МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

І. А. Терейковський, Л. О. Терейковська,
К. О. Радченко, С. О. Гнатюк

ЗАХИСТ ВЕБ-СЕРВІСІВ
ЛАБОРАТОРНИЙ ПРАКТИКУМ

Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для студентів,
які навчаються за спеціальністю 123 «Комп'ютерна інженерія»,
спеціалізацією «Комп'ютерні системи та компоненти»

Київ
КПІ ім. Ігоря Сікорського
2018

Рецензенти: *Козловський В. В.*, д-р техн. наук, проф.
Стеценко І. В., д-р техн. наук, проф.

Відповідальний редактор *Тесленко О. К.*, канд. техн. наук, доц.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 6 від 22.02.2018 р.) за поданням Вченої ради факультету прикладної математики (протокол № 5 від 21.12.2017 р.)

Електронне мережне навчальне видання

Терейковський Ігор Анатолійович, д-р техн. наук, доц.
Терейковська Людмила Олексіївна, канд. техн. наук, доц.
Радченко Костянтин Олександрович, асист.
Гнатюк Сергій Олександрович, д-р техн. наук, доц.

Захист веб-сервісів
Лабораторний практикум

Захист веб-сервісів: Лабораторний практикум [Електронний ресурс] : навч. посіб. для студ. спеціальності 123 «Комп'ютерна інженерія», спеціалізації «Комп'ютерні системи та компоненти» / І. А. Терейковський, Л. О. Терейковська, К. О. Радченко, С. О. Гнатюк; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,72 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2018. – 68 с.

Лабораторний практикум призначений для використання студентами під керівництвом викладача та самостійно на практичних та лабораторних заняттях із захисту інформації в комп'ютерних системах. Завданням даного практикуму є набуття студентами практичних навичок створення сучасних методів управління доступом до захищених ресурсів комп'ютерної системи; основних принципів захисту інформації, порядок формування комплексу засобів захисту інформації; принципів управління доступом до захищених ресурсів комп'ютерної системи;прийомів захисту інформації в операційних системах; проектування, розробки та застосування програмних засобів захисту інформації.

Зміст

ВСТУП

Дисципліна «Захист інформації в комп'ютерних системах» є важливою складовою підготовки кваліфікованих бакалаврів за спеціальністю 123 «Комп'ютерна інженерія».

Дисципліна «Захист інформації в комп'ютерних системах» включає такі важливі складові, як аналіз вимог до системи захисту інформації в комп'ютерних системах; обрання засобів захисту інформації об'єктів комп'ютерних систем; розробка системи захисту інформації в комп'ютерних системах; виконання базових операцій по застосуванню засобів захисту інформації в комп'ютерних системах тощо, які дозволяють вирішити задачі використання стеганографічних засобів захисту, визначення стійкості парольного захисту, налаштування оптимальних параметрів захищеності систем управління базами даних, оцінки стійкості захисту комп'ютерних мереж від атак з метою порушення доступності, розпізнання мережевих атак та практичного досвіду з розробки та використання відповідних засобів захисту.

Відповідно до наведених аспектів та згідно із робочою навчальною програмою дисципліни «Захист інформації в комп'ютерних системах» завданням даних методичних вказівок є набуття студентами практичних навичок створення сучасних методів управління доступом до захищених ресурсів комп'ютерної системи; особливостей інформації як об'єкту захисту нівелювання основних загроз інформації в комп'ютерних системах; основних принципів захисту інформації, порядок формування комплексу засобів захисту інформації; принципів управління доступом до захищених ресурсів комп'ютерної системи;прийомів захисту інформації в операційних системах; криптографічних методів і засобів захисту інформації; способів та засобів захисту інформації від витоку технічними каналами; порядок визначення вимог щодо захисту інформації в комп'ютерній системі; проектування, розробки та застосування програмних засобів захисту інформації.

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ЛАБОРАТОРНІ РОБОТИ

Даний лабораторний практикум охоплює наступні лабораторні роботи:

№ 1: "Технологія установки та першочергового налаштування Apache + PHP+ MySQL " (обсяг: 6 академічних годин).

№ 2: "Конфігурація параметрів захисту веб-серверу" (обсяг: 6 академічних годин).

№ 3: "Налаштування системи захисту СУБД MySQL" (обсяг: 6 академічних годин).

Порядок виконання лабораторних робіт

1. Ознайомлення з метою, загальним завданням та теоретичними відомостями відповідної лабораторної роботи.

2. Визначення варіанту завдання та розробка плану виконання роботи.

3. Виконання завдання, використовуючи вказані у завданні мови, технології, інструментальне програмне забезпечення тощо.

4. Тестування окремих програмних модулів та програми в цілому.

5. Підготовка відповідей на контрольні запитання до роботи.

6. Підготовка протоколу виконання лабораторної роботи.

7. Демонстрація викладачеві результатів функціонування програми.

Вимоги до формлення лабораторних робіт

Протокол має містити наступні складові частини, які розміщують кожний з нової сторінки: титульний аркуш, загальне завдання до лабораторної роботи, завдання за варіантом, діаграма структури програми із призначенням кожного модуля, текст програмного коду (2-4 сторінки), екранні форми («screenshots») візуального інтерфейсу програмних модулів, відповіді на контрольні запитання.

ЛАБОРАТОРНА РОБОТА № 1 «ТЕХНОЛОГІЯ УСТАНОВКИ ТА ПЕРШОЧЕРГОВОГО НАЛАШТУВАННЯ APACHE + PHP+ MYSQL»

Метою лабораторної роботи є оволодіння навичками установки та першочергового налаштування веб-сервера Apache, інтерпретатора PHP та бази даних MySQL.

Теоретичні відомості. Перед виконанням лабораторної роботи слід ознайомитись із розділами навчального посібника, що присвячені технології установки та першочергового налаштування веб-сервера Apache, інтерпретатора PHP та бази даних MySQL.

Завдання на лабораторну роботу:

1. Інсталювати веб-сервер Apache та вивчити особливості його налаштування.
2. Інсталювати інтерпретатор PHP5.
3. Інсталювати СУБД MySQL 5.
4. Перевірити працездатність Apache, PHP, MySQL в цілому.

Хід виконання роботи

Інсталяція веб-серверу Apache

1. Завантажуємо комп'ютер в режимі адміністратора. Відключаємо мережевий екран.

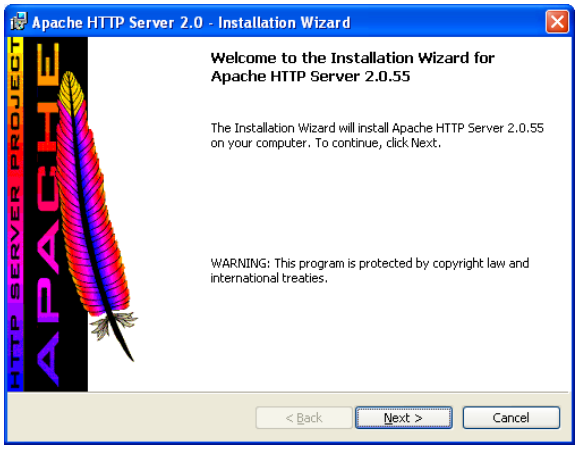

Рис. 1.1. Вікно першого етапу інсталяції Apache

2. Запускаємо інсталяційний пакет apache_2.0.55-win32-x86-no_ssl.msi (apache_2.2.9-win32-x86-no_ssl-r2.msi). У відповідь відкривається

показане на рис. 1.1 вікно першого етапу інсталяції Apache. Натискаємо кнопку „Next”.

3. У відповідь відкривається показане на рис. 1.2 вікно другого етапу інсталяції Apache. Встановлюємо показані на рис. 1.2 налаштування та натискаємо кнопку „Next”.

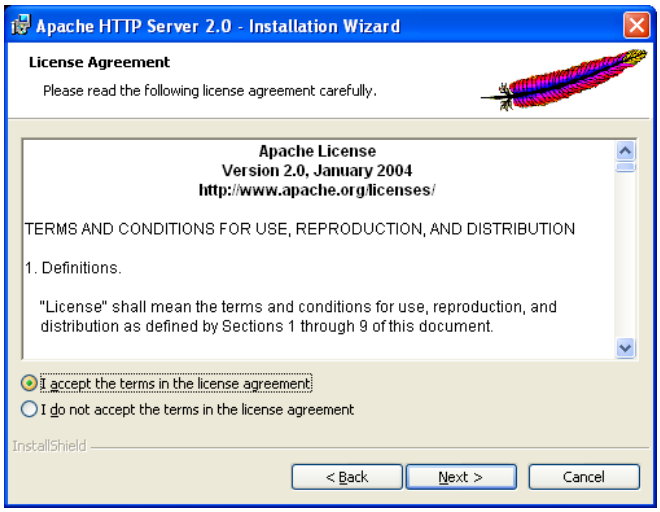

Рис. 1.2. Вікно другого етапу інсталяції Apache

4. У відповідь відкривається показане на рис. 1.3 вікно третього етапу інсталяції Apache. Ознайомлюємось з інформацією про веб-сервер та натискаємо кнопку „Next”.

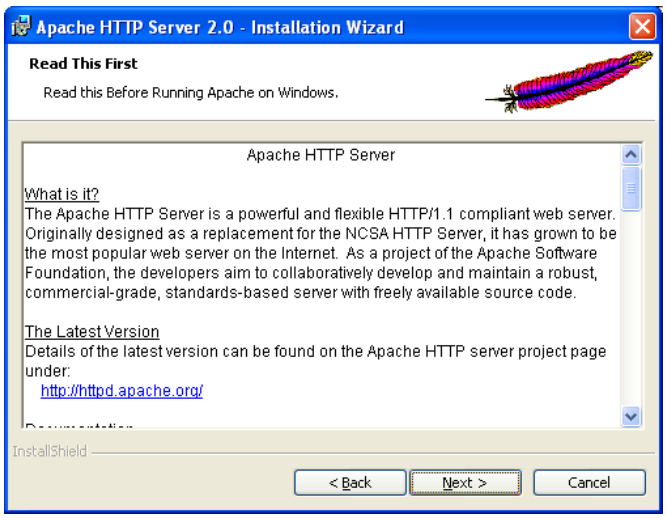

Рис. 1.3. Вікно третього етапу інсталяції Apache

5. У відповідь відкривається показане на рис. 1.4 вікно четвертого етапу інсталяції Apache. Встановлюємо показані на рис. 1.4 налаштування та натискаємо кнопку „Next”.

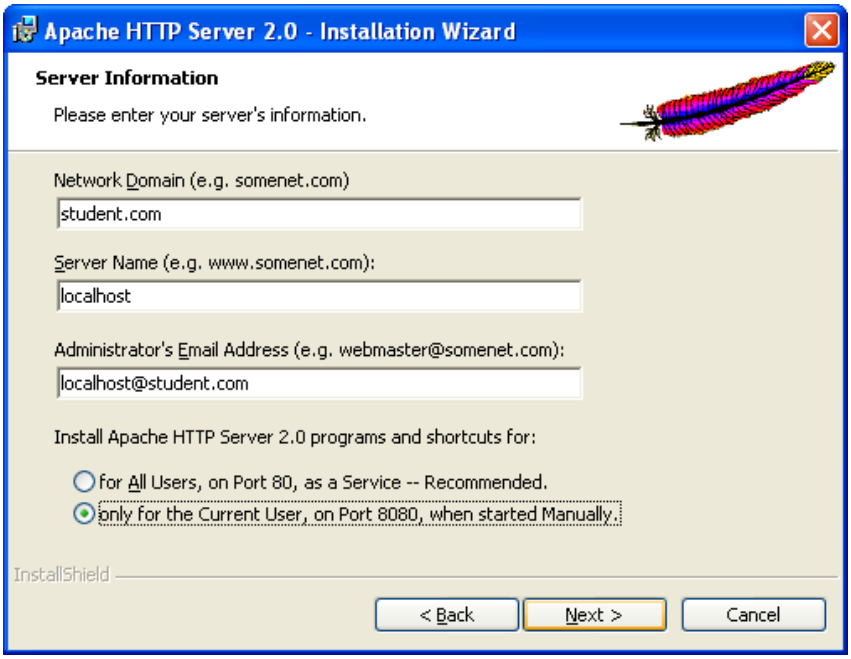

Рис. 1.4. Вікно четвертого етапу інсталяції Apache

6. У відповідь відкривається показане на рис. 1.5 вікно п’ятого етапу інсталяції Apache. Встановлюємо показані на рис. 1.5 налаштування та натискаємо кнопку „Next”.

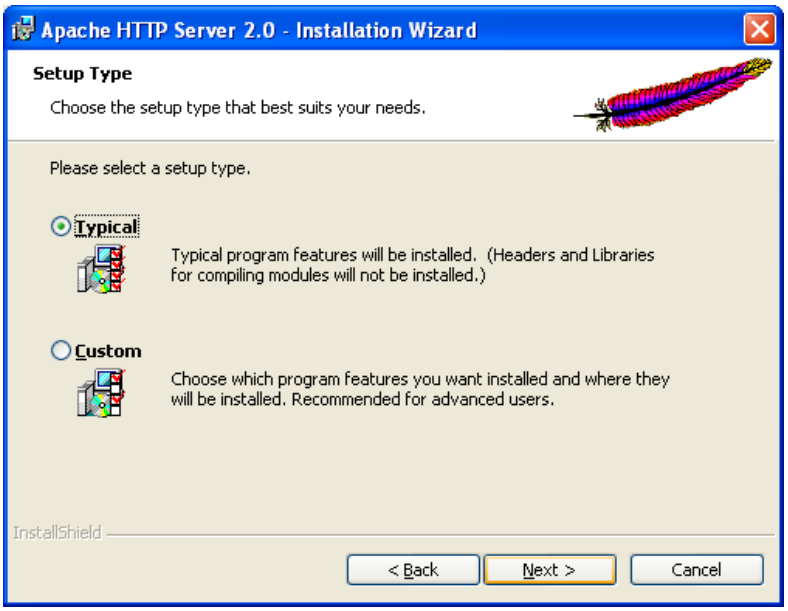

Рис. 1.5. Вікно п’ятого етапу інсталяції Apache

7. У відповідь відкривається показане на рис. 1.6 вікно шостого етапу інсталяції Apache. Залишаємо інсталяційну теку без змін та натискаємо кнопку „Next”. Якщо місцезнаходження до інсталяційної теки змінюється, то це слід відобразити у подальшому налаштуванню веб-серверу.

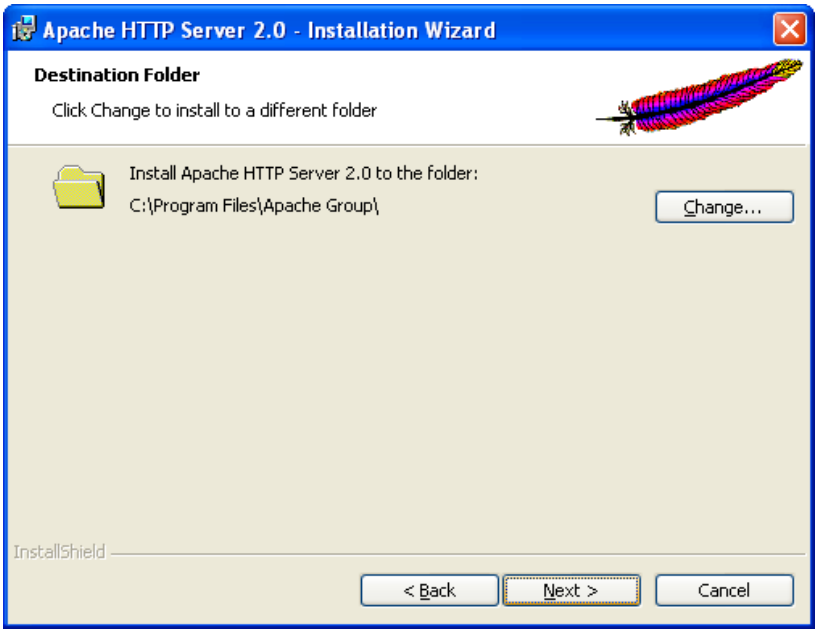

Рис. 1.6. Вікно шостого етапу інсталяції Apache

8. У відповідь відкривається показане на рис. 1.7 вікно сьомого етапу інсталяції Apache. Натискаємо кнопку „Install”.

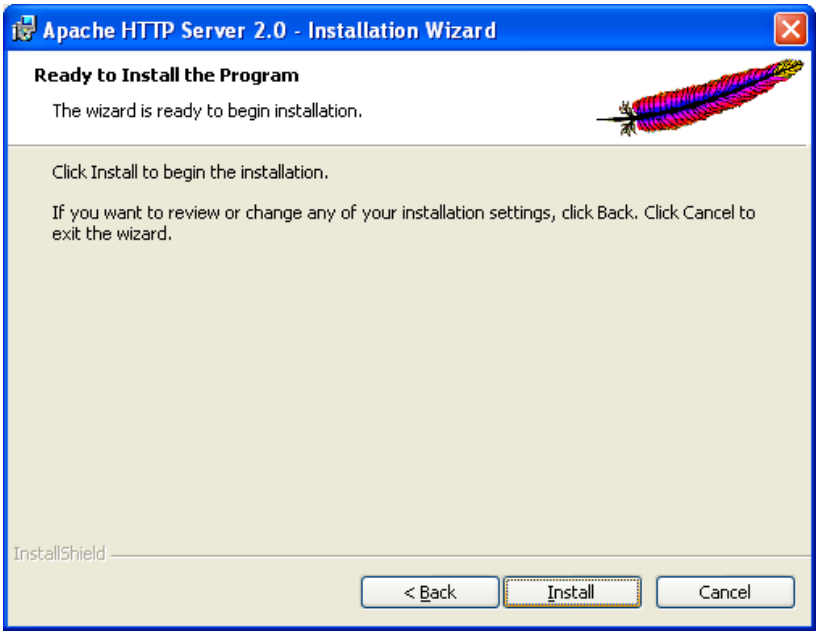

Рис. 1.7. Вікно сьомого етапу інсталяції Apache

9. У відповідь відкривається показане на рис. 1.8 вікно інформації про повноту та помилки при інсталяції Apache.

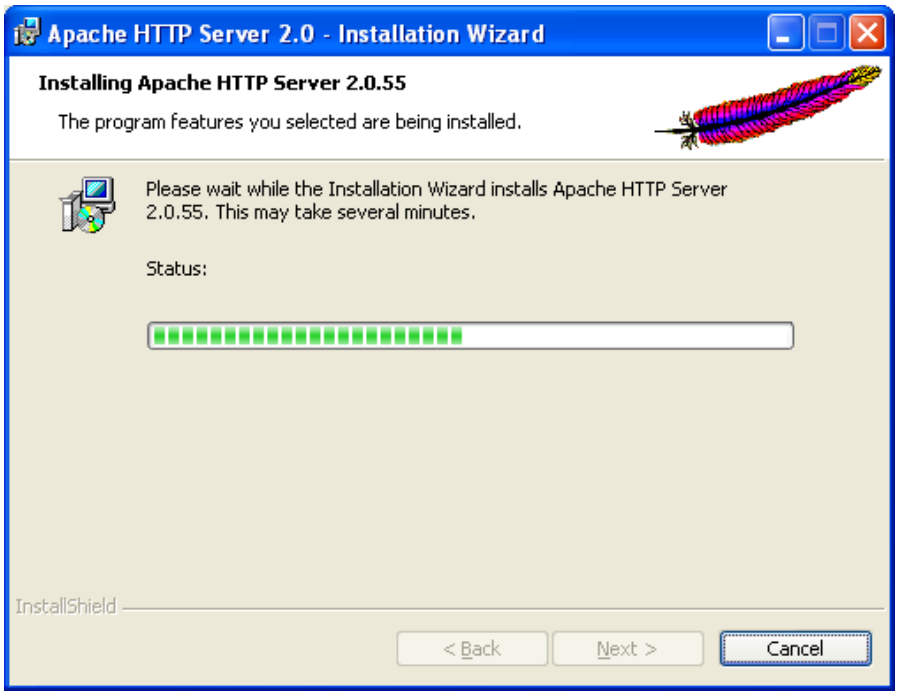

Рис. 1.8. Вікно восьмого етапу інсталяції Apache

10. Сигналом про успішну інсталяцію є поява показаного на рис. 1.9 вікна завершення установки веб-серверу.

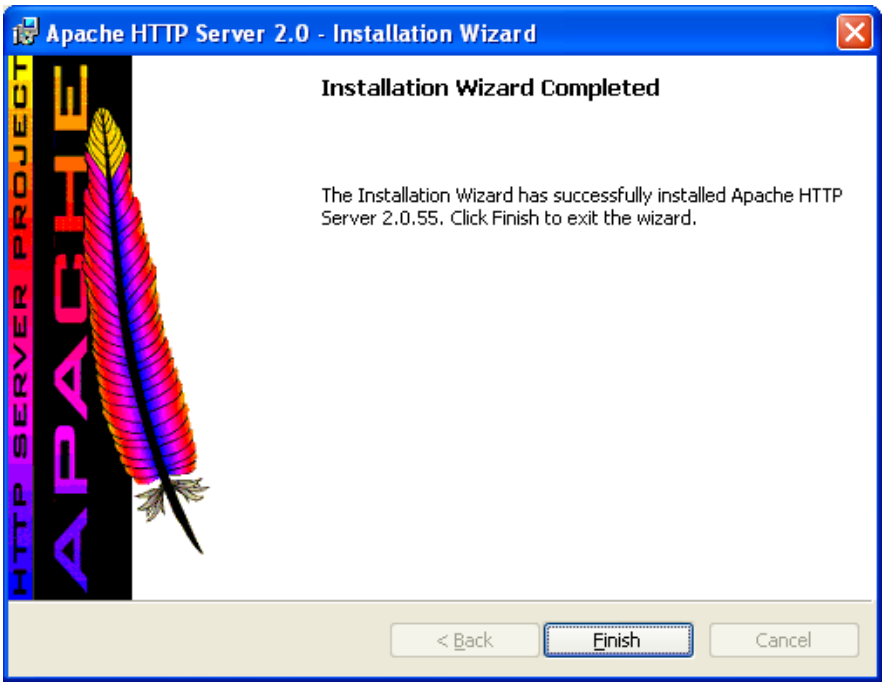

Рис. 1.9. Вікно завершального етапу інсталяції Apache

Налаштування веб-серверу

11. Відкриваємо теку *conf* розміщену за адресою C:\Program Files\Apache Group\Apache2\conf. Зміст теки показано на рис. 1.10. Знаходимо в означеній теці конфігураційний файл *httpd.conf*.

