

ОБГОВОРЮЄМО ПРОБЛЕМУ

УДК 378.174:004.588

ВАСИЛЬ ОЛЕКСЮК, ВАЛЕРІЙ ГАБРУСЕВ, АНАТОЛІЙ БАЛИК

**ДЕЯКІ АСПЕКТИ ІНТЕГРАЦІЇ ВЕБ-СЕРВІСІВ
ВИЩОГО НАВЧАЛЬНОГО ЗАКЛАДУ**

Розглянуто технологічні аспекти інтеграції веб-сервісів освітнього порталу. Визначено концептуальні підходи до організації єдиної системи автентифікації. Проаналізовано можливості протоколу та каталогів LDAP для збереження облікових записів користувачів. Запропоновано структуру об'єктів у каталозі Active Directory, який використано для розв'язання проблеми.

Ключові слова: веб-портал, автентифікація, сервер, каталог, MOODLE.

ВАСИЛИЙ ОЛЕКСЮК, ВАЛЕРИЙ ГАБРУСЕВ, АНАТОЛИЙ БАЛЫК

**НЕКОТОРЫЕ АСПЕКТЫ ИНТЕГРАЦИИ ВЕБ-СЕРВИСОВ
ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ**

Рассмотрены технологические аспекты интеграции веб-сервисов образовательного портала. Определены концептуальные подходы организации единой системы аутентификации. Проанализированы возможности протокола и каталогов LDAP для хранения учетных записей пользователей. Предложена структура каталога Active Directory.

Ключевые слова: веб-портал, аутентификация, сервер, каталог, MOODLE.

VASYL OLEKSYUK, VALERIY GABRUSEV, ANATOLIY BALYK

**SOME ASPECTS OF THE INTEGRATION OF WEB SERVICE
OF HIGHER EDUCATIONAL INSTITUTIONS**

The article describes the technological aspects of the integration of Web services education portal. Conceptual approaches of organization of the authentication system are distinguished. The possibility of protocol and LDAP directory for storing user accounts are analyzed. The structure of objects in the Active Directory, which is used to solve the problem, is proposed.

Key words: Web-portal, authentication, server, directory, MOODLE.

Упровадження інформаційно-комунікаційних технологій у навчальний процес ставить вимоги щодо функціональності та якості освітніх ресурсів. Інфраструктура мережних комплексів вищих навчальних закладів постійно оновлюється як апаратними, так і програмними засобами навчального призначення. При цьому постає проблема раціонального використання цих ресурсів, зокрема організація доступу користувачів до сервісів освітньої мережі. Однією з найефективніших форм організації освітніх ресурсів є веб-портал.

Теорією і практикою розробки та застосування освітніх порталів присвячені дослідження таких учених, як Є. Г. Грідін, Т. В. Єршова, В. М. Кухаренко, Н. В. Морзе, С. А. Раков, І. В. Роберт, А. В. Силаєв, Ю. В. Триус та ін.

Метою статті є розгляд аспектів інтеграції сервісів освітнього веб-порталу, зокрема завдяки створенню єдиної системи автентифікації його користувачів.

Основні відмінності портальної системи від звичайного веб-сайту полягають у наявності персоніфікованого інтерфейсу, що забезпечує можливість ідентифікації користувачів і визначення для них правил доступу до тих або інших інформаційних ресурсів; висока захищеність

інформаційних ресурсів, можливість інтеграції різнорідних програмних засобів і надання єдиної точки входу для роботи з ними.

Портал — це мережний телекомунікаційний веб-вузол, що має розвинений інтерфейс користувача і значний обсяг різноманітних даних, послуг і посилань [7, с. 48–58] і є інструментом об'єднання та систематизації ресурсів з метою подання їх користувачеві за допомогою простого для навігації інтерфейсу.

Т. В. Єршова виділяє принципи організації «Всеросійського порталу розвитку», які можуть бути покладені в основу розробки довільного освітнього порталу [3]:

1. Партнерство — портал є результатом спільної діяльності адміністрації, працівників, студентів освітнього закладу. Також до процесу створення варто залучати випускників закладу, спонсорів та інших небайдужих осіб.

