

## **ЄДИНА СИСТЕМА АВТЕНТИФІКАЦІЇ ЯК КРОК ДО СТВОРЕННЯ ОСВІТНЬОГО ПРОСТОРУ ЗАГАЛЬНООСВІТНЬОГО НАВЧАЛЬНОГО ЗАКЛАДУ**

Розвиток розвитку науки і техніки, постійний прогрес у створенні інформаційних технологій призвели до того, що комп'ютер та мережа Інтернет стали практично незамінними засобами здобуття знань. Зважаючи на це, педагоги все частіше використовують освітні веб-ресурси Всесвітньої мережі, а також створюють власні.

Впровадження інформаційно-комунікаційних технологій у навчальний процес ставить вимоги щодо функціональності та якості освітніх ресурсів. Не дивлячись на те, що кількість освітніх ресурсів Інтернету стрімко зростає, учитель не завжди може дібрати якісний навчальний ресурс, який задовольняв би вимоги інтерактивності, гіпертекстовості та мультимедійності. Особливо гостро стоїть проблема розробки освітніх ресурсів у загальноосвітніх навчальних закладах. Не викликає заперечень, що провідним фахівцем у цьому питанні є вчитель інформатики. Тому уміння створювати власні інформаційні освітні ресурси є важливим компонентом його інформаційної культури [4, 66].

Зрозуміло, що розв'язання зазначеної проблеми можливе лише в комплексі з іншими завданнями — оснащення шкіл комп'ютерною технікою та мультимедійними засобами підтримки навчання, приєднання їх до мережі Інтернет, підготовки та сертифікації вчителів. На вирішення цих завдань спрямована державна цільова програма «Сто відсотків», яка, зокрема, передбачає:

- забезпечення загальноосвітніх навчальних закладів сучасними навчальними комп'ютерними комплексами та системними і прикладними програмними продуктами;
- надання загальноосвітнім навчальним закладам швидкісного доступу до Інтернету з використанням сучасних технологій під'єднання для

високоєфективного доступу до освітніх ресурсів;

- удосконалення системи підготовки та підвищення кваліфікації педагогічних кадрів у сфері впровадження інформаційно-комунікаційних технологій у навчально-виховний процес, забезпечення стовідсоткового володіння такими знаннями усіма педагогічними працівниками;
- створення системи дистанційного навчання дітей з обмеженими можливостями та дітей, які перебувають на довготривалому лікуванні;
- створення системи веб-сайтів усіх загальноосвітніх навчальних закладів для опублікування кращих освітянських надбань;
- формування єдиного освітнього середовища, забезпечення інформаційної інтеграції освітніх ресурсів, інформаційної безпеки та централізованого фільтрування несумісного з навчальним процесом контенту [3].

Інфраструктура комп'ютерних комплексів загальноосвітніх навчальних закладів хоч і повільно, проте оновлюється апаратними і програмними засобами. Поряд з цим недостатньо поширеною є практика встановлення Інтернет (Інтранет)-сервера школи, як платформи для окремих інформаційних освітніх ресурсів, а також для їх інтеграції у навчальний простір.

**Метою** цієї статті є добір програмних засобів для організації освітнього простору загальноосвітньої школи, а також розгляд можливостей їх інтеграції через створення єдиної системи автентифікації користувачів.

Проблемі створення інформаційного освітнього простору присвячені дослідження В. Бикова, Р. Гуревича, М. Жалдака, І. Захарової, І. Кухаренка, В. Лапінського, О. Спіріна Ю. Машбиця та ін.

Використовуючи підхід В.Ю. Бикова [1] розглядатимемо освітній простір школи як підсистему Глобального інформаційного простору, інтегровані засоби і технології якого призначені для інформаційно-освітнього

ресурсного забезпечення цілей навчання і виховання та спрямовані на задоволення освітніх потреб школярів.