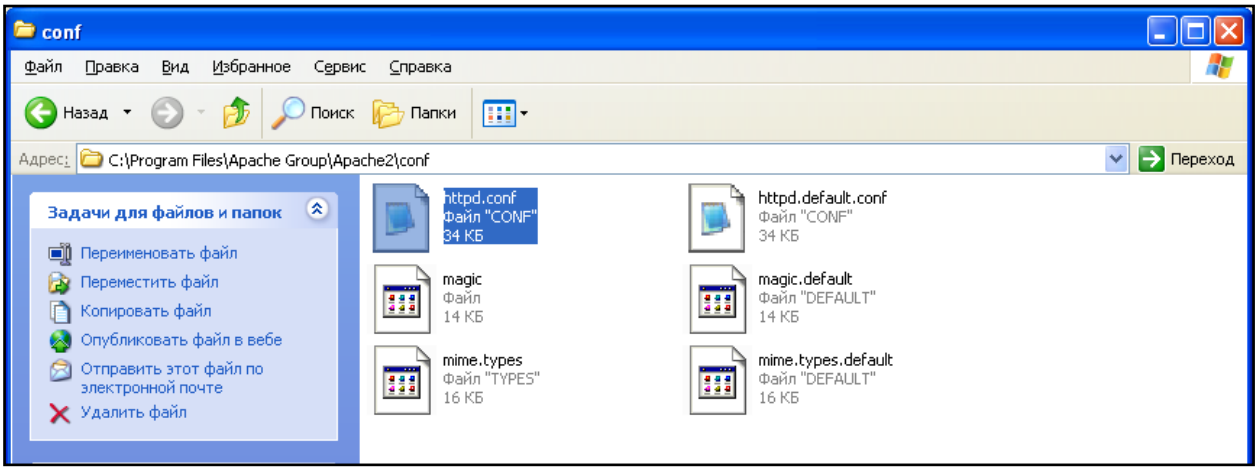

Рис. 1.10. Зміст конфігураційної теки веб-серверу Apache

12. Програмою „Блокнот” відкриваємо файл конфігураційний *httpd.conf*.

13. Змінюємо рядки

#Listen 12.34.56.78:80

Listen 8080

На

Listen 127.0.0.1:80

14. Рядок *DocumentRoot "C:/Program Files/Apache Group/Apache2/htdocs"* (або *DocumentRoot "C:/Program Files/Apache Software Foundation/Apache2.2/htdocs"* для apache 2.2)

Змінюємо на

DocumentRoot "D:/int"

В цій теці будуть зберігатись файли веб-сайту.

15. Знаходимо рядок

#ServerName localhost:8080

змінюємо його на

ServerName localhost:80

16. Рядок

<Directory "C:/Program Files/Apache Group/Apache2/htdocs">

змінюємо на

<Directory "D:/int">

Ця опція стосується налаштувань теки, асоційованої з веб-сайтом.

17. Зберігаємо та закриваємо файл *httpd.conf*.

18. За допомогою програми „Мій комп'ютер" на диску „D" створюємо теку „*int*".

19. Призначаємо цій теці повний доступ. Для цього в контекстному меню вибираємо команди „Доступ и безопасность".

20. У відповідь з'являється показане на рис. 1.11 вікно властивостей теки. Встановлюємо опції показані на рис. 1.11.

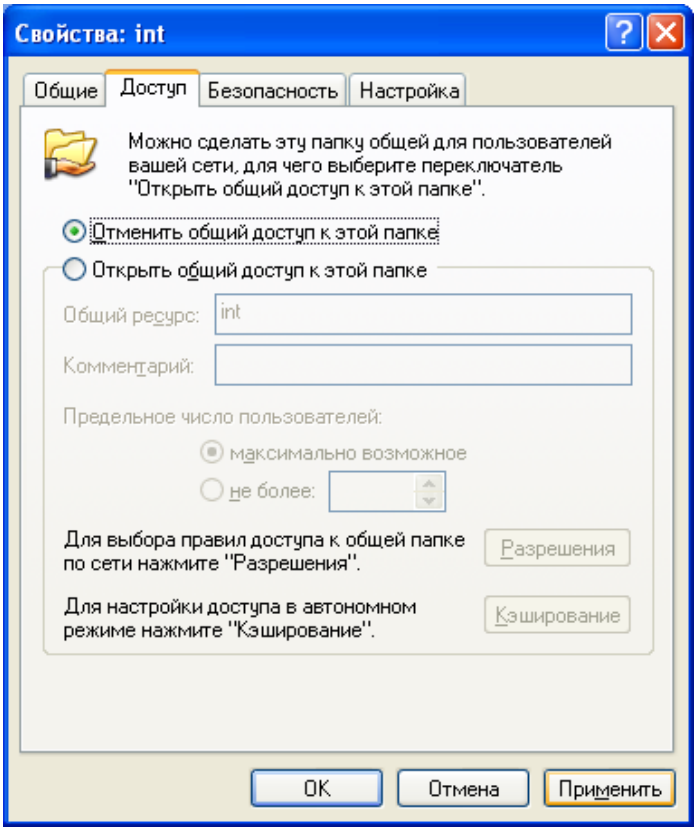

Рис. 1.11. Вікно властивостей теки

21. Підтвердженням встановлення загального доступу є зміна значка теки "D:/int" відповідно рис. 1.12

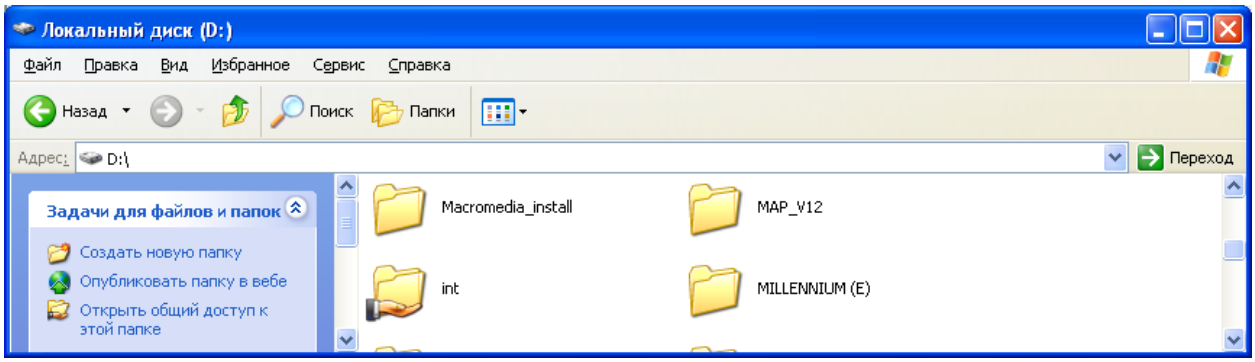

Рис. 1.12. Сигналізація про підтвердження загального доступу до теки "D:/int"

Перевірка працездатності веб-серверу

22. В теці "D:/int" створюємо текстовий документ та називаємо його *index.html* (Погоджуємось на зміну розширення файлу). За допомогою програми „Блокнот” відкриваємо даний файл та записуємо в нього:

<html><head>

<title>Hello</title></head>

<body>Hello</body>

</html>

Зберігаємо та закриваємо файл.

23. Запускаємо браузер. Виконуємо команди „Сервис-Свойства обозревателя”. У відповідь повинно відкритись, показане на рис. 1.13, вікно налаштувань браузера. Переходимо на вкладку „Подключения”. Натискаємо на кнопку „Настройка LAN…”.

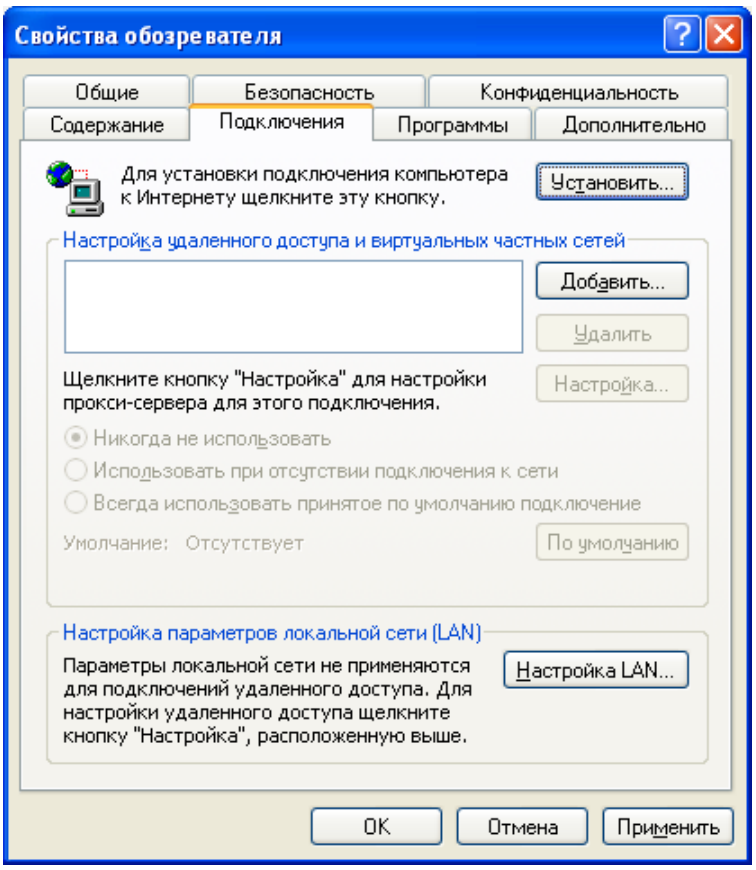

Рис. 1.13. Вікно налаштувань браузера Internet Explorer

24. Встановлюємо опції, показані на рис. 1.14.

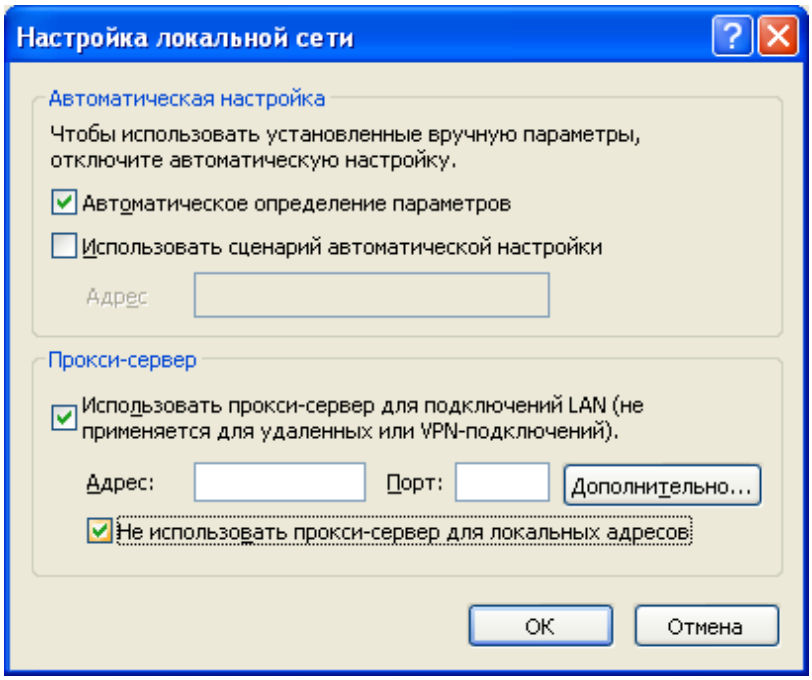

Рис. 1.14. Вікно налаштувань параметрів локальної мережі

25. Натискаємо кнопку „ОК” до виходу із режиму налаштування браузера.

26. За допомогою команд меню, показаних на рис. 1.15 запускаємо веб-сервер

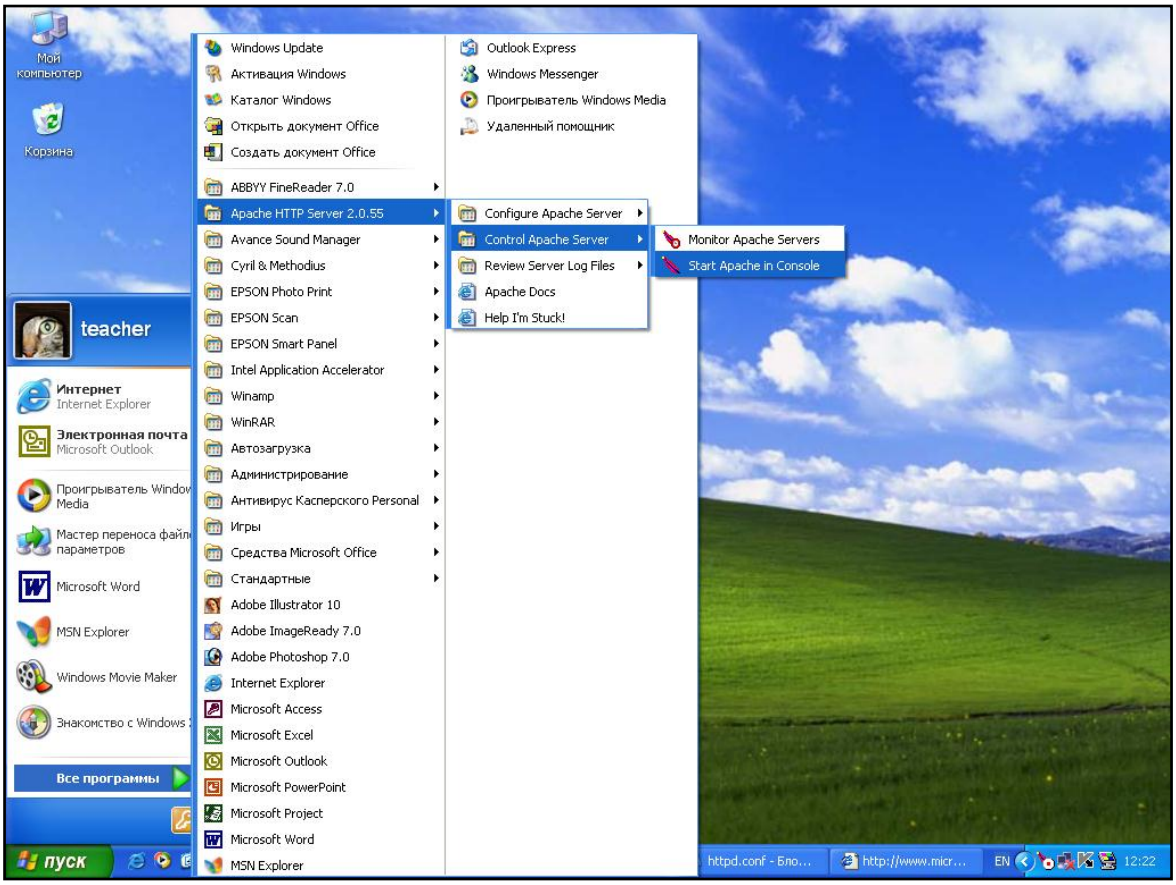

Рис. 1.15. Послідовність запуску веб-серверу

27. У відповідь повинно відкритись вікно показане на рис. 1.16. Це вікно необхідно згорнути. Зникнення вікна означає зупинку веб-серверу.

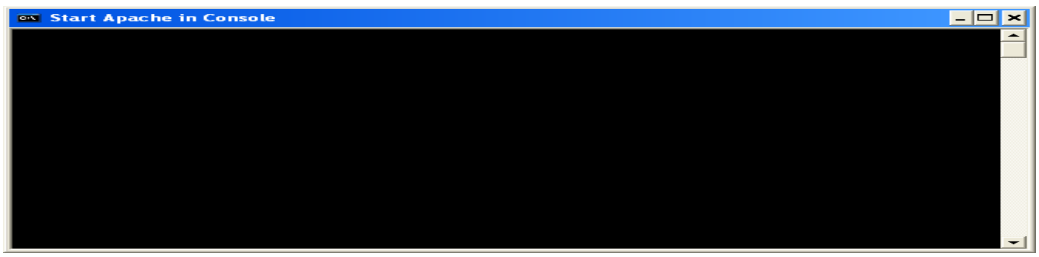

Рис. 1.16. Вікно веб серверу

28. У адресному рядку браузера набираємо „http://127.0.0.1”. Натискаємо „Enter”. Відповідне вікно браузеру показане на рис. 1.17. В випадку появи вікна запиту на підключення до Інтернет підтверджуємо запит.

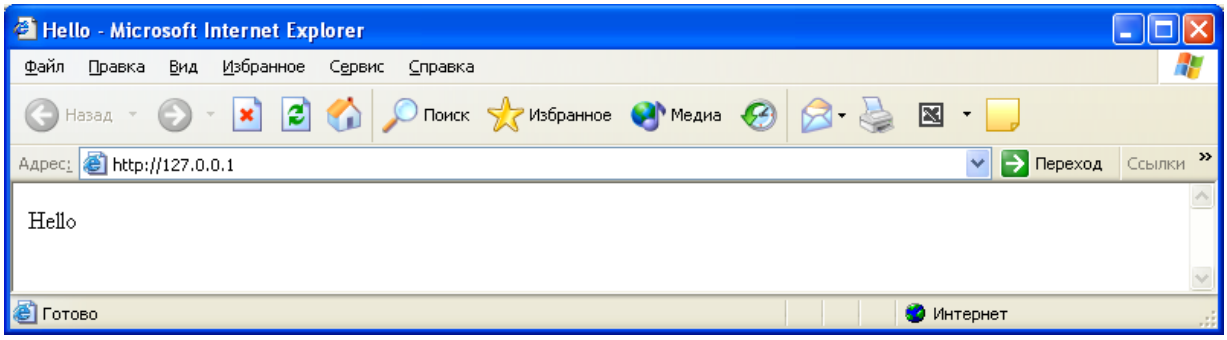

Рис. 1.17. Перевірка працездатності веб-серверу при запиті IP-адреси

29. У адресному рядку браузера набираємо „http://localhost”. Натискаємо „Enter”. Відповідне вікно браузеру показане на рис. 1.18.

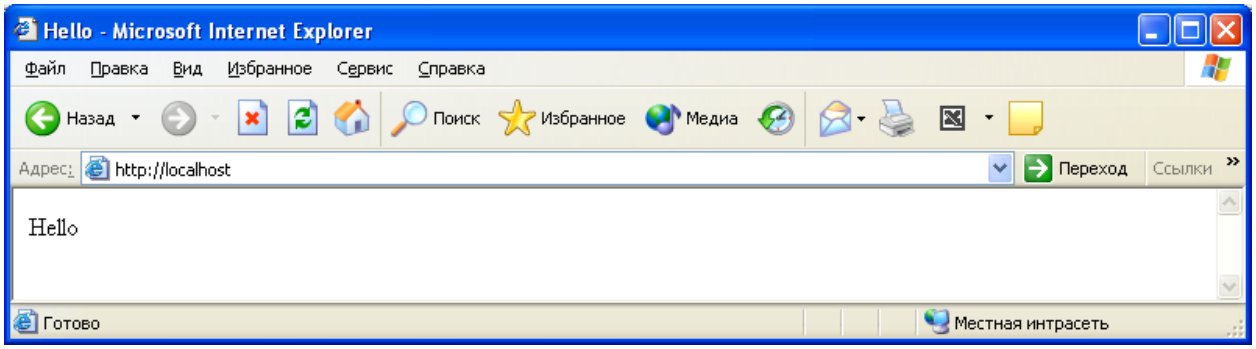

Рис. 1.18. Перевірка працездатності веб-серверу при запиті доменного імені

30. В випадку помилкових налаштувань (сервер не запускається, в браузері не відображається зміст файлу index.html і т.і.) слід зупинити сервер (закрити вікно серверу), у файлі httpd.conf перевірити та при необхідності змінити налаштування, перевірити на при необхідності змінити налаштування браузеру, перевірити та при необхідності змінити файл index.html. Після цього слід ще раз перевірити функціонування веб-серверу.

31. Зупиняємо веб-сервер. Для цього слід закрити відповідне вікно.

32. Проводимо розархівацію файлу php-5.2.1-Win32.zip в на диск „C” теку „php5” („C:\php5”).

33. Виконуємо команди „Пуск-Панель управления”. В новому вікні, яке показане на рис. 1.19 вибираємо „Система”.

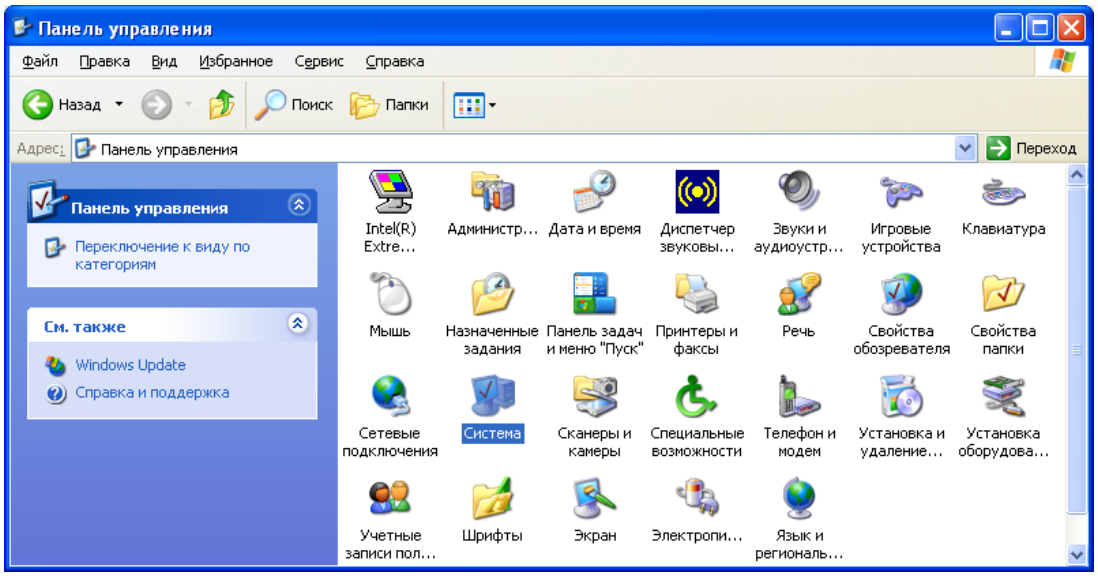

Рис. 1.19. Вікно панелі управління ОС Windows

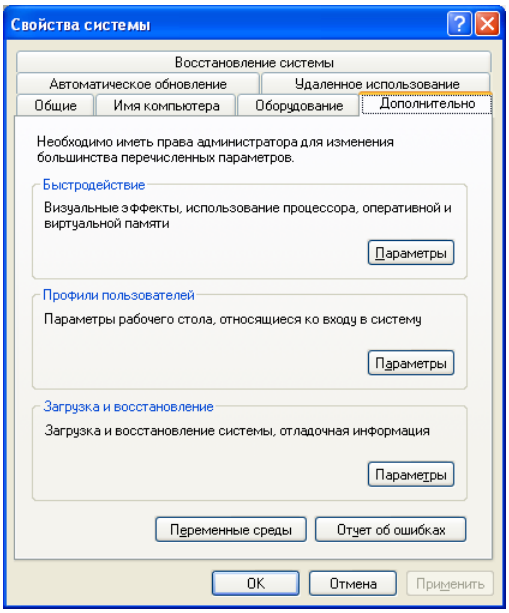

Рис. 1.20. Вікно властивостей системи ОС Windows

34. У відповідь повинно з’явитись вікно властивостей системи, яке показане на рис. 1.20. В означеному вікні переходимо на вкладку „Дополнительно” та натискаємо кнопку „Переменные среды”.

