**Лабораторна робота № 5**

# КЕРУВАННЯ КОРИСТУВАЧАМИ ВУЗЛА

**Мета:** набуття навичок налаштування особливих прав доступу користувачів за допомогою використання встановлених типів служб SharePoint.

## 1. КЛЮЧОВІ ПОЛОЖЕННЯ

У SharePoint управління доступом до веб-сайтів, списків, папок і елементів списків здійснюється за допомогою заснованої на ролях системи членства, за допомогою якої користувачам призначаються ролі, які дозволяють доступ до об'єктів SharePoint.

Щоб надати користувачу доступ до об'єкта, можна додати його в групу, яка вже володіє дозволами на доступ до об'єкта, або створити об'єкт призначення ролі, визначити користувача для призначення ролі, при необхідності прив'язавши призначення ролі до відповідного визначення ролі з базовими дозволами, а потім додати призначення в колекцію призначень ролей для елемента списку, папки, списку або веб-сайту. Нижче перераховані способи управління доступом до об'єктів в SharePoint:

* Об'єкти можуть використовувати ті самі дозволи, що і батьківський веб-сайт, список або папка (наслідуючи ролі і користувачів батьківського об'єкта) або можуть мати унікальні дозволи.
* Для веб-сайтів, списків, папок і елементів надаються окремі колекції призначень ролей, що дозволяє гнучко управляти доступом користувачів до об'єктів.
* Групи складаються з користувачів, і їм можуть призначатися або не призначатися ролі.

До складу SharePoint за замовчуванням входять наступні три групи:

* *owners* (адміністратор); - *members* (кореспондент); - *visitors* (читач).

При створенні веб-сайту з унікальними дозволами через призначений для користувача інтерфейс виконується перехід на сторінку, на якій користувачі поміщаються в групи для контролю доступу до сайту.

*Анонімний доступ* дозволяє користувачам анонімно брати участь в опитуваннях і переглядати сторінки. Крім того, можна дозволити доступ "всім користувачам, які пройшли перевірку", щоб всі члени домену могли звертатися до веб-сайту без необхідності включення анонімного доступу.

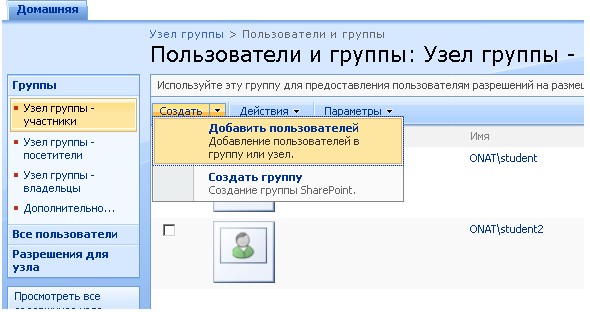
*Права створення веб-сайту* (CreateSSCSite і ManageSubwebs) керують правом користувачів на створення веб-сайтів верхнього рівня, дочірніх сайтів або робочих областей.

Користувачі можуть стати членами об'єкта SharePoint неявно, через групу, якій призначена відповідна роль, або безпосередньо за допомогою призначення. Користувачі також можуть бути членами групи домену Microsoft Windows NT, яка додається до групи або ролі. Визначення ролі пов'язує користувача або групу з правом або набором прав, що відповідають значенням перерахування Microsoft.SharePoint.SPBasePermissions. Кожен користувач або група має унікальний ідентифікатор ID. Можливості *об'єктної моделі* для створення або зміни призначень і визначень ролей відрізняються від можливостей, що надаються файлами addrole.aspx і editrole.aspx. На відміну від цих сторінок, представлених в інтерфейсі, об'єктна модель не вводить залежність прав, тому можливе створення визначення з будь-якою їх комбінацією. У той самий час при використанні об'єктної моделі для налаштування визначень ролей і дозволів слід ретельно продумувати план, так як погано сплановане визначення ролей і неправильно призначені права можуть привести до виникнення проблем при використанні.