На основі характеристики, наведеної у монографії [2, 35] освітній простір загальноосвітнього навчального закладу розглядатимемо як систему з такими параметрами:

- інформаційні ресурси містять дані у текстовому, графічному, аудіо та відеоформатах;
- кількість об'єктів, які взаємодіють у системі визначається кількістю учнів, учителів, працівників адміністрації школи, а також, за необхідності, можливе залучення батьків;
- територія, на якій розташовані об'єкти, охоплені простором, не може обмежуватися будівлею школи, оскільки передбачається можливість взаємодії учасників навчального процесу через Інтернет;
- швидкість обміну інформаційними ресурсами простору повинна бути на рівні сучасних стандартів локальних та глобальних комп'ютерних мереж;
- обмін інформаційними ресурсами має відбуватися за принципом «сервер»-«клієнт».

При цьому постають проблеми добору програмних засобів та раціонального використання освітніх інформаційних ресурсів, створених на їх основі. Вирішуючи обидві проблеми, слід враховувати як базову характеристику єдиного освітнього простору, необхідність інтеграції різних сервісів. У цьому контексті одним з першочергових завдань є організація доступу користувачів до ресурсів освітнього простору.

Враховавши специфіку загальноосвітнього закладу, спробуємо запропонувати типи програмних засобів, які формуватимуть його освітній простір. Зазвичай обмін інформаційними ресурсами у кожній розподіленій системі відбувається за принципом «клієнт-сервер». Тому технологічною основою розглядуваного простору повинна бути комп'ютерна мережа, разом з приєднаним до неї виділеним сервером.

Мережу загальноосвітнього закладу, як і корпоративні мережі, слід проектувати з урахуванням достатньо великої кількості користувачів, можливості здійснення ними активної навчальної діяльності. Ще однією особливістю мережі школи є той факт, що користувачі мережі (насамперед учні) не мають постійного, наперед визначеного місця діяльності. Зрозуміло, що такий підхід вимагає водночас впровадження та застосування розподіленої бази даних облікових записів користувачів, а також засобів централізації управління мережею.

Централізоване збереження облікових записів можливе за умови застосування доменної структури локальної мережі. У цьому випадку роль контролера домену повинен виконувати виділений сервер.

Загалом серед програмних засобів у складі освітнього простору виділимо дві групи;

- сервіси, які виконують функції надання доступу до ресурсів;
- ресурси, які власне містять освітній контент простору.

До першої групи зарахуємо сервіси:

- контролю доступу до Інтернету;
- надання доступу до мережі освітнього закладу, наприклад, за допомогою технології віртуальних приватних мереж;
- поштова система;
- загальноприйнятий сервіс передавання файлів у мережі Інтернет.

Складові другої групи важко окреслити, з огляду на їх постійний розвиток. Проте спробує описати їх базовий функціонал:

- презентація загальноосвітнього закладу;
- створення навчальних ресурсів, наприклад, через систему електронних навчальних курсів;
- забезпечення соціальних контактів учасників навчального процесу;
- наповнення online-енциклопедій;
- публікація та трансляція контенту у відеоформаті.

Аналізуючи ресурси та сервіси сучасного Інтернету, можна стверджувати, що описані складові реалізовані потужними корпораціями та досить часто надаються безкоштовно для освітніх закладів. Наприклад, загальновідомим лідером серед систем електронної пошти є система Gmail компанії Google Inc. Також важко порівняти функціонал і можливості ресурсів загальноосвітньої школи з «гігантами» Інтернету — системою відеохостингу YouTube чи соціальною мережею Facebook.

Проте створення і використання власних навчальних ресурсів у освітньому просторі має переваги:

- збереження навчального контенту (жодна стороння компанія, яка надає ресурси чи сервіси безкоштовно не має жодних зобов'язань перед освітнім закладом);
- відсутній рекламний чи інший контент, який не пов'язаний з навчанням і вихованням або суперечить нормам етики й моралі;
- можливість використання ресурсів без доступу до мережі Інтернет.

