ISSN 2076-8184. Інформаційні технології і засоби навчання. 2010. №4 (18).
Режим доступу до журналу: http://www.ime.edu-ua.net/em.htm

УДК 681.3;377.4

Золотаренко Ірина Владиславівна, провідний інженер відділу електронних інформаційних ресурсів і мережних технологій Інституту інформаційних технологій і засобів навчання НАПН України, м. Київ

Підходи до організації системи безпеки на базі MS SharePoint

Анотація

Актуальність матеріалу, викладеного у статті, обумовлена нагальними потребами суспільства у створенні безпечних інформаційних систем, сприянні впровадженню новітніх інформаційних технологій у процеси управління освітою. Питання безпеки є важливим для надійності і працездатності таких систем. Одним із шляхів вирішення проблеми безпеки є розподіл користувачів за категоріями і надання їм прав різних рівнів. У статті проведено аналіз загальних підходів до організації груп і рівнів дозволів користувачів у інформаційних системах, розроблених на базі MS SharePoint. На основі проведеного аналізу визначено основні проектні рішення щодо безпеки інформаційної системи «Планування наукових досліджень в Національній академії педагогічних наук України на базі мережі Інтернет».

Ключові слова: інформаційна система, система MS SharePoint, безпека, доступ користувачів, групи доступу, дозволи, групи безпеки.

Основним завданням у розробці та плануванні будь-якої електронної системи є планування системи безпеки і розмежування прав користувачів до вмісту цієї системи. Правильне планування дозволяє знизити витрати на адміністрування та супровід такої системи, а також забезпечити безперервність бізнес-процесів, які виконуються в інформаційній системі. Проектування перевірки автентичності та авторизації значно знижує кількість потенційно уразливих місць. Розмежування доступу коду дозволяє призначати програмному коду різні рівні довіри, залежно від його джерела та інших особливостей. Безпека зв'язку є складовою частиною системи безпеки, що відповідає за захист даних, що передаються між користувачами та вузлом, а також між серверами в інформаційному середовищі.

Технології безпеки системи MS SharePoint

У системі MS SharePoint використовується низка технологій, що знижують ризик порушення безпеки, у тому числі такі [1]:

- перевірка автентичності: спирається на концепцію учасників безпеки Windows, що дозволяє використовувати методи суворої перевірки, політики паролів, політики блокування облікових записів і шифрування;
- авторизація: заснована на моделі дозволів і забезпечує високий ступінь деталізації контролю доступу до вмісту сайту;
- розмежування доступу коду: політика. NET Framework, що дозволяє управляти доступом програмного коду до захищених ресурсів та операцій;
- протоколи безпеки, такі як SSL (Secure Sockets Layer) та IPSec: забезпечують захист даних, переданих всередині і поза зоною дії міжмережевого екрану;
- захист зовнішніх вузлів за допомогою брандмауера.

Розглянемо технології забезпечення безпеки MS SharePoint. Перевірка автентичності – це процес, що дозволяє точно ідентифікувати користувачів вузла, який гарантує, що користувачі дійсно є тими, за кого себе видають [4]. Клієнти, що пройшли перевірку автентичності, називаються учасниками безпеки.

У продуктах і технологіях MS SharePoint перевірка автентичності виконується на основі облікових записів безпеки Windows. У режимі перевірки автентичності Windows для виконання необхідної перевірки клієнта в ASP.NET залучається служба IIS. Вона перевіряє автентичність користувача, що видав запит, за обліковими записами безпеки Windows. Встановивши автентичність клієнта, IIS передає посвідчення користувача в ASP.NET.

У продуктах і технологіях MS SharePoint застосовуються різні схеми перевірки автентичності користувачів на базі IIS (рис. 1).