## 2. ХІД ПРАКТИЧНОГО ЗАНЯТТЯ

Розглянемо, як надавати користувачам певні права на перегляд і редагування веб-вузла, використовуючи для цього встановлені типи дозволів служб SharePoint:

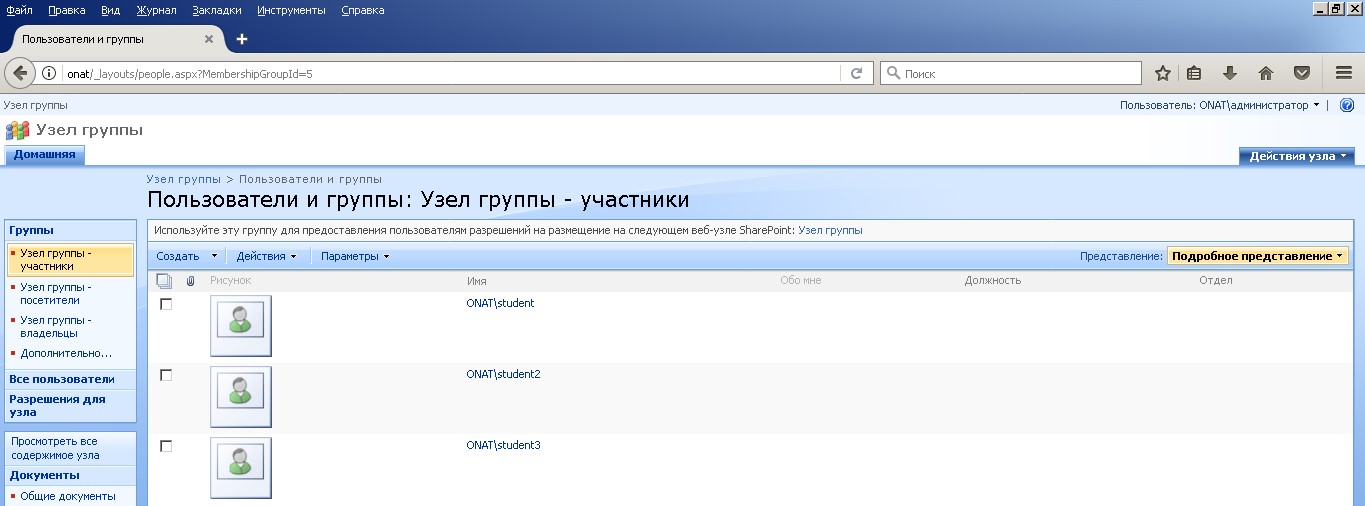
1. Увійдіть на веб-вузол, використовуючи обліковий запис його адміністратора.
2. Введіть команду *Дії вузла / Параметри вузла*.
3. На сторінці *Параметри вузла* в категорії *Користувачі та дозволи* виберіть посилання *Користувачі і групи*.
4. На сторінці *Користувачі та групи* учасників, натисніть кнопку **Створити** і виберіть в меню пункт **Додати** користувачів (рис. 5.1).



**Рисунок 5.1** – Додавання нового користувача у групу учасники

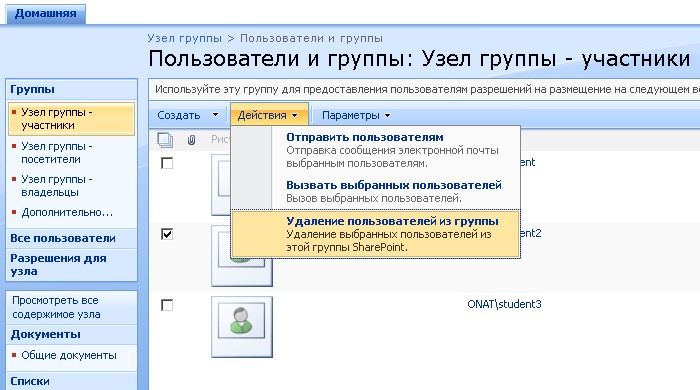
1. Задайте параметри нового користувача
2. Перегляньте поточний список користувачів, що мають значення

роздільної здатності участі (рис. 5.2)



**Рисунок 5.2** – Список учасників

1. Встановіть прапорець зліва від імені користувача, якого Ви бажаєте видалити з групи учасників.
2. Натисніть кнопку **Дії** та виберіть у меню пункт **Видалення користувачів із групи** (рис 5.3).