35. У відповідь повинно з’явитись показане на рис. 1.21 вікно налаштувань змінних середовища.

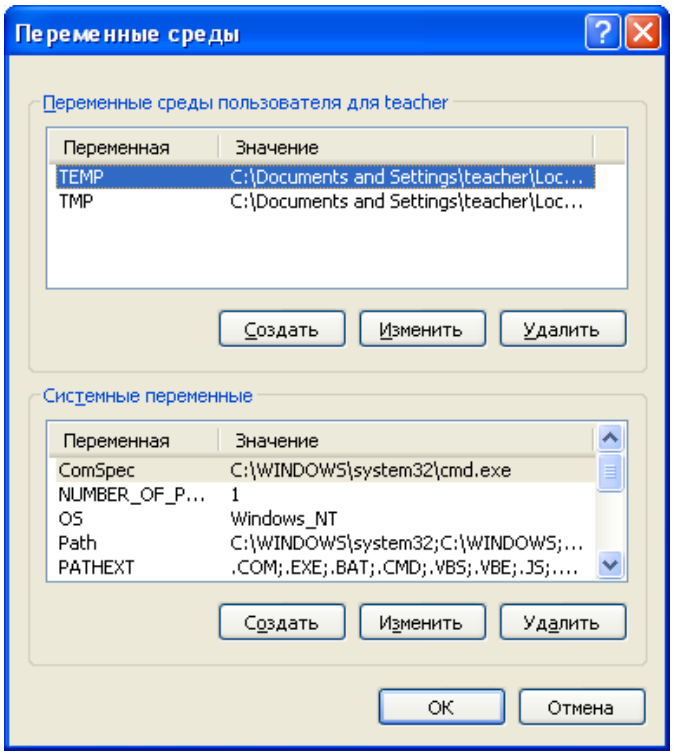

Рис. 1.21. Вікно налаштувань змінних середовища

36. Переходимо у розділ „Системные переменные”, вибираємо „Path” та натискаємо кнопку „Изменить”.

37. У новому, показаному на рис. 1. 22 вікні налаштувань, в полі „Значение переменной” в кінці рядка дописуємо:

;C:\php5;C:\php5\ext\

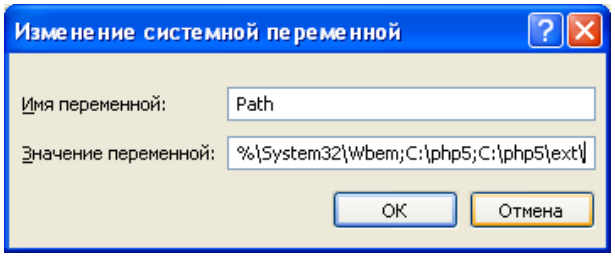

Рис. 1.22. Вікно налаштувань системних змінних

38. За допомогою кнопки „ОК” виходимо із режиму налаштувань операційної системи.

39. В теці „C:\php5” знаходимо файл *php.ini-dist*. Перейменовуємо його на *php.ini*.

40. За допомогою програми „Блокнот” відкриваємо цей файл.

41. Знаходимо рядок

error_reporting = E_ALL & ~E_NOTICE

та змінюємо його на

error_reporting = E_ALL

42. Знаходимо рядок

;include_path = ".;c:\php\includes"

та змінюємо його на

include_path = "c:\php5\pear"

43. Знаходимо рядок

extension_dir = "./"

та змінюємо його на

extension_dir = "c:\php5\ext"

44. Знаходимо рядок

;extension=php_xsl.dll

та змінюємо його на

extension=php_xsl.dll

45. Знаходимо рядок

;extension=php_mysql.dll

та змінюємо його на

extension=php_mysql.dll

46. Знаходимо рядок

;extension=php_pdo_mysql.dll

та змінюємо його на

extension=php_pdo_mysql.dll

Налаштування PHP5 у вигляді модулю веб-сервера Apache

47. Зупиняємо роботу веб-сервера Apache.

48. Відкриваємо конфігураційний файл веб-сервера Apache *httpd.conf*.

49. Знаходимо рядки

 # Example:

 # LoadModule foo_module modules/mod_foo.so

Вставляємо після них

 # Підключення PHP, у вигляді модулю

LoadModule php5_module "C:/php5/php5apache2.dll"

(У випадку використання apache2.2)

LoadModule php5_module "C:/php5/php5apache2_2.dll"

AddType application/x-httpd-php .php

PHPIniDir "C:/php5/"

Перевірка працездатності PHP5

50. В теці "D:/int" створюємо текстовий документ *1.php*

51. Записуємо в нього програмний код

```
<?php
 phpinfo();
?>
```

52. Зберігаємо та закриваємо файл *1.php*

53. Запускаємо веб-сервер.

54. В адресному рядку браузера набираємо http://127.0.0.1/1.php на натискаємо кнопку „Переход”. У відповідь повинно відкритись, показане на рис. 1.23, вікно з інформацією про інтерпретатор PHP5.

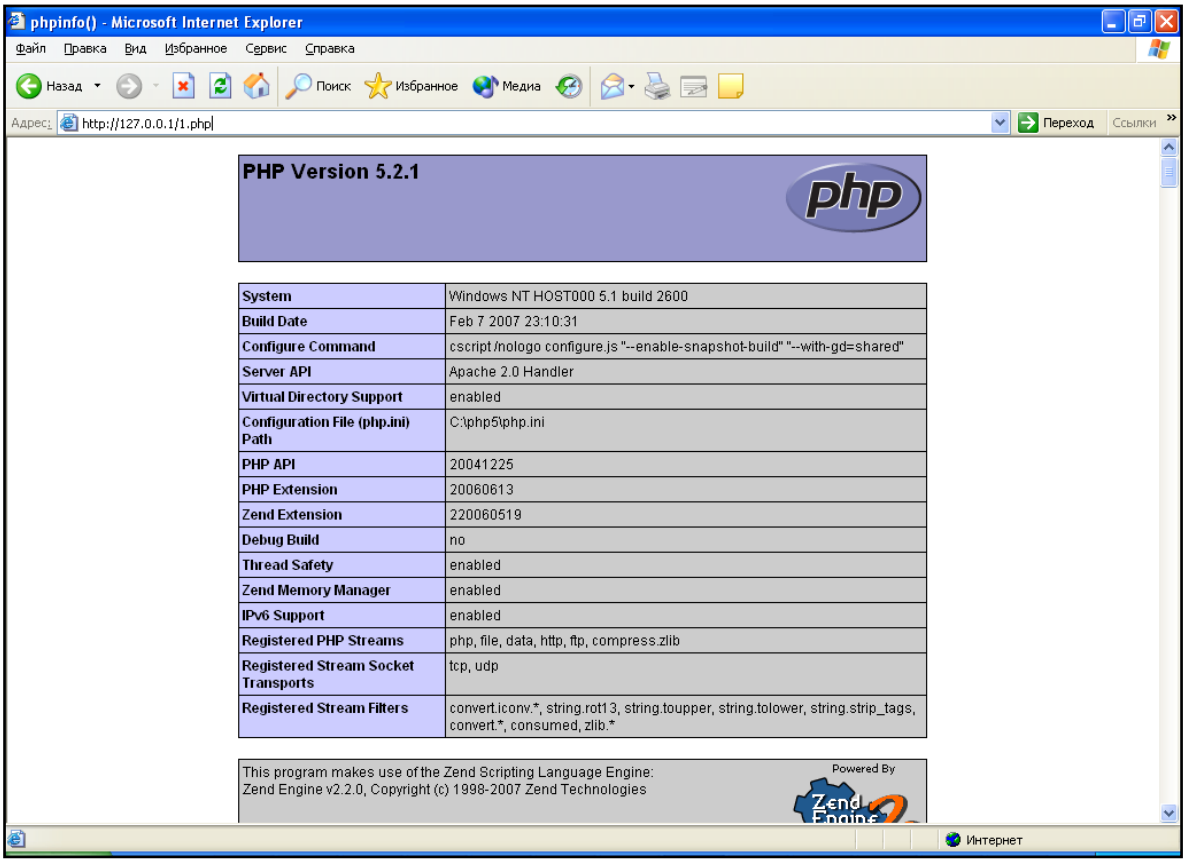

Рис. 1.23. Вікно браузеру з інформацією про інтерпретатор PHP

55. При виникненні помилок слід зупинити веб-сервер, знайти та виправити помилки в налаштуванні. Пересвідчитись в правильності функціонування.

Інсталяція СУБД MySQL 5

56. Зупиняємо веб-сервер. Для цього слід закрити відповідне вікно. Проводимо розархівацію файлу *mysql-5.0.45-win32.zip* в теку mysql-5.0.45-win32. Із означеної теки запускаємо інсталяційний пакет *Setup.exe*. У відповідь повинно з’явитись, показане на рис. 1.24 вікно першого етапу інсталяції. Надалі користуємось інструкціями показаними на рис. 1.24 – 1.34.

Рис. 1.24. Вікно першого етапу інсталяції серверу СУБД MySQL

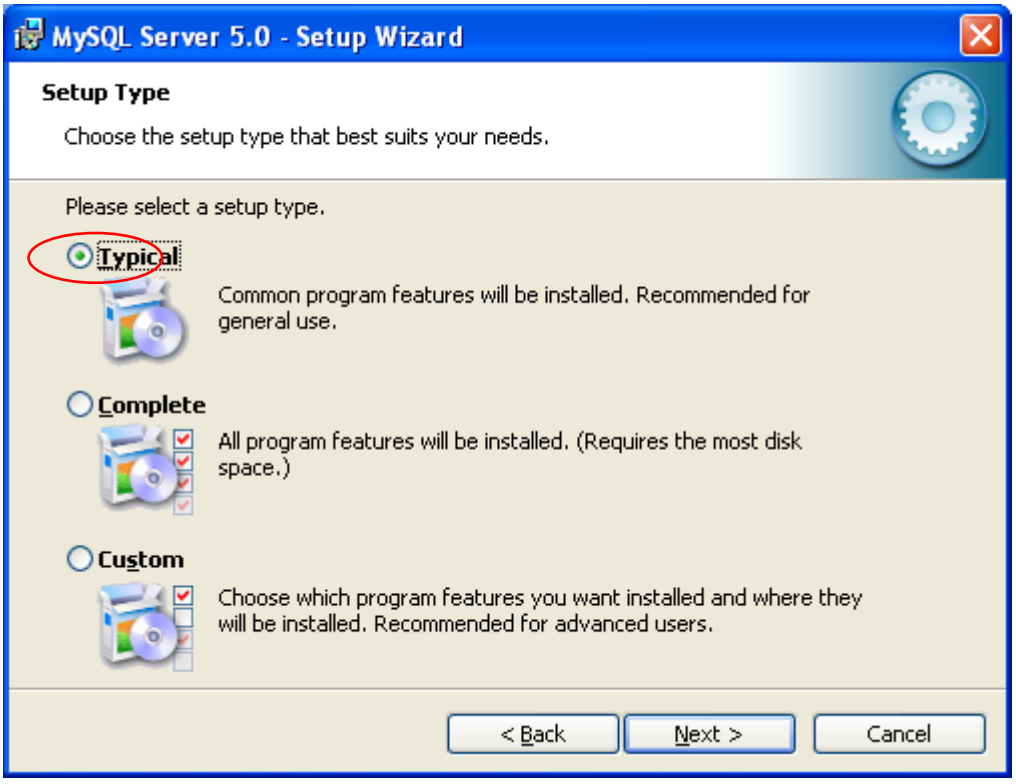

Рис. 1.25. Вікно другого етапу інсталяції серверу СУБД MySQL

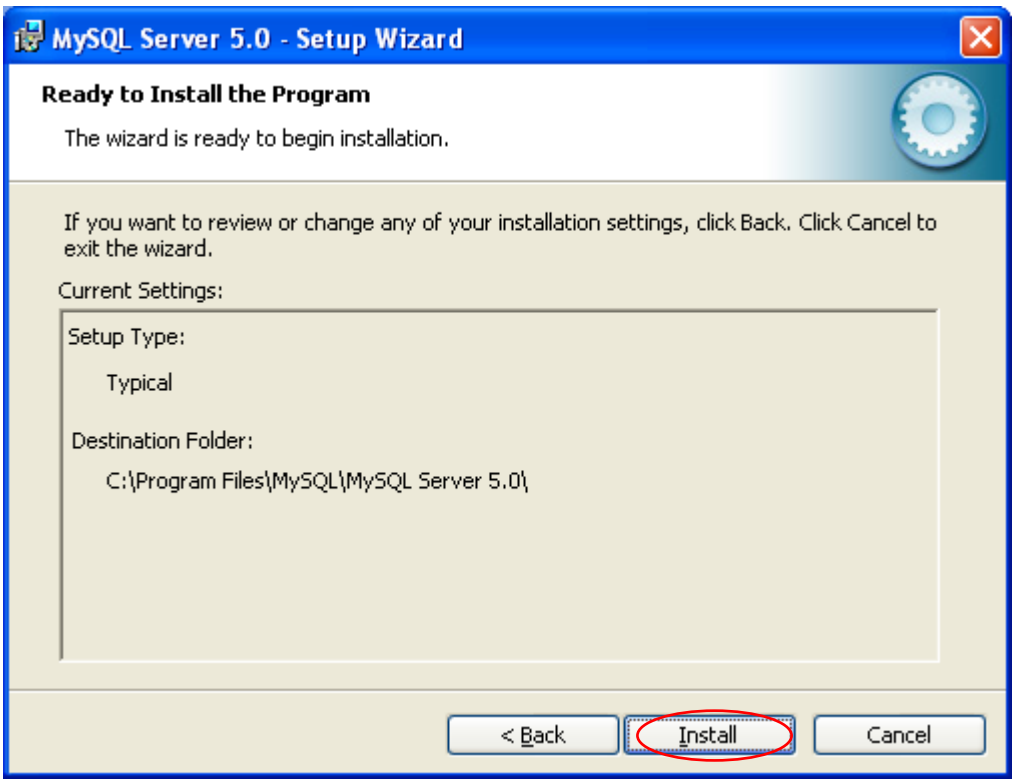

Рис. 1.26. Вікно третього етапу інсталяції серверу СУБД MySQL

Рис. 1.27. Вікно четвертого етапу інсталяції серверу СУБД MySQL

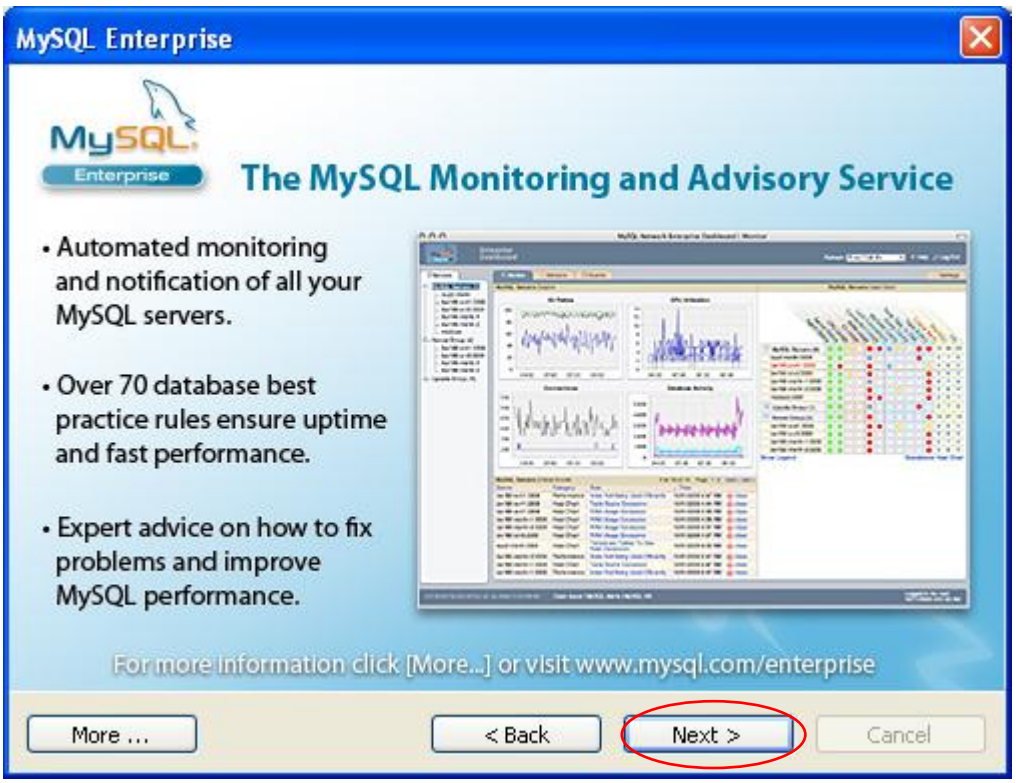

Рис. 1.28. Вікно п’ятого етапу інсталяції серверу СУБД MySQL

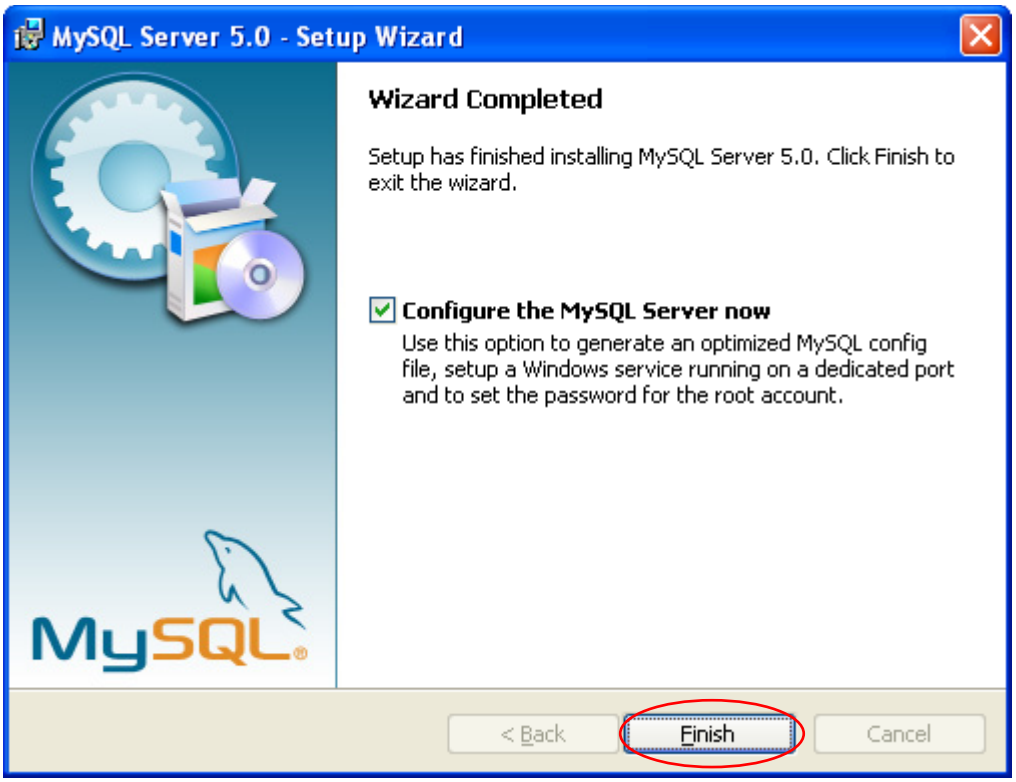

Рис. 1.29. Вікно завершального етапу інсталяції і першого етапу конфігурації серверу СУБД MySQL