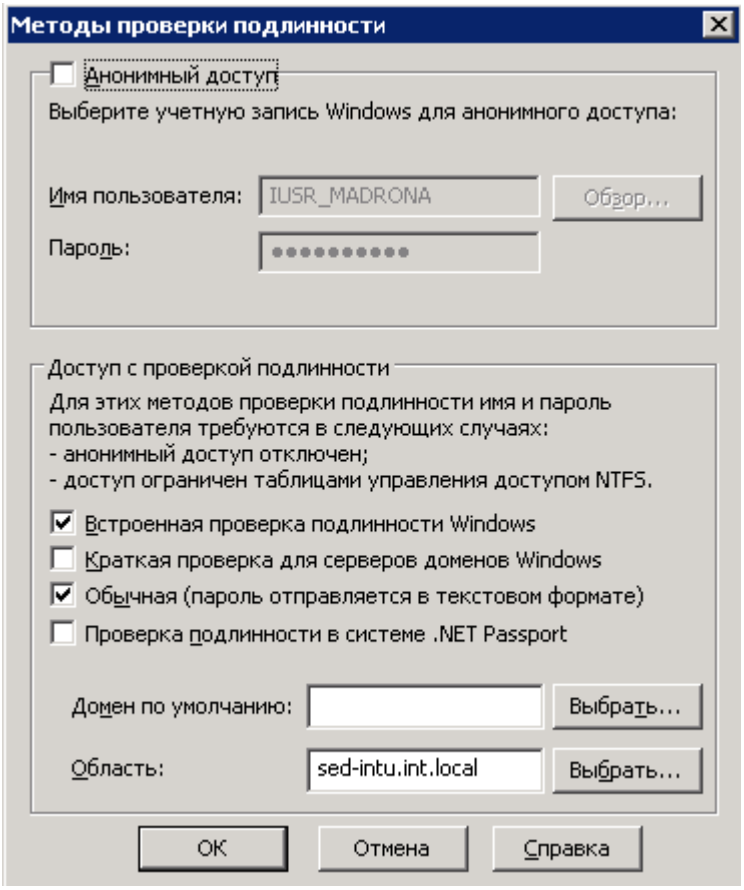


Рис. 1. Методи перевірки достовірності в IIS

- **Звичайна перевірка** автентичності реалізована у складі протоколу HTTP 1.1, який підтримується практично всіма браузерами. У разі використання продуктів і технологій MS SharePoint такий метод можна застосовувати в екстра мережі (екстрамережа – це захищена від несанкціонованого доступу корпоративна мережа, що використовує Інтернет-технології всередині для корпоративних цілей). Облікові дані передаються в незашифрованому вигляді. Звичайна перевірка автентичності повинна здійснюватися тільки за протоколом SSL, оскільки для інших випадків безпека не гарантується.

- **Вбудована перевірка автентичності Windows** – це безпечний метод перевірки автентичності, що найбільш підходить для вузлів MS SharePoint в інтрамережі (інтрамережа – це внутрішня приватна мережа організації). Цей метод не працює через проксі-сервери. Така перевірка реалізується на базі протоколів Kerberos чи NTLM. Для використання Kerberos необхідно, щоб на комп'ютерах серверів і клієнтів була встановлена операційна система Windows 2000 або більш пізні версії.

- **Зіставлення клієнтських сертифікатів**. Клієнти повинні мати сертифікати X.509. Мова йде про необов'язковий механізм перевірки автентичності, який можна використовувати, якщо між клієнтом і сервером включено підтримку SSL.
- **Анонімна перевірка** автентичності дозволяє отримати анонімний доступ до веб-сайту. Для анонімного доступу за замовчуванням використовується посвідчення користувача IUSR_імя_компьютера. Отримуючи анонімний запит, IIS уособлює обліковий запис IUSR_імя_компьютера. У цьому випадку в ASP.NET передається посвідчення IUSR_імякомпьютера.

У продуктах і технологіях MS SharePoint доступ користувачів здійснюється відповідно до повноважень учасників безпеки Windows, за які використовуються облікові записи окремих користувачів і облікові записи групи безпеки, причому дозволяються як доменні, так і локальні групи безпеки (DOMAIN \ користувач і DOMAIN \ группа_безпеки, або HOSTNAME \ користувач і HOSTNAME \ группа_безпеки). Для зручності управління та адміністрування MS SharePoint користувачів розподіляють за групами безпеки.

Рівні доступу до порталу на базі MS SharePoint

Розглянемо процес розмежування рівнів доступу для порталу на базі MS SharePoint на прикладі інформаційної системи «Планування наукових досліджень в Національній академії педагогічних наук України на базі мережі Інтернет», далі ІС «Планування».

Створимо три локальні групи безпеки:

1. Бухгалтерія.
2. Відділ кадрів.
3. Начальники відділів.

Кожна з цих груп містить певну кількість локальних користувачів і дозволяє надалі забезпечити різні рівні доступу до документів MS SharePoint сервера. Для створення груп і додавання користувачів використовуємо оснащення **Керування комп'ютером** (рис. 2).