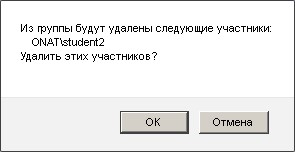
**Рисунок 5.3** – Видалення одного з користувачів із групи учасників

1. Натисканням кнопки *ОК* підтвердити видалення в проміжному

діалоговому вікні (рис. 5.4)

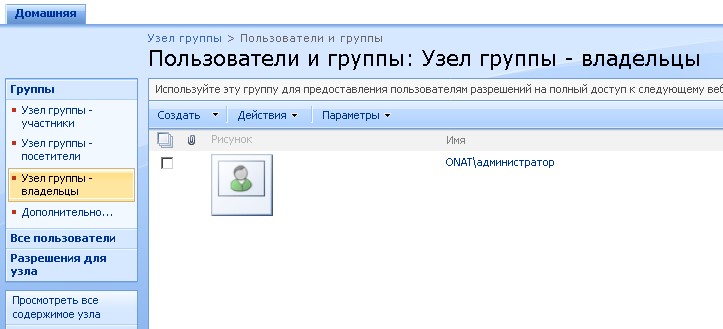
1. Знову перегляньте поточний список учасників, щоб переконатися в тому, що student2 було виключено з групи учасники.

*Примітка:* Це означає, що *student2* втратив дозвіл учасника (на правку контенту сайту), але не призводить до повного їх виключення з числа користувачів колекції сайтів.



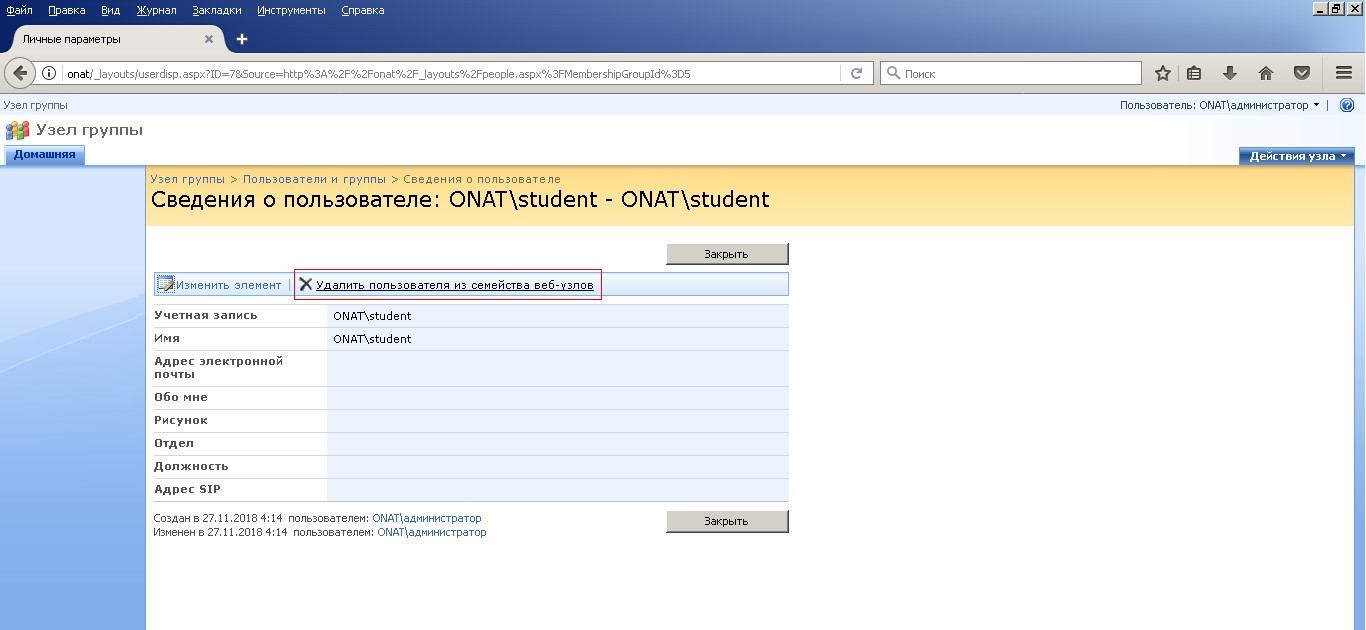
**Рисунок 5.4** – Підтвердження видалення student2 з групи учасники

1. Клацанням за посиланням – перегляньте список адміністраторів (власників) веб-сайту (рис. 5.5), а потім – список відвідувачів.
2. Додайте до групи відвідувачів обліковий запис.