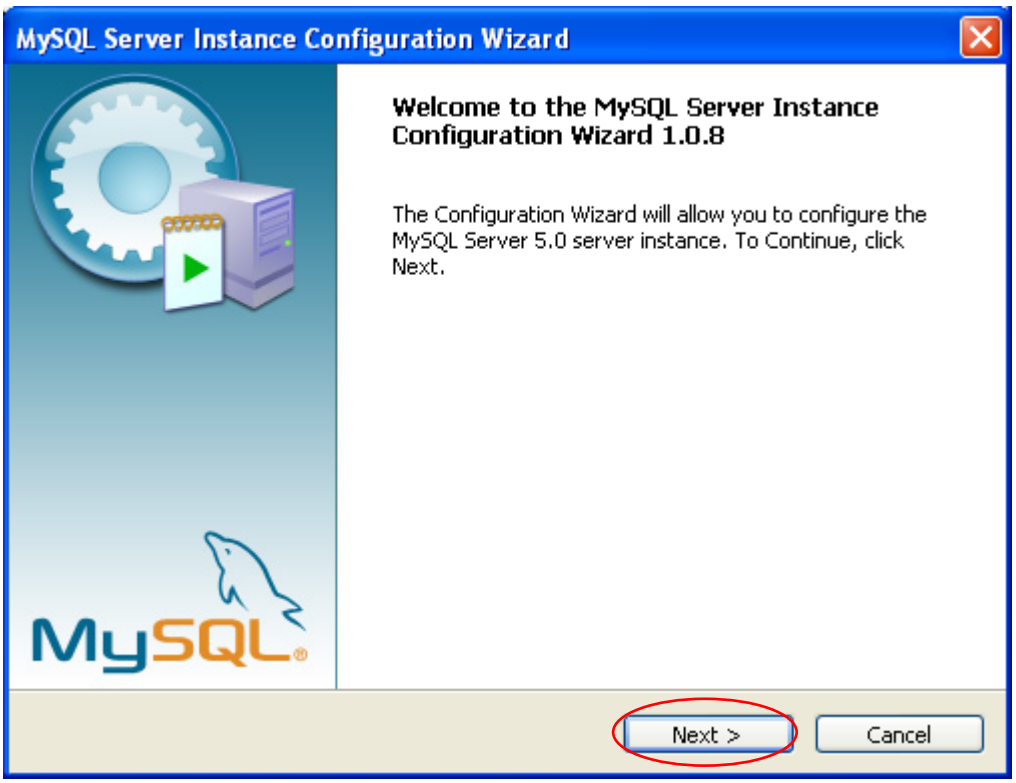

Рис. 1.30. Вікно другого етапу конфігурації серверу СУБД MySQL

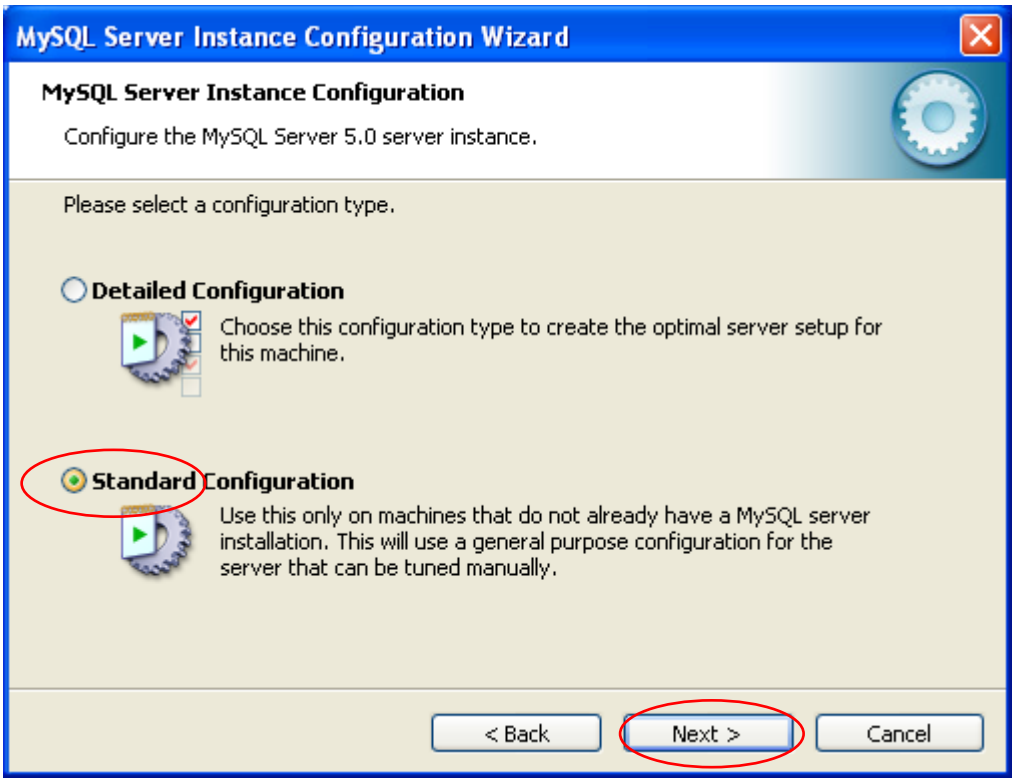

Рис. 1.31. Вікно третього етапу конфігурації серверу СУБД MySQL

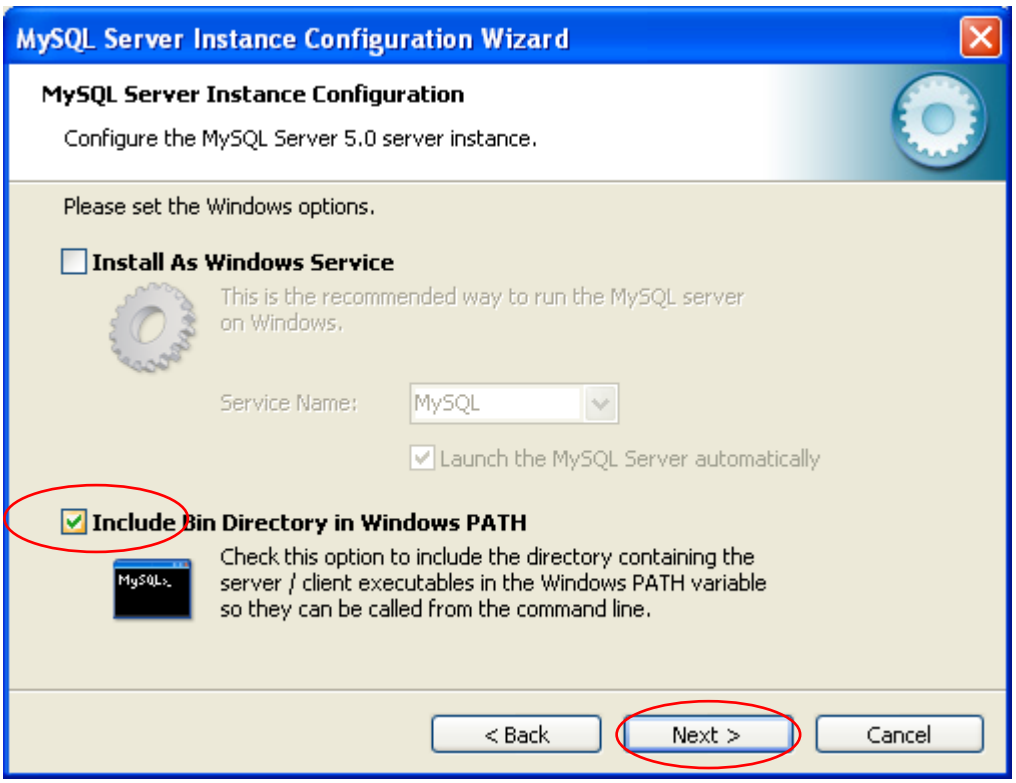

Рис. 1.32. Вікно четвертого етапу конфігурації серверу СУБД MySQL

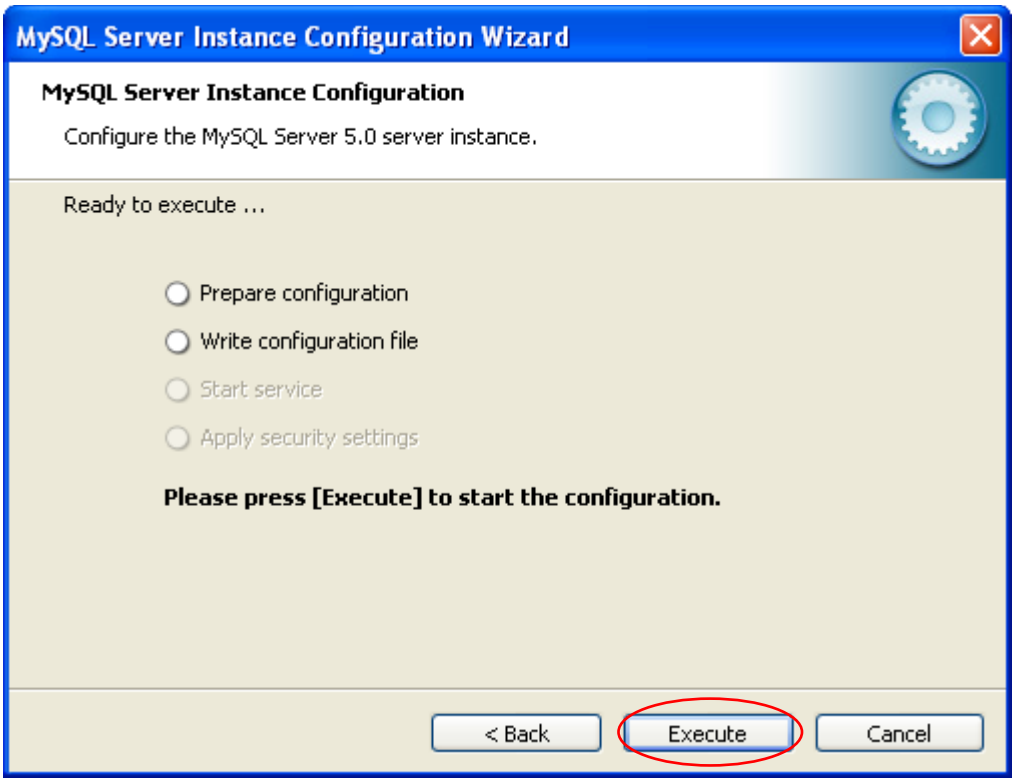

Рис. 1.33. Вікно п’ятого етапу конфігурації серверу СУБД MySQL

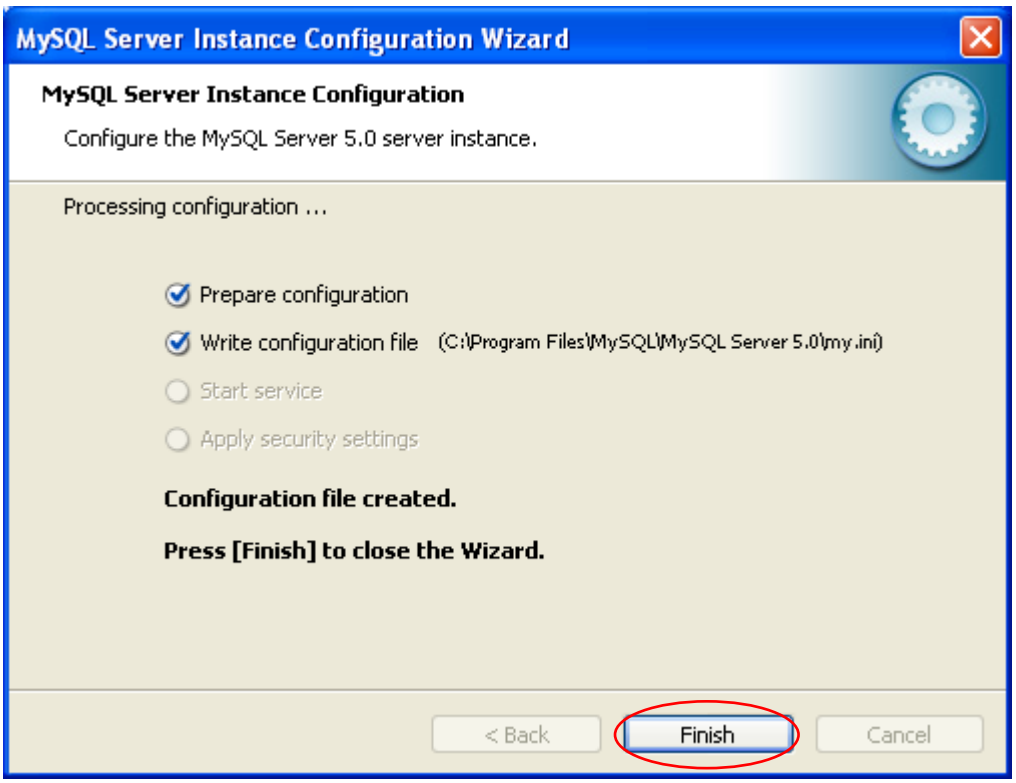

Рис. 1.34. Вікно завершального конфігурації серверу СУБД MySQL

57. Запускаємо сервер БД. Для цього виконуємо команди:

C:\Program Files\MySQL\MySQL Server 5.0\bin\mysqld-nt.exe.

(Для зміни налаштувань СУДБ необхідно модифікувати конфігураційний файл СУБД *my.ini*, який знаходиться в теці „C:\Program Files\MySQL\MySQL Server 5.0”.) У відповідь повинно з’явитись та через короткий проміжок часу зникнути вікно сигналізації про запуск серверу.

58. Для перевірки функціонування серверу СУБД необхідно за допомогою комбінації клавіш Ctr+Alt+Del викликати „Диспетчер задач” ОС Windows. Сервер працює, якщо його назва (*mysqld-nt.exe*) присутня на вкладці „Процеси”. Відповідне вікно показане на рис. 1.35. Якщо сервер не запускається, необхідно спробувати запустити його ще раз. При новому негативному результаті слід заново провести інсталяцію серверу.

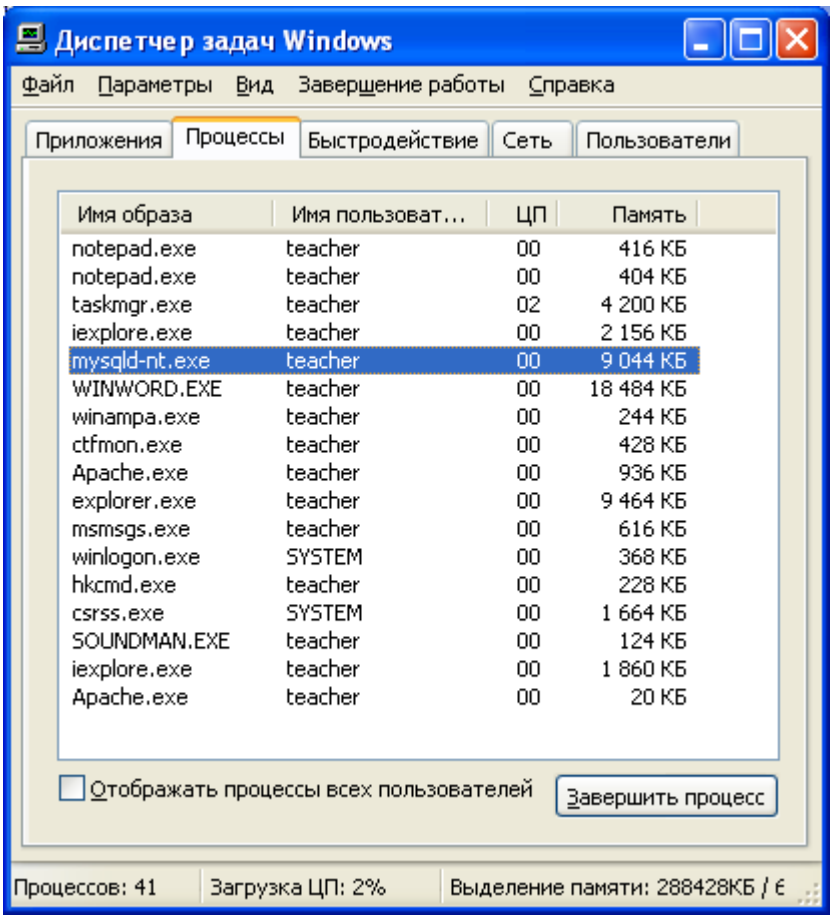

Рис. 1.35. Вікно „Диспетчер задач” ОС Windows

59. В випадку успішного запуску серверу СУБД зупиняємо його за допомогою кнопки „Завершить процесс” у вікні „Диспетчер задач” ОС Windows.

Перевірка працездатності Apache, PHP, MySQL в цілому

60. У власній теці (наприклад „D:/student”) створюємо текстовий документ та записуємо в нього:

@echo off

C:

cd Program Files/mysql/MySQL Server 5.0/bin

mysqladmin.exe -u root shutdown

Зберігаємо та закриваємо файл. Після цього перейменовуємо даний файл в *stop.bat*

Даний файл можливо використовувати для зупинки серверу СУБД.

61. Запускаємо сервер СУБД.

62. В теці "D:/int" створює текстовий документ *2.php*

63. Записуємо в нього програмний код

```
<?php
 print "Current PHP version: <b> ". phpversion() ."</b>";
 /*
Вцьому рядку можливо змінити пароль доступа до mysql на той, що був введений при інсталяції, якщо СУБД була встановлена у вигляді сервісу
$link = mysql_connect("localhost", "root","YOURPASSWORD") or die("Could not connect");
 */
$link = mysql_connect("localhost", "root","") or die("Could not connect");
if( !$link ) die( mysql_error() );
$db_list = mysql_list_dbs($link);
while ($row = mysql_fetch_object($db_list))
{
  echo "<h3>Database \"".$row->Database."\"</h3>\n";
  $result = mysql_list_tables($row->Database);
  if(!$result) die( "DB Error, could not list tables\n MySQL Error: ".mysql_error() );
  else {
    while ($row = mysql_fetch_row($result))
    print "Table: $row[0]<br>";
    mysql_free_result($result);
  }
}
?>
```

Зберігаємо та закриваємо файл *2.php*

64. Запускаємо веб-сервер.

65. В адресному рядку браузера набираємо http://127.0.0.1/2.php на натискаємо кнопку „Переход”

66. У відповідь повинно відкритись, показане на рис. 1.36 інформаційне вікно.

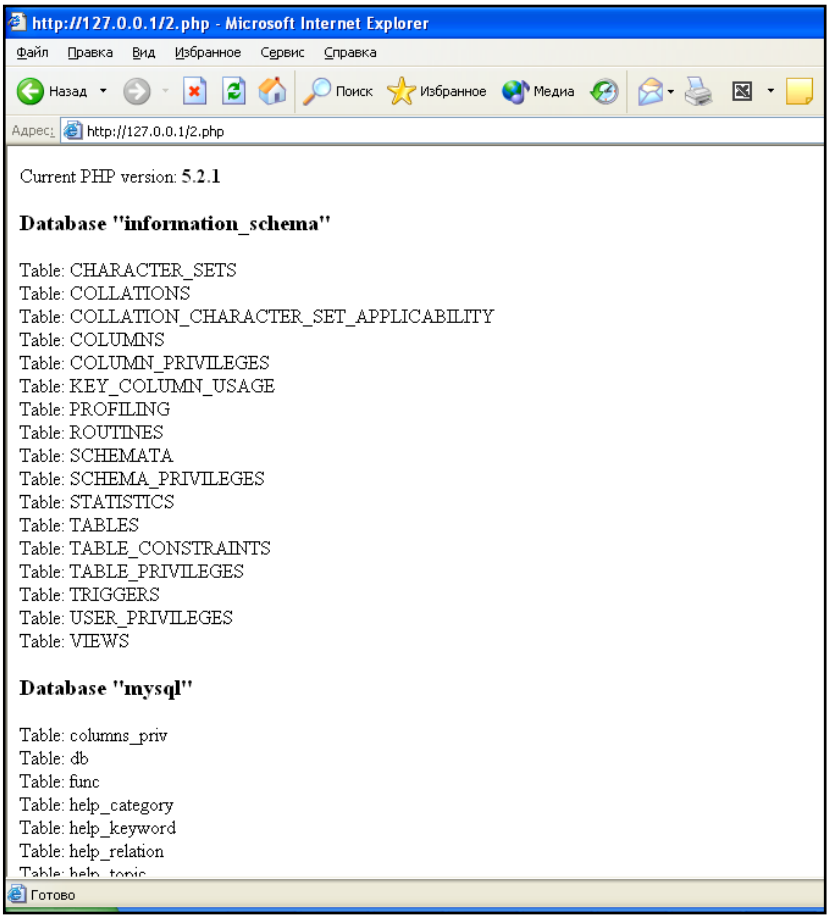

Рис. 1.36. Вікно перевірки працездатності Apache, PHP, MySQL

67. В випадку негативного результату слід зупинити веб-сервер та сервер СУБД. Перевірити та виправити неправильне налаштування (помилки можливі Apache, PHP, MySQL). Заново запустити веб-сервер та сервер СУБД. Впевнитись в працездатності пакету.

Додаткові завдання

68. Змінити місцезнаходження теки з файлами веб-сайту з "D:/int" на "D:/int/home/localhost/www" для цього слід створити цю теку та змінити налаштування в конфігураційному файлі веб-серверу на:

DocumentRoot " D:/int/home/localhost/www"

69. Змінити параметри налаштувань теки з файлами веб-сайту. Для цього в конфігураційному файлі змінити

<Directory "D:/int">

на

<Directory " D:/int/home/localhost/www">

Перевірити працездатність веб-серверу.

70. Додати можливість використання в якості головної сторінки сайту файлу *index.htm*. Для цього відповідний конфігураційний рядок змінити на:

DirectoryIndex index.htm index.html

Перевірити доступність та працездатність *index.htm*

71. Додати можливість виконання сервісу CGI. Для цього створити теку "D:/int:/home/localhost/cgi"

Знайти в конфігураційному файлі рядок

ScriptAlias /cgi-bin/ "C:/Program Files/…/cgi-bin/"

Виправити його так:

ScriptAlias /cgi-bin/ "D:/int/home/localhost/cgi-bin/"

Додати після нього рядок:

ScriptAlias /cgi/ "D:/int/home/localhost/cgi/"

Знайти та виправити рядок:

AddHandler cgi-script .bat .exe .cgi

Перевірити працездатність сервісу CGI. Для цього записати в теку "D:/int/home/localhost/cgi/" деяку програму (файл з розширенням .bat або .exe або .cgi). Запустити веб-сервер та в адресному рядку браузеру ввести

http://localhost/cgi/ ***ім'я файлу***

У відповідь повинна запуститись вибрана програма.

72. Додати можливість використання сервісу SSI. Для цього слід знайти рядок

AddType application/x-gzip .gz .tgz

та дописати після нього

AddType text/html .shtml

AddHandler server-parsed .shtml .html .htm

Перевірити працездатність сервісу. Для цього слід в теці „D:\int” створити текстовий документ та назвати його test.shtml. Відкрити цей файл за допомогою блокноту та записати в нього наступний текст:

SSI Test!<hr>

<!--#include virtual="/index.html" -->

<hr>

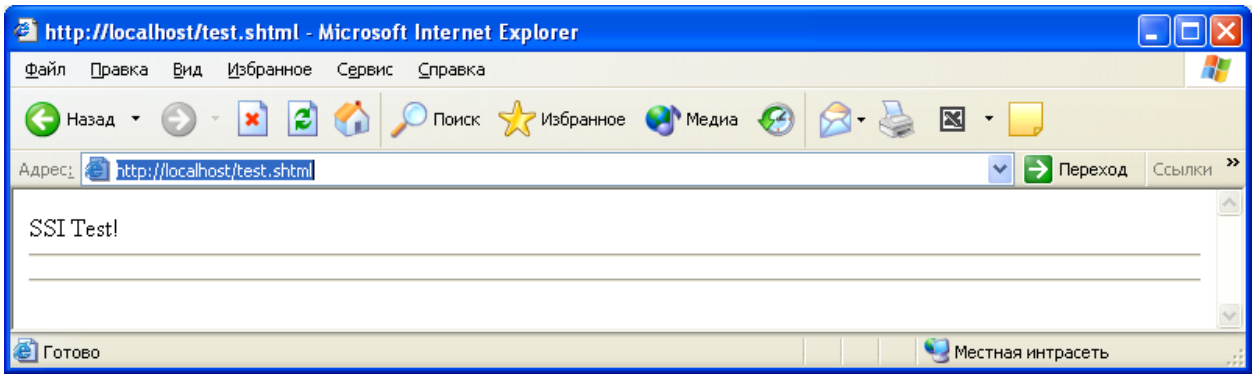

Рис. 1.37. Перевірка сервісу SSI

Запустити веб-сервер та перейти в браузері за адресою „http://localhost/test.shtml”. У відповідь повинно відкритись показане на рис. 1.37 вікно браузеру.

