. Пучок світла, переданий оптичним волокном, іноді використовується разом з лінзами – наприклад, в ендоскопі, який використовується для перегляду об'єктів через маленький отвір.

Література: основна [2]; ресурси мережі Інтернет [14].

Самостійна робота № 2. Створення й налаштування мережі Домашня група

Мета роботи: отримання практичних навичок зі створення й налаштування мережі комп'ютерів під управлінням операційної системи Windows 7.

У результаті виконання самостійної роботи у студента формуються **компетентності:** здатність проводити монтаж і налагодження простих локальних мереж.

Результатом виконання самостійної роботи є створення Домашньої групи і налаштування прав доступу.

Завдання для самостійної роботи

1. Вивчити довідкові матеріали до самостійної роботи і вказану літературу.
2. Створити мережу Домашня група з комп'ютерів лабораторії під управлінням Windows 7.
3. На студентському диску (D:) створити і зробити доступним дві папки, причому одну з правом повного доступу, а іншу тільки для читання.
4. Створити в кожній папці по 2 файли (короткі документи Word) і встановити для них такі ж права, що і для папок.
5. Те ж саме виконати з "чужими" файлами і папками на своєму комп'ютері. Які повідомлення про помилки будуть видані при спробі виконати недозволені дії з об'єктами?
6. Перемістити одну з раніше створених папок в іншу. Дослідити, як права доступу розповсюджуються на вкладені папки при різних моделях доступу.
7. Підключити і виключити спадкування права від батьківських об'єктів.
8. Надати права доступу на ресурси (папки, файли) іншим користувачам і перевірити можливість користуватись ними.

Контрольні запитання для самодіагностики

1. З якою метою створюється мережа Домашня група?
2. Яким чином Домашня група захищається від несанкціонованого доступу?
3. Як змінити права доступу до мультимедійної інформації в домашній групі?
4. Перелічити можливі права доступу для ресурсів (папок, файлів).
5. Як управляти правами доступу користувачів до ресурсів?

Довідкові матеріали до самостійної роботи

Усі основні настройки, які стосуються роботи з мережею в Windows 7, зібрані у вікні *Центр управления сетями и общим доступом* – Network and Sharing Center (рис. 4).

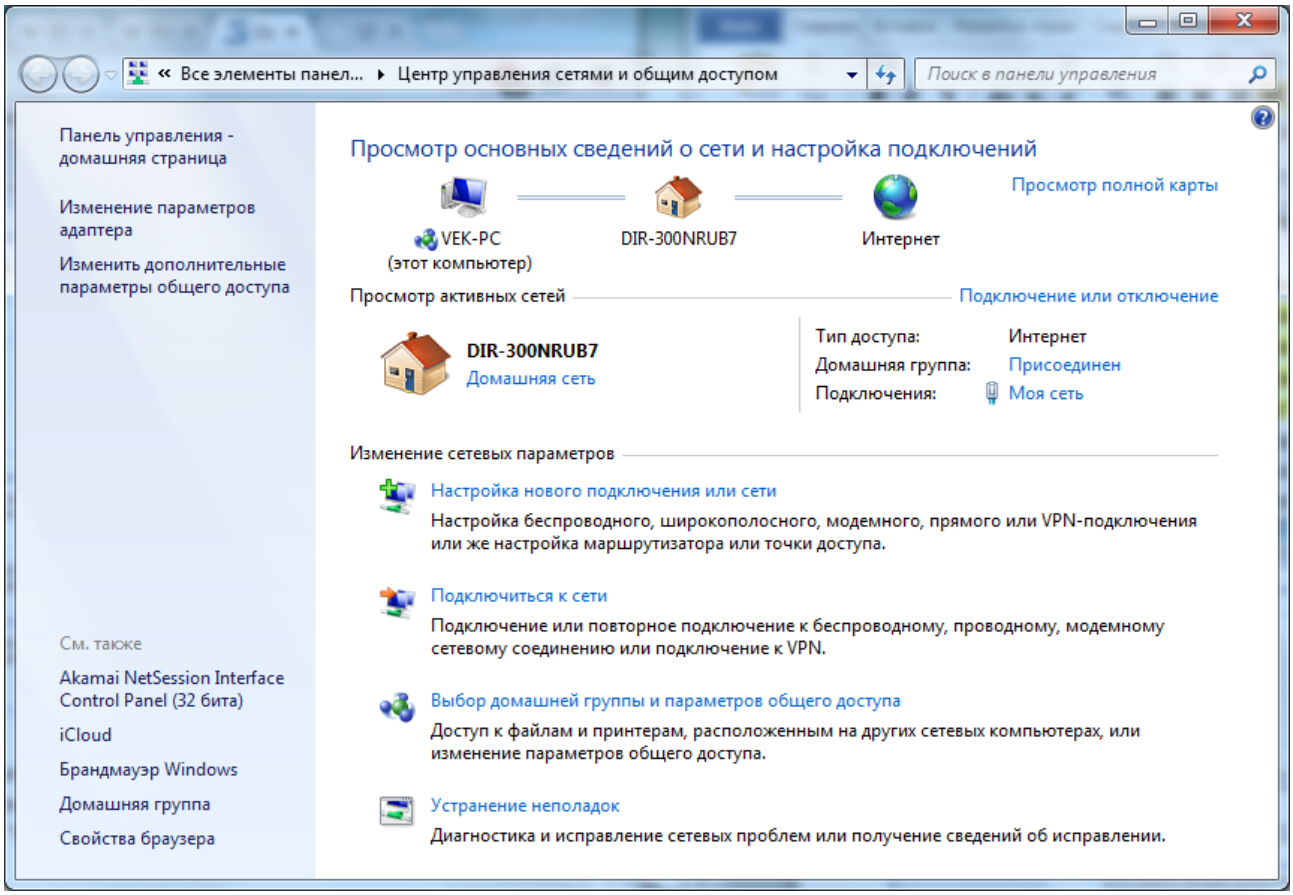

Рис. 4. **Вікно *Центр управления сетями и общим доступом***

Домашня група (HomeGroup) дозволяє організувати швидкий обмін даними між комп'ютерами, які підключені до домашньої локальної мережі.

Якщо на кожному з цих ПК встановлена Windows 7, то працювати із збереженими на них даними набагато простіше. Для того щоб отримати доступ до файлів, папок, загальних пристроїв, які є частиною домашньої групи, не потрібно щоразу вводити паролі. Досить вибрати на кожному комп'ютері папки та пристрої, які будуть спільними, і до них можна буде швидко отримати доступ з будь-якого комп'ютера в домашній мережі.

Домашні групи можуть бути створені тільки між комп'ютерами, які працюють під управлінням Windows 7.

Настройку домашньої групи можна здійснити з панелі управління – розділ *Домашняя группа*.

Для створення домашньої групи необхідно відкрити вікно *Центр управления сетями и общим доступом*, яке доступне з панелі управлін-

ня або після клацання миші по значку *Сеть* на Панелі задач. У розділі *Просмотр активных сетей (View your active networks)* можна побачити тип мережі, до якої підключений комп'ютер, наприклад, *Домашня мережа*.

Якщо в мережі ще немає домашніх груп, то доступне посилання *Готовность к созданию (Ready to create)*, яке запустить Майстер створення Домашньої групи.

На першому етапі створення домашньої групи необхідно визначитися з тим, до яких даних буде наданий спільний доступ. На цьому етапі неможливо додати до списку загальнодоступних елементів окремі папки, можна лише вказати, чи потрібно відкривати спільний доступ до принтерів, а також до стандартних бібліотек – зображення, Документи, Музика та Відео (рис. 5).

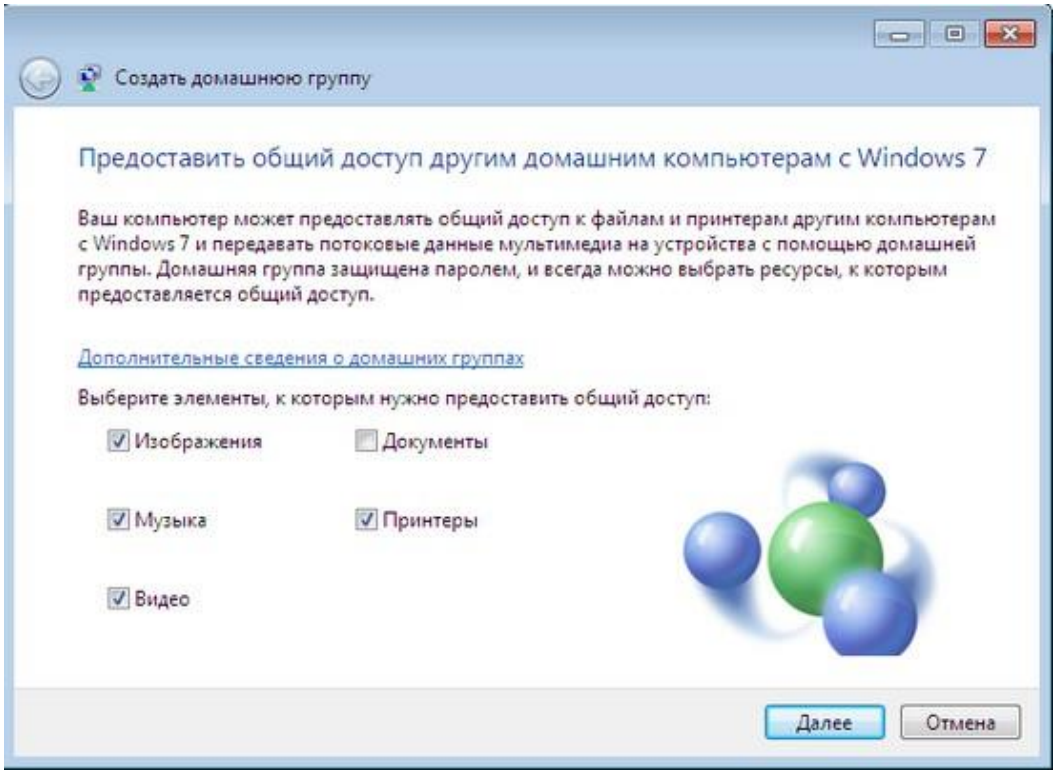

Рис. 5. **Вікно вибору загальнодоступних ресурсів**

Створення домашньої групи займе декілька секунд, після чого Windows згенерує пароль, який буде потрібен для додавання інших комп'ютерів у домашню групу (рис. 6). Оскільки цей пароль важко запам'ятати, на всіх комп'ютерах, які будуть приєднані до домашньої групи, для зручності його можна роздрукувати, скориставшись розміщеним тут посиланням. Вказати власний пароль на цьому етапі неможливо, проте його можна пізніше змінити в настройках домашньої групи.

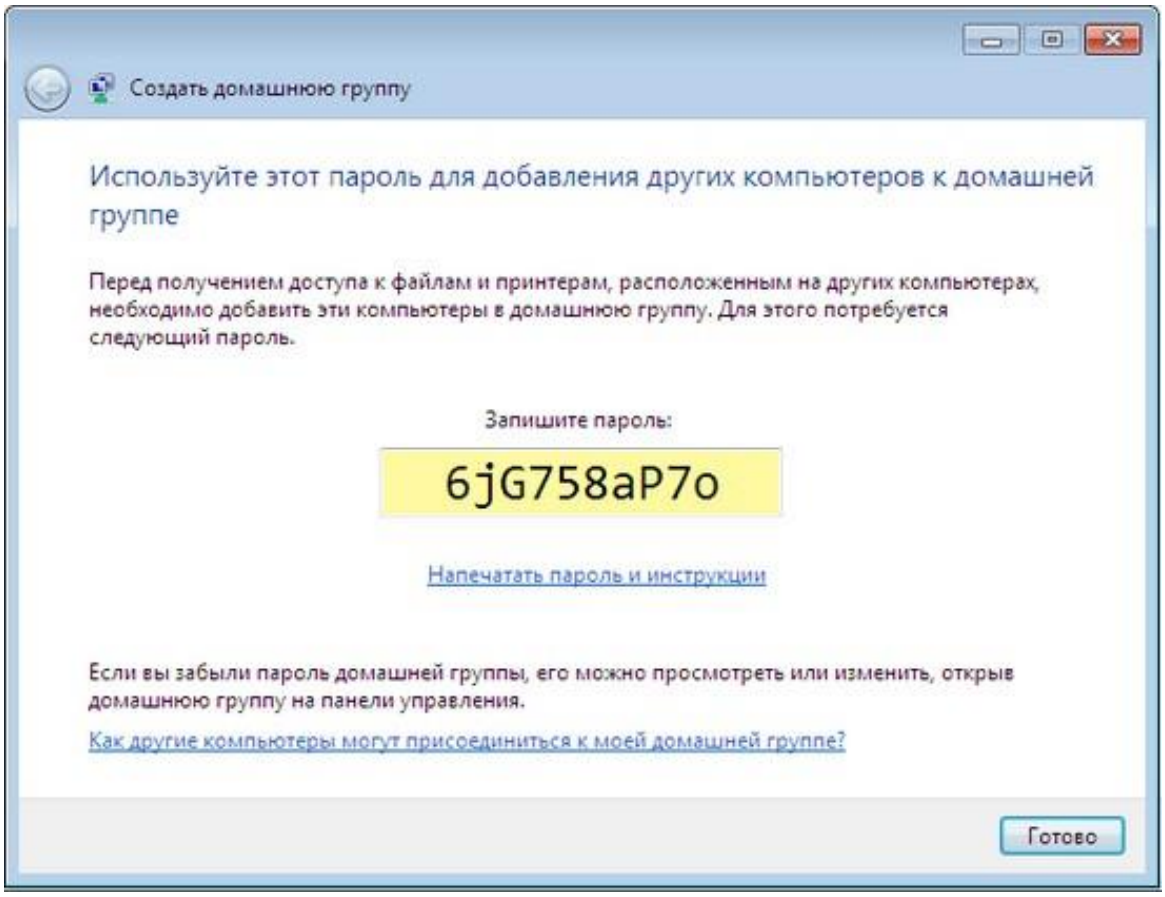

Рис. 6. **Вікно генерації пароля домашньої групи**

Після натискання кнопки *Готово* Майстер відкриє вікно налаштувань домашньої групи, в якому можна буде змінити параметри спільного доступу до різних типів даних, переглянути пароль або змінити його (рис. 7).

У процесі зміни пароля потрібно переконатися, що в домашній мережі немає комп'ютерів, які знаходяться в сплячому режимі. Після зміни пароля його необхідно буде змінити на всіх комп'ютерах, підключених до домашньої групи. Саме тому автоматично згенерований пароль набагато зручніше міняти відразу після створення домашньої групи, ще до того, як приєднаєте до неї інші комп'ютери.

Приєднання до домашньої групи здійснюється в тому ж вікні *Центр управления сетями и общим доступом*. Після того, як у локальній мережі створена домашня група, на інших комп'ютерах у розділі *Просмотр активных сетей* можна побачити посилання *Готовность к присоединению*. Клацнувши по ньому, необхідно вказати, які ресурси цього комп'ютера потрібно зробити загальними, після чого необхідно ввести пароль домашньої групи.