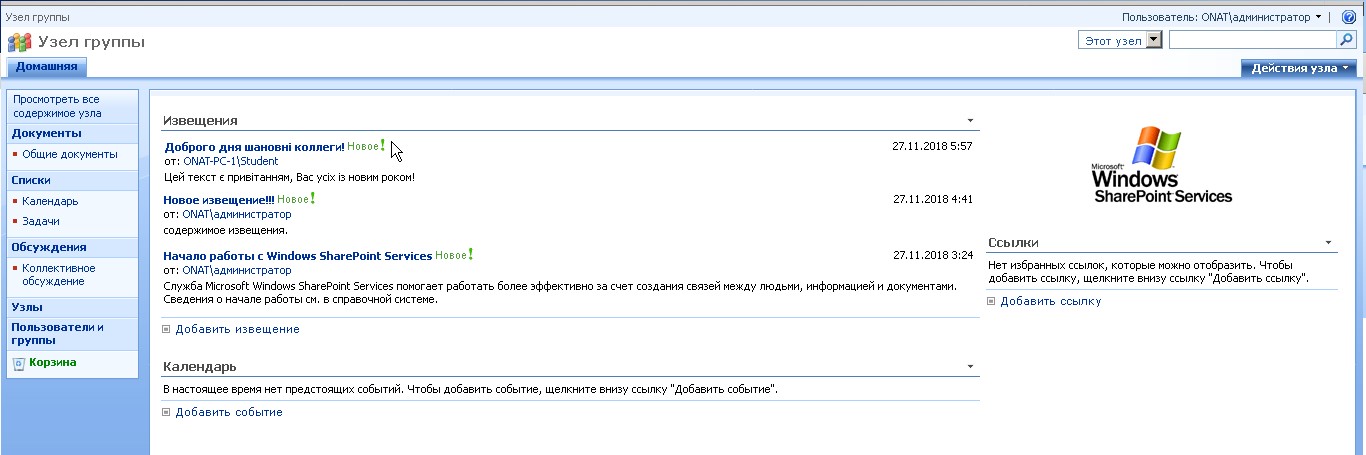
**Рисунок 5.5** – Список власників сайту

1. Перейдіть на домашню сторінку вузла і переконайтеся, що повідомлення, написане від *student* залишилося в списку *Повідомлення*
2. Клацніть по посиланню автора повідомлення *student.*
3. На сторінці **Відомості** про користувача клацніть посилання **Видалити користувача з сімейства веб-вузлів** (рис. 5.6).



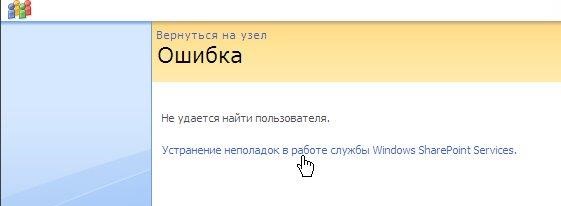
**Рисунок 5.6** – Видалення облікового запису student з числа користувачів сімейства вузлів

1. Знову перейдіть на домашню сторінку вузла і переконайтеся, що повідомлення, написані користувачем *student* як і раніше залишаються в списку *Повідомлення*.
2. Знову клацніть по посиланню student (рис. 5.7).



**Рисунок 5.7** – Користувач *student* залишається у списку Повідомлення

1. На сторінці, що говорить про помилку (оскільки *student* виключено з користувачів ***Колекція сайтів***) клацніть посилання **Повернутися на вузол** (рис. 5.8) *http: //www.intuit.ru/studies/courses/475/331/lecture/8026? Page = 6 - image.2.38.*