Питання для самоперевірки

1. Опишіть особливості налаштування веб-сервера Apache.
2. Опишіть особливості інтерпретатора PHP 5.
3. Опишіть особливості СУБД MySQL 5.
4. Як переглянути у браузері інформацію про інтерпретатор PHP?
5. Як призначити повний доспуп до папки?
6. Як налаштувати PHP для роботи у вигляді модулю веб-сервера Apache?
7. Як перевірити працездатність сервісу CGI?

8. Опишіть сервіс SSI.
9. Що таке змінні середовища Windows?
10. Для чого використовуються змінні середовища Windows?
11. Де знаходиться конфігураційний файл веб-сервера Apache?
12. Де знаходиться конфігураційний файл інтерпретатора PHP?
13. Як завершити роботу веб-сервера Apache?
14. Як перезапустити веб-сервер Apache?
15. За що відповідає файл .htaccess?

ЛАБОРАТОРНА РОБОТА №2 «КОНФІГУРАЦІЯ ПАРАМЕТРІВ ЗАХИСТУ ВЕБ-СЕРВЕРУ»

Метою лабораторної роботи є оволодіння практичними навичками налаштування базових параметрів захисту веб-сторінок за допомогою стандартних засобів веб-серверу Apache.

Теоретичні відомості. Перед виконанням лабораторної роботи слід ознайомитись із розділами навчального посібника, що присвячені засобам налаштування базових параметрів захисту веб-серверу Apache.

Завдання на лабораторну роботу:

1. Заборонити перегляд структури всіх веб-документів.
2. Заборонити доступ до всіх ресурсів за межами теки з веб-документами.
3. Заборонити перехід веб-сервера по символьним посиланням.
4. Обмежити параметр Timeout величиною 45 секунд.
5. Мінімізувати службову інформацію, що передається від веб-серверу.
6. Обмежити обсяг файлів, які можливо завантажити на веб-сервер величиною 1 МБ.
7. Встановити, що час очікування наступного запиту перед розривом з’єднання дорівнює 15 секунд.
8. Встановити, що максимальна кількість одночасно підтримуваних запитів на одне з'єднання дорівнює 200.
9. Заборонити запуск програм в теці з веб-документами.
10. Заборонити підтримку директив в файлах .htaccess.
11. Заборонити доступ до кореневої теки веб-документів з доменного імені www.rrr.ua та IP-адрес 172.16.16.0 і 172.16.16.8.
12. Дозволити доступ до теки AAA з IP-адреси 127.0.01 тільки користувачеві useraaa. Пароль – 1111. Використати базовий тип перевірки парольних даних.

13. Дозволити доступ до теки BBB з IP-адреси 127.0.01 тільки користувачеві userbbb. Пароль – 2222. Використати цифровий тип перевірки парольних даних.

14. Зняти всі обмеження доступу до теки CCC.

15. Встановити файл *q.html* в якості головного файлу директорії CCC.

16. Заборонити доступ до файлу CCC методом POST.

17. Заборонити доступ всіх користувачів веб-серверу до файлу *myf.html*, розміщеному в теці AAA.

18. Заборонити доступ всіх користувачів веб-серверу до теки DDD.

19. Дозволити доступ всіх користувачів до файлу *rrr.htm*, розміщеному в теці DDD.

20. Визначити файл *y.html* в якості відповіді веб-серверу при виникненні помилки (зверненні до неіснуючого файлу).

21. Використовуючи метод підбору паролю по словнику спробувати підібрати пароль до теки AAA. Визначити термін підбору.

22. Використовуючи метод підбору паролю по словнику спробувати підібрати пароль до теки BBB. Визначити термін підбору.

23. Використовуючи метод повного перебору підібрати пароль до теки AAA. Використати парольний алфавіт, що відповідає обмеженням парольних даних для веб-сторінки. Визначити термін підбору для кількості потоків 1,5, 20,50.

24. Використовуючи метод повного перебору підібрати пароль до теки BBB. Використати парольний алфавіт, що відповідає обмеженням парольних даних для веб-сторінки. Визначити термін підбору для кількості потоків 1,5, 20,50.

Хід виконання роботи

1. Підготовчі роботи:

- Перед виконанням лабораторної роботи слід ознайомитись із матеріалами лабораторного практикуму, що присвячені засобам безпеки та засобам перевірки стійкості парольного захисту веб-серверу Apache.

– В теці F:\int\home\localhost\www створює всі теки і файли потрібні для виконання лабораторних завдань. Це теки AAA, BBB, CCC, DDD та файли *q.html*, *rrr.html* та *y.html*.

– В теках AAA, BBB, CCC, DDD створити файли *index.html* зміст яких відповідає назві теки та назві файлу. Наприклад, на рис. 2.1 показано зміст файлу *index.html*, що розміщений в теці AAA.

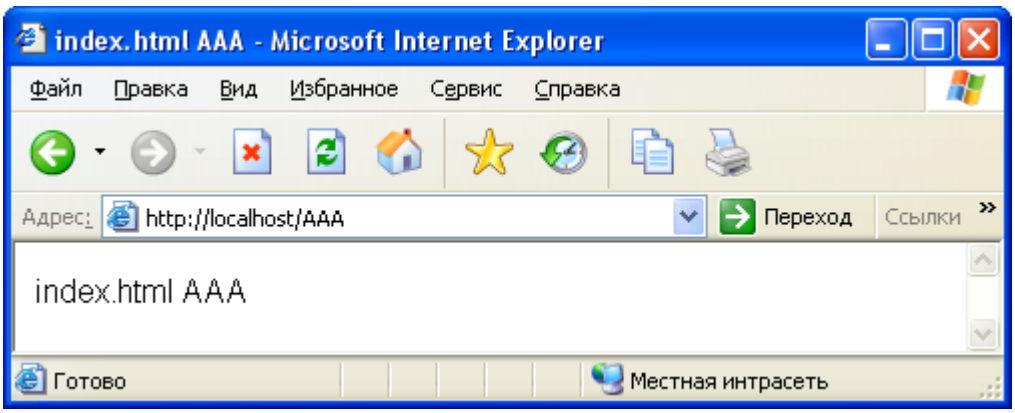

Рис. 2.1. Відображення файлу index.html, розміщеного в теці AAA

– Записати в файл *q.html* (розміщений в теці CCC) текст " q.html CCC".

– Записати в файл *rrr.html* (розміщений в теці DDD) текст " rrr.html DDD".

– Записати в файл *myf.htm* (розміщений в теці AAA) текст " myf.html AAA".

– Записати в файл *y.html* (розміщений в теці AAA) текст "Поганий запит".

2. Виконання кожного наступного пункту завдання лабораторної роботи містить однотипні етапи:

– Параметри записуються в конфігураційний файл веб-серверу – *http.conf*.

– Після запису файл *http.conf* слід зберегти *http.conf*, веб-сервер перезапустити та перевірити коректність виконання пункту завдання.

3. Для заборони перегляду структури всіх веб-документів в секції <Directory "F:/int/home/localhost/www"> слід записати

Options –Indexes

4. Для демонстрації заборони перегляду структури необхідно

– Знищити файл *index.html*, розміщений в теці F:\int\home\localhost\www.

– В адресному рядку браузера набрати http://localhost/. Очікувана відповідь веб-сервера показана на рис. 2.2.

5. Для заборони доступу до всіх ресурсів за межами теми з веб-документами слід виправити параметри секції <Directory /> :

<Directory />

AllowOverride None

Order deny,allow

Deny from all

</Directory>

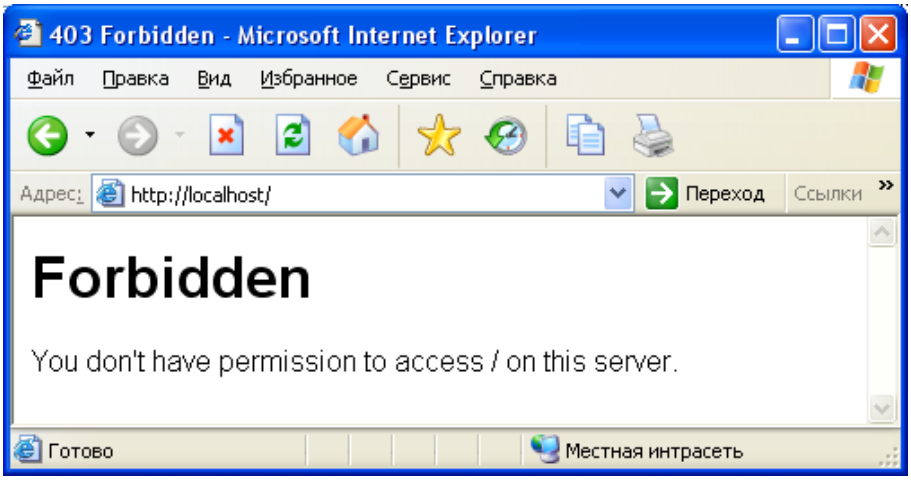

Рис. 2.2. Заборона перегляду структури веб-сайту

6. Для заборони переходу по символьним посиланням слід в секції <Directory "F:/int/home/localhost/www"> знищити рядок

Options Indexes FollowSymLinks

7. Для виконання послідовного виконання завдань 4 – 8 слід в кінці файлу *httpd.conf* слід записати:

Timeout 45

ServerSignature Off

ServerTokens Prod

LimitRequestBody 1048576

KeepAliveTimeout 15

MaxKeepAliveRequests 200

8. Для заборони запуску програм в теці з веб-документами та заборони підтримки директив в файлах *.htaccess* необхідно пересвідчитись, що в секції <Directory "F:/int/home/localhost/www"> є наступні рядки

Options IncludesNOEXEC

AllowOverrides None

9. Для заборони доступу до кореневої теки веб-документів з доменного імені www.rrr.ua та IP-адрес 172.16.16.0 і 172.16.16.8 в секції <Directory "F:/int/home/localhost/www"> після рядка

Allow from all

слід записати:

Deny from www.rrr.ua, 172.16.16.0, 172.16.16.8

10.Після тегу кінця секції <Directory "F:/int/home/localhost/www"> </Directory> записати:

<Directory "F:/int/home/localhost/www/aaa">

Order deny,allow

Deny from all

Allow from 127.0.0.1

AuthUserFile "C:/Program Files/Apache Software Foundation/Apache2.2/bin/pfile"

AuthName "useraaa"

AuthType Basic

require valid-user

</Directory>

11. За допомогою команд "Пуск→Выполнить→cmd" операційної системи Windows відкрити вікно командного рядка та послідовно виконати інструкції показані на рис. 2.3. При цьому пароль – 1111, а парольні дані записуються в файл – *pfile*.

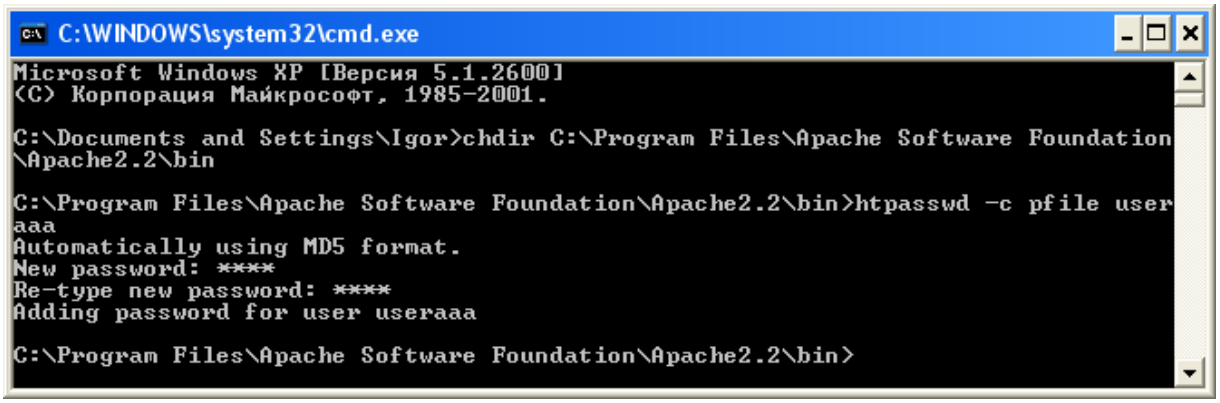

Рис. 2.3. Створення файлу з парольними даними для базової авторизації

Зазначимо, що при спробі доступу з IP-адреси 127.0.0.1 до теки http://localhost/aaa/ перед користувачем повинно з'явитись показане на рис. 2.4 вікно вводу парольних даних. Тека стане доступною тільки після вводу в поле "Пользователь" – useraaa, а в поле "Пароль" –1111. Таким чином реалізація пп.10, 11 відповідає за виконання дванадцятого завдання роботи.

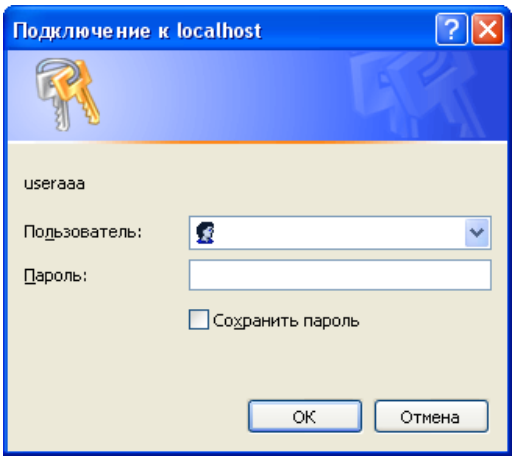

Рис. 2.4. Вікно вводу парольних даних при базовій авторизації

12. Для підключення модулю підтримки цифрової авторизації в файлі *httpd.conf* слід замінити рядок

#LoadModule auth_digest_module modules/mod_auth_digest.so

на

LoadModule auth_digest_module modules/mod_auth_digest.so

13. Після тегу кінця секції <Directory "F:/int/home/localhost/www/bbb"> </Directory> записати:

<Location /bbb/>

Order deny,allow

Deny from all

Allow from 127.0.0.1

AuthType Digest

AuthName "bbb"

AuthDigestDomain /bbb/ http:// 127.0.0.1/bbb/

AuthDigestProvider file

AuthUserFile "C:/Program Files/Apache Software Foundation/Apache2.2/bin/.hhh"

Require valid-user

</Location>

14. За допомогою команд "Пуск→Выполнить→cmd" операційної системи Windows відкрити вікно командного рядка та послідовно виконати інструкції показані на рис. 2.5. При цьому, пароль – 2222 а парольні дані записуються в файл – *.hhh*.

Зазначимо, що при спробі доступу з IP-адреси 127.0.0.1 до теки http://localhost/bbb/ перед користувачем повинно з'явитись показане на рис. 2.6 вікно вводу парольних даних. Тека стане доступною тільки після вводу в поле "Пользователь" – userbbb, а в поле "Пароль" –2222. Таким чином реалізація пп.12 – 14 відповідає за виконання завдання №13.

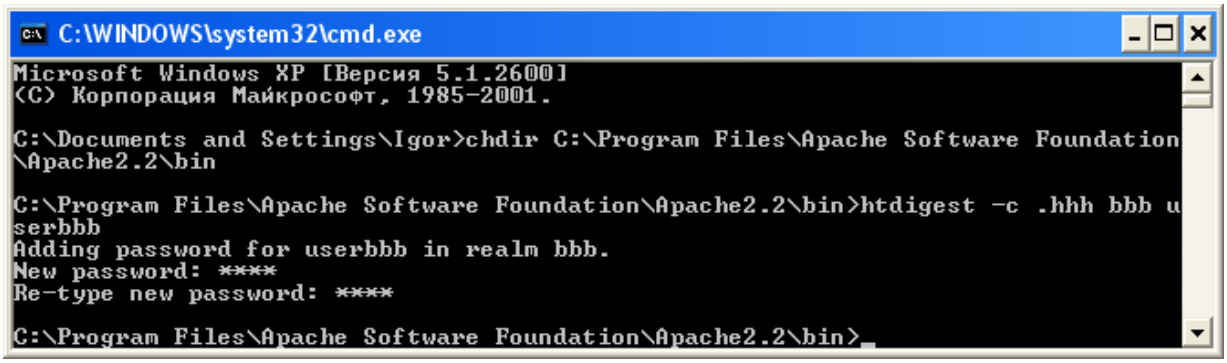

Рис. 2.5. Створення файлу з парольними даними для цифрової авторизації

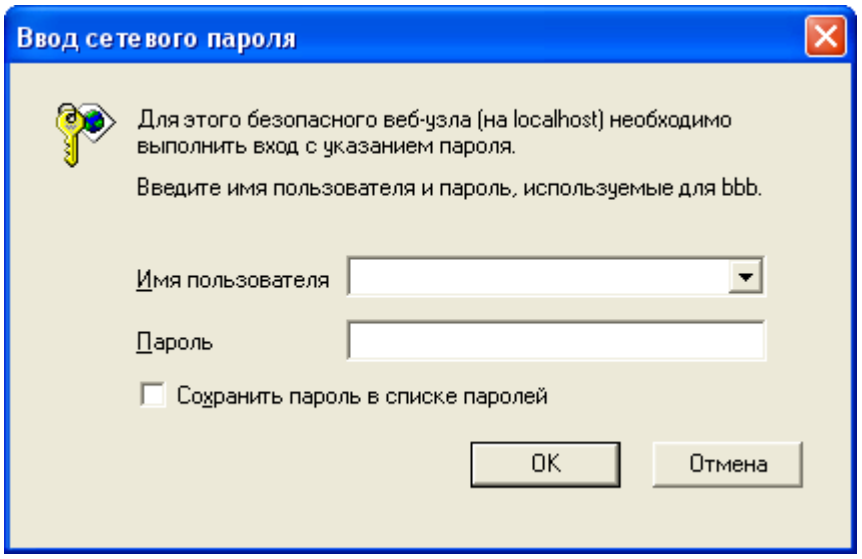

Рис. 2.6. Вікно вводу парольних даних при цифровій авторизації

15. Для того, щоб зняти всі обмеження доступу до теки CCC після тегу кінця секції *<Location /bbb/> </Location>* слід записати:

<Directory "F:/int/home/localhost/www/ccc">

Order deny,allow

allow from all

</Directory>

Зазначимо, що таким чином були перевизначені обмеження доступу задані для корневої теки веб-документів.

16. Пересвідчимось, що при доступі до теки *CCC* відкривається файл *index.html* (див. рис. 2.7).

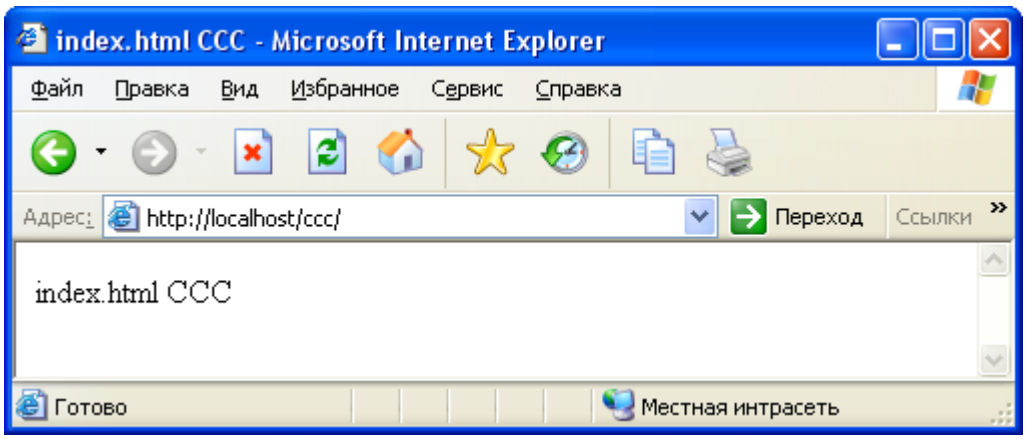

Рис. 2.7. Звернення до теки CCC при стандартному налаштуванні

17. В секцію <Directory "F:/int/home/localhost/www/ccc"> слід дописати рядок:

DirectoryIndex q.html

18. Пересвідчимось, що при доступі до теки *CCC* відкривається файл *q.html* (див. рис. 2.8).

Реалізація пп. 16 – 18 дозволяє встановити файл q.html в якості головного файлу директорії CCC.

19. Для заборони доступу до теки CCC методом POST в секцію <Directory "F:/int/home/localhost/www/ccc"> слід дописати:

<Limit POST>

order deny,allow

deny from all

</Limit>

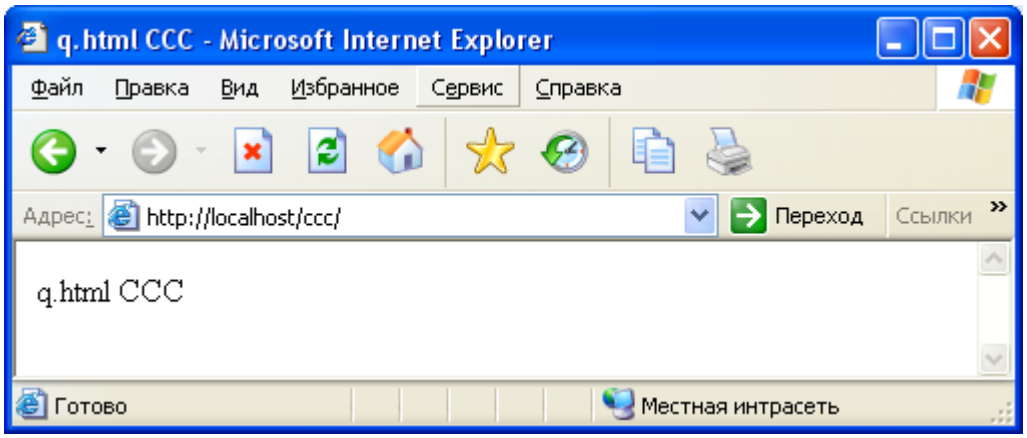

Рис. 2.8. Звернення до теки CCC при заміні головного файлу на q.html

20. Для заборони доступу всіх користувачів веб-серверу до файлу *myf.html*, розміщеному в теці AAA слід в секції <Directory "F:/int/home/localhost/www/aaa"> дописати:

<Files myf.html >

order deny,allow

deny from all

</Files>

Вікно, сигналізації заборони доступу показане на рис. 2.9. Зазначимо, що залишились доступними користувачеві useraaa з IP-адреси 127.0.01 інші файли розміщені в теці AAA.