2. Мотивованість — кожен учасник отримує можливість брати участь у прийнятті рішень щодо функціонування порталу.

3. Системність — портал є системою, яка є засобом об'єднання багатогранної діяльності щодо подолання інформаційної нерівності.

4. Відкритість — портал має бути доступним для всіх бажаючих внести вклад у розвиток інформаційного суспільства.

5. Стійкість — портальний проект повинен фінансуватись як із зовнішніх так із внутрішніх джерел.

Отже, освітній портал повинен бути основою інформаційного освітньо-наукового середовища вищого навчального закладу [8, с. 193].

Розглянемо освітній заклад як систему. Зазвичай взаємодія його структурних елементів з інформаційними ресурсами має взаємно-однозначний характер. Наприклад, кожен викладач створює та використовує власні навчальні ресурси. Проте з розвитком освітнього закладу зростає й обсяг інформаційних ресурсів. За таких умов інформаційну взаємодію можна уявити як структуру, у якій кожен користувач може створювати інформаційні ресурси для інших елементів системи.

Основні складові порталу є взаємопов'язаними — інформаційне наповнення складових порталу створюють адміністратори, викладачі, студенти. Децентралізована структура порталу забезпечує інтерактивність спілкування між учасниками освітнього процесу. У основі освітнього порталу повинна лежати модель, яка містить «тріаду» — суб'єкт, вид та об'єкт діяльності.

З точки зору функціональної структури, в освітньому порталі можна виділити чотири рівні:

1. Презентаційний, що відображає структуру навчального закладу, його кадровий склад і персоналії; блок новин.

2. Навчально-методичний, який містить навчальні плани та програми; навчально-методичні матеріали, систему управління навчальними курсами.

3. Сервісний, до складу якого входять служби автентифікації і авторизації доступу до вмісту порталу, сервіси пошуку даних, засоби моніторингу і статистики.

4. Соціальний, який містить засоби для обміну документами, колективної роботи студентів та викладачів (вікі, блог, миттєві повідомлення тощо).

Реалізація зазначених рівнів освітнього порталу можлива шляхом безпосередньої розробки або інтеграції вже готових систем відповідного функціонального призначення. Як показує досвід освітні заклади широко використовують вільно поширювані продукти для створення власних портальних систем. Проте віднайти систему, з допомогою якої можна було б реалізувати усі рівні освітнього порталу непросто. Наприклад, застосування систем управління контентом (CMS) дає можливість створити презентаційний і частково сервісний рівні.

На нашу думку, найбільш трудомістким є процес створення навчально-методичного рівня освітнього порталу, який, зазвичай, передбачає інтеграцію кількох програмних засобів навчального призначення.

Традиційно для роботи з кожним сервісом освітнього порталу викладачам та студентам пропонують окремі реєстраційні дані (логін та пароль). Недоліками такого підходу є значна кількість імен та паролів для облікових записів однієї особи, проблеми сумісності сервісів, їх складна архітектура, труднощі супроводу та підтримки.

Як було зазначено вище, одним із найважливіших аспектів такої інтеграції є організація єдиної системи автентифікації користувачів. Зазначена система може бути заснована на одній із концепцій:

- синхронізації даних з обліковими записами користувачів усіх сервісів;
- використання спільної бази даних облікових записів користувачів, проте для доступу до кожного сервісу необхідна окрема автентифікація;
- механізм, за допомогою якого єдина дія щодо автентифікації і авторизації користувача надає йому доступ до всіх сервісів системи.

Кожна з цих концепцій може бути реалізована через:

- внесення змін до коду програмних засобів для використання єдиної бази облікових записів;
- використання системи, яка дає можливість користувачеві використовувати єдиний обліковий запис для авторизації на окремих сайтах, порталах, блогах, форумах тощо;
- застосування зовнішньої стандартизованої бази даних, з якої складові порталу можуть автентифікувати користувача.