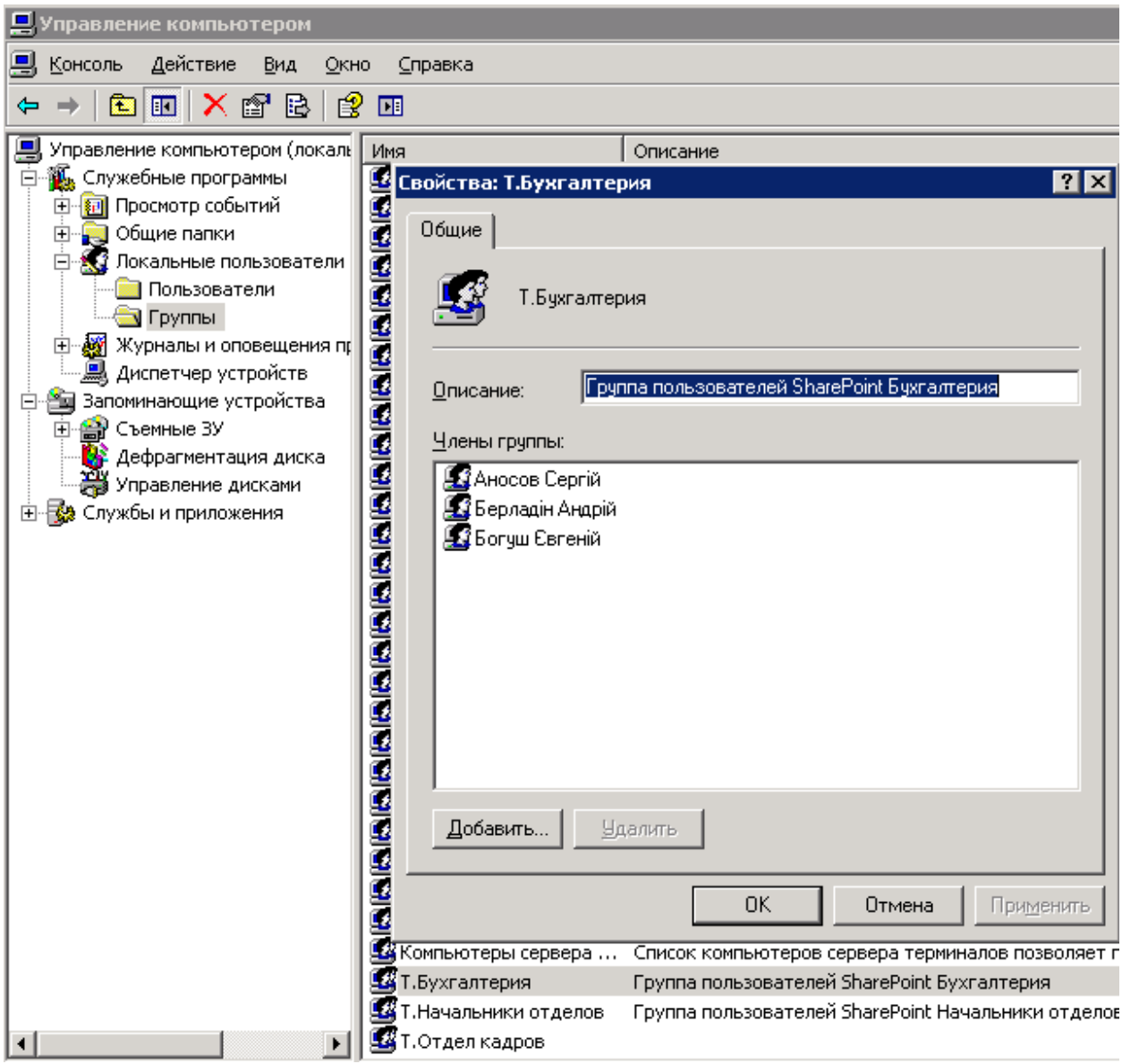


Рис. 2. Локальна група безпеки для використання в MS SharePoint

Крім перевірки автентичності користувачів під час доступу до вузлів MS SharePoint, сервер MS SharePoint Portal Server підтримує функцію єдиного входу в систему (SSO), що дозволяє перевірити автентичність користувача, що звернувся до вузла порталу, а потім витягнути з бази даних SSO збережені облікові дані користувача, коли вони будуть потрібні іншим корпоративним бізнес-застосуванням з ідентифікацією користувачів.

Авторизація визначає, до яких ресурсів та операцій дозволяється доступ користувачеві, який пройшов перевірку автентичності. У Windows SharePoint Services і SharePoint Portal Server доступ до вузлів контролюється за допомогою системи рольової приналежності, у якій кожному користувачеві або групі користувачів явно або неявно призначається дозвіл на виконання певних дій [2]. Ця система ґрунтується

на формуванні груп вузла. Створюючи групу вузла, можна налаштувати права користувачів і груп, виходячи з того, якого роду завдання вони виконують. Такий підхід ідеально підходить для організації багаторівневої системи доступу в системах електронного документообігу.

Групи вузла визначають, якими правами володіють користувачі в певному вузлі. Ці права вказують конкретні дії, які користувачі можуть виконувати на сайті. Дії, які користувачі можуть виконувати, задають права, тобто кожна група вузла – це сукупність прав.

Якщо потрібно, щоб вміст сайту могли переглядати всі користувачі, досить дозволити анонімний доступ до вузла. За замовчуванням анонімний доступ відключений. Щоб авторизуватися для виконання адміністративних завдань щодо налаштування всіх веб-вузлів і віртуальних серверів на сервері MS SharePoint, користувач повинен стати членом групи локальних адміністраторів комп'ютера сервера або групи адміністраторів MS SharePoint.

У Windows SharePoint Services підтримується 21 право, які використовуються в п'яти групах користувачів вузла, що визначаються за замовчуванням [6]. Ці п'ять стандартних груп прав користувачів містять такі категорії: «Гість», «Читач», «Співробітник», «Веб-дизайнер» і «Адміністратор». Права, призначені групам вузла «Гість» і «Адміністратор», не можуть бути змінені. Разом з тим, ті, що включаються до групи «Читач», «Співробітник» і «Веб-дизайнер», можна налаштувати, залишивши в кожній з них лише необхідні права. Можна додавати нові групи вузла, комбінуючи різні набори прав, змінювати права, призначати і видаляти будь-які групи. Користувачів не можна включати безпосередньо до групи «Гість»: до неї автоматично додаються користувачі, яким надано доступ до списків або бібліотек документів на основі дозволів для списків. Група вузла «Гість» не може бути налаштована або видалена.

Керувати групами вузла та дозволами на доступ можна на сторінках HTML-адміністрування або за допомогою командного рядка Stsadm.exe. Розглянемо процес створення користувачів і розподілу ролей на основі створених локально груп безпеки в ОС Windows в MS SharePoint.