21. Для заборони доступу всіх користувачів веб-серверу до теки DDD слід після кінця секції <Directory "F:/int/home/localhost/www/ccc"> </Directory> записати:

<Directory "F:/int/home/localhost/www/ddd">

Order deny,allow

Deny from all

</Directory>

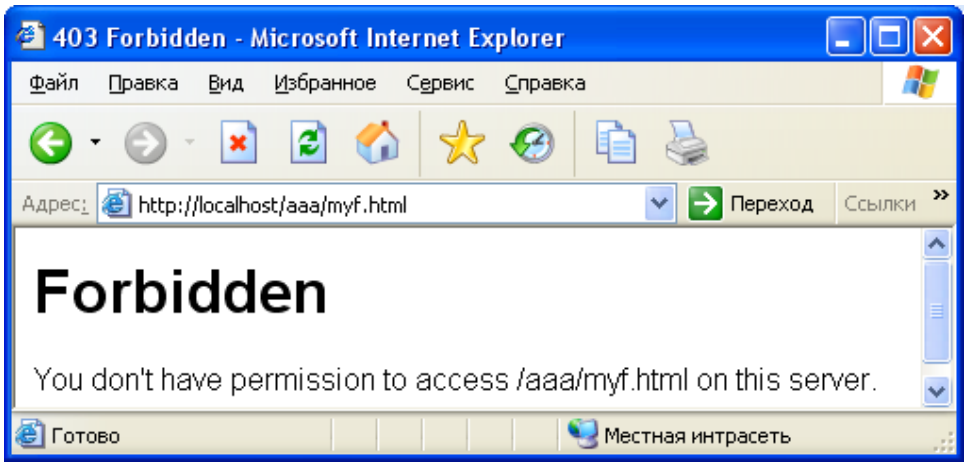

Рис. 2.9. Заборона доступу до файлу myf.html, розміщеному в теці AAA

22. Відповідно рис. 2.10 пересвідчимось в недоступності всіх файлів теки DDD.

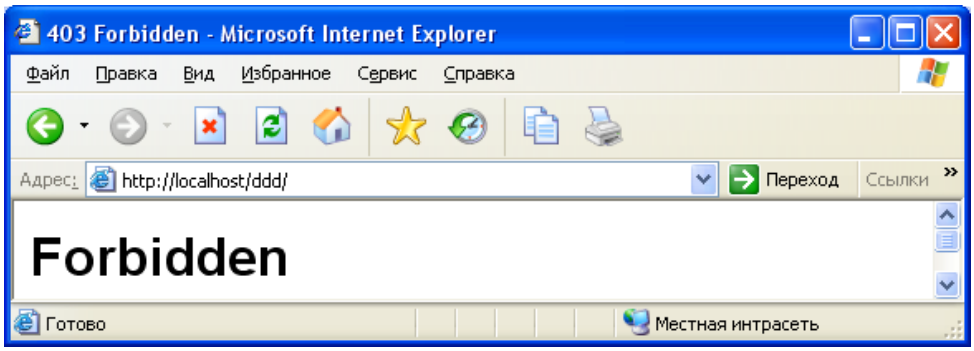

Рис. 2.10. Доступ до теки DDD заборонено

23. Для відкриття доступу всіх користувачів до файлу rrr.htm, розміщеному в теці DDD слід в кінці секції <Directory "F:/int/home/localhost/www/ddd"> дописати:

<Files rrr.html >

order deny,allow

allow from all

</Files>

24. Відповідно рис. 2.11 пересвідчимось у відкритті доступу до файлу rrr.htm, розміщеному в теці DDD.

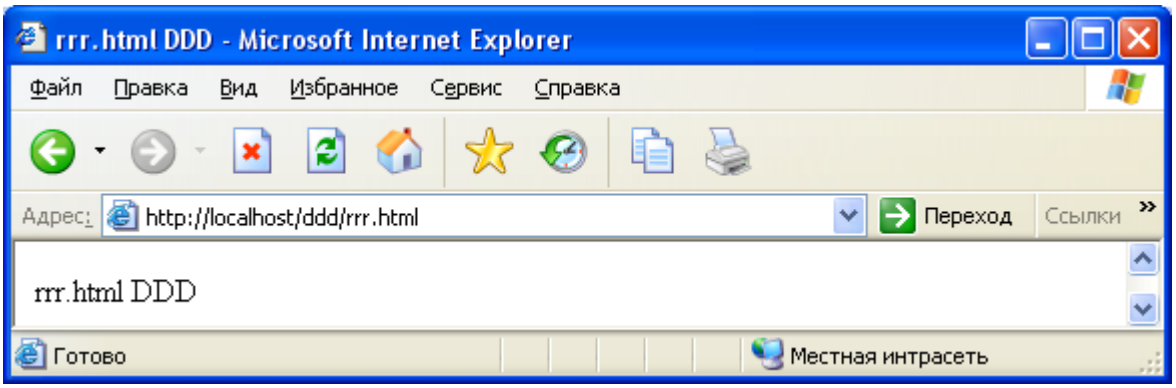

Рис. 2.11. Доступ до файлу rrr.htm теки DDD відкрито

25. Для визначення файлу *y.html* в якості відповіді веб-серверу при виникненні помилки типу 404 - «Ресурс не знайдено» слід:

– після рядка

#ErrorDocument 402 http://localhost/subscription_info.html

записати

ErrorDocument 404 http://localhost y.html

– в теці F:\int\home\localhost\www\ створити файл *y.html* та записати в нього потрібну інформацію

26. Для перевірки зміни відповіді слід звернутись до неіснуючого ресурсу веб-серверу, наприклад http://localhost/ccc/1.htm. У відповідь, як це показано на рис. 2.12, повинен відкритись файл *y.html*.

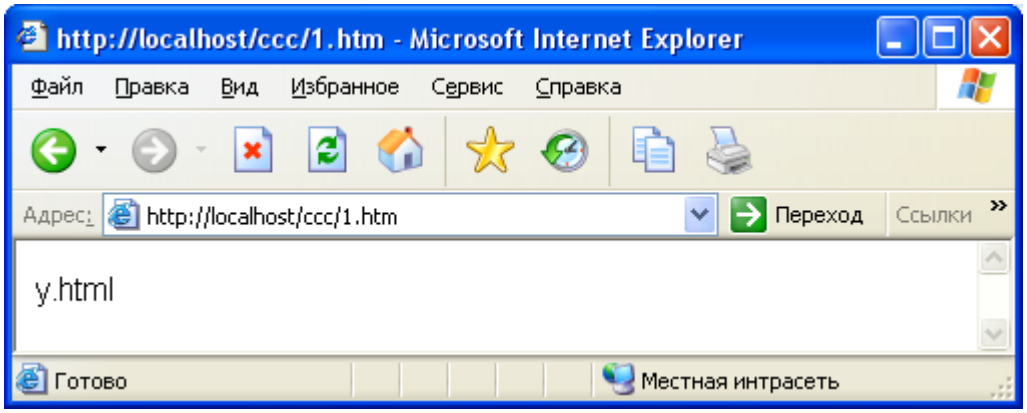

Рис. 2.12. Зміна файлу повідомлення про помилку

Питання для самоперевірки

16. Як заборонити перегляд структури веб-документів?
17. Як заборонити доступ до русерсів за межами теки з веб-документами?
18. Як заборонити всім користувачам доступ до певного файлу?
19. Як заборонити вім користувачам доступ до певної теки?
20. Як заборонити доступ до певного файлу методом POST?
21. Як заборонити доступ до певної теки методом POST?
22. Як заборонити доступ до певного файлу методом GET?
23. Як заборонити доступ до певної теки методом GET?
24. Як заборонити доступ до певної теки з визначеної IP-адреси?

25. Як заборонити доступ до певного файлу з визначеної IP-адреси?

26. Як дозволити доступ до певної теки тільки з визначеної IP-адреси?

27. Як дозволити доступ до певного файлу тільки з визначеної IP-адреси?

28. В чому різниця між базовою та цифровою ідентифікацією користувачів:

29. Як створити файл з парольними даними для базової ідентифікації?

30. Як створити файл з парольними даними для цифрової ідентифікації?

31. Як мінімізувати службову інформацію, що передається від веб-серверу?

32. Як обмежити обсяг файлів, які можливо завантажити на веб-сервер величиною?

33. Яке призначення параметру Timeout?

34. Як обмежити параметр Timeout величиною 12 секунд?

35. Як заборонити перехід веб-сервера по символьним посиланням?

36. Як обмежити час очікування наступного запиту перед розривом з'єднання величиною 25 секунд?

37. Як заборонити доступ до певної теки веб-документів з визначеного доменного імені?

ЛАБОРАТОРНА РОБОТА №3 «НАЛАШТУВАННЯ СИСТЕМИ ЗАХИСТУ СУБД MYSQL»

Метою лабораторної роботи є отримання практичних навичок налаштувань параметрів безпеки сервера СУБД MySQL

Теоретичні відомості. Перед виконанням лабораторної роботи слід ознайомитись із розділами навчального посібника, що присвячені засобам безпеки СУБД MySQL.

Завдання лабораторної роботи:

1. Настроїти сервер СУБД для виконання запитів тільки з комп'ютера на якому він встановлений.
2. Визначити основні параметри з'єднань сервера MySQL.
3. Встановити пароль адміністратора СУБД MySQL – 1111.
4. Встановити примусове використання системи привілеїв користувачів.
5. Визначити привілеї користувачів СУБД MySQL?
6. Визначити структуру таблиці прав користувачів яка використовується при вводі нового користувача СУБД?
7. Створити базу даних mytest.
8. В базі даних mytest створити таблицю myuser яка складається із двох символьних полів name довжиною 12 символів та login довжиною 24 символи. Записати в таблицю myuser декілька рядків довільної інформації.
9. Переглянути інформацію записану в таблицю myuser.
10. Ввести нового користувача my, який буде мати повні права доступу до бази даних mytest.
11. Ввести нового користувача one який буде мати можливість перегляду всієї бази даних mytest та вставки даних в поле login таблиці. myuser.
12. Заборонити користувачеві one вставляти дані в поле login таблиці myuser бази даних mytest.

Хід виконання роботи

1. Знайти конфігураційні файли СУБД *my.ini* або *my.cnf*. (Знаходяться в програмній теці СУБД або/та системних теках операційної системи). В цих файлах знайти рядки:

 # The TCP/IP Port the MySQL Server will listen on

port=3306

Змінити їх так:

 # The TCP/IP Port the MySQL Server will listen on

bind-address=127.0.0.1

port=3306

Завдяки цьому сервер СУБД MySQL буде сприймати запити тільки із комп'ютера на якому він встановлений.

2. Запустити сервер СУБД MySQL. Для цього:

– Відповідно інструкцій рис. 3.1 та рис. 3.2 запустити режим командного рядка.

– Відповідно інструкцій рис. 3.3, вказати шлях до теки в якій розміщені утілити СУБД та запустити файл *mysqld-nt.exe*. Після цього необхідно згорнути вікно командного рядка. Зазначимо, що закриття даного вікна не призводить до зупинки серверу MySQL.

3. Визначити основні параметри з'єднань сервера MySQL. Для цього:

– Відповідно рис. 3.2 та рис. 3.3, відкрити нове вікно командного рядка.

– Запустити утиліту *mysqladmin.exe* з параметрами, вказаними на рис.4.

– Основні параметри з'єднань повинні відобразитись у вікні командного рядка, так як це показано на рис. 3.4.

– Закрити вікно поточного командного рядка.

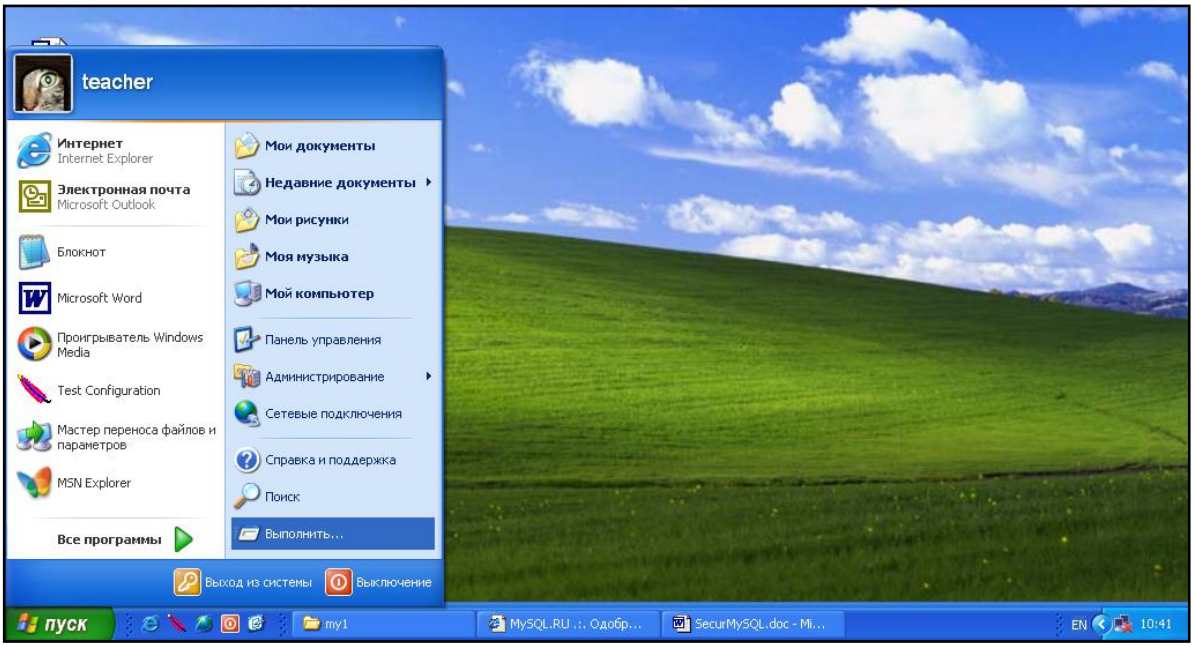

Рис. 3.1. Запуск команди „Выполнить” операційної системи Windows

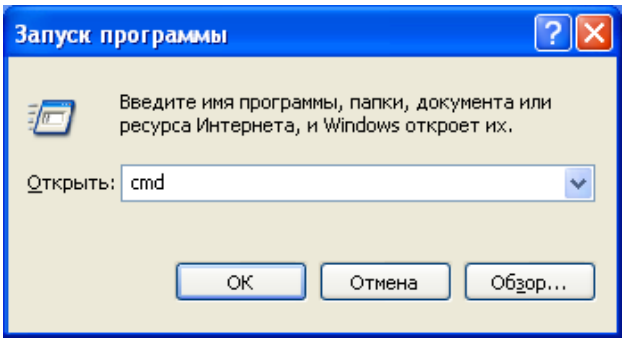

Рис. 3.2. Запуск режиму командного рядка

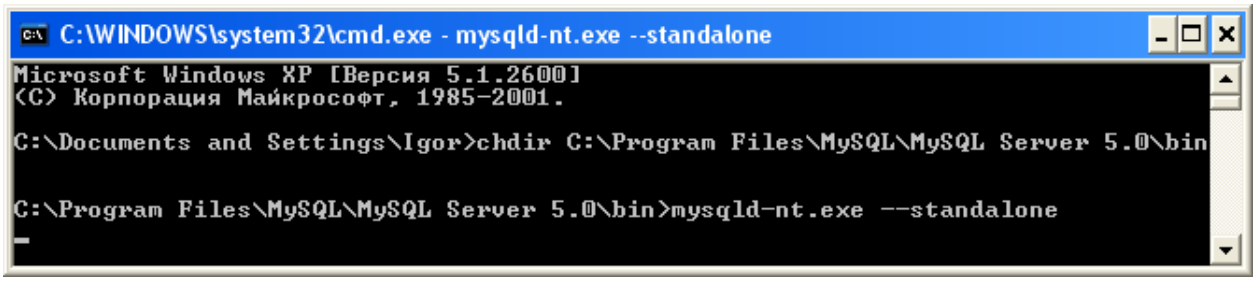

Рис. 3.3. Запуск сервера MySQL

4. Запустити клієнт СУБД MySQL та від імені користувача root (адміністратор СУБД), підключитись до бази даних mysql яка використовується для адміністрування серверу. Для цього:

– Відповідно рис. 3.2 та рис. 3.3, відкрити нове вікно командного рядка.

– Перейти в теку C:\Program Files\MySQL\MySQL Server 5.0\bin.

– Запустити клієнт MySQL. з параметрами, що показані на рис. 3.5.

У відповідь повинна з’явитись, показана на рис. 3.6 інформація з параметрами з’єднання та запитом на виконання нової команди.

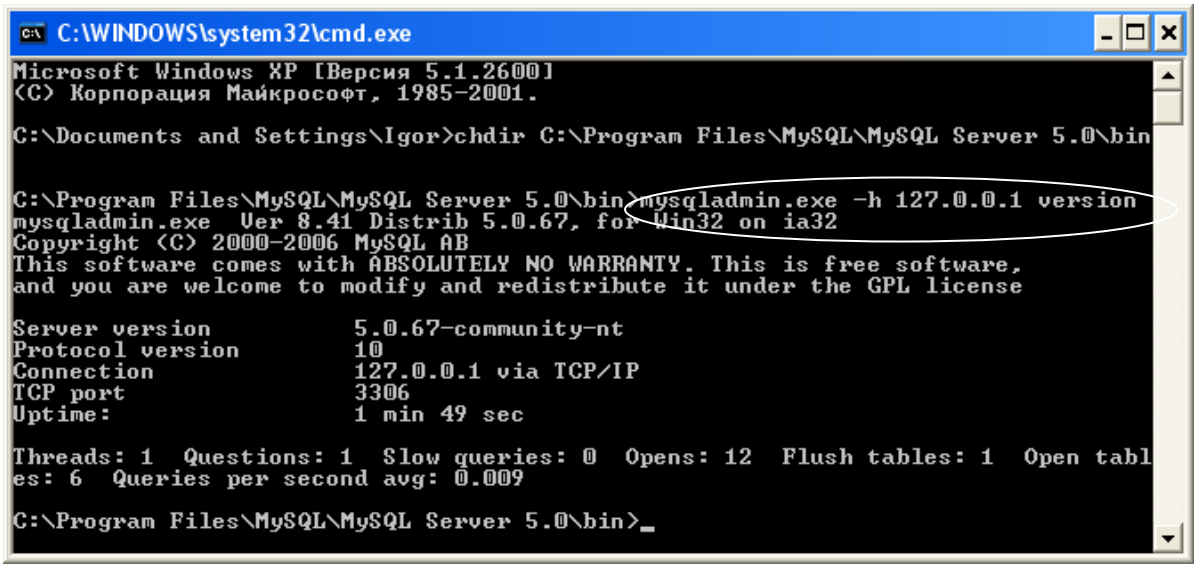

Рис. 3.4. Визначення параметрів з’єднань

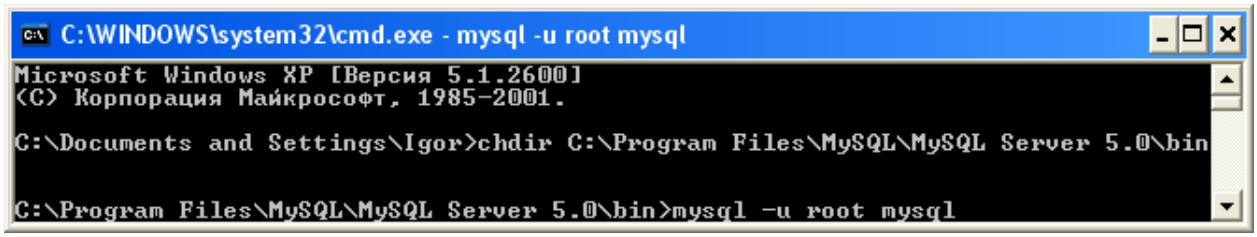

Рис. 3.5. Запуск клієнта MySQL

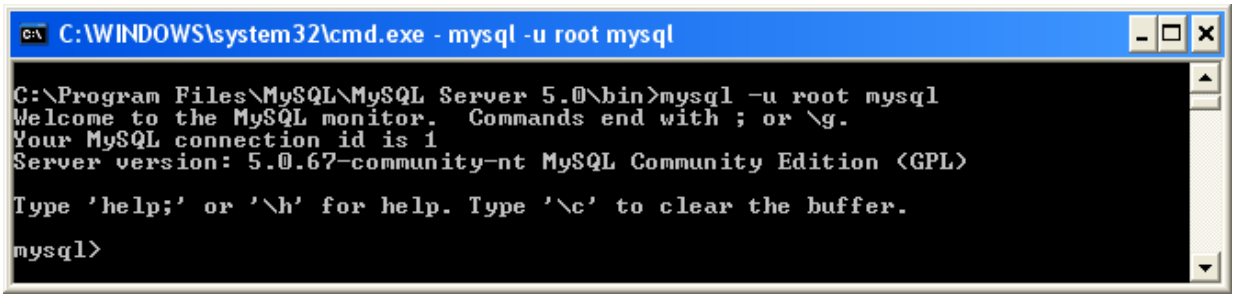

Рис. 3.6. Інформація про успішне підключення до серверу БД

5. Встановити пароль адміністратора – 1111. Для цього слід виконати команди показані на рис. 3.7. На цьому ж рисунку показано і підтвердження встановлення паролю.