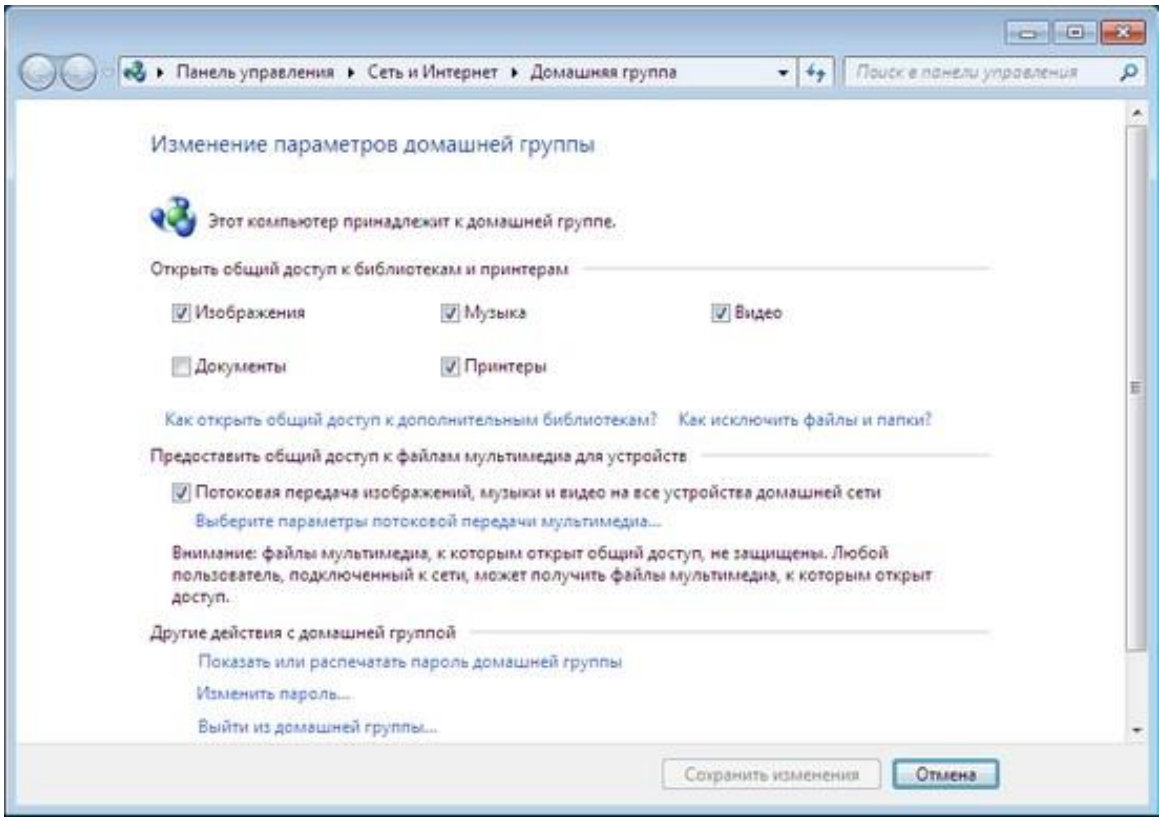

Рис. 7. **Вікно зміни параметрів загального доступу і (або) пароля**

Якщо необхідно приєднати до домашньої групи додатковий комп'ютер, а пароль загублений, його завжди можна переглянути на будь-якому з комп'ютерів, які є частиною домашньої групи. Для цього потрібно зайти в налаштування домашньої групи і клацнути по посиланню *Показать или распечатать пароль домашней группы*.

Якщо під час приєднання комп'ютера до домашньої групи видається повідомлення про те, що пароль неправильний, але при цьому є впевненість в тому, що він вводиться правильно, можливо, причина в налаштуваннях дати і часу. Згідно з офіційним повідомленням, опублікованим на сайті Microsoft у розділі підтримки користувачів, дана помилка виникає в тому випадку, якщо настройки дати і часу на комп'ютерах домашньої групи не збігаються. На комп'ютері, який необхідно приєднати до домашньої групи, потрібно встановити ту ж дату і той же час, що і на ПК, на якому була створена домашня група.

Після того як комп'ютери будуть приєднані до домашньої групи, вони стануть видні в Провіднику в розділі *Домашняя группа*, і всі користувачі зможуть швидко отримати доступ до файлів, які були відкриті для загального доступу.

Використовуючи контекстне меню Провідника, можна швидко управляти ресурсами, які будуть відкриті для інших користувачів, підключених до домашньої групи. Клацнувши по теці або по бібліотеці правою кнопкою миші і вибравши підменю *Общий доступ*, можна відкрити ресурси для читання або ж для читання і запису для користувачів домашньої групи (рис. 8).

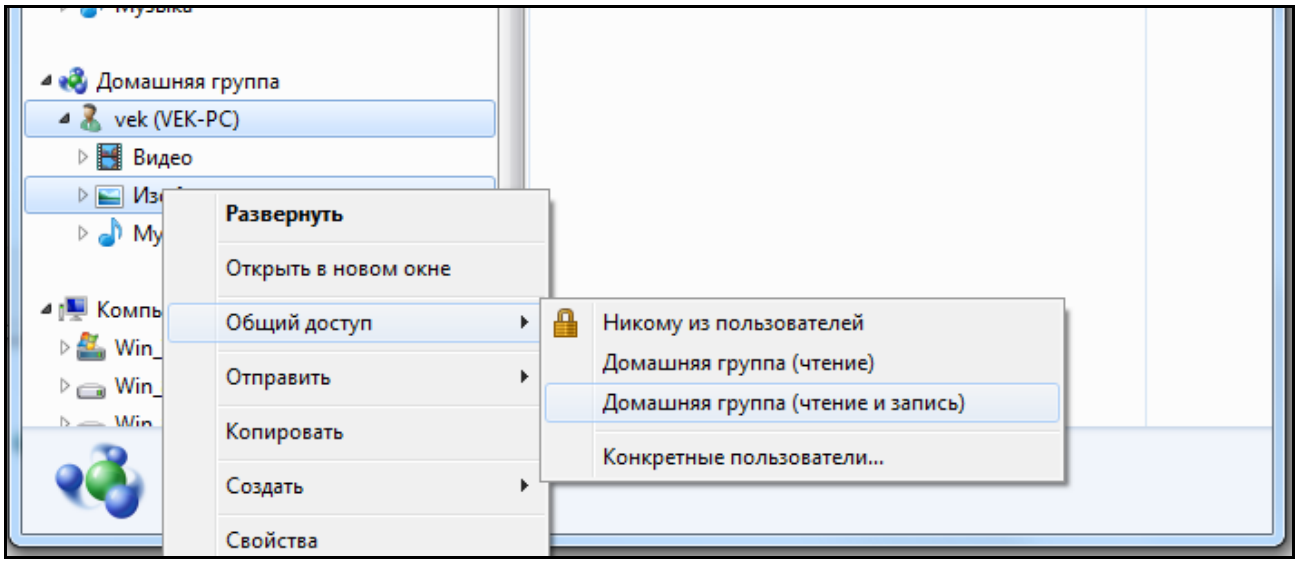

Рис. 8. **Управління загальним доступом у домашній групі**

Оскільки домашня група є спрощеним механізмом для обміну файлами, вона не передбачає налаштування прав доступу для кожного користувача окремо. Для більш тонкої настройки обмежень необхідно звернутися до параметрів загального доступу і вручну вказати тих користувачів, які зможуть переглядати або змінювати файли.

Комп'ютер не може одночасно бути підключений до декількох домашніх груп. Для підключення до іншої домашньої групи необхідно спочатку вийти з першої. Для цього потрібно відкрити вікно налаштувань домашньої групи і клацнути по посиланню *Выйти из домашней группы*, після чого підтвердити вихід.

Функція *Домашняя группа* недоступна в тому випадку, якщо в настройках системи зазначено, що комп'ютер підключено до офісної або до загальнодоступної мережі. Якщо потрібно на час приєднати комп'ютер до домашньої групи (наприклад, ноутбук, який зазвичай використовуєте в офісі), то необхідно спочатку змінити тип мережі, після чого можна буде стати частиною домашньої групи й отримати доступ до домашніх мережевих ресурсів.

Управління правами доступу до файлів і папок

Розглянемо управління параметрами безпеки на конкретному прикладі. Для початку нам потрібно створити папку на будь-якому відмінному від системного диску. Назвемо її, наприклад, *Різне*. Тепер відкриємо властивості папки і перейдемо на закладку *Безопасность*.

У верхній секції вікна знаходиться список користувачів і груп, а в нижній – права, якими володіє зазначена група. Для того щоб змінити права необхідно натиснути на кнопку *Изменить*, вибрати групу або користувача і відзначити відповідні пункти (рис. 9).

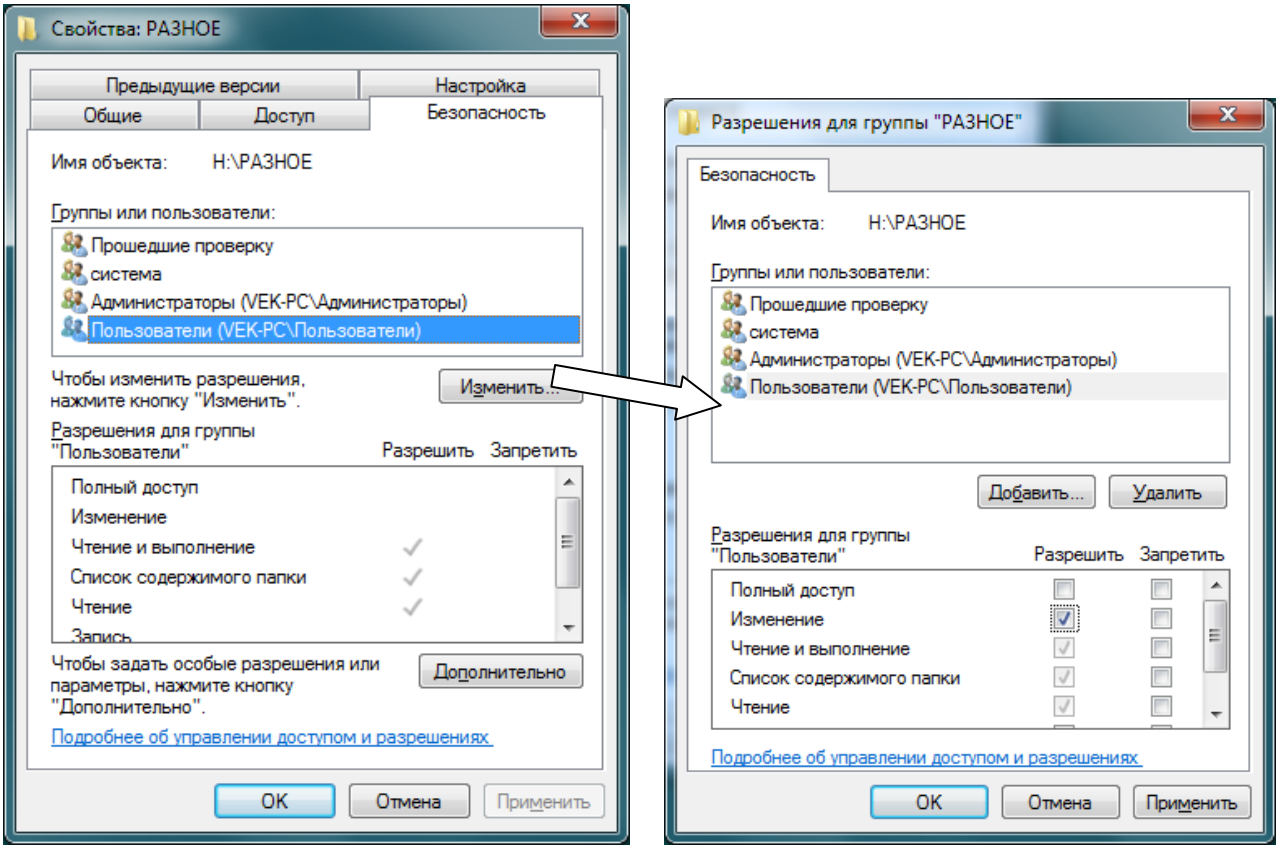

Рис. 9. **Властивості папки**

Іноді система не дозволяє змінити права. Це пов'язано з тим, що папки успадковують дозволи від батьківських об'єктів. Наприклад, папка *Різне* буде наслідувати права доступу від дозволів диска, на якому вона знаходиться. Відключити спадкування можна таким чином. На закладці *Безопасность* натиснути кнопку *Дополнительно*, потім *Изменить разрешения*, зняти прапорець *Добавить разрешения, наследуемые от родительских объектов* і натиснути кнопки *Применить* та *Удалить* (рис. 10).

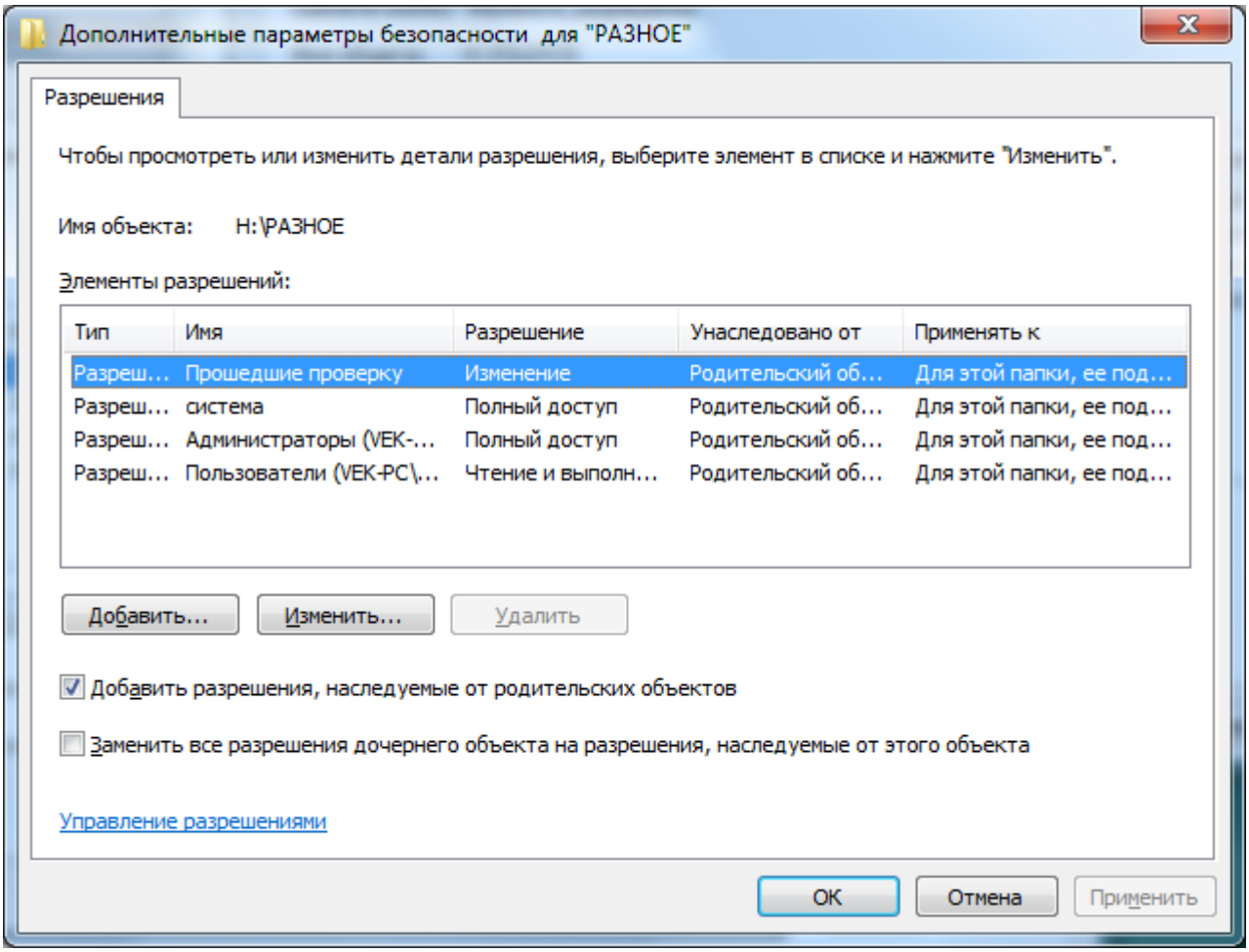

Рис. 10. **Відключення прав наслідування**

Якщо потрібно додати користувача або групу в список дозволів, то для цього на закладці *Безопасность* необхідно натиснути кнопки *Изменить*, а потім *Добавить*. У вікні ввести ім'я користувача або групи, натиснути кнопки *Проверить имена* і *ОК*. Вибрати зі списку груп і користувачів можна таким чином. У вікні *Выбор: Пользователи или Группы* натиснути кнопку *Дополнительно* і в новому вікні *Поиск*. У нижньому вікні з'явиться список, з якого можна вибрати суб'єкт подвійним клацанням.

Якщо необхідно змінити власника папки або файла, то на закладці *Безопасность* необхідно натиснути кнопку *Дополнительно*, перейти на закладку *Владелец* и натиснути кнопку *Изменить*. Тут можна вибрати користувача зі списку або за допомогою кнопки *Другие пользователи или группы*.

Література: основна [4]; ресурси мережі Інтернет [13].

Тема 2. Система адресації вузлів мережі

Самостійна робота № 3. Протокол IPv6

Мета роботи: отримання знань з теорії адресації в IP-мережах, особливостях і проблемах застосування протоколу IPv6 у сучасних операційних системах.

У результаті виконання самостійної роботи у студента формуються **компетентності:** знання принципів адресації в IP-мережах, порозуміння проблем щодо адресації вузлів і їх вирішення.

Результатом виконання самостійної роботи є звіт з виконання завдання.

Завдання для самостійної роботи

1. Вивчити довідкові матеріали до самостійної роботи і вказану літературу.
2. Самостійно вивчити чинники появи, а також особливості протоколу IPv6 і визначити принципову його відмінність від протоколу IPv4.
3. Розглянути можливість застосування протоколу IPv6 на вашій мережі.
4. Провести налаштування мережного підключення на роботу з протоколом IPv6.