Переходимо до сторінки адміністрування MS SharePoint **Shared Services Administartion – Дії сайту – Користувачі та групи**.

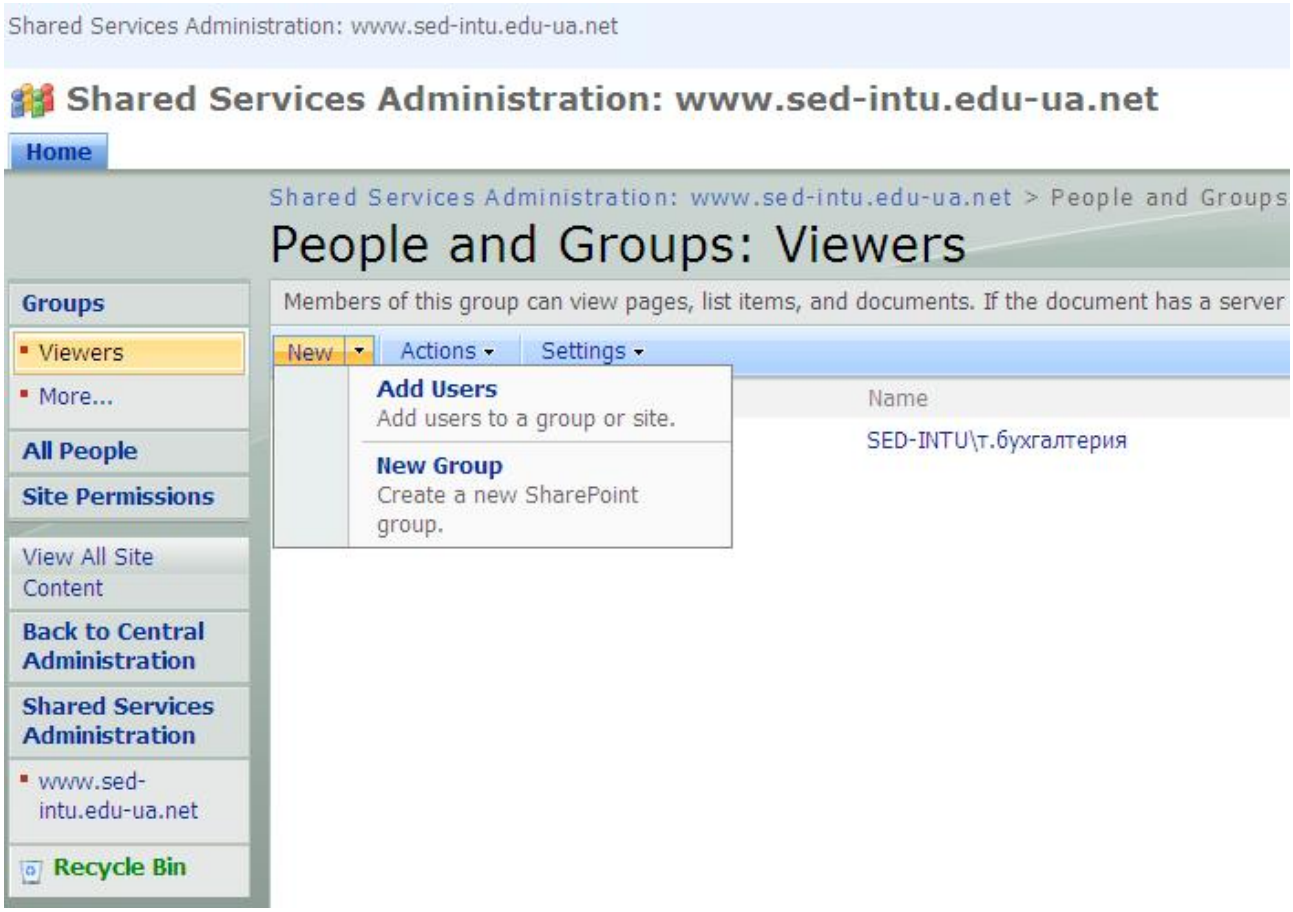


Рис. 3. Додавання груп безпеки Windows у MS SharePoint

Додаємо створені раніше групи безпеки – Бухгалтерія, Відділ кадрів, Начальники відділів (рис. 3). Встановимо права, що дозволяють додавати, видаляти й оновлювати компоненти вузла.