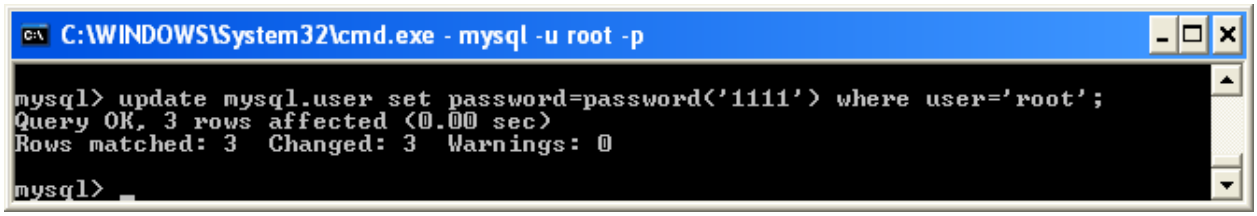

Рис. 3.7. Зміна паролю адміністратора серверу СУБД

6. Відповідно інструкцій показаних на рис. 3.8, завершити роботу клієнта MySQL.

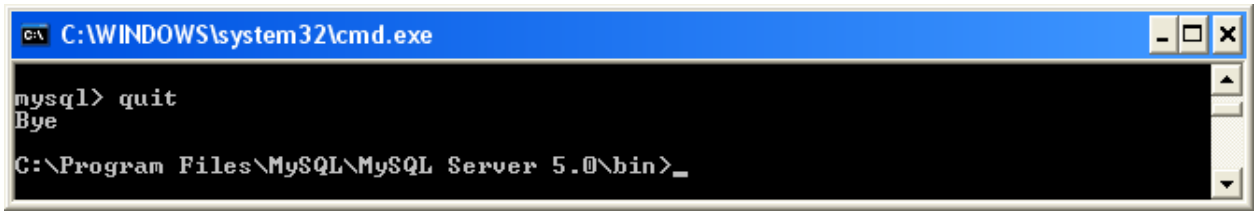

Рис. 3.8. Завершення роботи клієнта

7. Використовуючи встановлений пароль перезавантажити сервер MySQL. Для цього скористатись інструкціями рис. 3.9.

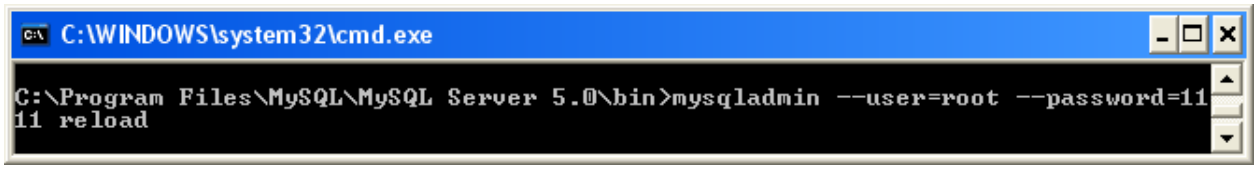

Рис. 3.9. Перезавантаження серверу MySQL

8. Використовуючи інструкції рис. 3.10 запустити клієнт MySQL та від імені користувача root під'єднатись до серверу.

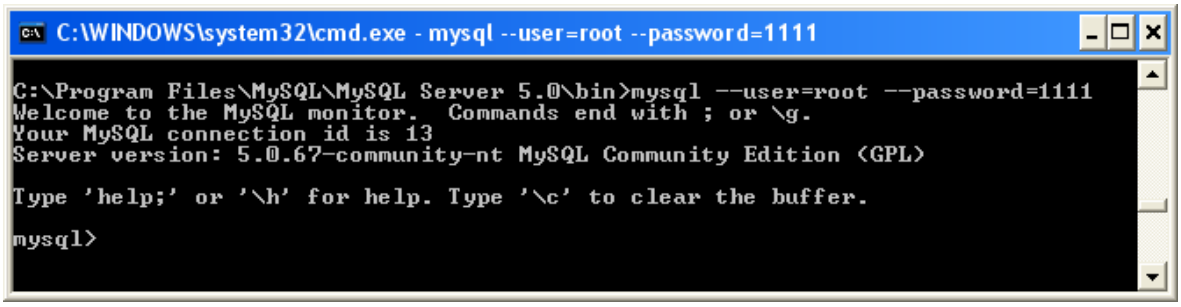

Рис. 3.10. Використання паролю при з'єднанні з сервером MySQL

9. Встановити примусове використання системи привілеїв користувачів. Для цього слід скористатись інструкціями рис. 3.11.

10. Відповідно інструкцій рис. 3.11 переглянути привілеї користувачів серверу MySQL.

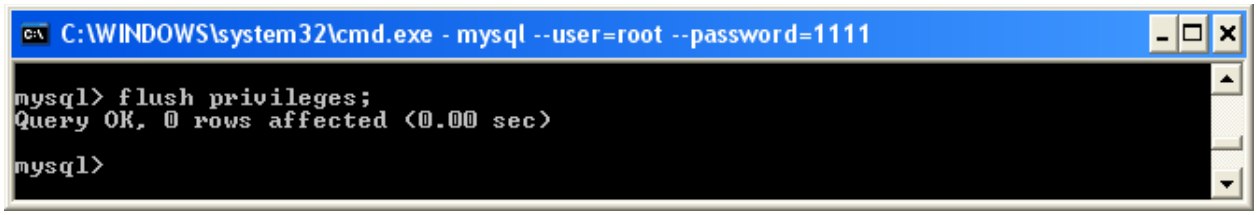

Рис. 3.11. Встановлення привілеїв користувачів

11. Переглянути структуру таблиці прав користувачів яка використовується при вводі нового користувача. Для цього слід скористатись інструкціями рис. 3.12 на якому також показано фрагмент вказаної структури.

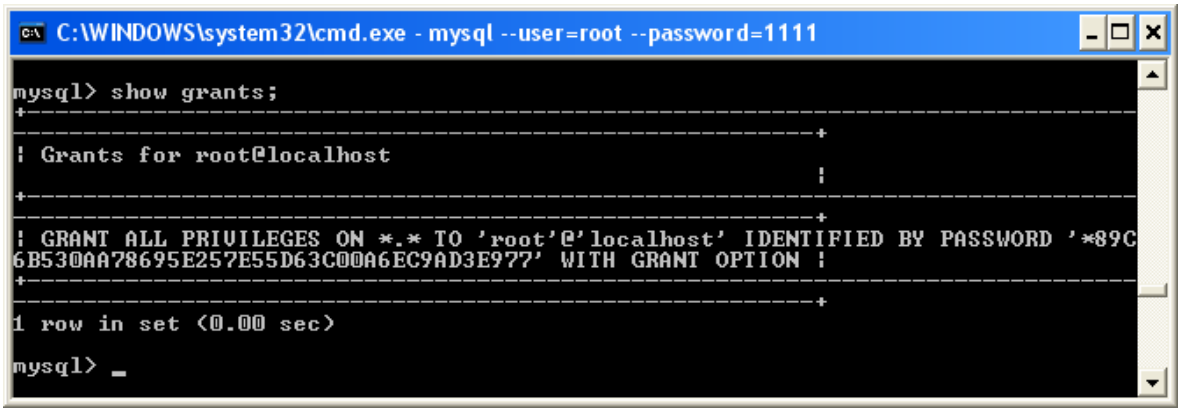

Рис. 3.12. Перегляд привілеїв користувачів

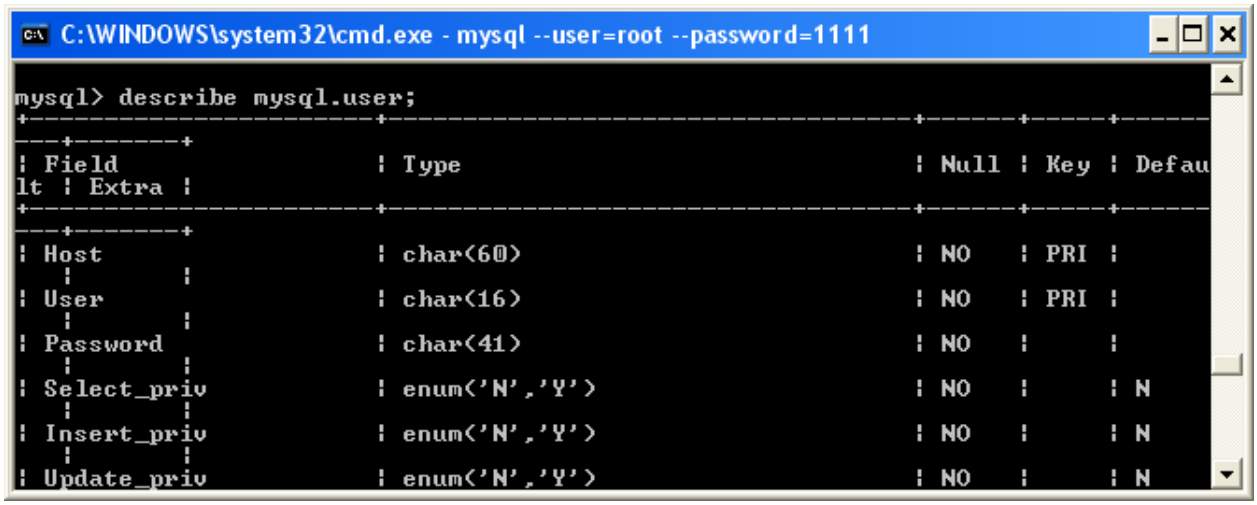

Рис. 3.13. Структура таблиці прав користувачів

12. Переглянути дані користувача root. Для цього слід, використовуючи інструкції рис. 3.14, зробити вибірку всіх даних із таблиці user бази даних mysql.

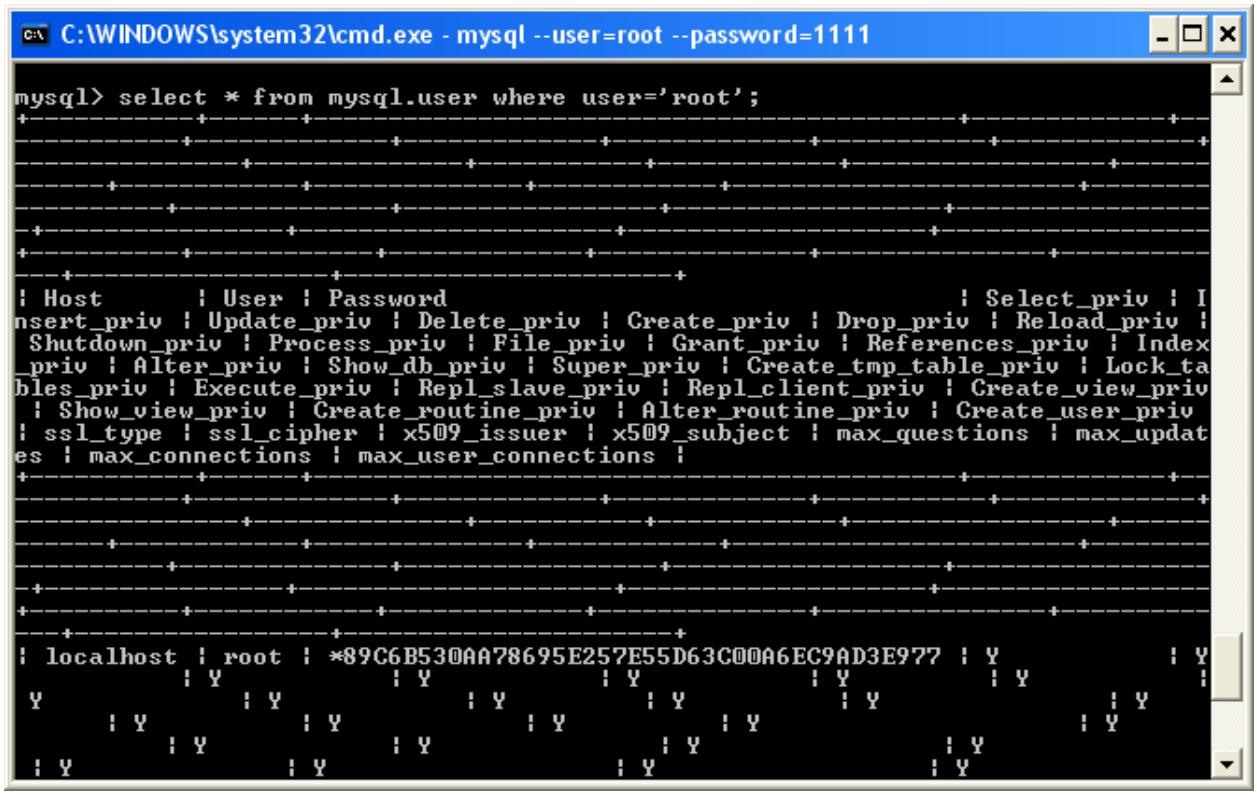

Рис 3.14. Права користувача root

13. Використовуючи інструкції рис. 3.15, створити нову базу даних з

назвою mytest.

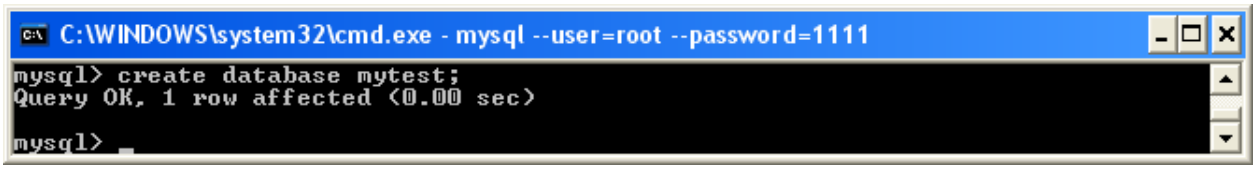

Рис. 3.15. Створення нової бази даних mytest

14. Відповідно інструкцій рис. 3.16, в базі даних mytest створимо таблицю myuser яка складається із двох символьних полів name довжиною 12 символів та login довжиною 24 символи.

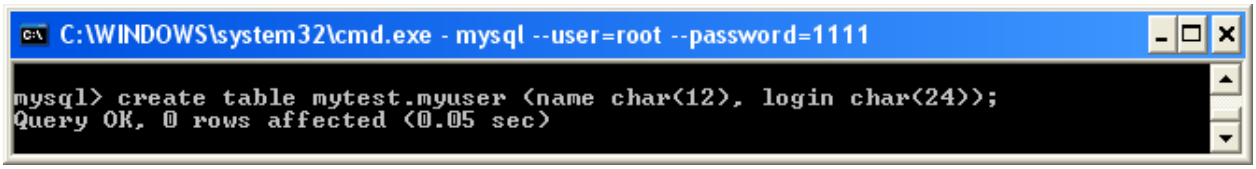

Рис. 3.16. Створення таблиці

15. Записати в таблицю myuser бази даних mytest три рядки довільної інформації. Для цього слід скористатись інструкціями рис. 3.17.

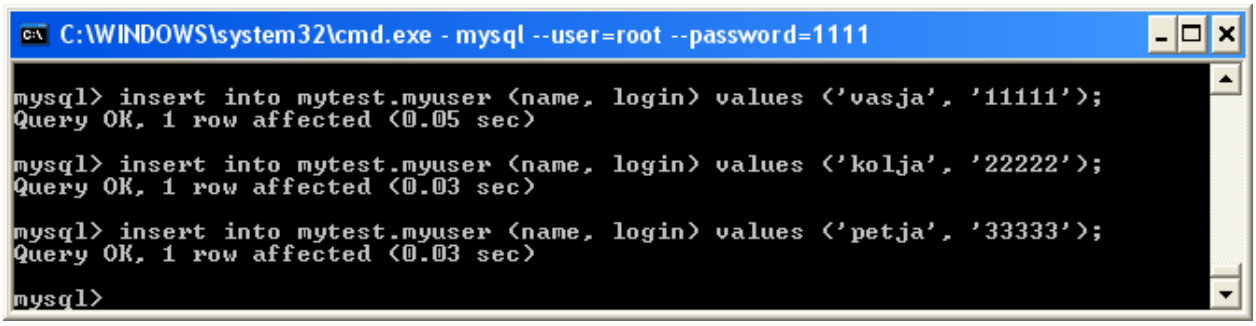

Рис. 3.17. Запис даних в таблицю

16. За допомогою команди select, параметри якої показано на рис. 3.18, переглянемо інформацію таблиці myuser.

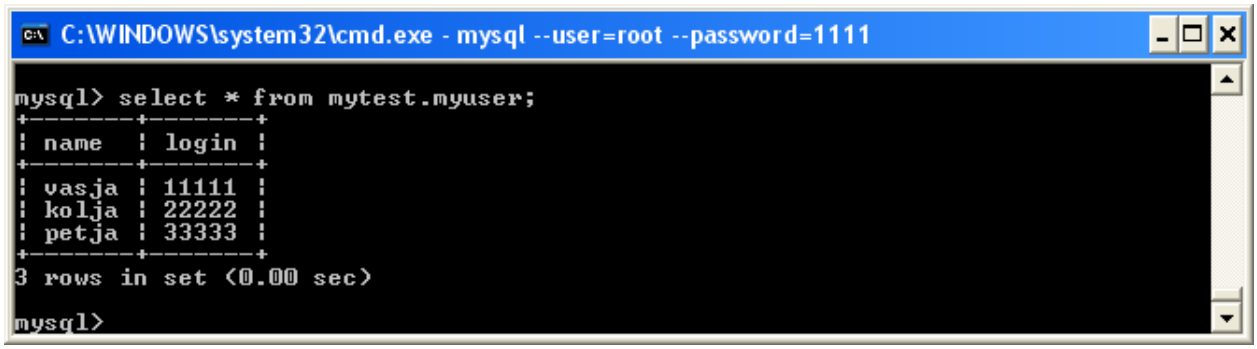

Рис. 3.18. Перегляд даних таблиці

17. За допомогою команди grant, параметри якої показано на рис. 3.19 введемо нового користувача my, який буде мати повні права на доступ до бази даних mytest. Зазначимо, що даний користувач отримав пароль "123" і може під'єднуватись до серверу MySQL тільки з локального комп'ютера.

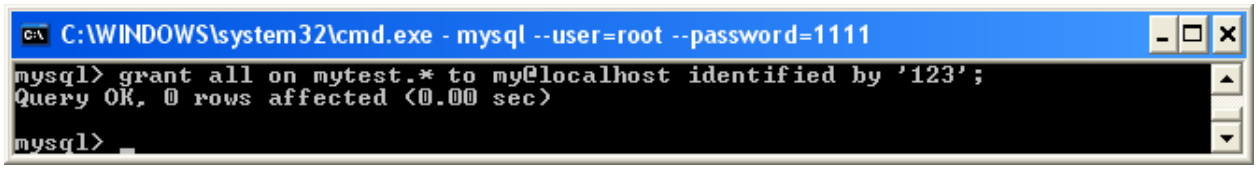

Рис. 3.19. Введення нового користувача, що має всі права на базу даних mytest

18. Відповідно інструкцій рис. 3.8 завершуємо роботу від імені користувача root та підключаємось до серверу MySQL від імені користувача my. Для цього скористаємось інструкціями рис. 3.20.

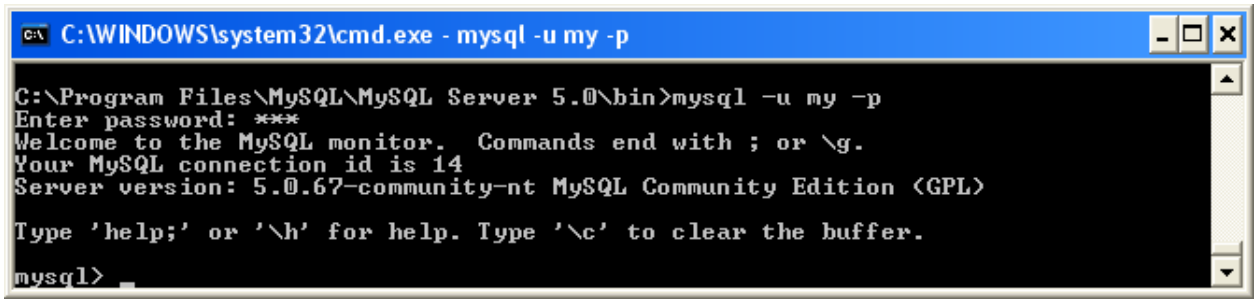

Рис. 3.20. Підключення від імені користувача my

19. Пересвідчимось в можливостях користувача my відносно бази даних mytest. Для цього від імені користувача my додамо в таблицю myuser бази даних mytest один рядок інформації. Інструкції показані на рис. 3.21.

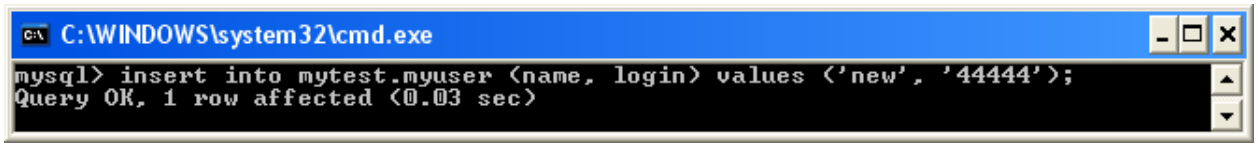

Рис. 3.21. Вставка одного рядка інформації

20. Введемо нового користувача one який буде мати можливість перегляду всієї бази даних mytest та вставки даних в поле login таблиці. myuser. Для цього слід:

– Закінчити роботу від імені користувача my.
– Підключитись від імені користувача root.
– Виконати команду grant.

Відповідні інструкції показані на рис. 3.22.