Контрольні запитання для самодіагностики

1. Який адресний простір забезпечують протоколи IPv4 і IPv6?
2. Як можна збільшити адресний простір у процесі використання протоколу IPv4?
3. Дайте характеристику технологій NAT, DHCP.
4. Наведіть формат заголовка пакета з протоколом IPv6.
5. Яке ставлення адміністратора IPv6-мережі до масок? Варіанти відповідей:

повністю ігнорує як непотрібний засіб;

використовує під час об'єднання підмереж;

використовує під час поділу на підмережі;

використовує і під час об'єднання підмереж, і під час поділу на підмережі.

6. Чи правильне твердження, що широкомовлення є окремим випадком групового розсилання?

7. Чи може один мережевий інтерфейс мати кілька IPv6-адрес різних типів: унікальна адреса, адреса довільної розсилки, групова адреса?

Довідкові матеріали до самостійної роботи

Переважна більшість мереж зараз використовує протокол IPv4 (інтернет-протокол версії 4), хоча вже розроблена шоста версія протоколу IP. IP-адреса будь-якої робочої станції складається з адреси мережі й адреси комп'ютера в цій мережі.

Схема адресації протоколу IPv4 передбачає розмір адресного поля 32 біта, що дає 2^{32} = 4294967296 потенційних адрес. Насправді через особливості адресації мереж спеціального призначення адресний простір приблизно вдвічі менше.

Зростаюча популярність технології TCP/IP привела до виснаження плану нумерації протоколу. Додатковою проблемою є той факт, що дуже велика кількість адрес класу A і класу B було виділено великим організаціям, які їх насправді не потребували, й оскільки фактично використовувався тільки невеликий відсоток адрес, величезну кількість доступних адрес було втрачено.

На початку 90-х років стек протоколів TCP/IP зіткнувся з серйозними проблемами. Саме в цей час почалося активне промислове використання Інтернету: перехід до побудови мереж підприємств на основі транспорту Інтернету, застосування веб-технології для доступу до корпоративної інформації, ведення електронної комерції через Інтернет, упровадження Інтернету в індустрію розваг (поширення відеофільмів, звукозаписів, інтерактивних ігор).

Усе це призвело до різкого зростання кількості вузлів мережі (на початку 90-х років новий вузол в Інтернеті з'являвся кожні 30 секунд), зміни характеру трафіку і до посилення вимог, що пред'являються до якості обслуговування мережею її користувачів.

Найбільш нагальною проблемою все частіше стає нестача адресного простору, що вимагає зміни формату адреси.

Іншою проблемою є недостатня масштабованість процедури маршрутизації – основи IP-мереж. Швидке зростання мережі викликає перевантаження маршрутизаторів, які вже сьогодні змушені підтримувати таблиці маршрутизації з десятками і сотнями тисяч записів, а також вирішувати проблеми фрагментації пакетів. Полегшити роботу маршрутизаторів можна, зокрема, шляхом модернізації протоколу IP.

Крім того, в протоколі не передбачено механізми інформаційної безпеки, наприклад, відсутня можливість шифрування даних.

Нарешті, в IPv4 не дозволені якість обслуговування, тобто інформація про пропускну здатність і затримки, яка необхідна для роботи деяких мережевих додатків.

Поряд із введенням нових функцій безпосередньо в протокол IP, доцільно забезпечити більш тісну взаємодію його з новими протоколами шляхом введення в заголовок пакета нових полів.

У результаті було вирішено піддати протокол IP модернізації, переслідуючи такі основні цілі:

створення нової розширеної схеми адресації;

поліпшення масштабованості мереж за рахунок скорочення функцій магістральних маршрутизаторів;

надання гарантій якості транспортних послуг.

забезпечення захисту даних.

Розширення адресного простору. Протокол IP (1998 р.) вирішує потенційну проблему браку адрес за рахунок розширення розрядності адреси до 128.

Таким чином адресний простір розширюється до 2^{128} = = 340282366920938463463374607431762211456. Якщо поділити таку теоретично можливу кількість IP-адрес на всіх мешканців Землі, то на кожного доведеться неймовірно велика кількість адрес 5×10^{28}. Однак таке істотне збільшення довжини адреси було зроблено значною мірою не з метою зняти проблему дефіциту адрес, а для підвищення ефективності роботи мереж на основі цього протоколу. Головною метою була структурна зміна системи адресації, розширення функціональних можливостей стека протоколів TCP/IP в цілому.

Замість існуючих двох рівнів ієрархії адреси (номер мережі і номер вузла) в протоколі IPv6 пропонується використовувати чотири рівні, що передбачає трирівневу ідентифікацію мереж і один рівень для ідентифікації вузлів. Такий підхід дозволяє знизити витрати на маршрутизацію.

Замість десяткової форми тепер адреса записується в шістнадцятковому вигляді, причому кожні чотири цифри відокремлюються один від одного двокрапкою, наприклад:

FEDC: 0A96: 0:0:0:0:7733:567 A

Якщо в адресі зустрічається довга послідовність нулів, то запис адреси можна скоротити:

FEDC: 0A96::7733:567 A

Для мереж, що підтримують обидві версії протоколу IPv4 і IPv6, є можливість використовувати для молодших 4 байтів традиційну десятковий запис, а для старших – шістнадцятковий:

0:0:0:0: FFFF 194.135.75.104

Скорочення у вигляді двох двокрапок (::) може вживатися в адресі лише один раз. Можна також опускати незначущі нулі на початку кожного поля адреси, наприклад, замість FEDC: 0A98:: 7654:3210 можна писати FEDC: A98:: 7654:3210.

У рамках системи адресації IPv6 є також виділений простір адрес для локального використання, тобто для мереж, що не входять в Інтернет.

У новій версії IPv6 передбачено три основні типи адрес: індивідуальні адреси, групові адреси та адреси довільної розсилки. Тип адреси визначається значенням декількох старших бітів адреси, які названі префіксом формату.

Індивідуальна адреса (unicast) визначає унікальний ідентифікатор окремого інтерфейсу кінцевого вузла або маршрутизатора. Призначення адреси цього типу збігається з призначенням унікальних адрес у версії IPv4 – за їх допомогою пакети доставляються до певного інтерфейсу вузла призначення. У версії IPv6, на відміну від версії IPv4, відсутнє поняття класу мережі (A, B, C і D) і пов'язане з ним фіксоване розбиття адреси на номер мережі та номер вузла по межах байтів.

Групова адреса (multicast) IPv6 аналогічна за призначенням груповій адресі IPv4. Вона ідентифікує групу інтерфейсів, що відносяться, як правило, до різних вузлів. Пакет з такою адресою доставляється *всім* інтерфейсам з цією адресою. Групові адреси використовуються в IPv6 для заміни широкомовних адрес – для цього вводиться адреса особливої групи, що об'єднує всі інтерфейси підмережі.

Адреса довільної розсилки (anycast) – це новий тип адреси, яка так само, як і групова адреса, визначає групу інтерфейсів. Однак пакет з такою адресою доставляється *будь-якому* з інтерфейсів групи, як правило, "найближчого" відповідно з метрикою, яка використовується протоколами маршрутизації. Синтаксично адреса довільної розсилки

нічим не відрізняється від індивідуальної адреси і призначається з того самого діапазону адрес. Адреса довільної розсилки може бути призначена тільки інтерфейсам маршрутизатора. Інтерфейси маршрутизаторів, що входять в одну групу довільної розсилки, мають індивідуальні адреси і, крім того, загальну адресу групи довільної розсилки. Адреси такого типу орієнтовані на маршрутизацію від джерела, у процесі якої маршрут проходження пакета визначається вузлом-відправником шляхом зазначення IP-адрес усіх проміжних маршрутизаторів. Наприклад, постачальник послуг може присвоїти всім своїм маршрутизаторам одну і ту саму адресу довільної розсилки і повідомити його абонентам. Якщо абонент бажає, щоб його пакети передавалися через мережу цього постачальника послуг, то йому достатньо вказати його адресу в ланцюжку адрес маршруту від джерела, і пакет буде переданий через найближчий маршрутизатор даного постачальника послуг.

Так само як і в IPv4, в IPv6 є так звані приватні адреси, призначені для використання в автономних мережах. На відміну від версії IPv4 у версії IPv6 ці адреси представлені двома різновидами:

Адреси локальних мереж, не розділених на підмережі, містять тільки 64-розрядне поле ідентифікатора інтерфейсу, а інші розряди, крім префікса формату, повинні бути нульовими, оскільки потреба в номері підмережі тут відсутня.

Адреси локальних мереж, розділених на підмережі, містять порівняно з попередніми адресами додаткове двохбайтове поле номера підмережі.

Основним підтипом індивідуальної адреси є **глобальна агрегована унікальна адреса**. Такі адреси можуть агрегуватися для спрощення маршрутизації. На відміну від унікальних адрес вузлів версії IPv4, які складаються з двох полів – номера мережі і номера вузла, глобальні агреговані унікальні адреси IPv6 мають складнішу структуру, що включає шість полів (рис. 11).

3	13	8	24	16	64
FP	TLA	Резерв	NLA	SLA	Ідентифікатор інтерфейсу

Рис. 11. **Структура глобальної агрегованої унікальної адреси**

Префікс формату (Format Prefix, FP) для цього типу адрес має розмір три біта і значення 001.

Наступні три поля – агрегування верхнього (Top-Level Aggregation, TLA), наступного (Next Level Aggregation, NLA) і місцевого (Site-Level Aggregation, SLA) рівнів – описують три рівні ідентифікації мереж.

Поле TLA призначене для ідентифікації мереж найбільших постачальників послуг. Конкретне значення цього поля становить загальну частину адрес, якими володіє даний постачальник послуг. Порівняно невелика кількість розрядів, відведених під це поле (13), вибрано спеціально для обмеження розміру таблиць маршрутизації в магістральних маршрутизаторах самого верхнього рівня Інтернету. Це поле дозволяє перенумерувати 8196 мереж постачальників послуг верхнього рівня, а значить, кількість записів, що описують маршрути між цими мережами, також буде обмежено значенням 8196, що прискорить роботу магістральних маршрутизаторів. Наступні 8 розрядів зарезервовані на майбутнє для розширення за необхідності поля TLA.

Поле NLA призначене для нумерації мереж середніх і дрібних постачальників послуг. Значний розмір поля NLA дозволяє шляхом агрегування адрес відобразити багаторівневу ієрархію постачальників послуг.

Поле SLA призначено для адресації підмереж окремого абонента, наприклад, підмереж однієї корпоративної мережі. Передбачається, що постачальник послуг призначає деякому підприємству номер його мережі, що складається з фіксованого значення полів TLA і NLA, які в сукупності є аналогом номеру мережі версії IPv4. Інша частина адреси – поля SLA та ідентифікатор інтерфейсу – надходить у розпорядження адміністратора корпоративної мережі, який повністю бере на себе формування адреси і не повинен погоджувати цей процес із постачальником послуг. Причому поле ідентифікатора інтерфейсу має цілком певне призначення – воно має зберігати фізичну адресу вузла. На цьому рівні також можна агрегувати адреси невеликих підмереж у більші підмережі, і розмір поля SLA в 16 біт забезпечує достатню свободу і гнучкість побудови внутрішньокорпоративної ієрархії адрес.

Ідентифікатор інтерфейсу є аналогом номера вузла в IPv4. Відмінністю версії IPv6 є те, що в загальному випадку ідентифікатор інтерфейсу *просто збігається з його локальною (апаратною) адресою*, а не становить довільно призначений адміністратором номер вузла.

Ідентифікатор інтерфейсу має довжину 64 біта, що дозволяє помістити туди MAC-адресу(48 біт), адресу X.25 (до 60 біт), адресу кінцевого вузла ATM (48 біт) або номер віртуального з'єднання ATM (до 28 біт), а також, ймовірно, дасть можливість використовувати локальні адреси технології, які можуть з'явитися в майбутньому. Такий підхід робить непотрібним протокол ARP, оскільки процедура відображення IP-адреси на локальну адресу стає тривіальною – вона зводиться до простого відкидання старшої частини адреси. Крім того, в більшості випадків відпадає необхідність ручного конфігурування кінцевих вузлів, так як молодшу частину адреси – ідентифікатор інтерфейсу – вузол дізнається від апаратури (мережного адаптера і т. п.), а старшу – номер підмережі – йому повідомляє маршрутизатор.

Очевидно, що при такому достатку мереж, яке надається клієнтові в IPv6, зовсім втрачає сенс операція використання масок для розділення мереж на підмережі, у той час як зворотна процедура – об'єднання підмереж – набуває особливого значення. Розробники стандарту IPv6 вважають, що агрегування адрес є основним засобом ефективного використання адресного простору в новій версії протоколу IP.

Приклад [5]

Нехай клієнт отримав від постачальника послуг пул адрес IPv6, який визначається наступним префіксом:

20:0 A: 00: C9: 74:05/48

Проведемо аналіз цього числа. Оскільки його перші 3 біти рівні 001, отже, це глобальна агрегована унікальна адреса (рис. 12).

Ця адреса належить постачальнику послуг верхнього рівня, у яких всі мережі мають префікс 20:0 A/16. Він може виділити постачальнику послуг другого рівня деякий діапазон адрес із загальним префіксом, утвореним його власним префіксом, а також частиною поля NLA, Довжина поля NLA, що відведена під префікс, визначається маскою, яку постачальник послуг верхнього рівня також повинен повідомити своєму клієнтові постачальнику послуг другого рівня. Нехай у даному прикладі маска складається з 32 одиниць у старших розрядах, а результуючий префікс постачальника послуг другого рівня має вигляд:

20:0 A:00: C9/32.

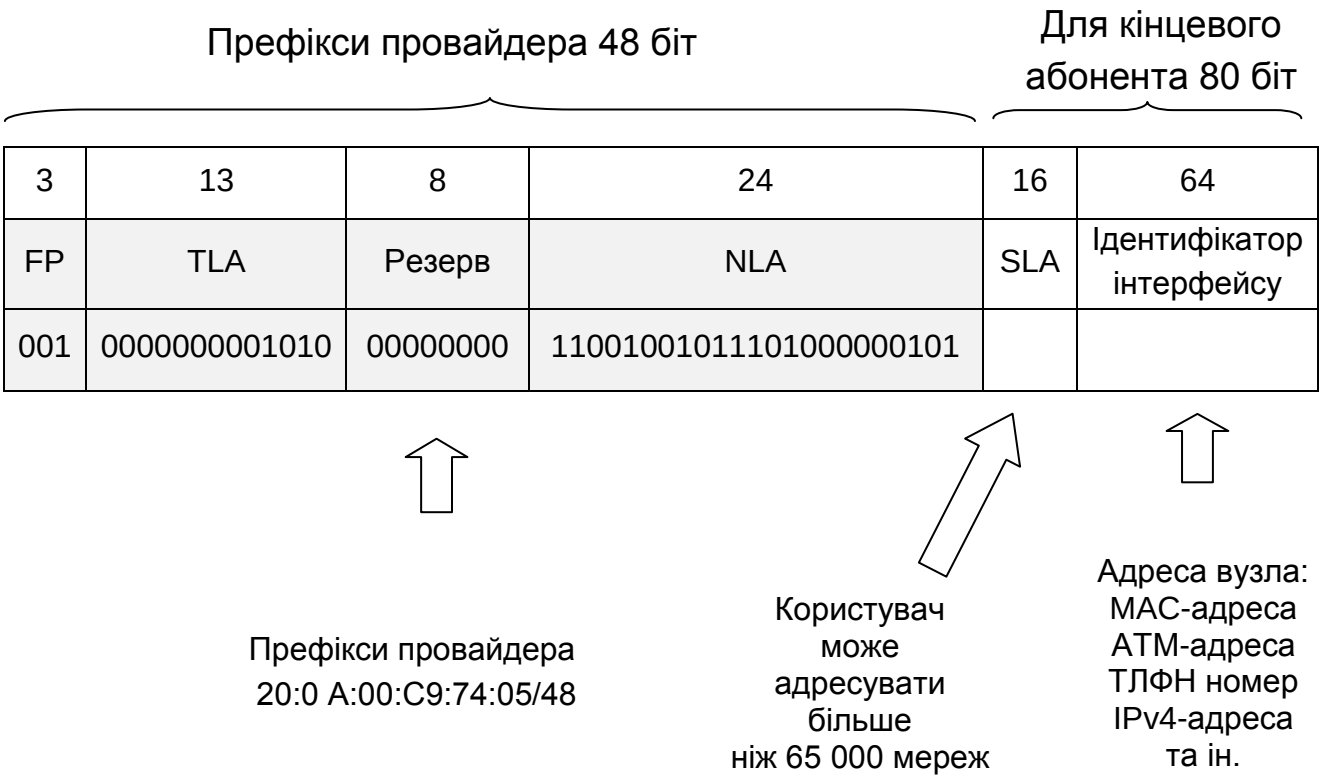

Рис. 12. **Приклад глобальної агрегованої адреси**

У розпорядженні постачальника послуг другого рівня залишається 16 розрядів поля NLA для нумерації мереж своїх клієнтів. Як клієнти можуть виступати постачальники послуг третього і більш низьких рівнів, а також кінцеві абоненти – підприємства та організації. Нехай, наприклад, наступний байт (01110100), в полі NLA постачальник послуг використовував для передачі постачальнику послуг більш низького (третього) рівня а той, у свою чергу, використовував останній байт поля NLA для призначення пулу адрес клієнта. Таким чином, за участю постачальників послуг трьох рівнів був сформований префікс 20:0 A:00: C9:74:05/48, який отримав клієнт.