Оскільки перший спосіб вимагає значних затрат, розглянемо другий і третій. Типовою системою в мережі Інтернет, яка надає можливість єдиної автентифікації є OpenID [10, с. 81]. Проте вона передбачає конфігурування додаткового сервісу — провайдера OpenID або звертання до зовнішнього провайдера. Останній спосіб є цікавим у випадку використання в освітньому закладі стандартної бази користувачів, наприклад доменної. Принциповою особливістю домену є централізоване збереження та опрацювання даних облікових записів користувачів. На практиці це дає змогу кожному студенту працювати із будь-яким комп'ютером домену так, ніби в системі цього комп'ютера окремо створено його обліковий запис [6, с. 46–53]. Централізоване збереження даних передбачає розподілений спосіб доступу до них. Стандартним засобом для організації доменів у локальних мережах є служба Microsoft Active Directory [6]. Для доступу до бази облікових записів користувачів Active Directory можна використати полегшений протокол доступу до каталогів (LDAP — Lightweight Directory Access Protocol).

Суть протоколу полягає у можливості зберігання даних в ієрархічній структурі [9]. Як правило сховищем даних є каталог на сервері LDAP. Основне поняття — об'єкт каталогу можна уявити як таблицю бази даних. Вузли в ієрархії каталогу LDAP містять дані про об'єкт і є аналогічними записам реляційної бази. Характеристики об'єкта містять атрибути, які є аналогом полів. Рівні у ієрархічному дереві іменують за допомогою загально прийнятих позначень: країна — «C» (country), рівень організації — «OU», імена користувачів — «CN» (common name). Оскільки об'єкт у структурі LDAP має бути унікальним, то для його опису використовують унікальне ім'я (DN — Distinguished Name). Унікальне ім'я отримують послідовним визначенням значень атрибутів (C, OU, CN тощо).

Поряд з цим організація даних у каталогах відрізняється від реляційних баз:

- у каталозі LDAP може існувати атрибут (поле) з іменем, але кількома значеннями; а можуть існувати два поля з однаковим іменем, але різними значеннями;
- у каталогах LDAP дані упорядковані ієрархічно, а також можуть бути об'єднані у групи, наприклад, за значенням певного атрибута.
- об'єкти в каталогах можна розширити в об'єктно-орієнтованому значенні, додавши нові атрибути.

Серед дій із каталогом LDAP слід виділити операції автентифікації (bind, unbind) та відмови. Операцію bind використовують для автентифікації користувача на основі наданих даних (DN, пароль тощо). Завершує сеанс роботи операція unbind. Операцію відмови використовують для скасування дій в каталозі. Для захисту з'єднань у протоколі LDAP інкапсульовано загальноприйняті протоколи шифрування (SASL, SSL, TLS).

Розглянемо застосування каталогу LDAP на прикладі автентифікації користувачів мережі фізико-математичного факультету ТНПУ імені Володимира Гнатюка. Основою мережного комплексу факультету є три сервери, один з яких функціонує під управлінням ОС Linux, й, зокрема, надає користувачам доступ до таких сервісів:

- сайт факультету, побудований на основі CMS Joomla!, який реалізує презентаційний рівень освітнього порталу;

- сервер електронних курсів, що організовано на основі системи управління навчанням Moodle, яка реалізує навчально-методичний рівень освітнього порталу;
- вікіпедія факультету — відкрита Інтернет-енциклопедія, яка функціонує на платформі MediaWiki;
- поштова система — надає користувачам факультету доступ до персональних поштових скриньок. Програмною основою поштової системи є сервери Postfix та Dovecot.

Інші сервери працюють під управлінням ОС Windows Server 2003 та виконують функції маршрутизаторів, контролерів домену, а також основного та резервного файлового сервера (рис. 1).