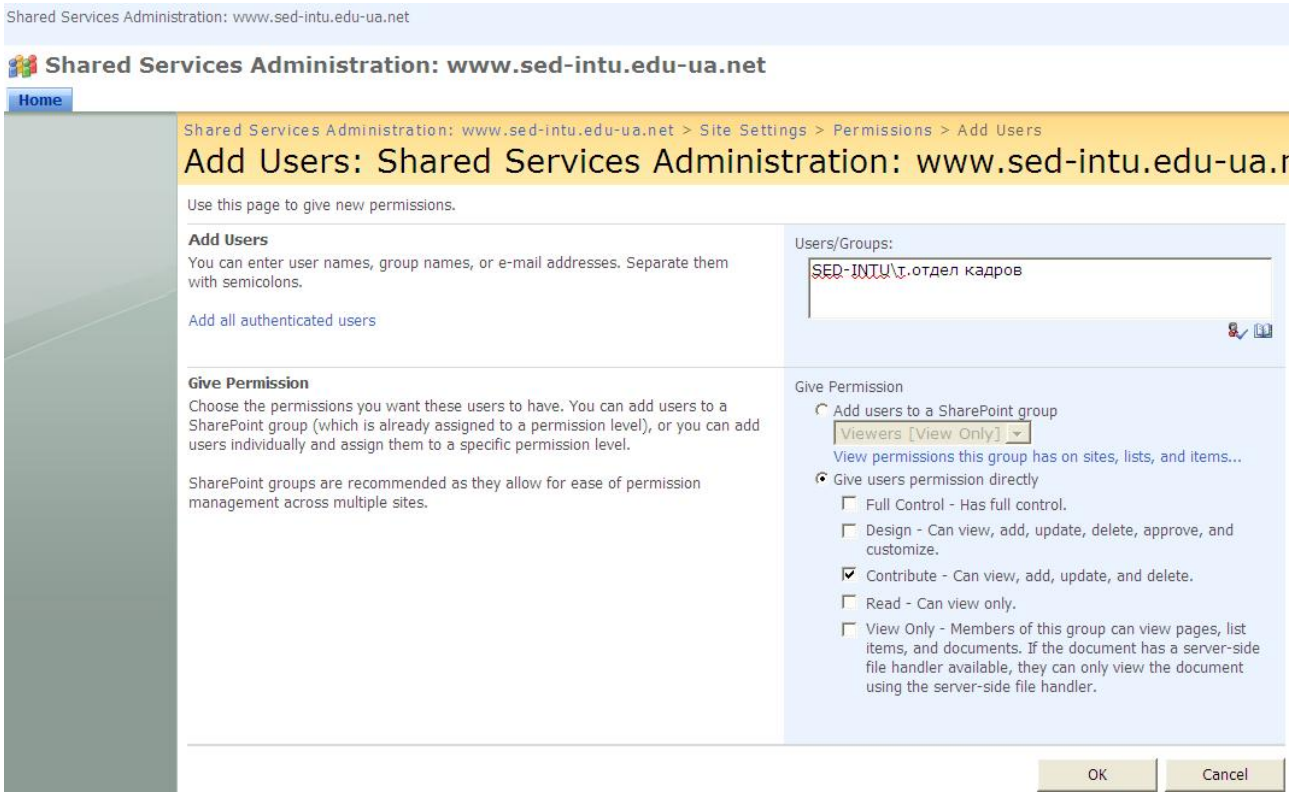


Рис. 4. Налаштування права доступу груп безпеки у MS SharePoint

Унікальні права доступу можна задавати для кожного списку (рис. 4) [3]. У список, на відміну від вузла, користувачів можна додавати безпосередньо, разом із зазначеними дозволами; водночас користувачі автоматично включаються до групи «Гість» поточного вузла, якщо той унікальний і не успадковує дозволи батьківського сайту. Якщо поточний вузол успадковує права доступу, користувачі додаються до групи «Гість» найближчого унікального вузла-предка.

Користувачам надаються права доступу до вузла або списку на підставі прямої або непрямої належності до тієї чи іншої групи вузла [5]. Їх можна додавати безпосередньо до групи вузла або до міжвузлової групи, яка є членом групи вузла, або користувач може бути членом групи домену Windows, включеної до групи вузла. Крім того, окремого користувача можна безпосередньо додати до списку разом із зазначеними правами доступу.