Протокол IPv6 залишає в повному розпорядженні клієнта 2 байти (поле SLA) нумерації мереж і 8 байт (поле ідентифікатора інтерфейсу) для нумерації вузлів. Маючи такий величезний діапазон номерів підмереж, адміністратор може використовувати його по-різному. Він може вибрати просту плоску організацію своєї мережі, призначаючи кожній наявній підмережі певне значення з діапазону в 65535 адрес, ігноруючи решту. У великих мережах більш ефективним способом (скорочує розміри таблиць корпоративних маршрутизаторів) може виявитися ієрархічна структуризація мережі на основі агрегування адрес.

Крім докладно розглянутої вище глобальної агрегованої адреси, існують й інші різновиди індивідуальної адреси.

Адреса зворотної петлі 0:0:0:0:0:0:0:1 відіграє у версії IPv6 ту саму роль, що й адреса 127.0.0.1 у версії IPv4.

Невизначена адреса, що складається з одних нулів, є аналогом адреси 0.0.0.0 протоколу IPv4. Ця адреса може з'являтися в IP-пакетах тільки як адреса джерела, і це означає, що пакет посланий до того, як вузол вивчив свій IP-адресу.

Передбачається, що досить великий час співіснуватимуть острівці Інтернету, що працюють по протоколу IPv6, й інша частина Інтернету працює на версії IPv4. Для того щоб вузли, що підтримують версію IPv6, могли використовувати техніку передачі пакетів IPv6 через мережу IPv4 в автоматичному режимі, розроблений спеціальний підтип адрес, які переносять IPv4-адресу в молодших 4-х байтах IPv6-адреси, а в старших 12 байтах адреси містять нулі. Такі індивідуальні адреси роблять дуже просту процедуру перетворення адрес між двома версіями протоколу IP і називаються IPv4-сумісними IPv6-адресами.

Для вирішення зворотного завдання – передачі IPv4-пакетів через частини Інтернету, що працюють по протоколу IPv6, – призначена **IPv4-відображена IPv6-адреса**. Цей тип адреси раніше містить в 4-х молодших байтах IPv4-адресу, в старших 10-ти байтах нулі, а в 5-у і 6-у байтах IPv6-адреси – одиниці, які показують, що вузол підтримує тільки 4-у версію протоколу IP.

Робота з деталізації підтипів IPv6-адрес ще далека від завершення. Сьогодні визначено призначення тільки 15 % адресного простору IPv6, а решта адрес ще чекає своєї черги, щоб знайти застосування для вирішення однієї з численних проблем Інтернету.

Зміна формату заголовків пакетів. Реалізувати це дозволяє нова схема організації "вкладених заголовків", що забезпечує поділ заголовка на основний, який містить необхідний мінімум інформації, і додаткові, які можуть бути відсутні. Такий підхід відкриває багаті можливості для розширення протоколу шляхом визначення нових опціональних заголовків, роблячи протокол відкритим.

Гнучкий формат заголовка

Однією з основних цілей зміни формату заголовка в IPv6 було зниження накладних витрат, тобто зменшення обсягу службової інформації, що передається з кожним пакетом. Для цього в новому протоколі

IP були введені поняття основного і додаткового заголовків. Основний заголовок присутній завжди, а додаткові є опціональними. Додаткові заголовки можуть містити, наприклад, інформацію про фрагментацію вихідного пакета, повний маршрут прямування пакета під час маршрутизації від джерела, інформацію, необхідну для захисту переданих даних.

Основний заголовок дейтаграми IPv6 довжиною 40 байтів має наступний формат (рис. 13).

<table>
<tr><td>Версія (4 біти)</td><td>Клас трафіку (8 біт)</td><td>Позначка потоку (20 біт)</td></tr>
<tr><td>Довжина (16 біт)</td><td>Наст. заголовок (8 біт)</td><td>Ліміт переходів (8 біт)</td></tr>
<tr><td colspan="3">Адреса відправника (128 біт)</td></tr>
<tr><td colspan="3">Адреса одержувача (128 біт)</td></tr>
</table>

Рис. 13. **Формат основного заголовка дейтаграми IPv6**

Поле *Клас трафіку* (*Traffic Class*) еквівалентно за призначенням полю *Тип обслуговування* (*Type Of Service*), а поле *Ліміт переходів* (*Hop Limit*) – полю *Час життя* (*Time To Live*) протоколу IPv4.

Поле *Позначка потоку* (*Flow Label*) дозволяє виділяти й особливим чином обробляти окремі потоки даних без необхідності аналізувати вміст пакетів. Це дуже важливо з точки зору зниження навантаження на маршрутизатори.

Поле *Наступний заголовок* (*Next Header*) є аналогом поля *Протокол* (*Protocol*) IPv4 і визначає тип заголовка, наступного за основним. Кожен наступний додатковий заголовок також містить поле *Next Header*.

У пропозиціях з приводу протоколу IPv6 фігурують поки такі типи додаткових заголовків:

заголовок маршрутизації – вказівка повного маршруту під час маршрутизації від джерела;

заголовок фрагментації – інформація, що відноситься до фрагментації IP-пакета (поле обробляється тільки в кінцевих вузлах);

заголовок аутентифікації – інформація, необхідна для аутентифікації кінцевих вузлів і забезпечення цілісності вмісту IP-пакетів;

заголовок системи безпеки – інформація, необхідна для забезпечення конфіденційності даних шляхом шифрування і дешифрування;

спеціальні параметри – параметри, необхідні для послідовної обробки пакетів на кожній ретрансляційній ділянці;

параметри одержувача – додаткова інформація для вузла призначення.

Оскільки для маршрутизації пакета обов'язковим є тільки основний заголовок (майже всі додаткові заголовки обробляються тільки в кінцевих вузлах), це знижує навантаження на маршрутизатори. З іншого боку, можливість використання великої кількості додаткових параметрів розширює функціональність протоколу IP і робить його відкритим для впровадження нових механізмів.

Зниження навантаження на маршрутизатори

Для того щоб підвищити продуктивність маршрутизаторів Інтернету в частині виконання їх основної функції – просування пакетів, у версії IPv6 вжито низку заходів зі звільнення маршрутизаторів від деяких допоміжних завдань.

Перенесення функцій фрагментації з маршрутизаторів на кінцеві вузли.

Агрегування адрес, провідне до зменшення розміру адресних таблиць маршрутизаторів, а значить, – до скорочення часу перегляду й оновлення таблиць. При цьому також скорочується службовий трафік, створюваний протоколами маршрутизації.

Широке використання маршрутизації від джерела, коли вузол-джерело задає повний маршрут проходження пакета через мережі. Така техніка звільняє маршрутизатори від необхідності перегляду адресних таблиць під час вибору наступного маршрутизатора.

Відмова від обробки не обов'язкових параметрів заголовка.

Використання як номерів вузла його MAC-адреси, що позбавляє маршрутизаторів від необхідності застосовувати протокол ARP.

Перехід від версії IPv4 до версії IPv6 тільки починається. Сьогодні вже існують фрагменти Інтернету, в яких маршрутизатори підтримують обидві версії протоколу.

Література: основна [5]; ресурси мережі Інтернет [10].

Тема 3. Архітектура і стандартизація мереж

Самостійна робота № 4. Мережі для передачі ММ інформації. Мережі ATM

Мета роботи: отримання знань з технології асинхронних мереж (ATM): про особливості їх застосування для передачі мультимедійної інформації.

У результаті виконання самостійної роботи у студента формуються **компетентності:** знання принципів роботи асинхронних мереж, порозуміння проблем щодо їх застосування.

Результатом виконання самостійної роботи є звіт з виконання завдання.

Завдання для самостійної роботи

1. Вивчити довідкові матеріали до самостійної роботи і вказану літературу.
2. Самостійно вивчити чинники появи, а також особливості мереж ATM і визначити принципову його відмінність від мереж TCP/IP.
3. Розглянути можливість мережі ATM для передачі мультимедійної інформації.

Контрольні запитання для самодіагностики

1. Для яких мереж можна застосувати технологію ATM?
2. Перелічіть переваги і недоліки технології ATM.
3. Перелічіть 5 класів трафіку, на які орієнтується ATM.
4. Яку категорію послуг доцільно вибрати для передачі голосу через мережу ATM?
5. Який формат кадру (комірки) ATM?
6. Яку максимальну швидкість передачі даних забезпечує технологія ATM?
7. Дайте загальну характеристику комутаторів ATM.
8. Яка різниця між віртуальним каналом і віртуальним шляхом?
9. Які рівні моделі OSI підтримує ATM?
10. Назвіть перспективи застосування мереж ATM.

Довідкові матеріали до самостійної роботи

Оптоволоконні лінії зв'язку дозволяли забезпечити передачу даних на високій швидкості з малими втратами, але цифрова мережа з комутацією пакетів не забезпечує надійну передачу голосу. На противагу мережі пакетної передачі даних у громадських телефонних мережах застосовували технологію комутації каналів. Ця технологія ідеальна для передачі голосу, але для передачі даних вона неефективна. Виникла

необхідність розробити новий стандарт для передачі даних і голосового трафіку в мережах з широкою смугою пропускання.

Технологія асинхронного режиму передачі (Asynchronous Transfer Mode, ATM) – технологія передачі даних є однією з технологій побудови високошвидкісних мереж (від локальних до глобальних). ATM – це комунікаційна технологія, яка об'єднує принципи комутації пакетів і каналів для передачі інформації різного типу.

Технологія ATM розроблялася для передачі всіх видів трафіку в локальних і глобальних мережах, тобто передачі різнорідного трафіку (цифрових, голосових і мультимедійних даних) по одних і тих самих системах і лініях зв'язку. Так як час доставки для багатьох видів мережевих послуг реального часу є вкрай важливою характеристикою, ATM знаходить широке застосування в телефонії, кабельному телебаченні та інших областях. Швидкість передачі даних у магістралях ATM складає 155–2200 Мбіт/с.

При номінальній швидкості 155,52 Мбіт/с користувачеві доступна реальна швидкість обміну 135 Мбіт/с, це пов'язано з витратами на заголовки і керування.

У технології ATM інформація передається в комірках (cell) фіксованого розміру в 53 байти, з них 48 байт призначені для даних, а 5 байт – для службової інформації (для заголовка комірки ATM). Комірки не містять адресної інформації та контрольної суми даних, що прискорює їх обробку та комутацію (рис. 14).

5 байт	48 байт
Службова інформація	Корисні дані

Рис. 14. **Формат комірки ATM**

20-байтовими адресами приймач і передавач обмінюються тільки в момент встановлення віртуального з'єднання. Основна функція заголовка зводиться до ідентифікації віртуального з'єднання. У процесі передачі інформації комірки пересилаються між вузлами через мережу комутаторів, з'єднаних між собою цифровими лініями зв'язку. На відміну від маршрутизаторів комутатори ATM виконують свої функції апаратно, що прискорює читання ідентифікатора в заголовку комірки, після чого комутатор переправляє її з одного порту в інший.

Малий розмір комірок забезпечує якісну передачу трафіку, чутливого до затримок. Фіксований формат комірки спрощує її обробку комунікаційним обладнанням, яке апаратно реалізує функції комутації осередків. Однак при цьому різко зростає рівень навантаження на АТМ-комутатори під час роботи на високих швидкостях, так як вона пропорційна кількості оброблюваних за одиницю часу пакетів або кадрів.

Саме поєднання фіксованого розміру комірок для передачі даних і реалізація протоколів АТМ в апаратному забезпеченні дає цій технології можливість передавати всі типи трафіку по одних і тих самих системах і лініях зв'язку.

Невеликий, постійний розмір комірки, що використовується в АТМ, дозволяє:

спільно передавати дані з різними класами вимог до затримок в мережі, причому по каналах як з високою, так і з низькою пропускною здатністю;

працювати з постійними і змінними потоками даних;

інтегрувати на одному каналі будь-які види інформації: дані, голос, потокове аудіо- та відеомовлення, телеметрія та ін.;

підтримувати з'єднання типу "точка-точка", "точка-багатоточка" і "багатоточка-багатоточка".

Телекомунікаційна мережа, що використовує технологію АТМ, складається з набору комутаторів, пов'язаних між собою. Комутатори АТМ підтримують два види інтерфейсів: UNI(UNI – user-network interface) і NNI(NNI – network-network interface). Інтерфейс користувача UNI (користувач – мережа) використовується для підключення до комутатора кінцевих систем. Міжмережевий інтерфейс NNI (мережа – мережа) використовується для з'єднань між комутаторами.

Комутатор АТМ складається з:

комутатора віртуальних шляхів;

комутатора віртуальних каналів.

Комутатор АТМ аналізує значення ідентифікаторів віртуального шляху і віртуального каналу комірки, яка надходить на його вхід і направляє комірку на один з його вихідних портів. Номер вихідного порту визначається динамічно створюваною таблицею комутації.

Технологія АТМ використовує для передачі даних техніку **віртуальних з'єднань** (комутованих і постійних). Віртуальне з'єднання визначається поєднанням ідентифікатора віртуального шляху і ідентифікатора

віртуального каналу. Ідентифікатор дозволяє маршрутизувати комірку для доставки на шлях призначення, тобто комутація комірок відбувається на основі ідентифікатора віртуального шляху й ідентифікатора віртуального каналу, що визначають віртуальне з'єднання. Кілька віртуальних шляхів складають віртуальний канал.

Віртуальний канал є з'єднанням, встановленим між двома кінцевими вузлами на час їх взаємодії, а **віртуальний шлях** – це шлях між двома комутаторами. У процесі створення віртуального каналу комутатори визначають, який віртуальний шлях використовувати для досягнення пункту призначення. По одному і тому самому віртуальному шляху може передаватися одночасно трафік безлічі віртуальних каналів.

ATM підтримує фізичний і канальний рівні OSI.

Фізичний рівень

Фізичний рівень аналогічно фізичному рівню OSI визначає способи передачі залежно від середовища. Стандарти ATM для фізичного рівня встановлюють, яким чином біти повинні проходити через середовище передачі, і як біти перетворювати в осередки.

На фізичному рівні ATM використовують цифрові канали передачі даних, з різними протоколами, а як лінії зв'язку використовуються кабелі "вита пара", екранована "вита пара"(< 100м для обох варіантів), оптоволоконний кабель(~ 2км).

Канальний рівень (рівень ATM + рівень адаптації)

Рівень ATM разом з рівнем адаптації приблизно еквівалентний другому рівню моделі OSI. Рівень ATM відповідає за передачу комірок через мережу ATM, використовуючи інформацію їх заголовків. Заголовок містить ідентифікатор віртуального каналу, який призначається з'єднанню під час його встановлення і віддаляється під час розриву з'єднання.

Класи обслуговування і категорії послуг

Для мереж ATM визначено п'ять класів трафіку, які відрізняються наступними якісними характеристиками:

трафік CBR (Constant Bit Rate), тобто відсутність пульсації трафіку. CBR не передбачає контролю помилок, управління трафіком або яку-небудь іншу обробку. Клас CBR придатний для роботи з мультимедіа реального часу;

трафік rtVBR (real-time Variable Bit Rate) – зі змінною бітовою швидкістю і вимогами до синхронізації даних проміжними сторонами;

трафік nrtVBR (non real-time Variable Bit Rate) – зі змінною бітовою швидкістю, без вимог до синхронізації даних. Для трафіків VBR ATM у процесі доставки не вносить ніякого розкиду комірок за часом. Випадки втрати комірок ігноруються;

трафік ABR (Available Bit Rate) – призначений для роботи в умовах миттєвих варіацій трафіку. Система гарантує деяку пропускну здатність, але протягом короткого часу може витримати і велике навантаження. Цей клас передбачає наявність зворотного зв'язку між приймачем і відправником, яка дозволяє знизити завантаження каналу, якщо це необхідно;

трафік UBR (Unspecified Bit Rate) – без вимог до швидкості пересилання даних і синхронізації. Добре придатний для відправки IP-пакетів (немає гарантії доставки і в разі перевантаження неминучі втрати).