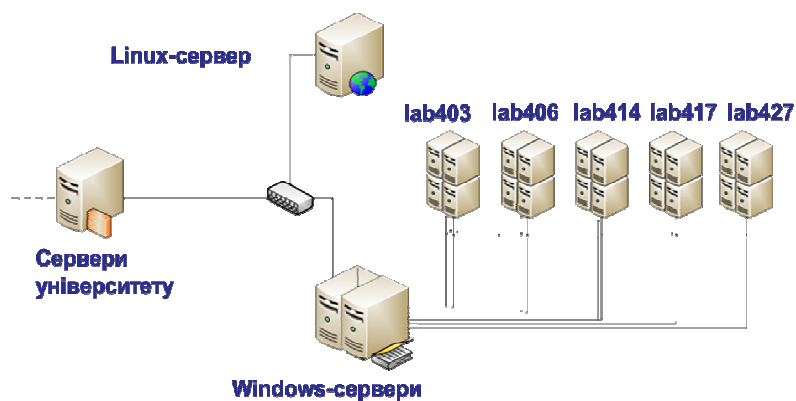


Рис. 1. Структура комп'ютерної мережі фізико-математичного факультету

Оскільки домен побудовано на основі Active Directory — службі каталогів компанії Microsoft, то функції сервера LDAP природно виконує Windows-сервер. Розглянемо фрагмент каталогу LDAP, у якому зберігаються облікові записи користувачів домену (рис. 2).

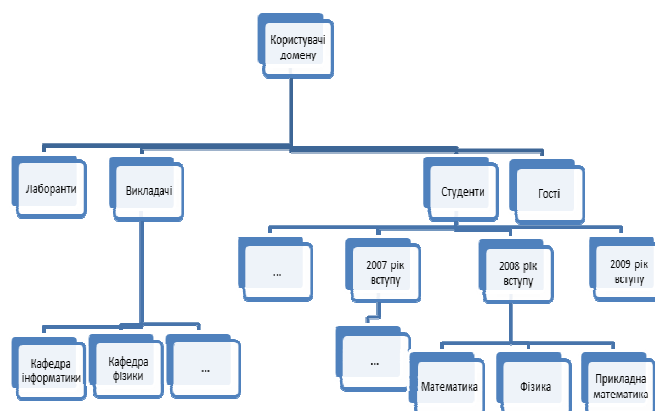


Рис. 2. Фрагмент каталогу LDAP, реалізованого в мережі фізико-математичного факультету

ОБГОВОРИЮЄМО ПРОБЛЕМУ

Автентифікація у каталозі LDAP здійснюється на основі атрибутів (див. табл.).

Атрибут	Значення	Опис
objectClass	Person	клас даного об'єкта (особа)
Description	IM_2005	опис даного об'єкта (спеціальність, рік вступу)
distinguishedName	CN=kanteruk,OU=IM,OU=2005,OU=Fizmat,OU=Students,OU=Domain Users,DC=w,DC=fizmat,DC=tnpu,DC=edu,DC=ua	місцезнаходження об'єкта в дереві каталогів Active Directory
displayName	Кантерук Богдан Миколайович	ім'я користувача
homeDirectory	\\FDC\Users\Students\Fizmat\2005\IM\kanteruk	шлях до домашньої папки
profilePath	\\FDC\Users\Students\Fizmat\2005\IM\kanteruk\Document and Settings	шлях до профілю
sAMAccountName	kanteruk	ім'я облікового запису
mail	kanteruk@fizmat.tnpu.edu.ua	електронна пошта користувача

Оскільки Active Directory є службою каталогів, яка не підтримує анонімні запити, то необхідно створити окремий обліковий запис користувача, від імені якого здійснюватиметься зчитування даних.

Для взаємодії розглянутих веб-сервісів із каталогом LDAP використано додаткові модулі авторизації, які були встановлені та сконфігуровані як складові Linux-сервера. Незважаючи на те, що кожен сервіс має власні особливості конфігурування, наведемо спільні параметри, які були використані у процесі конфігурування:

- адреса та порт сервера LDAP;
- ім'я та пароль облікового запису для доступу до каталогу;
- унікальне ім'я об'єкта (DN);
- атрибут користувача, який слід знайти у каталозі (sAMAccountName);
- електронна пошта користувача (mail).

Налаштовуючи у такий спосіб веб-сервіси, слід з'ясувати, чи повинні сервіси використовувати інші (окрім каталога LDAP) бази облікових записів. Зокрема слід вказати, чи існує можливість реєстрації нових користувачів кожного із сервісів. У корпоративній мережі фізико-математичного факультету встановлено правила, за якими облікові записи користувачів створюються адміністратором централізовано в службі каталогів Active Directory.