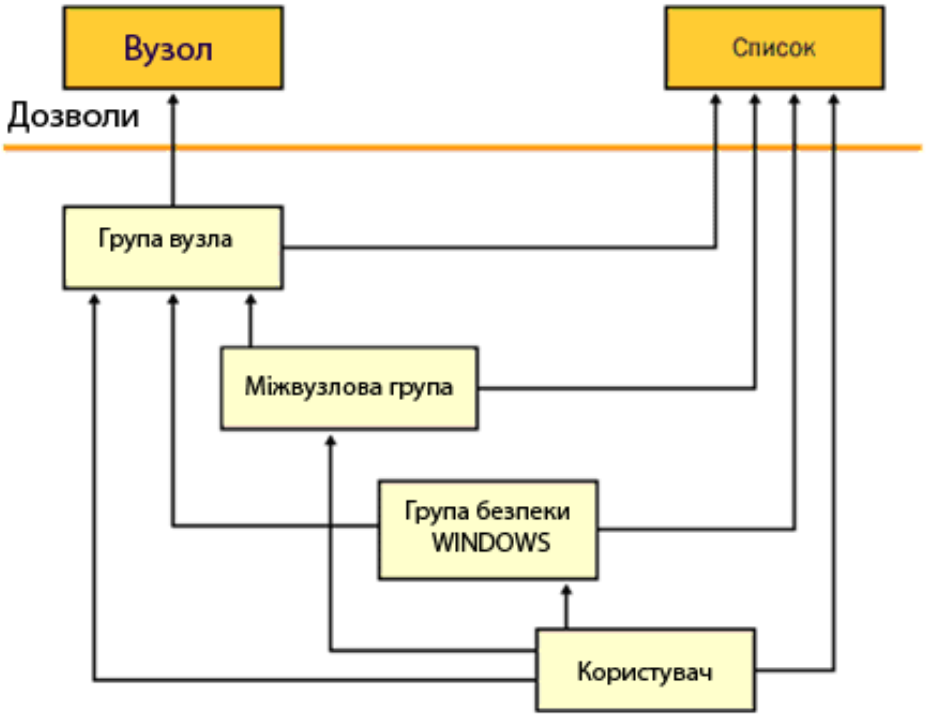
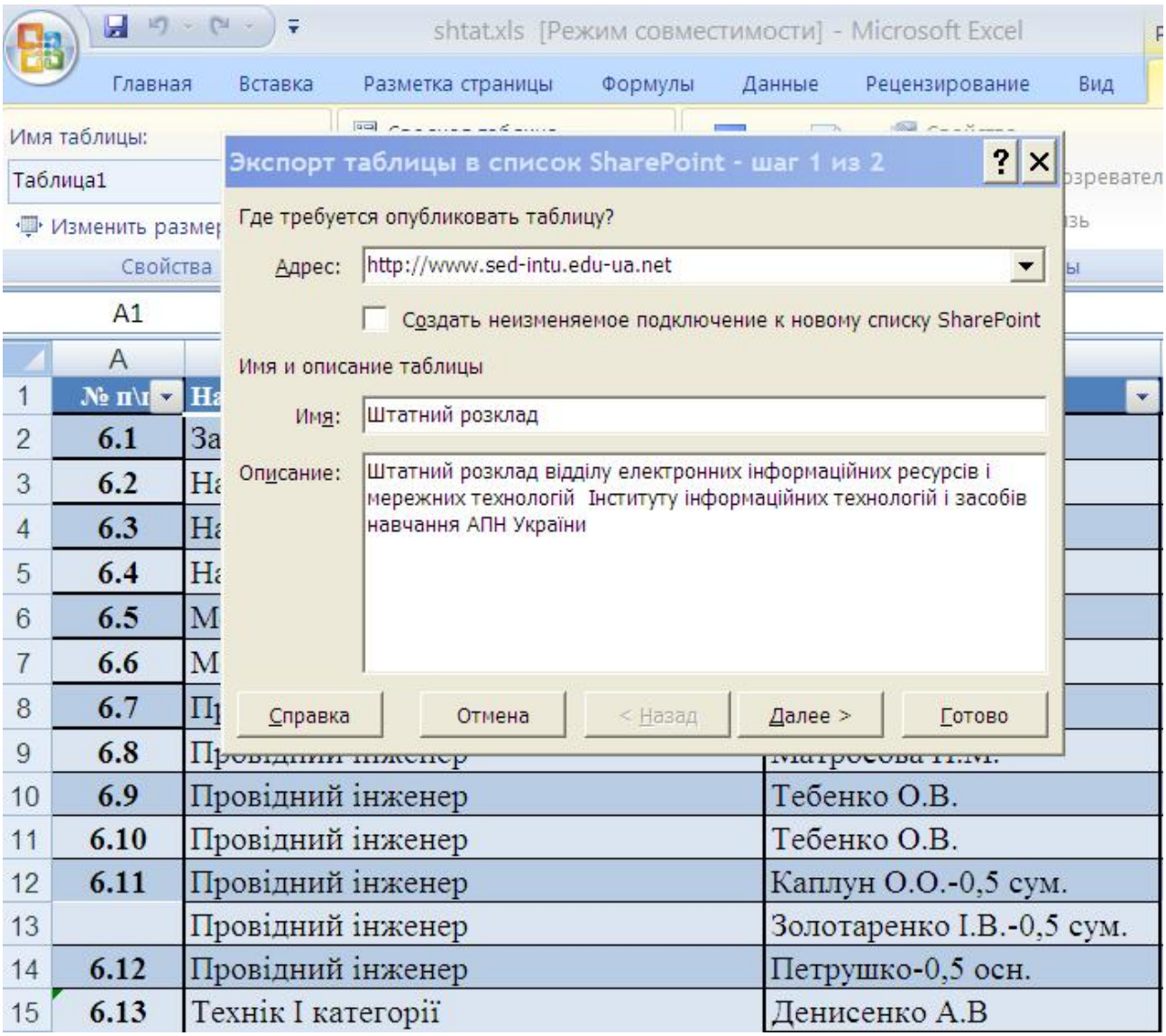


Рис. 5. Надання користувачам дозволів на доступ до вузла або списку в MS SharePoint

Розглянемо процес визначення прав користувачів на рівні списку (рис. 5). Створимо електронний список «Штатний розклад» з файлу формату Excel. Для цього виділений діапазон клітинок в Excel файлі перетворюємо в таблицю (меню **Вставка** / **Таблиця**). Далі в меню **Конструктор** скористаємося пунктом **Експорт**: **Експорт таблиці до списку MS SharePoint**. Зазначимо сервер для розміщення списку, у запиті авторизації вкажемо користувача, який має відповідні права на сервері MS SharePoint (рис. 6).