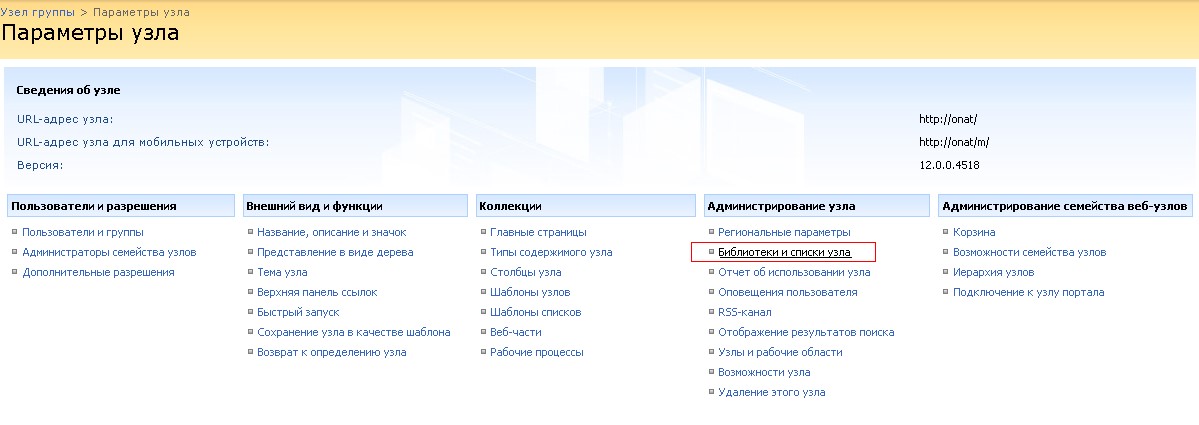


**Рисунок 5.8** – Спроба отримати дані про відсутнього користувача, призводить до помилки

**Керування дозволами для дочірніх елементів вузла**

Служби SharePoint 3.0 передбачають налаштування параметрів безпеки на різних рівнях. Самий верхній рівень – це рівень колекція сайтів і рівень вебдодатків. Цей рівень повинен налаштовуватися на сервері, і далі адміністратором сервера делегуються певні права адміністратора вузла SharePoint. Адміністратор батьківського вузла може налаштовувати незалежні дозволи для дочірнього вузла. Наступний рівень безпеки – це безпека окремих елементів вузла: списків і бібліотек документів, а також безпеку окремих елементів списків і бібліотек. В рамках цієї вправи зупинимося на можливості налаштування незалежних дозволів для дочірніх елементів веб-вузлів таких, як дочірні вузли, бібліотеки і списки на прикладі списку **Повідомлення**.

1. Увійдіть на веб-вузол, використовуючи обліковий запис його адміністратора.
2. Введіть команду **Дії вузла** / **Параметри вузла**.
3. На сторінці **Параметри вузла** в категорії **Адміністрування вузла** клацніть посилання **Бібліотеки та списки вузла** (рис. 5.9).



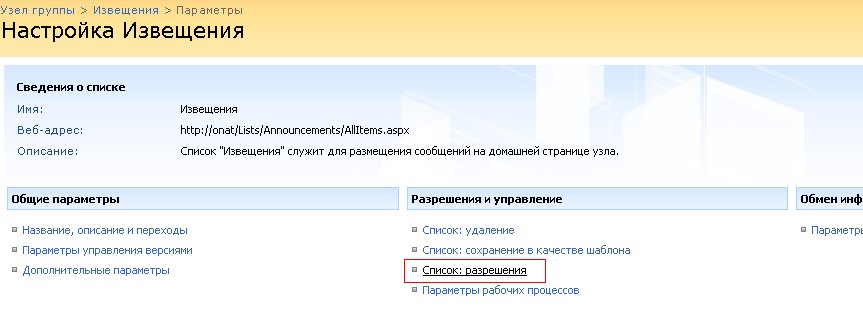
**Рисунок 5.9** – Параметри бібліотек та списків

1. На сторінці **Бібліотеки** та списки вузла виберіть посилання **Налаштувати Повідомлення** (рис. 5.10).



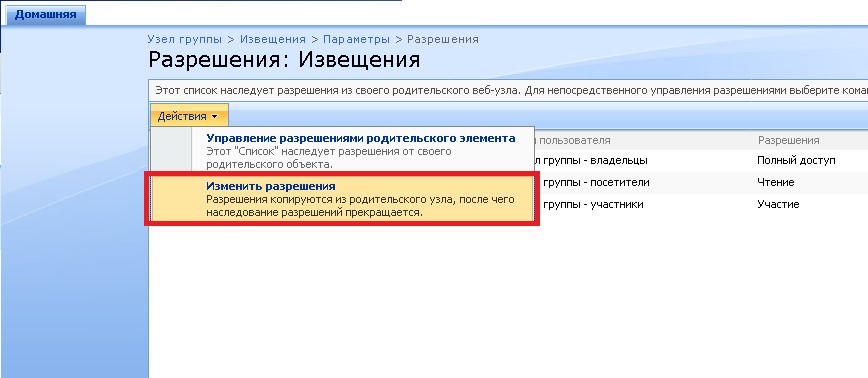
**Рисунок 5.10** – Налаштування списку повідомлення

1. На сторінці **Налаштування Повідомлення** клацніть посилання **Список: дозволу** (рис. 5.11).