Застосування каталогу LDAP як бази даних вносить специфіку у процес функціонування сервісів. Так у системі управління контентом Joomla! слід передбачити, до якої групи облікових записів належатиме користувач домену. Враховуючи вище наведену «суб'єкт, вид та об'єкт діяльності», слід було б авторизувати користувачів як таких, що належать до групи «Видавець», або «Автор». Проте належність до згаданих груп є потенційною небезпекою щодо функціонування CMS Joomla! [5, с. 145–149]. Розв'язання проблеми, на нашу думку, полягає у застосуванні сервісів, які дають можливість користувачам із групи «Зареєстровані» створювати контент. Доцільно встановлювати такі сервіси, які не належать до ядра CMS, а реалізовані у вигляді окремих модулів.

Використовуючи каталог для автентифікації користувачів у системі управління навчанням MOODLE, слід урахувати той факт, що обліковий запис користувача буде відображено у LMS лише після його автентифікації у системі MOODLE. У зв'язку з цим доцільним є проведення підготовчого етапу, який полягає у попередній підготовці студентів до роботи в системі управління навчанням, який передбачає їх попередню автентифікацію. Альтернативним шляхом розв'язання проблеми є розробка програмного засобу, який би поряд із створенням облікових записів домену авторизував їх на відповідних сервісах порталу. Також доцільним вважаємо розподіл облікових записів студентів за групами, які відповідають їх академічним групам. На сьогодні здійснити такий розподіл на основі атрибутів каталогу LDAP неможливо.

Оскільки платформа Wiki ELGG є відкритою для створення контенту, то розподіляти її користувачів за групами є недоцільно. Оскільки система ELGG реалізує соціальну мережу, ініціативу створення груп варто надати студентам.

Описана система була введена на фізико-математичному факультеті в квітні 2010 року. За цей час кількість звертань до порталу факультету зросла (рис. 3).

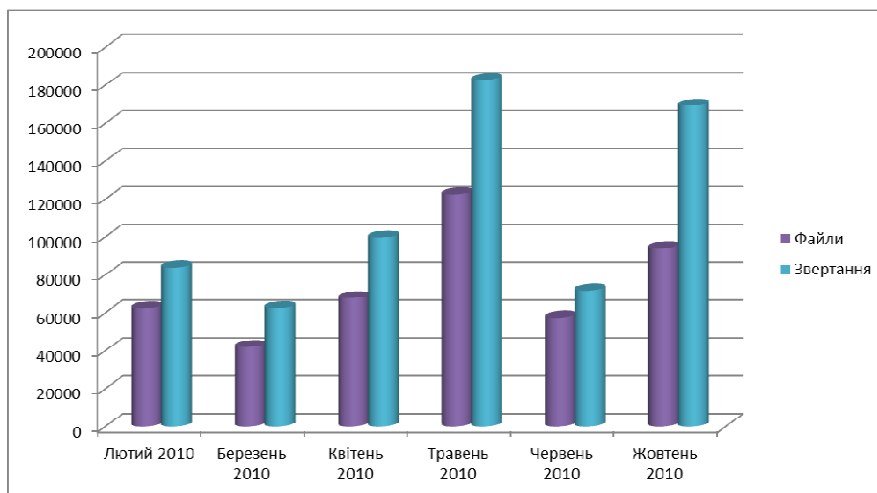


Рис. 3. Кількість звертань до порталу факультету

Таку динаміку продемонстрував і сервер електронних курсів (рис. 4).