	A		
1	№ п\п	На	
2	6.1	За	
3	6.2	На	
4	6.3	На	
5	6.4	На	
6	6.5	М	
7	6.6	М	
8	6.7	Пр	
9	6.8	Провідний інженер	Матросова Н.М.
10	6.9	Провідний інженер	Тебенко О.В.
11	6.10	Провідний інженер	Тебенко О.В.
12	6.11	Провідний інженер	Каплун О.О.-0,5 сум.
13		Провідний інженер	Золотаренко І.В.-0,5 сум.
14	6.12	Провідний інженер	Петрушко-0,5 осн.
15	6.13	Технік І категорії	Денисенко А.В

Рис. 6. Експорт списку з MS Excel в MS SharePoint

У результаті на зазначеному сайті буде створено новий список «Штатний розклад» (рис. 7).

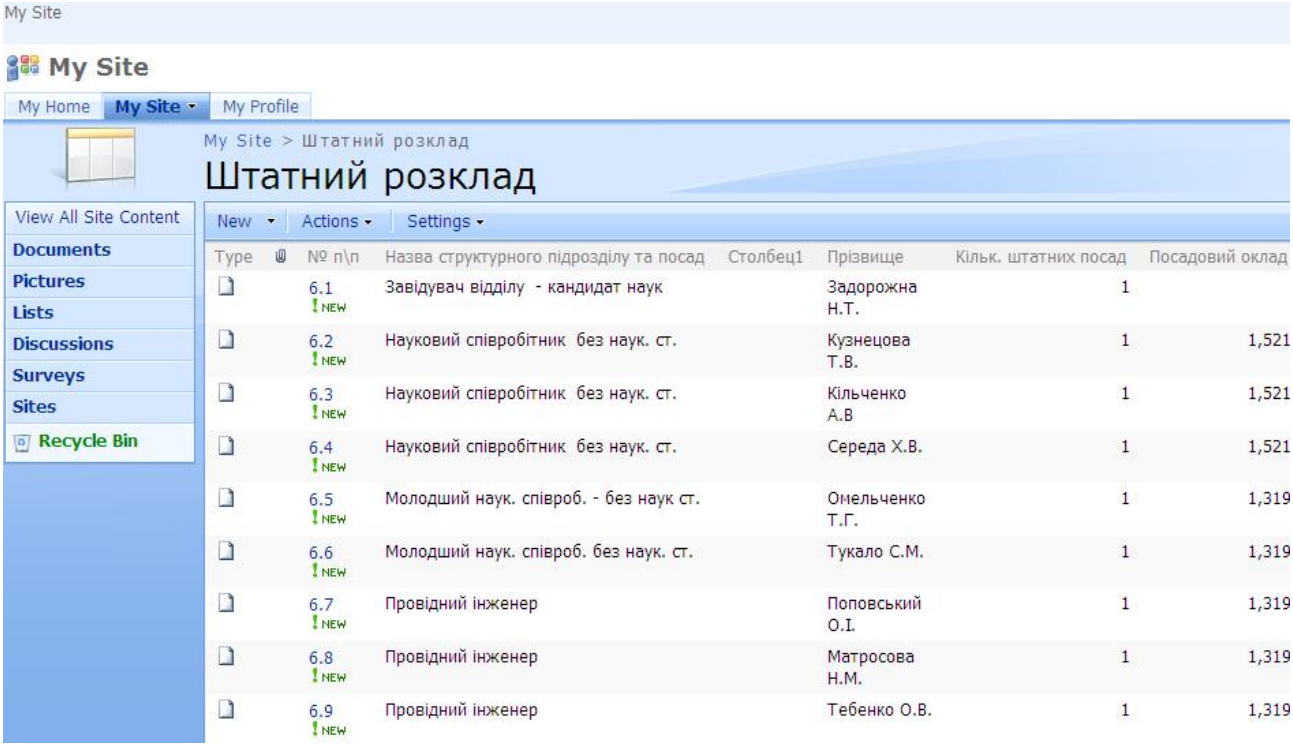


Рис. 7. Опублікований в MS SharePoint список «Штатний розклад»

Розглянемо, як можна задати права доступу для створеного списку.

За допомогою таких дій можна додати користувачів до наявної групи MS SharePoint, пов'язаної з елементом списку. Якщо для налаштованого об'єкта, що захищається, використовуються унікальні дозволи, можна додати до нього користувачів безпосередньо з необхідними правами доступу або додати наявні групи MS SharePoint до цього списку з необхідними правами доступу.

Якщо права доступу успадковуються від батьківського об'єкта, що захищається, то додавати користувачів або групи MS SharePoint безпосередньо до нього не можна. У цьому випадку можна тільки додавати користувачів до наявних груп MS SharePoint, пов'язаних з даними, які захищаються. Проте користувачів можна додавати до об'єкта, що захищається, якщо для нього створено унікальні дозволи.

1. Відкриваємо список або бібліотеку, яка містить папки, документ або елемент списку, для якого потрібно додати користувачів або групи MS SharePoint.

2. Розміщуємо покажчик миші на елемент списку, для якого потрібно додати користувачів або групи MS SharePoint, вибираємо **Управління правами доступу**.

3. У меню **Створити** вибираємо команду **Додати користувачів**.