Переваги технології ATM:

одна з найважливіших переваг ATM є забезпечення високої швидкості передачі інформації;

ATM усуває відмінності між локальними та глобальними мережами, перетворюючи їх в єдину інтегровану мережу;

стандарти ATM забезпечують передачу різнорідного трафіку (цифрових, голосових і мультимедійних даних) по одних і тих самих системах і лініях зв'язку.

ATM забезпечує будь-які послуги в мережі:

передача голосу на швидкостях 64 Кбіт/с. Одна комірка ATM відповідає 6 мсек;

передача музики з використанням схеми кодування MUSICAM;

так як для випадку зображення передається тільки змінна частина картинки, ATM ідеально підходить для вирішення такого роду завдань;

завдання управління вирішуються менш економно, але, тим не менш, досить ефективно (передбачено кілька пріоритетів для управління потоками даних).

Недоліки технології ATM:

висока вартість устаткування, тому технології ATM гальмуються наявністю більш дешевих технологій;

високі вимоги до якості ліній передачі даних.

Наприкінці 90-х рр. з'являється технологія Gigabit Ethernet, яка починає конкурувати з ATM. Головними перевагами першої є значно нижча вартість, простота, легкість в налаштуванні й експлуатації. Також, пере-

хід з Ethernet або Fast Ethernet на Gigabit Ethernet можна було здійснити значно легше і дешевше. До закінчення 90-х рр. стало ясно, що ATM буде продовжувати домінувати тільки в глобальних мережах.

Література: основна [5].

Змістовий модуль 2. Технології комп'ютерних мереж і захист мультимедійної інформації

Тема 6. Бездротові комп'ютерні мережі

Самостійна робота № 5. Налаштування та підключення Wi-Fi мережі до Інтернету в Windows 7

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

Формування компетентностей: застосування технологій бездротових комп'ютерних мереж.

Результатом виконання самостійної роботи є практичне створення бездротових комп'ютерних мереж і звіт з виконання завдання.

Завдання для самостійної роботи

1. Вивчити теоретичні положення про бездротові технології.
2. Вивчити довідкові матеріали до самостійної роботи і вказану літературу.
3. Створити бездротову Wi-Fi мережу між двома комп'ютерами з віртуальним мережним адаптером.
4. Створити бездротову Wi-Fi локальну мережу з підключенням до Інтернету.

Контрольні запитання для самодіагностики

1. Які особливості передачі інформації в бездротових мережах?
2. Назвати 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 не через супутник?

5. Які типи сучасних WLAN ви знаєте?
6. Назвати режими доступу до середовища у мережі Wi-Fi.
7. Назвати різновиди стандарту 802.11.
8. Назвати основні схеми підключення вузлів у бездротовій мережі Wi-Fi.
9. Яка структура бездротової мережі WiMAX?
10. Як працюють пікомережі Bluetooth?

Довідкові матеріали до самостійної роботи

Розглянемо два випадки – бездротова мережа між двома комп'ютерами (Wi-Fi пристроями) і повноцінна Wi-Fi між декількома комп'ютерами.

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

Часто треба швидко і просто створити бездротову Wi-Fi локальну мережу між двома комп'ютерами, комп'ютером і ноутбуком, ноутбуком і будь-яким іншим бездротовим пристроєм: смартфоном, планшетом, телевізором з інтегрованим бездротовим модулем без окремої бездротової точки доступу.

Ситуація № 1. Мається Інтернет через кабель на ноутбуці з встановленою Windows 7, а потрібно вийти в Інтернет через інші пристрої – смартфон, iPhone, планшетний комп'ютер і т.п.

Ситуація № 2. Виникла регулярна необхідність копіювати файли з ноутбука на другий комп'ютер або на мобільний пристрій з підтримкою Wi-Fi.

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

Крок 1 – створення віртуального мережевого адаптера на ноутбуці Virtual Wi-Fi, який транслюватиме бездротову мережу та Інтернет.

Крок 2 – налаштування доступу до Інтернету.

Крок 1. починається з того, що на ноутбуці, який стане точкою доступу і до якого можна буде підключити будь-який бездротовий пристрій, створюється віртуальний адаптер. 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="MS Virtual WiFi" key="Pass for virtual wifi" keyUsage=persistent

Де **ssid** – це назва створюваної мережі, а значення **key** – це пароль для підключення, від 8 до 63 символів у кодуванні ASCII. Наприклад значення типу: ArQ564u10.

У цьому випадку у вікно командного режиму вводиться такий рядок:

netsh wlan set hostednetwork mode=allow ssid="MS Virtual WiFi" key= "ArQ564u10" keyUsage=persistent

У результаті цих дій у ноутбуці повинен з'явитися ще один бездротовий пристрій – *Адаптер мини-порта виртуального Wi-Fi Microsoft (Microsoft Virtual Wi-Fi miniport adapter)*.

Це віртуальний бездротовий адаптер. Створюється він як окремий пристрій для трансляції мережі, так як у технології Wi-Fi не бажано використання одного адаптера для кількох цілей.

Мережа створена, але знаходиться в неактивному стані.

Важливо: якщо в диспетчері пристроїв не з'явився новий бездротовий пристрій під назвою Microsoft Virtual Wi-Fi miniport adapter, значить з драйвером модуля Wi-Fi проблема – необхідно завантажити та встановити оригінальний драйвер. Інакше мережа працювати не буде.

Для активації (старту) створеної бездротової мережі знову запускаємо 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 в міру необхідності, 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 вище рядку. Запускаються bat-файли клацанням миші.

Після запуску мережі її можна визначити за допомогою будь-якого Wi-Fi пристрою (ноутбука, планшетного комп'ютера, смартфона і т.п.). Наприклад, зайшовши в меню пошуку та підключення мереж смартфона на Andoid OS (**Настройка-Сеть-Настройки Wi-Fi-Включить Wi-Fi-Сети Wi-Fi**) можна виявити мережу *MS Virtual Wi-Fi*. Підключитися до мережі можна натиснувши кнопку *Подключение* в списку доступних мереж і ввівши пароль, який був заданий під час створення мережі. У даному випадку це – ArQ564u10.

Крок 1 виконаний. Бездротова програмна точка доступу (SoftAP) з парольним захистом створена і готова до використання.

Крок 2. На даному кроці необхідно отримати доступ до мережі Інтернет 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 з панелі управління або після клацання миші по значку *Сеть* на Панелі задач. У вікні перейти за посиланням *Изменение параметров адаптера* і знайти мережевий (кабельний) адаптер. Клацанням правою кнопкою миші по значку адаптера викликати вікно *Свойства*. На вкладці *Доступ* відзначити прапорцем режим *Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера*. Крім цього необхідно вказати конкретно якому адаптеру дається доступ у мережу в випадаючому меню трохи нижче **Подключение домашней сети**. Тут треба вказати щойно створену віртуальну мережу (*Беспроводное сетевое соединение 2*).

Після натиснення кнопки *ОК* для збереження параметрів мережа повинна відразу ж 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

Визначимо в мережі 2 класу комп'ютерів, які будуть налаштовуватися по-різному:

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

Інші комп'ютери мережі – комп'ютери або ноутбуки підключення до Wi-Fi мережі створеної на головному комп'ютері і мають доступ в Інтернет через цей комп'ютер.

Налаштування головного комп'ютера мережі

Припустимо, що всі комп'ютери мережі забезпечені Wi-Fi адаптерами, 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.

Ім'я робочої групи і комп'ютера можна змінити, клацнувши правою кнопкою миші по значку *Компьютер*, вибравши меню *Свойства* і перейшовши за посиланням *Дополнительные параметры системы*.

На вкладці *Имя компьютера* в поле *Описание* ввести довільний опис комп'ютера і натиснути кнопку *Изменить.*

У вікні *Изменение имени компьютере или домена* у полі *Имя компьютера:* задати унікальне ім'я комп'ютера (рис. 15).

У полі *рабочей группы:* ім'я робочої групи. Ім'я робочої групи має бути однаковим на всіх комп'ютерах мережі. За замовчуванням ім'я робочої групи WORKGROUP. Після зміни імені комп'ютера і робочої групи необхідно перезавантажити комп'ютер.

На головному комп'ютері включити Wi-Fi адаптер і для створення домашньої групи необхідно відкрити вікно *Центр управления сетями и общим доступом*, яке доступне з панелі управління або після клацання миші по 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. 16) клацанням по кнопці *Добавить* створити бездротову мережу. У вікні *Подключение к беспроводной сети вручную* перейти за посиланням *Создать сеть "компьютер–компьютер".*

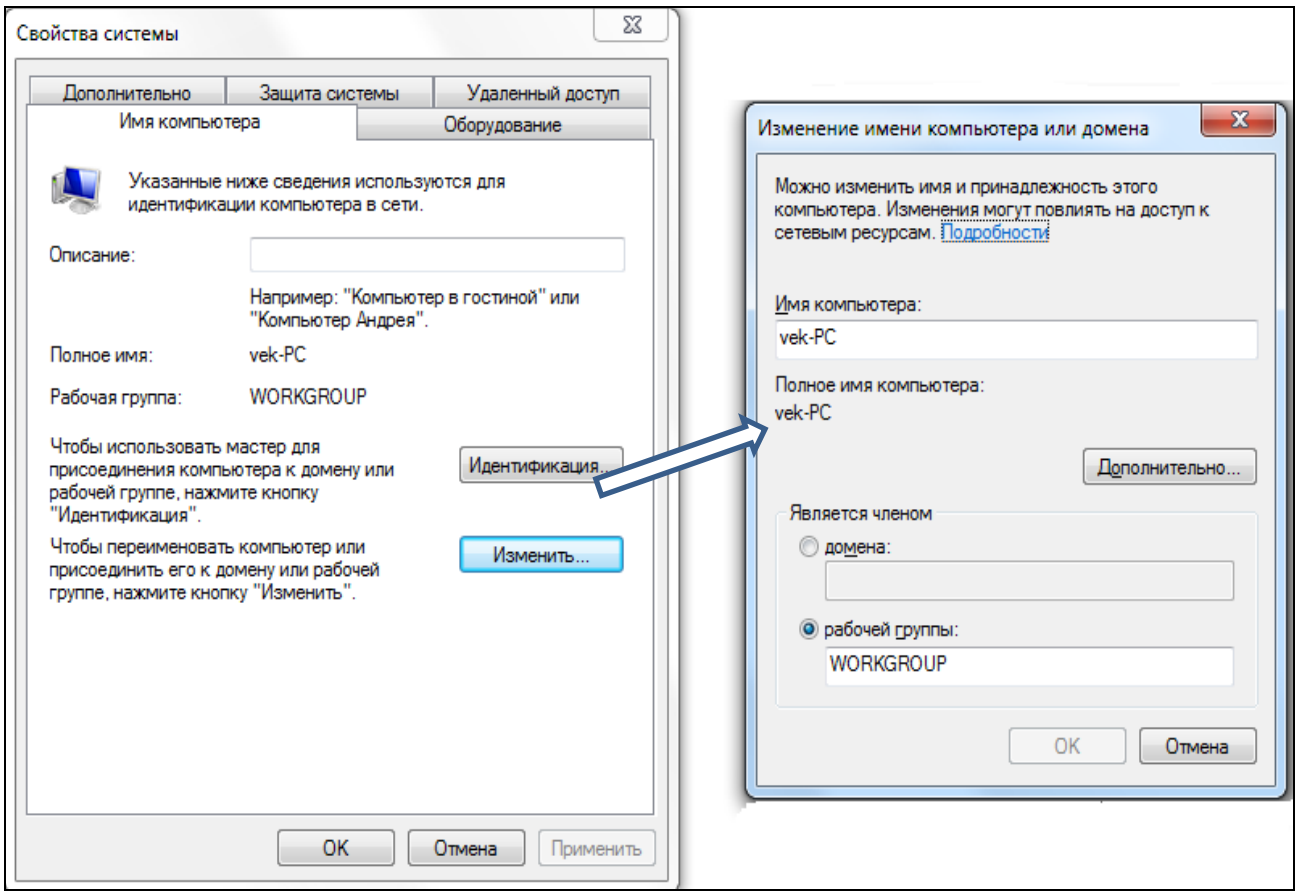

Рис. 15. **Зміна імені робочої групи та комп'ютера**

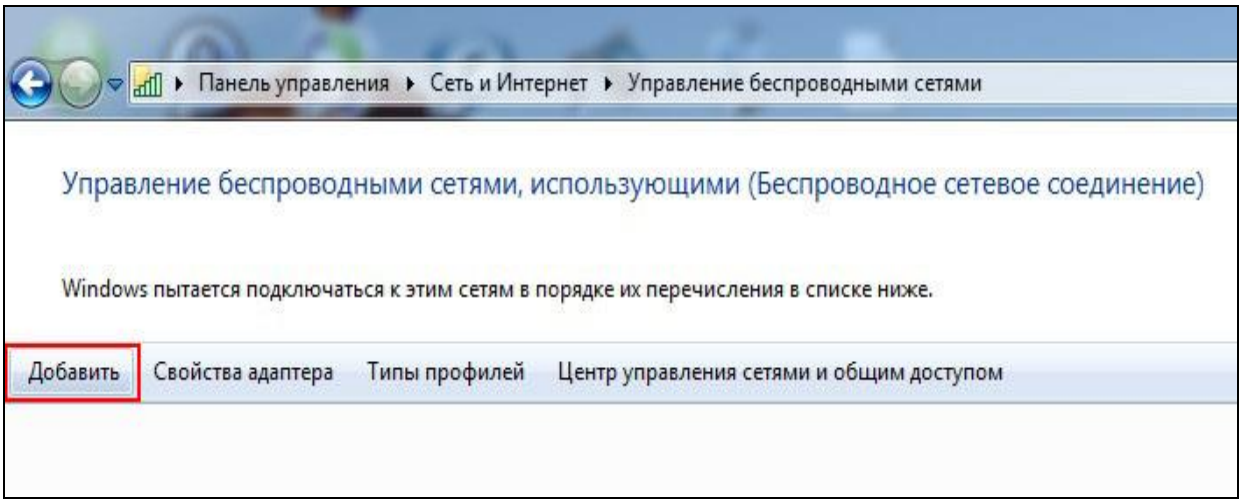

Рис. 16. **Управління бездротовими мережами**

Уважно ознайомтеся з визначенням мережа "комп'ютер–комп'ютер" і обмеженнями на її використання (рис. 17) і натиснути кнопку *Далее*.

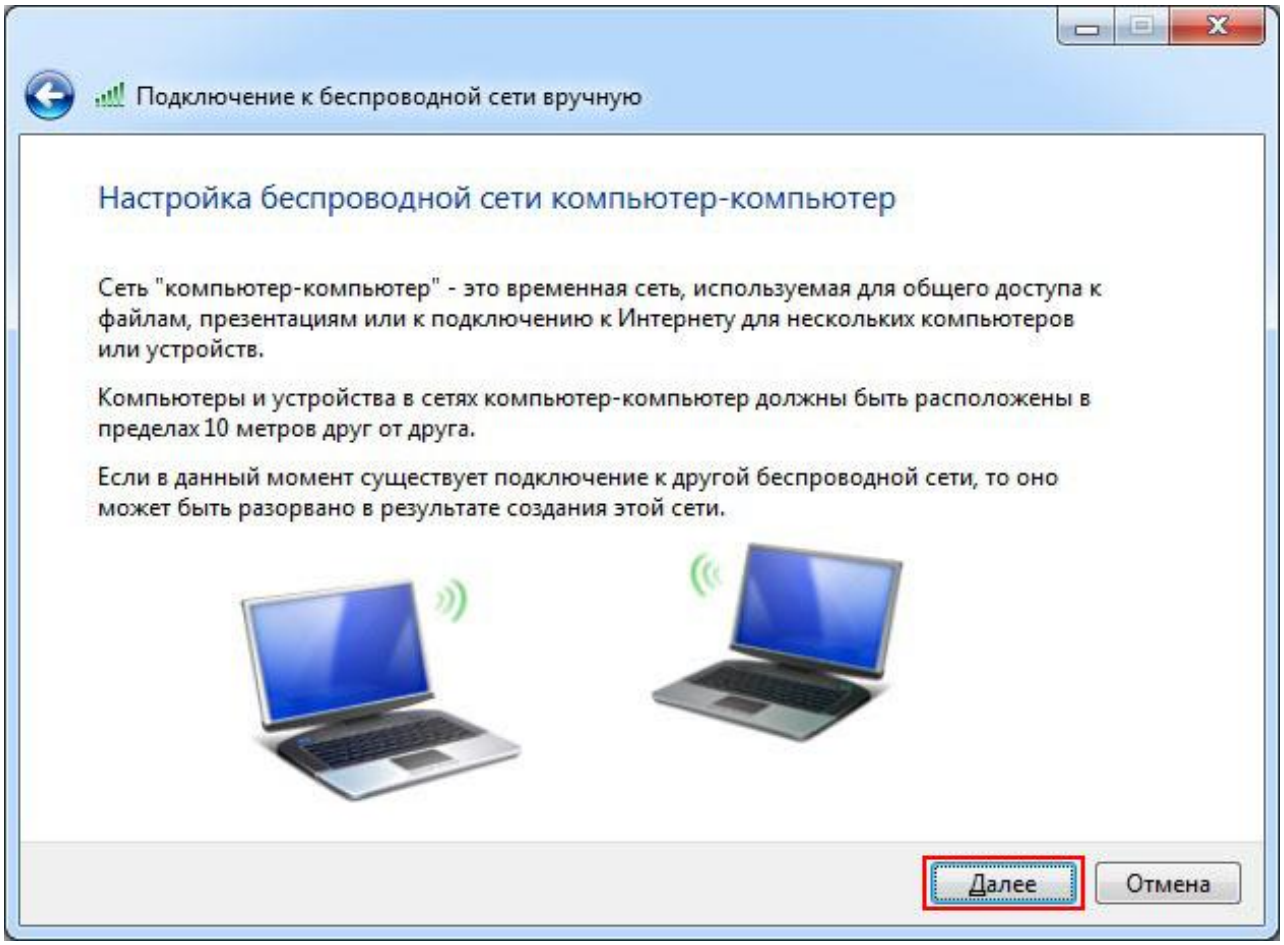

Рис. 17. **Бездротова мережа "комп'ютер–комп'ютер"**

У полі *Имя сети:* задати довільне ім'я мережі (рис. 18).