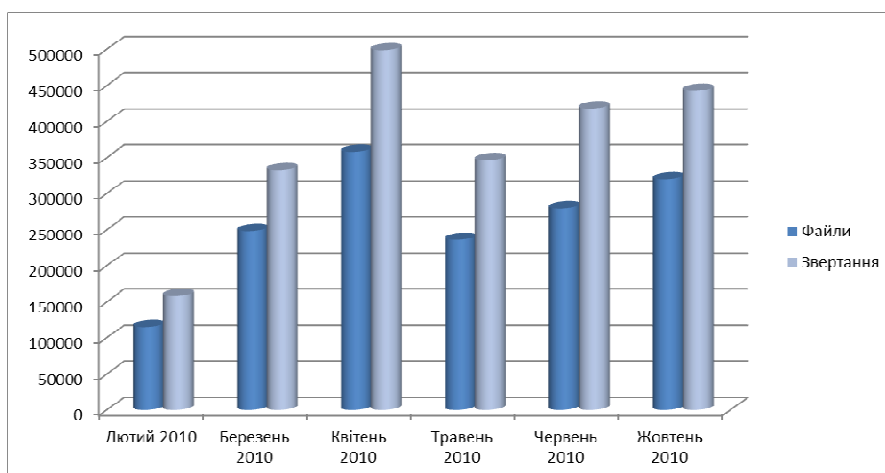


Рис. 4. Кількість звертань до сервера електронних курсів

Звичайно, динаміка кількості звертань до веб-сервісів має тенденцію до збільшення в кінці семестру (модульні, підсумкові контролі). Проте статистика звертань до обох сервісів у жовтні 2010 року показує, що сезонний приріст не є визначальним.

Висновки. Отже, можна стверджувати, що збільшенню інтенсивності використання веб-ресурсів фізико-математичного факультету сприяє впроваджена система автентифікації користувачів. Слід зазначити, що зменшилася й кількість звертань до системного адміністратора мережі факультету стосовно відновлення логінів та паролів.

Перспективи подальших досліджень. Подальший розвиток системи єдиної автентифікації може бути пов'язаний із застосування технології єдиного входу (SSO — Single Sign On). За такого підходу користувачеві достатньо один раз пройти автентифікацію, наприклад, при вході в ОС Windows. Також важливим є напрям розробки систем єдиної автентифікації для загальноосвітніх шкіл, де застосування каталогів LDAP є практично неможливою. Як наслідок, потребує розробки технологія застосування інтегрованих сервісів освітнього порталу та підготовки майбутніх учителів інформатики до створення освітніх ресурсів на основі розглянутих платформ.

ЛІТЕРАТУРА

1. Булгаков М. В. Реализация каталога образовательных Интернет-ресурсов федерального портала «Российское образование» / М. В. Булгаков, С. С. Внотченко, Е. Г. Гридина // Интернет-порталы: содержание и технологии. — 2003. — № 1. — С. 460–497.
2. Дунаев С. Б. Реализация базовых сервисов и программных блоков типового образовательного портала и проблемы информационного взаимодействия в форме метаописаний в рамках РЕОИС / С. Б. Дунаев, А. С. Высоков, И. А. Левенец, М. Н. Павлов, Л. В. Щавелев // Интернет-порталы: содержание и технологии. — 2004. — № 2. — С. 394–431.
3. Ершова Т. В. Российский портал развития: деятельность в рамках программы всемирного банка «Портал развития» / Т. В. Ершова // Информационное общество. — 2001. — № 1. — С. 63–65.
4. Зубанов Ф. В. Active Directory: подход профессионала / Федор Зубанов.— М.: Русская Редакция, 2003. — 544 с.
5. Колисниченко Д. Н. Joomla 1.5. Руководство пользователя / Дмитрий Колисниченко. — М.: Диалектика, 2009. — 217 с.
6. Рамський Ю. С. Адміністрування комп'ютерних мереж і систем / Рамський Ю. С., Олексюк В. П., Балик А. В. — Тернопіль : ТНПУ, 2010.— 180 с.
7. Семин Ю. Н. Интегративный подход к проектированию содержания общеинженерной подготовки в техническом вузе / Ю. Н. Семин // Известия Уральского научно-образовательного центра РАО. — 2000.— № 3. — С. 48–58.
8. Триус Ю. В. Комп'ютерно-орієнтовані методичні системи навчання математичних дисциплін у вищих навчальних закладах: дис. доктора пед. наук: 13.00.02 / Триус Ю. В. — Черкаси, 2005. — 410 с.
9. Carter G. LDAP System Administration. / Gerald Carter. — O'Reilly, 2003.— 308 p.
10. Yuan J. X. Liferay Portal Enterprise Intranets / Jonas X. Yuan. — Packt Publishing, 2008. — 386 p.