4. У розділі **Додавання користувачів** вказуємо користувачів та групи MS SharePoint, яких потрібно додати.

5. У розділі **Надання дозволу** додаємо користувачів до наявної групи MS SharePoint або надаємо дозволи безпосередньо для списку, і встановлюємо один або кілька прапорців, щоб надати цим користувачам потрібні дозволи на даному об'єкті.

Якщо права доступу успадковуються від батьківського об'єкта, що захищається, то додавати користувачів або групи MS SharePoint безпосередньо до об'єкта захисту не можна. У цьому випадку можна тільки додавати користувачів до наявних груп MS SharePoint.

Не можна додати групу MS SharePoint до іншої групи MS SharePoint.

Видалення користувачів зі списку здійснюється з використанням описані вище форм.

Висновки. У статті проаналізовано механізми безпеки, які використовуються в продуктах і технологіях MS SharePoint для забезпечення безпечного доступу користувачів і зниження ступеня уразливості. Перевірка автентичності користувачів проводиться на базі таких технологій, як IIS і ASP.NET, а також концепції учасників безпеки Windows, у той час як авторизація доступу заснована на членстві в групах вузла, які пов'язують (прямо чи опосередковано) кожного користувача з роздільною здатністю, що вказує, які саме дії він може виконувати. Розмежування доступу коду дозволяє деталізувати можливості доступу для коду застосувань, продуктів і технологій MS SharePoint. Безпека зв'язку має ключове значення для підтримки безпечного передавання даних всередині і поза зоною дії міжмережевого екрану. Система безпеки продуктів і технологій Microsoft SharePoint має багаторівневу структуру, яка будується на основі служб безпеки низки базових технологій, тому важливо дотримуватися всебічного підходу до безпеки, формуючи систему ешелонованого захисту, яка охоплює всі компоненти розгорнутого середовища продуктів і технологій MS SharePoint.

На основі підходу, поданому у статті, розроблено систему безпеки для ІС «Планування». Отримані результати можуть використовуватися для проектування інших інформаційних систем як у галузі освіти, так в інших предметних галузях.

Список використаних джерел

1. Архитектура безопасности в продуктах и технологиях MS SharePoint. – [Електрон. дані]. – Режим доступу: http://www.oszone.net/4632/Sharepoint – Дата доступу: квітень. 2010. – Назва з екрана.

2. Управление разрешениями для списка, библиотеки, папки, документа или элемента списка. – [Електрон. дані]. – Режим доступу: http://office.microsoft.com/ru-ru/sharepointserver/HA100215641049.aspx?pid=CH101248581049. – Дата доступу: квітень. 2010. – Назва з екрана.

3. Использование Word, Excel и Excel Services с SharePoint 2007. – [Електрон. дані]. – Режим доступу: http://www.williamspublishing.com/PDF/978-5-8459-1328-9/part.pdf. Дата доступу: березень. 2010. – Назва з екрана.

4. Эволюция безопасности SharePoint. – [Електрон. дані]. – Режим доступу: http://www.interface.ru/home.asp?artId=22892. Дата доступу: березень. 2010. – Назва з екрана.

5. Программирование средств безопасности в SharePoint. – [Електрон. дані]. – Режим доступу: http://www.cyberguru.ru/web/sharepoint/secutiry-features-dev-page7.html. Дата доступу: березень. 2010. – Назва з екрана.

6. Основы работы с SharePoint. – [Електрон. дані]. – Режим доступу: http://www.intuit.ru/department/internet/bwsharepoint/9/#sect4. Дата доступу: березень. 2010. – Назва з екрана.

ПОДХОДЫ К ОРГАНИЗАЦИИ СИСТЕМЫ БЕЗОПАСНОСТИ НА БАЗЕ MS SHAREPOINT

Золотаренко И. В.

Аннотация

Актуальность материала, изложенного в статье, обусловлена насущными потребностями общества в создании безопасных информационных систем, содействии внедрению новейших информационных технологий в процессы управления образованием. Вопрос безопасности является важным для надежности и работоспособности таких систем. Одним из путей решения проблемы безопасности является разделение пользователей по категориям и предоставления им прав разных уровней. В статье проведен анализ общих подходов к организации групп и уровней разрешений пользователей в информационных системах, разработанных на базе MS SharePoint. На основе проведенного анализа определены основные проектные решения по безопасности в информационной системе «Планирование научных исследований в Национальной академии педагогических наук Украины на базе сети Интернет».

Ключевые слова: информационная система, система MS SharePoint, безопасность, доступ пользователей, группы доступа, разрешения, группы безопасности.

Approaches to the Security System at the MS SharePoint

Zolotarenko I.

Resume

Relevance of the material contained in the article is conditioned by pressing needs of society in creating secure information systems, facilitating the introduction of advanced information technologies in the education department. Security is important for the reliability and efficiency of such systems. One way of solving the security problem is the distribution of categories of users and granting their rights at different levels. The paper analyzes general approaches to organize groups and permission levels of users in information systems developed based on MS SharePoint. The main design decisions on security in information system planning research at the National Academy of Pedagogical Sciences of Ukraine based on the Internet use the conceptual results of this article.

Keywords: information system, system of MS SharePoint, security, user access, group access, permissions, security groups.