У полі *Тип безопасности:* вибрати *WPA2-Personal*. Якщо інші комп'ютери мережі працюють під Windows XP, то вибрати WEP.

У полі *Ключ безопасности:* ввести пароль. Пароль повинен складатися від 8 до 63 знаків. Якщо вибрано шифрування WEP, то пароль повинен складатися з 5 або 13 знаків. Чим довше пароль, тим краще. Для створення пароля краще використовувати генератор паролів. Натиснути кнопку *Далее*. У вікні, яке з'явилося (рис. 19), включити режим *Включить общий доступ к подключению Интернет* і закрити вікно. На цьому налаштування головного комп'ютера закінчується.

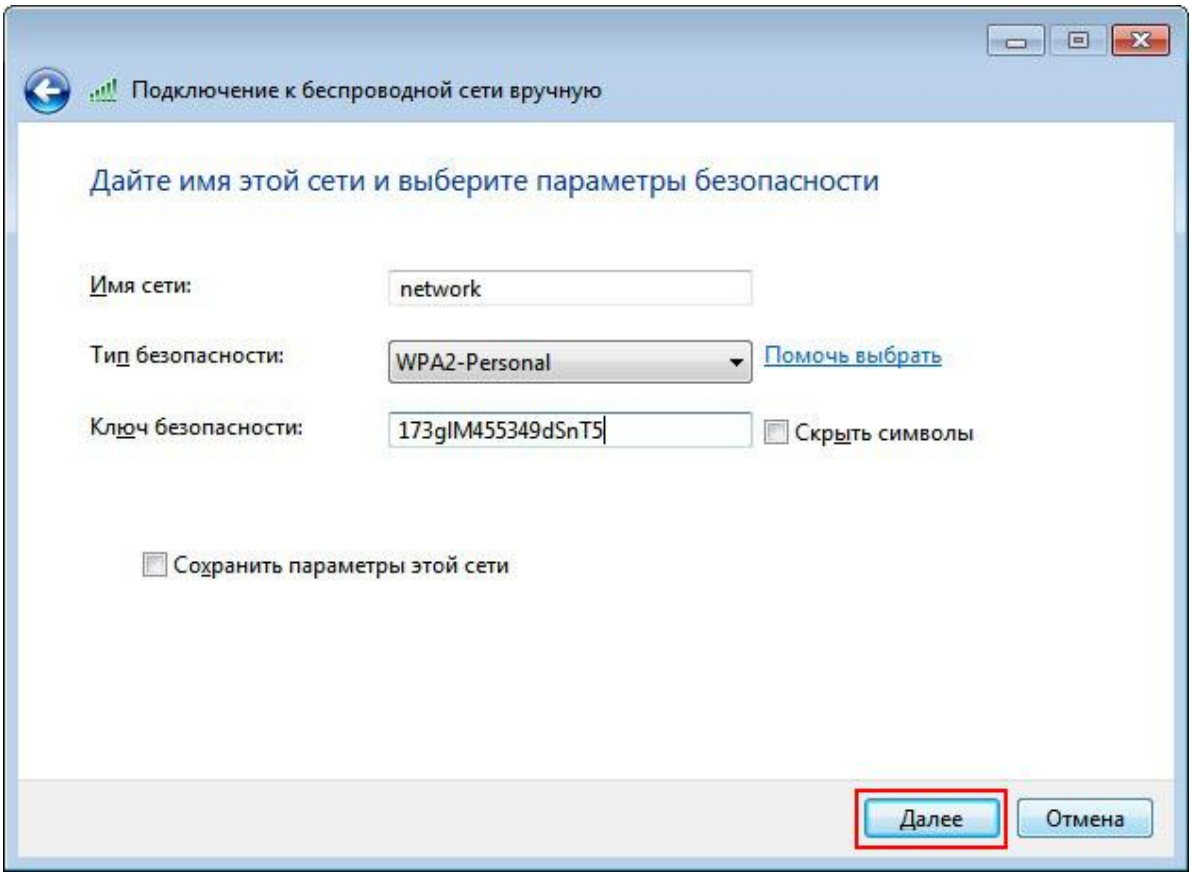

Рис. 18. **Підключення до бездротової мережі**

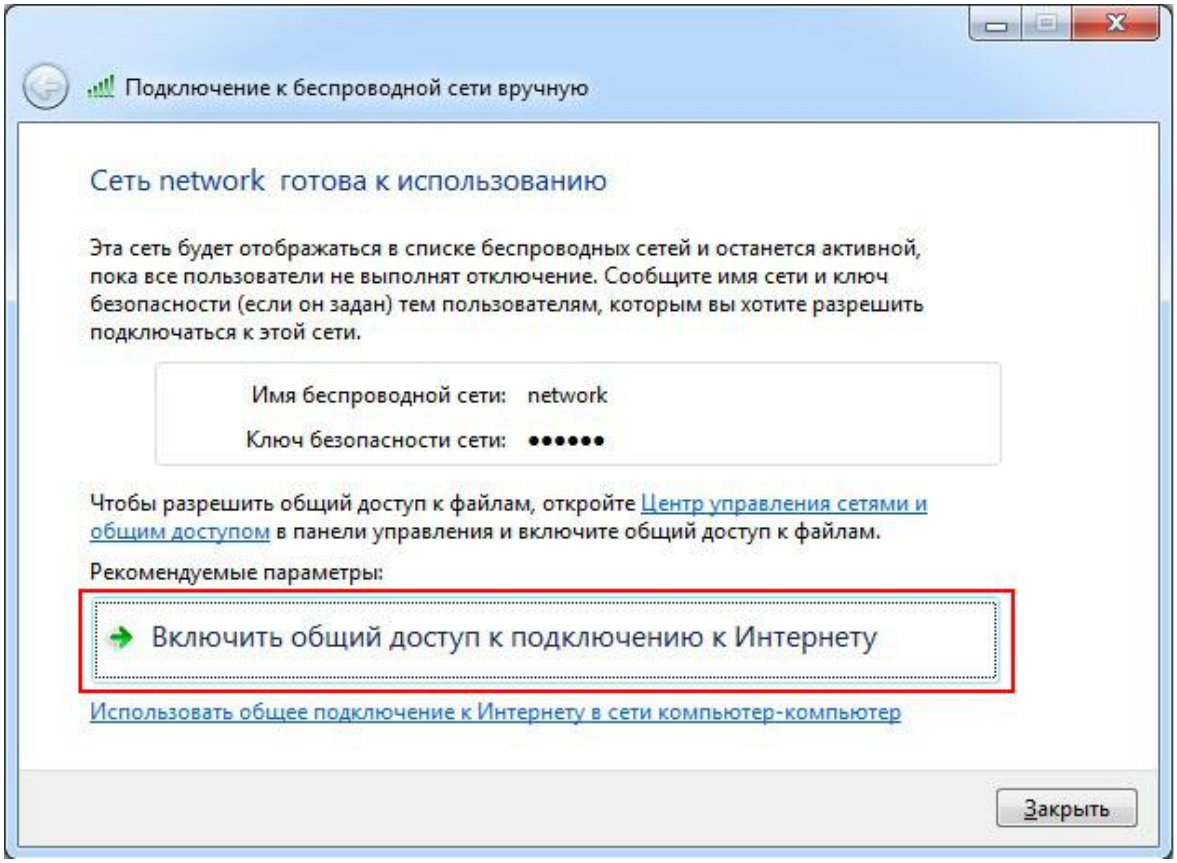

Рис. 19. **Підключення загального доступу**

Налаштування інших комп'ютерів мережі

На кожному комп'ютері налаштувати ім'я робочої групи і комп'ютера так само, як і для головного комп'ютера. Слід пам'ятати, що кожен комп'ютер мережі повинен мати унікальне ім'я і входити до складу однієї і тієї ж робочої групи.

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. 20).

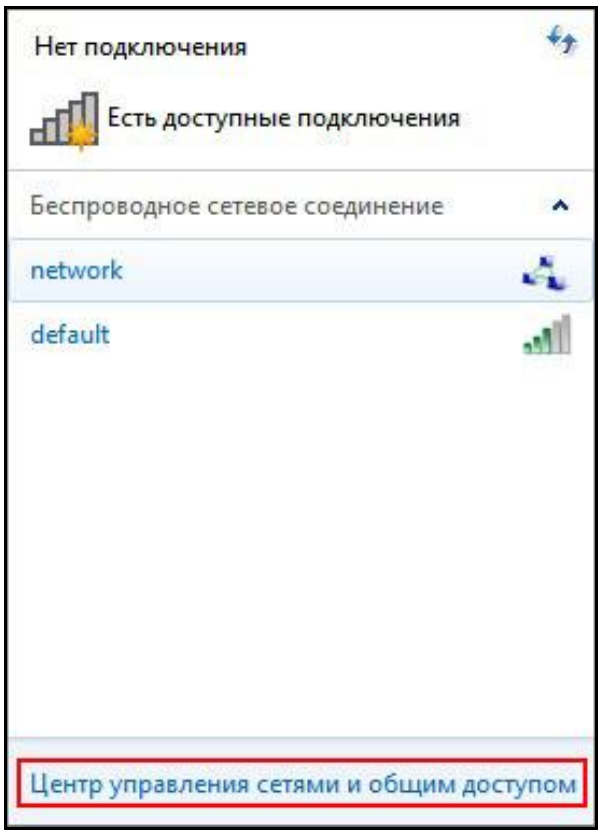

Рис. 20. **Вибір бездротової мережі для підключення**

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

Клацнувши правою кнопкою миші по значку бездротового мережевого адаптера, вибрати пункт *Свойства*. У вікні, що відкрилося, вибрати пункт *Протокол Интернета версии 4 (TCP/IPv4)* і змінити його властивості (рис. 21).

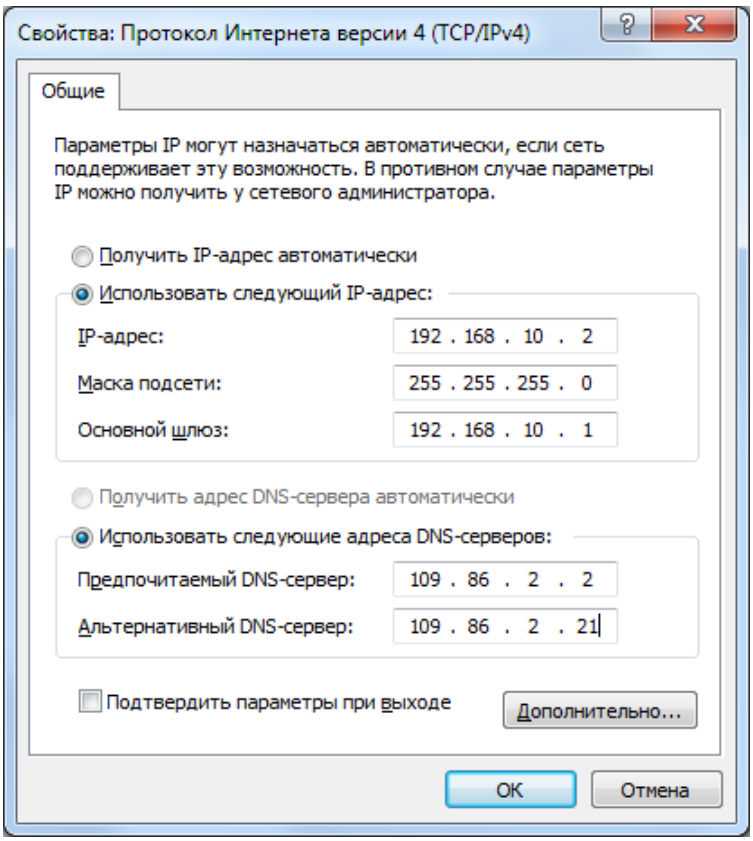

Рис. 21. **Налаштування властивостей протокола (TCP/IPv4)**

Відзначити пункт *Использовать следующий IP-адрес:*

У полі *IP-адрес:* назначити 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. Так як на головному комп'ютері бездротовому адаптеру 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 натисканням кнопки *ОК*.

На цьому настройки бездротової мережі Wi-Fi "комп'ютер–комп'ютер" в Windows 7 закінчені.

Для підключення комп'ютера до бездротової мережі клацнути по значку мережевого з'єднання, а потім двічі по створеній мережі. Ввести пароль (ключ безпеки) і натиснути кнопку *ОК*.

Література: основна [2; 5]; додаткова [7]; ресурси мережі Інтернет [9].

Тема 7. Основи інформаційної безпеки

Самостійна робота № 6. Застосування засобів шифрування операційної системи Windows

Мета роботи: практичні навички з застосування стандартних програм шифрування операційної системи (ОС) Windows.

У результаті виконання самостійної роботи у студента формуються **компетентності** з практичного застосовувати програмних засобів захисту ОС.

Результатом виконання самостійної роботи є практичне застосування засобів ОС для шифрування файлів.

Завдання для самостійної роботи

1. Уважно вивчити особливості системи шифрування ОС Windows. Пам'ятайте – можливі помилки у використанні системи шифрування можуть призвести до втрати інформації!
2. Створити тимчасову папку, де зберегти 2–3 текстових файлів.
3. Створити пару ключів – закритий і публічний за допомогою системи шифрування Windows.
4. Додати 2 користувачів, які б могли теж користуватись зашифрованим файлом.
5. Використовуючи щойно створений закритий ключ зашифрувати файли в тимчасовій папці.
6. Зберегти особистий ключ для подальшого використання.

Контрольні запитання для самодіагностики

1. Які методи захисту інформації ви знаєте?
2. Що таке цифровий підпис?
3. Перелічіть ситуації, коли необхідно застосовувати засоби шифрування інформації в мультимедійному видавництві.
4. Назвіть основні помилки у процесі вибору паролів.
5. Яку кримінальну відповідальність визначають закони України за комп'ютерні злочини?

6. Чому фізичний захист не може гарантувати безпеку?

7. Як інакше називається шифрування з секретним ключем?

8. У чому відмінність симетричних і несиметричних алгоритмів шифрування?

9. Перелічіть можливості програми PGP.

Довідкові матеріали до самостійної роботи

Засоби шифрування ОС Windows

Отже, один із методів, який може захистити дані без величезних витрат, це шифрування. З появою Windows2000 фірма Microsoft вирішила надати користувачам можливість досить серйозного шифрування. Той же алгоритм шифрування, практично без змін, перейшов і в Windows XP, і в Windows 7.

Шифрування вбудовано в операційну систему, шифрується все просто, працює дуже швидко, але досить надійно. Але може бути й недоліком й іноді користувачі, які не розуміють того, як це працює, замість того щоб зберегти, безповоротно втрачають свої дані. Тим часом, якщо трохи подбати заздалегідь, то можна повністю убезпечити себе від цього, і мати можливість відновити свої дані навіть після повного краху системи.