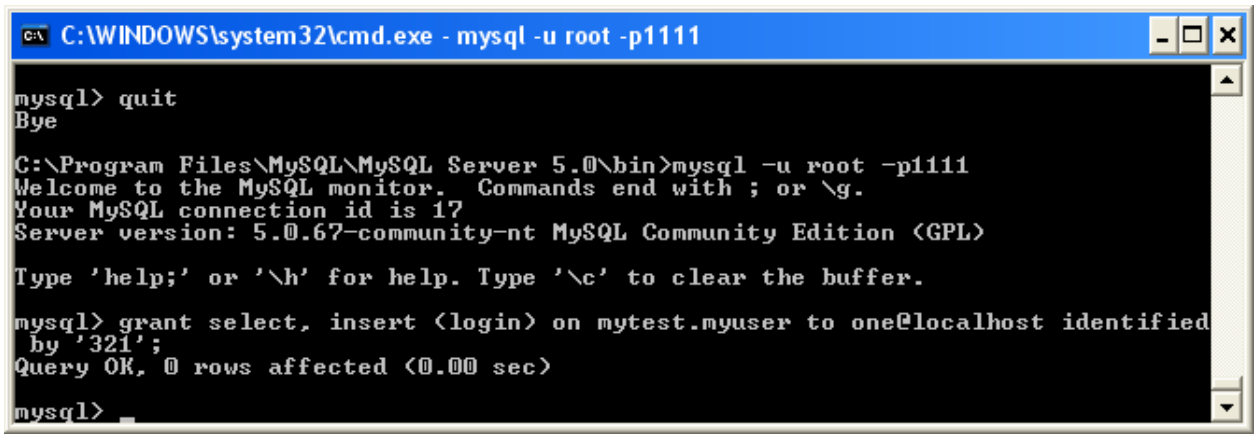

Рис. 3.22. Введення користувача з обмеженими правами

21. Пересвідчимось в можливостях користувача one. Для цього слід:

A. Закінчити роботу від імені користувача root.
B. Підключитись до серверу від імені користувача one.

C. За допомогою команди select переглянути дані таблиці myuser бази даних mytest.

D. За допомогою команди insert ввести дані в поле login таблиці myuser та пересвідчитись у коректності введення.

E. Пересвідчитись у неможливості ввести дані в поле name.

Виконання пунктів A-D показано на рис. 3.23. Виконання пункту E проілюстровано на рис. 3.24.

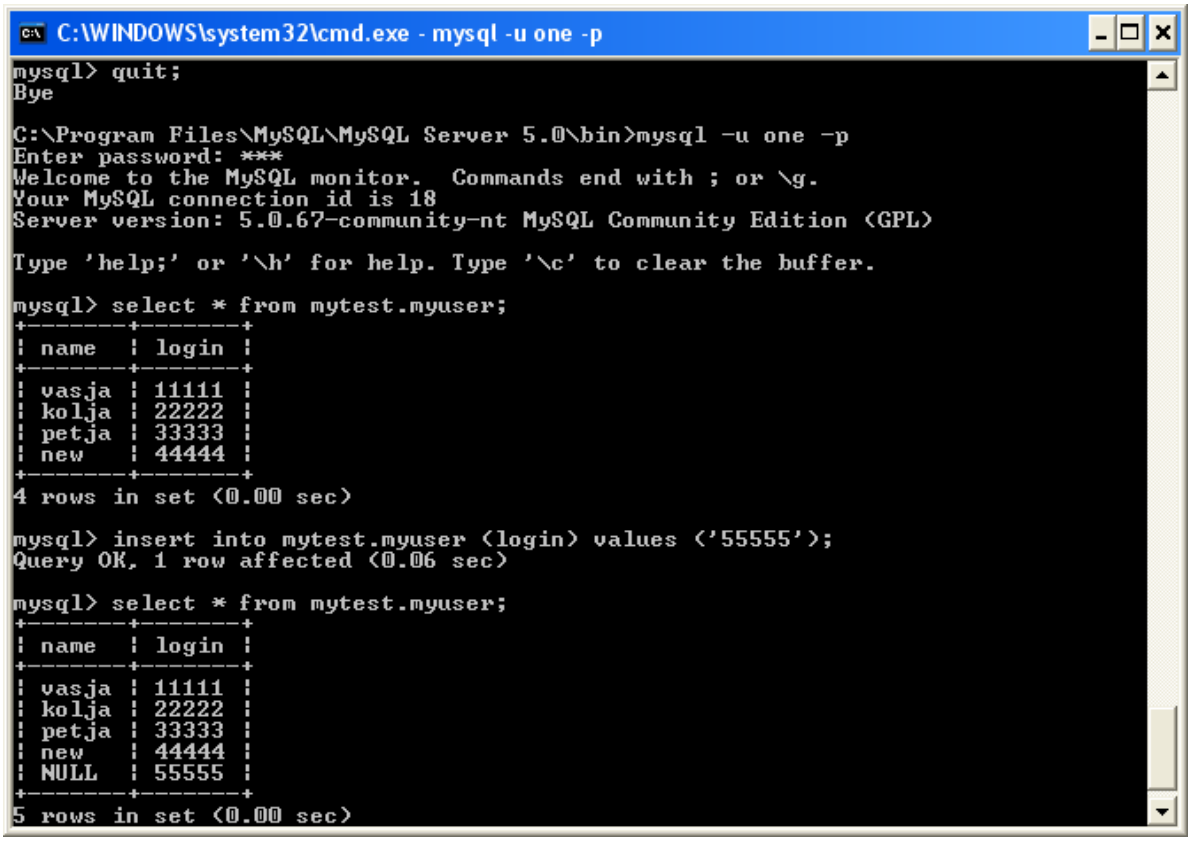

Рис. 3.23. Перегляд можливостей користувача one

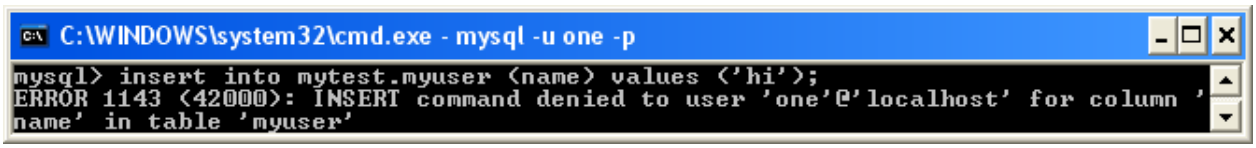

Рис. 3.24. Відмова у виконання запиту на вставку даних в поле name

22. Заборонимо користувачеві one вставляти дані в поле login таблиці myuser бази даних mytest. Для цього слід:

A. Закінчити роботу від імені користувача one.

B. Підключитись до серверу від імені користувача root.

C. За допомогою команди revoke заборонити користувачеві one вставляти дані в поле login.

D. Закінчити роботу від імені користувача root.

E. Підключитись до серверу від імені користувача one.

F. Пересвідчитись у неможливості ввести дані в поле login.

G. Пересвідчитись у можливості перегляду даних.

Виконання пунктів A-C показано на рис. 3.25. Виконання пунктів D-G проілюстровано рис. 3.26.

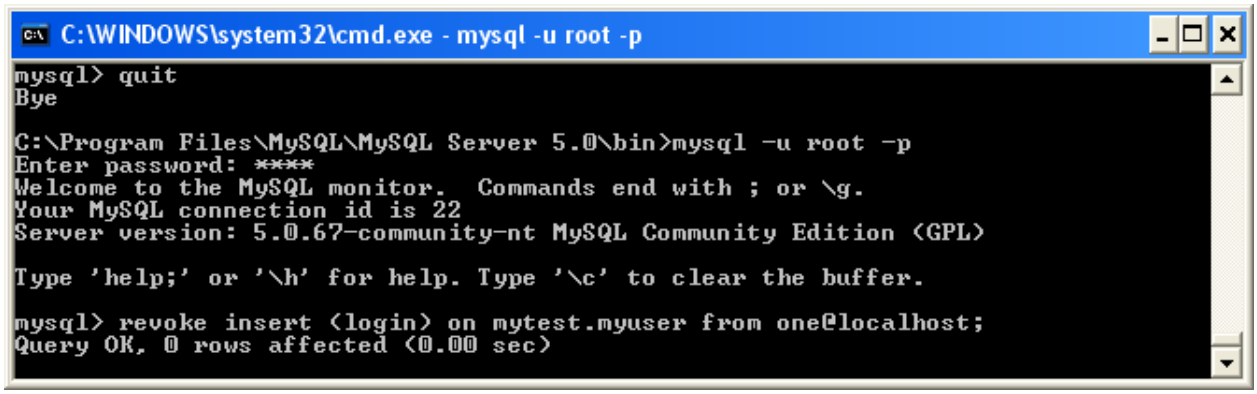

Рис. 3.25. Перевизначення прав користувача one

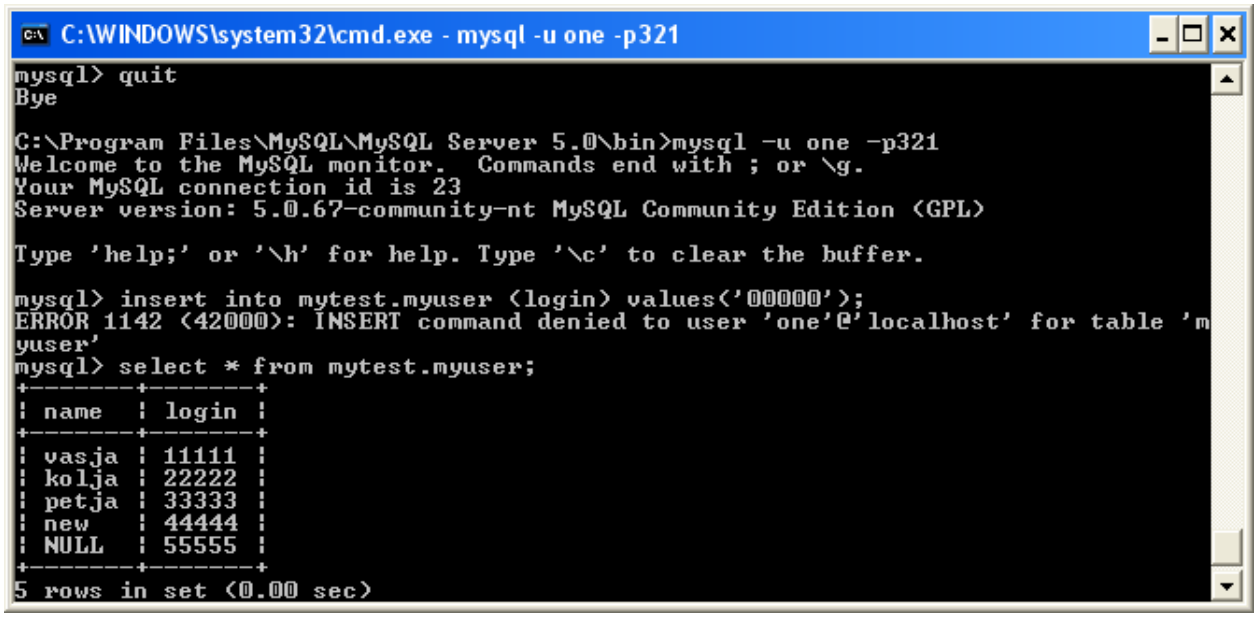

Рис. 3.26. Використання нових прав користувачем one

Питання для самоперевірки

1. Де знаходиться конфігураційний файл СУБД MySQL?
2. Яке призначення рядка *port=3306*, який знаходиться в конфігураційному файлі СУБД MySQL?
3. Як створити нову базу даних?
4. Як створити нову таблицю в базі даних?
5. Як ввести нового користувача?
6. Як встановити пароль адміністратора?
7. Як ввести нові дані в існуючу таблицю бази даних?
8. Як заборонити користувачеві вставку даних в таблицю?
9. Яке призначення команди grant?
10. Яке призначення команди revoke?
11. Як встановити примусове використання системи привілеїв користувачів?
12. Як переглянути привілеї користувачів серверу СУБД MySQL?
13. Як запустити клієнт MySQL та від імені користувача root під'єднатись до серверу?
14. Як завершити роботу клієнта MySQL?
15. Як перезапустити сервер MySQL?
16. Як обмежити права користувача серверу MySQL?
17. Як називається конфігураційний файл СУБД MySQL?
18. Як переглянути дані деякої таблиці?
19. Яке призначення параметру "u" програми mysql?
20. Яке призначення параметру "p" програми mysql?
21. Яке призначення конфігураційного файлу СУБД MySQL?
22. Яке призначення програми mysqladmin?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література

1. Безруков Н. Н. Компьютерная вирусология / Н. Н. Безруков. – К. : Инкомбук, 1990. – 450 с.
2. Богуш В.М. Моніторинг систем інформаційної безпеки: навч. посібник [для студ. вищ. навч. закл.] / В.М. Богуш, А. М. Кудін. – К. : ДУІКТ, 2006. – 414 с.
3. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. – СПб. : БХВ-Петербург, 2000. – 450 с.
4. Лукацкий А.В. Обнаружение атак. – СПб.:БХВ-Петербург,2010. – 624 с.
5. Касперски К. Техника и философия хакерских атак / К. Касперски. – М. : Солон, 2010. – 256 с.
6. Колисниченко Д.Н. Rootkits под Windows / Д. Н. Колисниченко. – СПб. : Наука и техника, 2011. – 320 с.
7. Коробейников А.Г. Математические основы криптографии. СПб, 2004 – 106с.
8. Менаске Д. Производительность Web-служб. Анализ, оценка и планирование / Менаске Д., Виргилио А. ; пер. с англ. – СПб. : ДиаСофтЮп", 2012. – 480 с.
9. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
10. Таненбаум Э. Компьютерные сети / Таненбаум Э. ; пер. с англ. А. Леонтьева. – СПб.: Питер, 2002. – 848 с.
11. Таненбаум Э. Современные операционные системы. 2-е изд. / Таненбаум Э. ; пер. с англ. – СПб. : Питер, 2002. – 1036 с.

12. Терейковський І. Нейронні мережі в засобах захисту комп’ютерної інформації / І. Терейковський. – К. : ПоліграфКонсалтинг. – 2007. – 209 с.

13. Ульман Л. Руководство по изучению языка MySQL / Ульман Л.; Пер. с англ. Слинкина А.А - М.: ДМК Пресс; СПб.: Питер, 2004. – 352 с.

14. Уэнстром М. Организация защиты сетей Cisco / Уэнстром М. ; пер. с англ. – М. : Вильяме, 2012. – 768 с.

15. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и техника, 2012. – 384 с.

Допоміжна література

16. Науково-технічний журнал "Захист інформації".

17. Науково-технічний журнал "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні".

18. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.

19. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

20. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

21. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

22. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

23. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

24. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

25. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

26. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

Інформаційні ресурси

27. Електронний кампус НТУУ «КПІ». Матерали з дисципліни «Методи та засоби захисту інформації в комп'ютерних системах». – Режим доступу : http://login.kpi.ua.

28. Веб-портал Державної служби технічного захисту інформації України». – Режим доступу : www.dstszi.gov.ua

29. Веб-портал компанії «DrWeb». – Режим доступу : www.drweb.ru

30. Веб-портал компанії «Безпека». – Режим доступу : www.bezpeka.biz

31. Веб-портал компанії «Searchinform». – Режим доступу : www.searchinform.ru

32. Веб-портал системи виявлення вразливостей Snort. – Режим доступу : www.snort.com

ДОДАТОК 1

ВАРІАНТИ ЗАВДАНЬ ДЛЯ РОЗРАХУНКОВОЇ РОБОТИ

З даної навчальної дисципліни передбачено індивідуальне завдання у вигляді розрахунково-графічної роботи. Тематика розрахункової роботи: дослідження, розробка та налаштування засобів захисту інформації в комп'ютерних системах.

Варіант 1. Настроїти систему захисту операційної системи.

Варіант 2. Розробити додаткові компонентів захисту операційної системи.

Варіант 3. Настроїти систему захисту електронної пошти від спаму.

Варіант 4. Розробити систему захисту електронної пошти від спаму.

Варіант 5. Настроїти мережевий екран.

Варіант 6. Розробити додаткові компонентів захисту мережевих екранів.

Варіант 7. Дослідити систему розповсюдження спаму, з метою виявлення їх вразливостей.

Варіант 8. Дослідити мережеві сканери та розробити відповідну систему захисту.

Варіант 9. Дослідити Dos та Ddos атаки та розробити систему захисту від них.

Варіант 10. Дослідити особливості програмного забезпечення мобільних пристроїв.

Варіант 11. Настроїти систему захисту СУБД.

Варіант 12. Розробити додаткові компоненти захисту СУБД.

Варіант 13. Розробити засоби захисту СУБД від SQL ін'єкцій.

Варіант 14. Настроїти антивірусні засоби.

Варіант 15. Розробити систему антивірусного захисту.

Варіант 16. Настроїти систему захисту від кейлогерів.

Варіант 17. Розробити компонент захисту від кейлогерів.

Варіант 18. Настроїти захист віртуальної мережі.

Варіант 19. Дослідити засоби зламу парольного захисту операційних систем та розробити відповідну систему захисту.

Варіант 20. Розробити систему захисту офісних документів від несанкціонованого копіювання.

Варіант 21. Настроїти систему захисту програм та даних від несанкціонованого розповсюдження.

Варіант 22. Настроїти систему резервного копіювання інформації операційної системи.

Варіант 23. Дослідити стійкість віртуальної машини Java від атаки на відмову в обслуговуванні.

Варіант 24. Дослідити стійкість Framework від атаки на відмову в обслуговуванні.

Варіант 25. Настроїти систему безпеки веб-серверів.

Варіант 26. Розробити додаткові модулі захисту веб-серверів.

Варіант 27. Дослідити засоби зламу захисту програм з метою розробки відповідних систем захисту.

Варіант 28. Розробити систему захисту програм від вивчення.

Варіант 29. Настроїти систему виявлення вторгнень.

Варіант 30. Настроїти систему виявлення вразливостей.

Варіант 31. Розробити систему виявлення вторгнень.

Варіант 32. Розробити систему виявлення вразливостей.

Варіант 33. Дослідити вразливості програмного забезпечення мобільних пристроїв з метою розробки системи їхнього захисту.

ДОДАТОК 2

ЗАПИТАННЯ МОДУЛЬНИХ КОНТРОЛЬНИХ РОБІТ

Модульна контрольна робота № 1

1. Охарактеризуйте проблему захисту інформації в комп'ютерних системах.
2. Наведіть основні визначення в області захисту інформації.
3. Охарактеризуйте нормативне забезпечення системи технічного захисту інформації в Україні.
4. Охарактеризуйте нормативні документи системи криптографічного захисту інформації в Україні.
5. Охарактеризуйте зарубіжні та міжнародні стандарти щодо захисту інформації в комп'ютерних системах.
6. Охарактеризуйте загрози конфіденційності, цілісності, доступності.
7. Охарактеризуйте канали порушення безпеки інформації.
8. Охарактеризуйте політику безпеки інформації.
9. Охарактеризуйте комплекс засобів захисту і об'єкти комп'ютерної системи.
10. Що таке несанкціонований доступ?
11. Охарактеризуйте модель порушника.
12. Охарактеризуйте планування захисту і керування системою захисту.
13. Охарактеризуйте основні принципи керування доступом.
14. Охарактеризуйте послуги безпеки.
15. Охарактеризуйте загальні вимоги до засобів захисту інформації.
16. Охарактеризуйте економічні та технічні критерії оптимізації системи захисту інформації.
17. Охарактеризуйте поняття режиму захисту.
18. Охарактеризуйте особливості моделі загроз ресурсам ОС.
19. Охарактеризуйте основні функції підсистеми захисту ОС.

20. Охарактеризуйте типову структуру підсистеми безпеки ОС.
21. Охарактеризуйте керування доступом до ресурсів ОС.
22. Охарактеризуйте особливості забезпечення безпеки ресурсів ОС сімейств Windows.
23. Охарактеризуйте особливості забезпечення безпеки ресурсів ОС сімейств UNIX.
24. Охарактеризуйте причини, види, основні методи порушення конфіденційності в СУБД.
25. Охарактеризуйте методи захисту СУБД.
26. Охарактеризуйте типові загрози інформації офісних СУБД.
27. Охарактеризуйте особливості системи захисту офісних СУБД.
28. Охарактеризуйте типові загрози інформації промислових СУБД.
29. Що таке руйнуючі програмні засоби?
30. Охарактеризуйте підходи до класифікація шкідливого програмного забезпечення.
31. Охарактеризуйте методи і засоби захисту програмного забезпечення.
32. Охарактеризуйте методи захисту програм від вивчення.
33. Охарактеризуйте типову архітектуру системи захисту програмного забезпечення.
34. Охарактеризуйте критерії оцінки ефективності систем захисту від шкідливого програмного забезпечення.
35. Охарактеризуйте системи антивірусного захисту провідних виробників.

Модульна контрольна робота № 2

1. Охарактеризуйте загальні положення про інформаційну безпеку мереж передачі даних.
2. Охарактеризуйте особливості моделі загроз мереж передачі даних.
3. Охарактеризуйте технологію міжмережних екранів.
4. Охарактеризуйте технологію віртуальних приватних мереж (ВПМ).
5. Охарактеризуйте особливості захисту мобільних програмних компонентів.
6. Охарактеризуйте особливості архітектури безпеки COM/DCOM, CORBA, ActiveX, Java, Flash Macromedia.
7. Охарактеризуйте типові загрози інформації комп'ютерної системи при використанні електронної пошти?
8. Охарактеризуйте методи захисту від несанкціонованої передачі даних?
9. Охарактеризуйте поняття спаму.
10. Охарактеризуйте основні методи захисту від спаму.
11. Охарактеризуйте методи захисту від спаму на основі чорного та білого списків.
12. Охарактеризуйте методи захисті від спаму на основі ключових словосполучень.
13. Охарактеризуйте метди захисту від спаму на основі байєсовської фільтрації.
14. Охарактеризуйте особливості сучасних спам-засобів.
15. Охарактеризуйте системи виявлення вторгнень.
16. Охарактеризуйте системи керування захищеністю.
17. Охарактеризуйте системи аналізу вразливостей.
18. Охарактеризуйте системи виявлення вторгнень.

19. Охарактеризуйте підходи до оптимізації параметрів систем розпізнавання атак та вразливостей?

20. Охарактеризуйте методологію побудови марківської моделі динаміки параметрів захисту.

21. Охарактеризуйте приклад створення марківської моделі оптимізації параметрів захисту веб-серверу.

22. Що таке симетрична криптографія?

23. Охарактеризуйте методи шифрування заміною.

24. Охарактеризуйте методи шифрування перестановкою

25. Охарактеризуйте методи шифрування шляхом аналітичних перетворень.

26. Що таке криптоаналіз?

27. Охарактеризуйте принципи асиметричної криптографії?

28. Охарактеризуйте поняття цифрового підпису?

29. Охарактеризуйте поняття криптографічних протоколів.

30. Охарактеризуйте використання протоколу SSL для безпечного обміну інформацією в мережі.

31. Охарактеризуйте задачі захисту інформації, розв'язання яких потребує застосування методів штучного інтелекту.

32. Охарактеризуйте приклади використання нейронних мереж в задачах захисту інформації.