**Рисунок 5.11** – Налаштування дозволу списку Повідомлення

1. На сторінці **Дозволи**: **Повідомлення** натисніть кнопку **Дії**.
2. Виберіть у меню **Дії** команду **Змінити дозволи** (рис. 5.12).

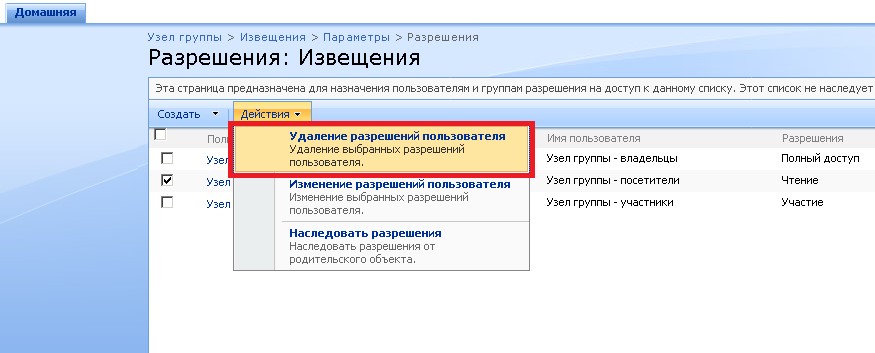


**Рисунок 5.12 –** Установка для списку Повідомлення нової схеми дозволу

1. Встановіть прапорець зліва від назви групи користувачів, доступ якої до списку **Повідомлення** Ви хочете заборонити, наприклад, групи відвідувачі.
2. У меню **Дії** виберіть пункт **Видалення дозволів користувача** (рис.

5.13).

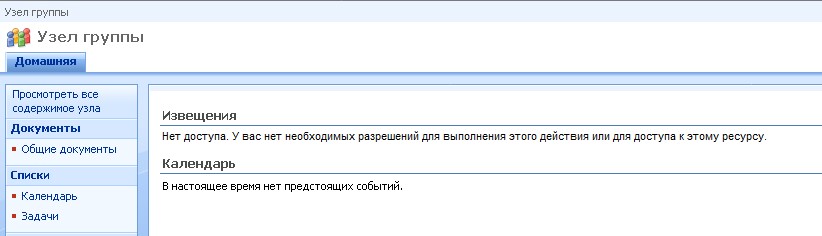
1. Дайте підтвердження своєму наміру в проміжному діалозіпопередженні.



**Рисунок 5.13** - Заборона доступу до списку для користувачів з групи відвідувачі

1. Увійдіть на веб-вузол, використовуючи обліковий запис користувача.
2. Відкрийте **Домашню сторінку вузла** і зверніть увагу на список

**Повідомлення**, вміст якого стало недоступним для користувача (рис. 5.14).



**Рисунок 5.14** – Доступ відвідувача до списку Повідомлень заборонений

Отже, права на доступ до конкретного списку, бібліотеки або дочірнього вузла, за замовчуванням, успадковуються від батьківського веб-вузла. Однак, є можливість встановити для них і власні дозволи, обмеживши доступ до ресурсу для одних груп користувачів або, навпаки, розширивши права для інших груп. Таким чином, будь-який дочірній елемент вузла SharePoint володіє гнучкою можливістю визначення параметрів доступу до нього окремих груп користувачів.

## 3. КОНТРОЛЬНІ ЗАПИТАННЯ

1. Опишіть типи дозволів служб SharePoint?
2. Перерахуйте способи керування доступом до об’єктів в SharePoint?
3. Які групи користувачів входять до складу SharePoint за замовчуванням?
4. Які можливості об’єктної моделі?
5. Які можливості щодо визначення параметрів доступу є у дочірніх елементів вузла SharePoint?

## 4. ДОМАШНЄ ЗАВДАННЯ

1. Вивчити ключові положення.
2. Письмово відповісти на контрольні питання.

## 5. ЛАБОРАТОРНЕ ЗАВДАННЯ

1. За завданням викладача створити дві групи з різними правами доступу до сайту.
2. В кожній групі додати користувачів та настроїти їм права доступу.
3. Перевірити облікові записи створених користувачів.
4. Від імені адміністратору сайту настроїти сповіщення та надіслати створеним користувачам повідомлення.
5. Перевірити чи отримали користувачі надіслані їм повідомлення.

**3. ЗМІСТ ПРОТОКОЛУ**

1. Тема
2. Мета
3. Відповіді на контрольні питання
4. Хід виконання роботи
5. Висновок про виконану роботу