Що бачить користувач

Убудовані в ОС функції шифрування можна задіяти тільки на дискових розділах, які відформатовані під NTFS. Але якщо ця умова дотримана, то зашифрувати що-небудь елементарно. Для цього достатньо відкрити властивості файла або папки, натиснути кнопку *Другие*, й у вікні, встановити прапорець *Шифровать содержимое для защиты данных*. Натисканням на OK закрити вікна. Тепер, якщо відкрити це ж вікно ще раз, стане доступною кнопка *Подробно*, натиснувши на яку можна побачити ще одне вікно. З його допомогою можна додати, хто ще із зареєстрованих на машині користувачів може користуватися зашифрованим файлом. Якщо користувача, якого ви хочете додати, немає в списку можливих, це означає, що він не має відповідного сертифіката та ключа. Зашифруйте цим користувачем хоч один файл або папку, після чого спробуйте ще раз, потрібний користувач повинен з'явитися. Дозволяючи іншим користувачам користуватися зашифрованими файлами, не забувайте, що таким чином ви надаєте йому той же рівень контролю над шифруванням файла, який маєте самі. Тобто, він отримує можливість додавати або видаляти користувачів, які мають доступ до файла, а при бажанні зможе розшифрувати файл. Якщо після цього він зашифрує

його заново, з-під свого облікового запису, то ви втратите доступ до власного файла.

Залишається дати кілька порад, які допоможуть використовувати шифрування більш ефективно. Найбільш часто зустрічається помилка, яку здійснюють користувачі, бажаючі захистити свої файли, це шифрування всього одного файла, який, власне, і захищається. Однак, найчастіше цього недостатньо. У процесі роботи ваші файли цілком можуть виявитися і в інших місцях, таких, як TEMP або TMP папки. Крім цього, деякі програми (наприклад, Microsoft Office) у процесі роботи роблять тимчасові копії файлів, з якими працюють у тій же директорії, де знаходиться і оригінальний файл. Задумано це з благою метою, у випадку з Microsoft Office, наприклад, ці копії використовуються для відновлення файлів у разі збою. Але ці копії не зашифровані автоматично, тому ваші документи цілком можуть виявитися прочитаними не тими, ким вам хотілося б. Що б цього не сталося, доцільно шифрувати не окремі файли, а папки де вони зберігаються. Крім цього, не забудьте зашифрувати і TEMP папку. Цим ви захистите себе, і якщо які-небудь тимчасові файли або копії ваших даних, або документів будуть створюватися, вони будуть автоматично зашифровані.

Це що стосується зовнішнього боку, який видимий для користувача. Але для повного розуміння всіх потенційних проблем, які можуть виникнути під час використання шифрування, щоб знати чого варто і чого не варто очікувати від шифрування, не обійтися без того, щоб розглянути як працює шифрування "зсередини". Ця інформація необхідна і для того, щоб знати як вирішувати проблеми, що виникають з шифруванням. Найбільш частою проблемою, що зустрічається, є втрата інформації в результаті техногенних "катаклізмів", від яких не гарантований жоден комп'ютер, або в результаті помилок користувача, від яких не гарантований жоден із читачів.

Як це працює

Для шифрування EFS (Encrypted File System) використовує особистий і публічний ключі користувача, які генеруються коли користувач користується функцією шифрування вперше, і залишаються незмінними весь час, поки існує обліковий запис користувача. Причому на ці ключі нічого не впливає, користувач може змінювати свій пароль для входу в систему, перейменовувати свій обліковий запис, ключі залишаться незмінними так довго, як довго користувач буде мати той самий "security identifie " (SID). Під час видалення облікового запису віддаляються і ключі, і якщо створити заново обліковий запис з таким самим ім'ям, паролем,

і всім іншим, то новостворений користувач не буде мати ніякого ключа, до тих пір поки не зашифрує хоча б один файл або папку. Як тільки він це зробить, згенерує нові ключі, які, звичайно ж, не матимуть нічого спільного з ключами, які використовував обліковий запис з таким самим ім'ям раніше. Під час шифрування файла EFS генерує випадковий симетричний ключ, довжиною 128 біт, для кожного файла різний, який називається "File Encryption Key" (FEK). Цей ключ використовується для шифрування файла з використанням одного з варіантів Data Encryption Standard (DES) алгоритму – DESX. Після того як файл зашифрований, FEK зберігається разом з файлом, але теж шифрується, вже за алгоритмом RSA, який заснований на використанні публічного та відомого всім (для шифрування) і особистого, що не відомий нікому (для розшифровки) ключів користувача (рис. 22).

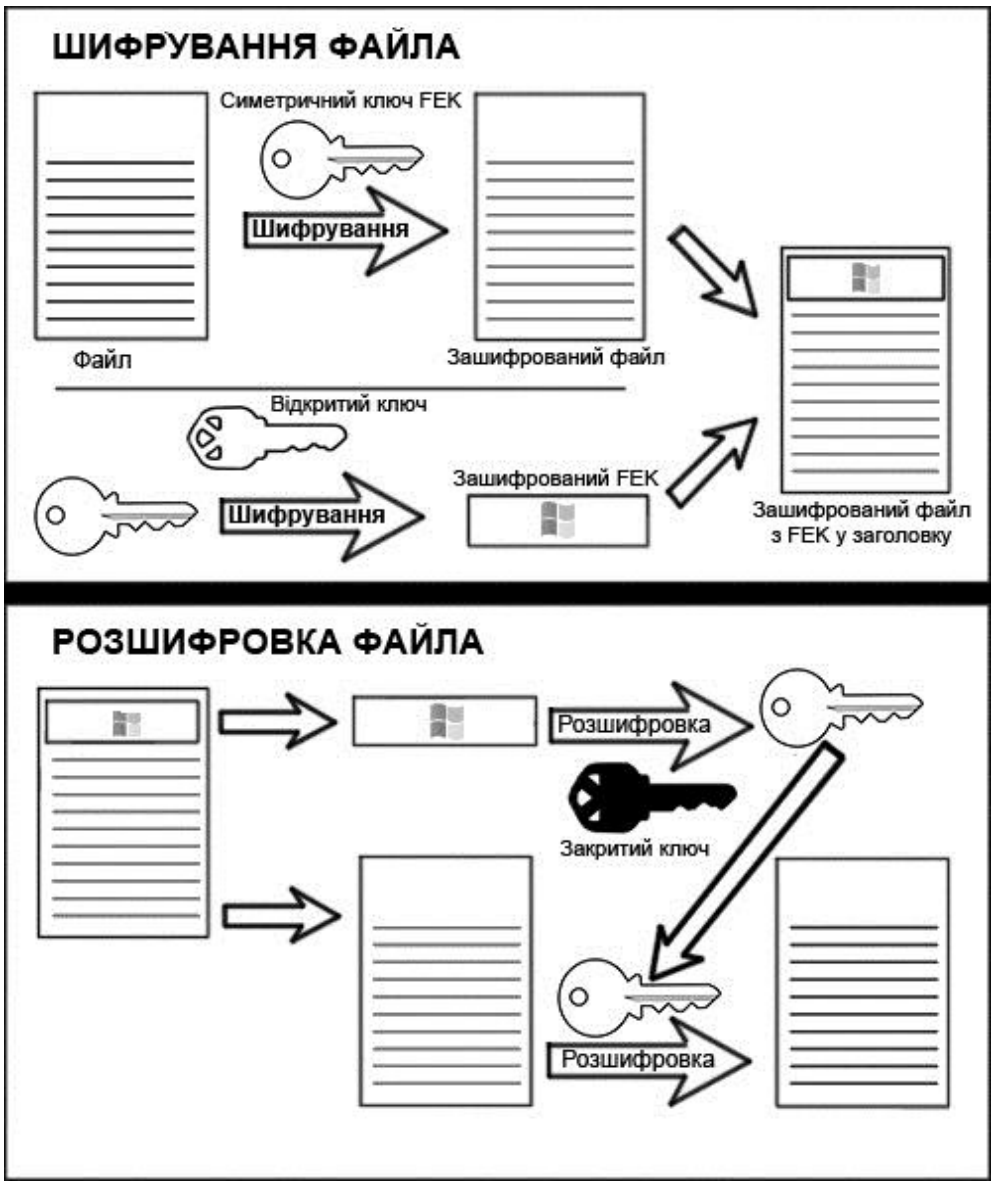

Рис. 22. **Алгоритм EFS**

Таким чином, для того, щоб розшифрувати вміст файла, потрібно знати FEK, але для того, щоб розшифрувати FEK, потрібно знати особистий ключ користувача, який зашифрував файл. Такі складнощі потрібні для прискорення роботи функцій шифрування, із збереженням досить високої надійності. DESX є симетричним алгоритмом, тобто для шифрування і розшифровки використовується один і той самий ключ. Це не дуже надійно, зате працює такий алгоритм дуже швидко, і з його допомогою можна шифрувати і розшифровувати великі обсяги даних практично в реальному часі. Для того, щоб забезпечити надійність шифрування FEK і шифрується по асиметричному алгоритму RSA, коли для шифрування і розшифровки використовуються різні ключі. Це занадто повільно, щоб шифрувати таким чином великі обсяги даних, але для шифрування FEK, RSA з використанням відкритого та особистого ключів підходить якнайкраще.

Збереження ключа

Що робити користувачеві, який працює на своєму комп'ютері та хоче мати можливість відновити свої файли в разі краху або переустановлення системи? Це зробити не складно. Все що потрібно, це зберегти свій особистий ключ, який використовується для розшифровки FEK захищених файлів, зашифрованих за допомогою відкритого ключа цього користувача. Для експорту особистого ключа можна запустити Internet Explorer, виконати команду **Сервис-Свойства браузера**. На закладці *Содержание* натисканням на кнопку *Сертификати* відкрити вікно сертифікатів. На закладці *Личные* вибираємо користувача, для якого потрібно експортувати особистий ключ, і натискаємо на кнопку *Экспорт*.

Якщо потрібного користувача в цьому вікні немає, це означає що цей користувач не має особистого і публічного ключа. Це означає, що цей користувач ще жодного разу не використовував функцій шифрування. Закрийте вікно, зашифруйте який-небудь файл або папку, і спробуйте ще раз. Після натискання на кнопку *Экспорт* відкриється вже знайоме вам вікно майстра експорту сертифікатів. Натискаємо на *Далее*, у наступному вікні встановлюємо перемикач *Да, экспортировать закрытый ключ*, знову натискаємо на *Далее*. На наступній закладці залишаємо настройки за замовчуванням, не потрібно відзначати пункт *Удалить закрытый ключ*, тому що в цьому випадку ви втратите можливість розшифровувати зашифровані вами файли. Натискаємо на *Далее*, вводимо і підтверджуємо пароль, яким хочемо захистити експортований ключ,

знову тиснемо на *Далее*, вказуємо де слід зберегти файл, задаємо йому ім'я, і ми маємо черговий PFX файл, в якому зберігається ваш особистий ключ. Цей ключ підходить для всіх файлів, зашифрованих цим користувачем. Збережіть його в надійному місці, у разі чого-небудь непередбаченого цей файл ваша остання надія на відновлення зашифрованих даних. Але не забувайте, що цей самий файл може допомогти не тільки вам, але і будь-якому зловмисникові, який захоче отримати доступ до ваших файлів.

Але, так чи інакше, перед нами стоїть завдання як отримати доступ до зашифрованого файла, профіль користувача загублений, але, на щастя, залишився особистий ключ користувача. Все що потрібно, це імпортувати цей ключ у профіль користувача, який повинен мати доступ до файлів.

Для того щоб імпортувати ключ, потрібно знову запустити Internet Explorer, виконати команду **Сервис-Свойства обозревателя**. На закладці *Содержание* натисканням на кнопку *Сертификаты* відкрити вікно сертифікатів. На закладці *Личные* вибираємо користувача, для якого потрібно імпортувати особистий ключ, і натискаємо на кнопку Імпорт. Запуститься майстер імпорту сертифікатів. Натискаємо на *Далее*, вказуємо на заздалегідь збережений PFX файл з особистим ключем, знову натискаємо на *Далее*, в наступному вікні вводимо пароль, яким захищено файл, знову натискаємо на *Далее*, на наступній закладці відзначаємо пункт *Поместить все сертификаты в следующее хранилище*, натискаємо на кнопку *Обзор*, вказуємо папку *Личные*, клацаємо на *ОК*, *Далее* і *Готово*.

Якщо все було зроблено правильно, і ви нічого не наплутали з експортом та імпортом, якщо всі ключі і файли підходять один до одного, то в результаті всіх цих заплутаних операцій ви отримаєте можливість прочитати здавалося б безповоротно втрачені файли.

Мережеві екрани (firewall, або брандмауери)

Брандмауер (firewall) – це пристрій контролю доступу в мережу, призначене для блокування всього трафіку, за винятком дозволених даних.

Екран – це засіб розмежування доступу клієнтів з серверів однієї множини інформаційних систем до серверів з іншої множини. Екран здійснює свої функції, контролюючи всі інформаційні потоки між двома множинами систем (рис. 23). Контроль потоків полягає в їхній фільтрації, можливо, з виконанням деяких перетворень.

Міжмережеві екрани дозволяють здійснювати централізоване управління безпекою. В одній конфігурації адміністратор може налаштувати дозволений вхідний трафік для всіх внутрішніх систем організації.

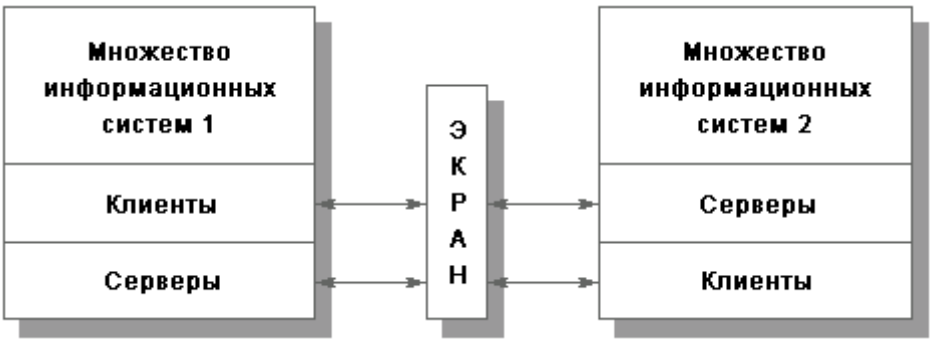

Рис. 23. **Екран як засіб розмежування доступу**

Визначення типів міжмережевих екранів

Існують два основних типи міжмережевих екранів : міжмережеві екрани прикладного рівня і міжмережеві екрани з пакетною фільтрацією. В їх основі лежать різні принципи роботи, але при правильному налаштуванні обидва типи пристроїв забезпечують правильне виконання функцій безпеки, які полягають у блокуванні забороненого трафіку.

Міжмережеві екрани прикладного рівня, або проксі – екрани, які становлять програмні пакети, що базуються на операційних системах загального призначення (таких, як Windows NT, XP,7) або на апаратній платформі міжмережевих екранів. Міжмережевий екран володіє декількома інтерфейсами, по одному на кожну з мереж, до яких він підключений. Набір правил визначає, яким чином трафік передається з однієї мережі в іншу. Якщо в правилі відсутній явний дозвіл на пропуск трафіку, міжмережевий екран відхиляє чи анулює пакети.

У процесі використання брандмауера прикладного рівня всі з'єднання проходять через нього (рис. 24). Як показано на малюнку, з'єднання починається на системі-клієнті і надходить на внутрішній інтерфейс брандмауера. Брандмауер приймає з'єднання, аналізує вміст пакету та використовуваний протокол і визначає, чи відповідає даний трафік правилам політики безпеки. Якщо це так, то міжмережевий екран ініціює нове з'єднання між своїм зовнішнім інтерфейсом і системою-сервером.

Міжмережеві екрани прикладного рівня використовують модулі доступу для вхідних підключень. Модуль доступу в міжмережевому екрані приймає вхідне підключення і обробляє команди перед відправкою трафіку одержувачу. Таким чином, міжмережевий екран захищає системи від атак, які виконуються за допомогою додатків.

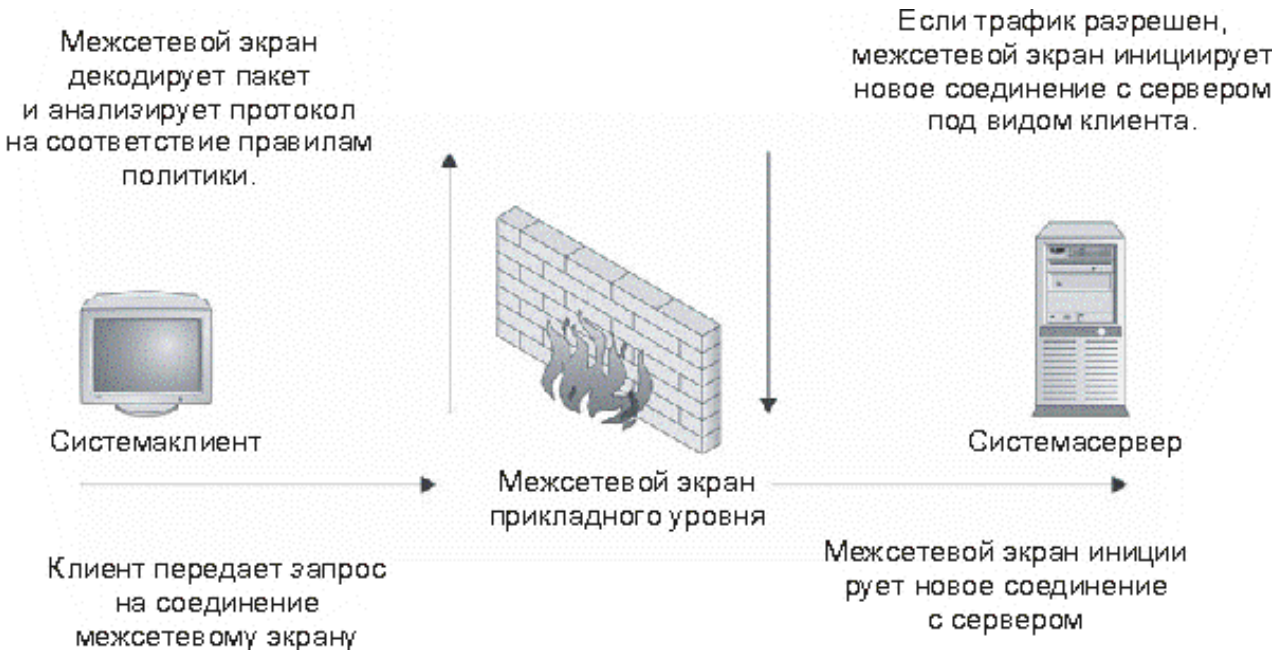

Рис. 24. **Сполуки модуля доступу брандмауера прикладного рівня**

Міжмережеві екрани прикладного рівня містять модулі доступу для найбільш часто використовуваних протоколів, таких, як HTTP, SMTP, FTP і Telnet. Деякі модулі доступу можуть бути відсутні. Якщо модуль доступу відсутній, то конкретний протокол не може використовуватися для з'єднання через міжмережевий екран.

Брандмауер також приховує адреси систем, розташованих по інший бік від нього. Так як усі з'єднання ініціюються і завершуються на інтерфейсах брандмауера, внутрішні системи мережі не видно безпосередньо ззовні, що дозволяє приховати схему внутрішньої адресації мережі.

Брандмауер в ОС Windows

Як записано в довідці Windows – Брандмауер використовується для захисту комп'ютера від несанкціонованого доступу через мережу або Інтернет. Брандмауер вбудований у Windows і включений автоматично для захисту комп'ютера від вірусів та інших погроз безпеці.

Брандмауер відрізняється від антивірусного програмного забезпечення, проте їх спільна робота забезпечує надійний захист комп'ютера. Можна сказати, що брандмауер охороняє вікна та двері від проникнення невідомих і небажаних програм, у той час як антивірусне програмне забезпечення запобігає появі вірусів або інших загроз безпеці, які прагнуть пробратися через парадний вхід.

Щоб відкрити і налаштувати компонент "Брандмауер Windows", натисніть кнопку Пуск, вибрати команду **Настройка-Панель управления**, а потім двічі клацніть значок Брандмауер Windows.

Література: основна [2]; додаткова [6]; ресурси мережі Інтернет [16].

Самостійна робота № 7. Робота з програмою PGP

Мета роботи: практичні навички з застосування програми шифрування PGP.

У результаті виконання самостійної роботи у студента формуються **компетентності** з практичного застосування програмних засобів захисту.

Результатом виконання самостійної роботи є практичне застосування програми PGP для шифрування файлів і цифрового підпису електронної пошти.

Завдання для самостійної роботи

1. Створити закритий ключ. Використовувати в рядку "Full name" своє ім'я та групу, наприклад "Коваленко О. І., група 6.04.61.11.0".

2. Використовуючи щойно створений закритий ключ створити на диску відкритий ключ.

3. Надіслати відкритий ключ викладачеві електронною поштою у вигляді вкладеного файла. Адресу електронної пошти уточнити у викладача.

4. Дочекатися, коли вам прийде поштою відкритий ключ викладача, зберегти його на диску і встановити в програмі PGP.

5. Створити у редакторі MS Word документ з коротким звітом про виконану самостійну роботу. Вставити в документ свою фотографію. Підписати файл цифровим підписом, використовуючи для цього свій закритий ключ і відкритий ключ викладача.

6. Відправити цей файл по електронній пошті у вигляді вкладення викладачу.

7. Дочекатися відповіді від викладача з повідомленням про те, що самостійна робота здана. Розшифрувати вкладений в лист файл.

8. Пред'явити вміст цього файла викладачеві.

Контрольні запитання для самодіагностики

1. Які методи захисту інформації ви знаєте?
2. Що таке цифровий підпис?
3. Перелічіть ситуації, коли необхідно застосовувати засоби шифрування інформації в мультимедійному видавництві.
4. Назвіть основні помилки у процесі вибору паролів.
5. Яку кримінальну відповідальність визначають закони України за комп'ютерні злочини?
6. Чому фізичний захист не може гарантувати безпеку?
7. Як інакше називається шифрування з секретним ключем?
8. У чому відмінність симетричних і несиметричних алгоритмів шифрування?
9. Перелічіть можливості програми PGP.

Довідкові матеріали до самостійної роботи

PGP – це криптографічна (шифрувальна) програма з високим ступенем надійності, яка дозволяє користувачам обмінюватися інформацією в електронному вигляді в режимі повної конфіденційності. Творець PGP Пилип Циммерман відкрито опублікував код програми, який неодноразово був досліджений фахівцями – криптоаналітиками високого класу – і жоден з них не знайшов у програмі яких-небудь слабких місць.

Головна перевага цієї програми полягає в тому, що для обміну зашифрованими повідомленнями користувачам немає необхідності передавати один одному секретні ключі, оскільки в програмі PGP застосовується принцип використання відкритого і закритого ключів. До закритого ключа має доступ тільки користувач програми, а відкритий ключ розповсюджується серед кореспондентів користувача за допомогою мережі Інтернет або будь-яким іншим способом. Ключі – це дуже великі числа (1024 біт і більше), і їх практично неможливо зламати.

1. Створення закритого та відкритого ключа

Щоб створити закритий ключ необхідно відкрити головне вікно роботи з ключами (рис. 25). Зробити це можна через меню **Пуск-Programs-PGP-GPkeys**.

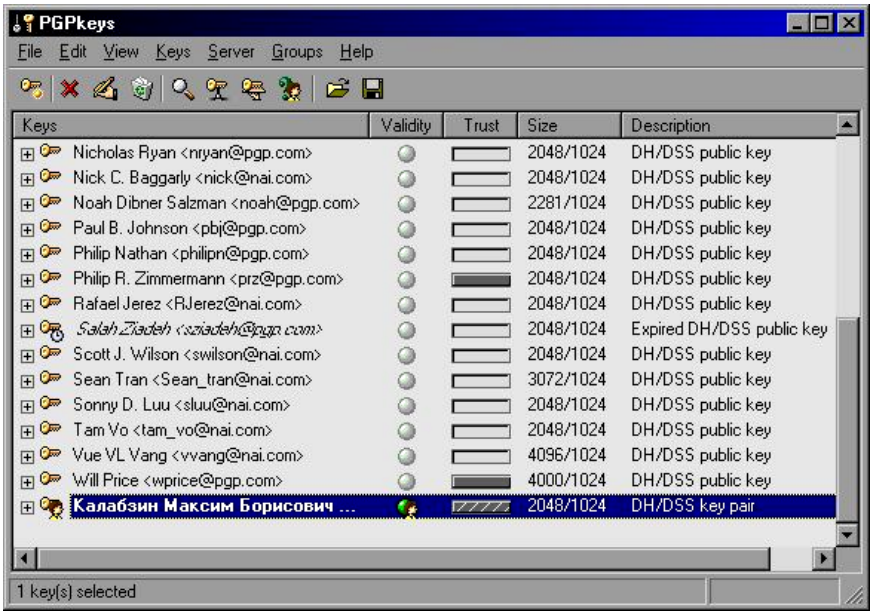

Рис. 25. **Вікно роботи з ключами**

Для створення закритого ключа:

1. Натиснути на кнопку або вибрати команду **Keys-New key**. Запуститься Майстер створення нового закритого ключа.

2. Ввести своє ім'я, прізвище, по батькові та адресу електронної пошти (якщо його немає, поле можна залишити порожнім і на наступне попередження про відсутність адреси натиснути **Да (Yes)**) та натиснути кнопку *Далее*.

3. Далі Майстер запросить спеціальні параметри шифрування: тип криптоалгоритма, довжина ключа (чим довший ключ, тим надійніший) можна залишити ті, які він пропонує встановити за замовчуванням, натискаючи кожного разу кнопку *Далее.*

4. Введення ключової фрази. Дуже важливий пункт. Ключова фраза потрібна для того, щоб ніяка стороння людина не змогла скористатися вашим ключем (наприклад, якщо він буде вкрадений з диска). Фразу необхідно ввести в обох полях відповідного вікна (рис. 26).

Довжина фрази – не менше 8 символів і не повинна містити спеціальних символів. Цю фразу необхідно завжди пам'ятати, в іншому випадку ви не зможете скористатися вашим ключем.

5. Після введення ключової фрази і відповідей ще на два питання (необхідно вибрати те, яке запропонує програма за замовчуванням і натиснути кнопку *Далее*) відбудеться генерація закритого ключа, після чого він відразу ж з'явиться в основному вікні управління ключами. Таким же чином можна створити будь-яку кількість закритих ключів.

Рис. 26. **Введення ключової фрази**

Створення відкритого ключа

Відкритий ключ потрібен для того щоб користувач, якому адресовано документ, міг його розшифрувати. Для генерації відкритого ключа вибрати потрібний закритий ключ і натиснути кнопку, або вибрати команду **Keys/Export**. У вікні ввести ім'я файла, вибрати каталог і натиснути кнопку *Сохранить*. Програма створить закритий ключ і збереже його на диск. Цей ключ потрібно передати користувачеві, з яким ви будете обмінюватися документами.

Установка відкритого ключа на комп'ютер

Щоб розшифрувати документ, надісланий іншим користувачем, необхідно встановити на свій комп'ютер його відкритий ключ. Для цього запустити *Провідник*, вибрати за допомогою нього файл з відкритим ключем користувача (він має розширення *.asc) і запустити його. З'явиться вікно з інформацією про користувача (рис. 27).

Рис. 27. **Вікно користувача**

Натиснути кнопку *Import* для імпортування відкритого ключа в список ключів. Відкриється основне вікно для роботи з ключами і в списку з'явиться відповідний відкритий ключ.

2. Шифрування документів цифровим підписом

Для шифрування документів цифровим підписом необхідно мінімум два ключа: свій власний закритий ключ і відкритий ключ, який будь-яким способом необхідно дати користувачеві, з яким відбувається обмін документами.

Щоб зашифрувати документ цифровим підписом:

1. Відкрити будь-яку програму для роботи з файлами, наприклад, *Провідник*. Вибрати потрібний файл, групу файлів або каталог правою кнопкою миші. Відкриється меню операцій над файлами. Вибрати у контекстному меню пункт **PGP/Encrypt & Sign**.

У вікні для вибору ключів необхідно вибрати зі списку ключів свій закритий ключ, а також відкритий ключ того користувача, якому призначений цей документ. Якщо документ призначений для декількох користувачів, необхідно вибрати їх відкриті ключі. Вибір проводиться подвійним клацанням миші по потрібному ключу у списку. Натиснути кнопку *ОК* після завершення вибору.

2. Ввести ключову фразу. Ключову фразу потрібно вводити для обраного закритого ключа (у кожного закритого ключа може бути своя ключова фраза).

Натиснути кнопку *ОК*. Якщо ключова фраза введена, відбудеться шифрування документа цифровим підписом. В іншому випадку необхідно повторити введення ключової фрази.

3. Розшифровка документа, підписаного цифровим підписом

Для розшифровки документа, підписаного цифровим підписом, відкрийте *Провідник*, вибрати зашифрований файл (він має розширення *.pgp), клацнути по ньому правою кнопкою миші і вибрати у контекстному меню пункт **PGP/Decrypt & Verify**. З'явиться вікно для введення ключової фрази. Необхідно ввести ключову фразу для закритого ключа, на основі якого був створений відкритий ключ, що використовується у документі.

Натиснути кнопку *ОК*. Якщо ключова фраза введена правильно, відбудеться розшифровка документа, про що свідчить повідомлення на

екрані. В іншому випадку (якщо повідомлення не з'явилося) ключову фразу необхідно ввести заново.

4. Завершення роботи програми PGP

Під час закриття програми PGP на екран видається повідомлення, що пропонується створити копії бази даних з ключами (це робиться з метою підвищення безпеки). Якщо копія не потрібна натиснути кнопку *Don't Save*.

Література: основна [2]; додаткова [6]; ресурси мережі Інтернет [15].

Рекомендована література

Основна

1. Климнюк В. Є. Комп'ютерні мережі та захист інформації : конспект лекцій. Ч. 1 / В. Є. Климнюк, В. М. Гіковатий. – Х. : Вид. ХНЕУ, 2008. – 98 с.

2. Климнюк В. Є. Комп'ютерні мережі та захист інформації : конспект лекцій / В. Є. Климнюк. – Х. : Вид. ХНЕУ, 2011. – 128 с.

3. 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.

4. Методичні рекомендації до виконання лабораторних робіт з навчальної дисципліни "Комп'ютерні мережі" для студентів спеціалізації "Комп'ютеризовані технології та системи видавничо-поліграфічного виробництва усіх форм навчання / укл. В. Є. Климнюк, В. М. Гіковатий. – Х. : Вид. ХДЕУ, 2009. – 64 с.

5. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. Г. Олифер. – 3-е изд. – СПб. : Питер, 2006. – 958 с.

Додаткова

6. Пономаренко В. С. Основи захисту інформації : навч. посібн. / В. С. Пономаренко, І. В. Журавльова, В. В. Туманов. – Х. : Вид. ХДЕУ, 2003. – 176 с.

7. Рошан Педжман. Основы построения беспроводных локальных сетей стандарта 802.11 / Педжман Рошан, Джонатан Лиери ; пер. с англ. – М. : Изд. дом "Вильямс", 2004. – 304 с.

Ресурси мережі Інтернет

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

9. Настройка Wi-Fi сети компьютер-компьютер в Windows 7 [Електроний ресурс]. – Режим доступу : http://www.notebook-media.ru/glavnaya-kategoriya/nastroyka-wi-fi-seti-kompiuter-kompiuter-v-windows-7.html.

10. Обзор протокола IPv6. [Електроний ресурс]. – Режим доступу : http://www.asmodeus.com.ua/library/nets/proto/ip_v6/ip_v6.html.

11. Портал Безпека [Электронный ресурс]. – Режим доступа : www.bezpeka.com.

12. Программа шифрования PGP [Электронный ресурс]. – Режим доступа : http://www.nexus.ua/programma-shifrovaniya-pgp.

13. Скрытый потенциал Windows 7: настройка сети, управление устройствами [Электронный ресурс]. – Режим доступа : http://www.3dnews.ru/590575.

14. Что такое оптоволокно? [Электронный ресурс]. – Режим доступа : http://d-lan.dp.ua/optovolokno.

15. PGP. Краткое руководство. [Электронный ресурс]. – Режим доступа : http://uvsr.stu.ru/f/index.php?action=downloadfile&filename=pgp.doc&directory=CKCiT/4_KURS&PHPSESSID=a62duiv1gdj9ujg20323b1em86.

16. Шифрование файлов — EFS. [Электронный ресурс]. – Режим доступа : http://youpk.ru/shifrovanie-faylov-efs/.

НАВЧАЛЬНЕ ВИДАННЯ

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

Укладач **Климнюк** Віктор Євгенович

Відповідальний за випуск **Пушкар О. І.**

Редактор **Лященко О. Г.**

Коректор **Маркова Т. А.**

План 2014 р. Поз. № 135.
Підп. до друку Формат 60×90 1/16. Папір MultiCopy. Друк Riso.
Ум.-друк. арк. 3,75. Обл.-вид. арк. 4,69. Тираж прим. Зам. №

Видавець і виготівник – видавництво ХНЕУ ім. С. Кузнеця, 61166, м. Харків, пр. Леніна, 9-А

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи ***Дк № 481 від 13.06.2001 р.***