Традиційно для роботи з кожним таким сервісом чи ресурсом учителям та учням 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:

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

Кожна з цих концепцій може бути зреалізована через:

- внесення змін до коду програмних засобів, для використання єдиної

бази облікових засобів;

- використання системи, яка дозволяє 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 [6, 81]. Проте вона передбачає конфігурування додаткового сервісу — провайдера OpenID або звертання до зовнішнього провайдера. Останній спосіб є цікавим у випадку використанням в освітньому закладі стандартної бази користувачів, наприклад, доменної. Принциповою особливістю домену є централізоване збереження та опрацювання даних облікових записів користувачів. Стандартним засобом для організації доменів у локальних мережах є служба Microsoft Active Directory, використання якої у загальноосвітній школі є проблематичним через:

- високі вимоги щодо апаратного забезпечення сервера;
- досить дорогу ліцензію для використання серверної операційної системи, складовою якої є служба каталогів Active Directory.

Тому, на нашу думку, у процесі організації освітнього простору школи слід звернути увагу на вільно поширюване програмне забезпечення з відкритим кодом. Вартими уваги вважаємо Open Source Unix-подібні операційні системи, наприклад, Linux та FreeBSD.

У комерційній ОС Windows для доступу до бази облікових записів користувачів домену Active Directory використовують полегшений протокол доступу до каталогів (LDAP — Lightweight Directory Access Protocol). Для пропонованих операційних систем реалізовано власну систему доступу до каталогів — програмний сервер OpenLdap, який також працює за протоколом LDAP.

Суть протоколу полягає у можливості зберігання даних в ієрархічній структурі [7]. 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 смислі, 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 криптування (SASL, SSL, TLS).

Для організації домену локальної мережі у пропонуваніх ОС Linux (FreeBSD) на сьогодні використовують застарілий програмний сервер Samba3. До недоліків домену, функції контролера якого виконує сервер Samba3 належать неможливість побудови ієрархії доменів з подальшою

реплікацією їх даних, відсутність засобів адміністрування комп'ютерів домену (делегування повноважень, політики безпеки), а особливо — недосконала система безпеки, яка заснована на застарілому протоколі NTLM.

Проте зазначені недоліки можуть бути частково скомпенсовані завдяки обмеженню доступу до сервера Samba з мережі Інтернет, побудові домену на основі каталогу LDAP, розробці скриптів для віддаленого адміністрування. Додатково слід зазначити, що в межах одного зазальноосвітнього навчального закладу відсутня потреба створення кількох ієрархічних доменів локальної мережі.

Розглянемо застосування каталогу LDAP для створення єдиної системи автентифікації загальноосвітнього навчального закладу. Оскільки, більшість ресурсів сучасного Інтернету розроблено у формі веб-сторінок (веб-сайтів, веб-порталів), то програмною основою для обміну навчальними ресурсами у освітньому просторі школи повинен бути веб-сервер. Він надаватиме користувачам доступ до таких ресурсів:

- сайту школи, який виконує презентаційну функцію; для розробки сайту на сьогодні використовують системи управління контентом (CMS), наприклад, Joomla!, WordPress, TYPO3.
- сервера електронних курсів, який можна організувати на основі системи управління навчанням, наприклад, MOODLE, тим самим реалізувавши навчально-методичну функцію;
- вікіпедії школи — відкритої Інтернет-енциклопедії, яку можна побудувати на платформі MediaWiki;
- соціальної мережі, яка забезпечуватиме можливість соціальної взаємодії учасників навчального процесу; для її створення можна використати вільно поширювану платформу Elgg;

Сервіси освітнього простору школи можуть бути представлені:

- поштовою системою, яка надаватиме користувачам доступ до персональних поштових скриньок. Як програмну основу поштової системи можна використати сервери Postfix та Dovecot (Courier IMAP);



- проксі-сервером, який можна сконфігурувати на основі відомого пакету Squid.

Функції сервера LDAP може виконувати один і той же сервер під управлінням ОС Linux (FreeBSD). Розглянемо фрагмент каталогу LDAP (рис. 1), у якому зберігаються облікові записи користувачів домену (наприклад, znz.org.ua).

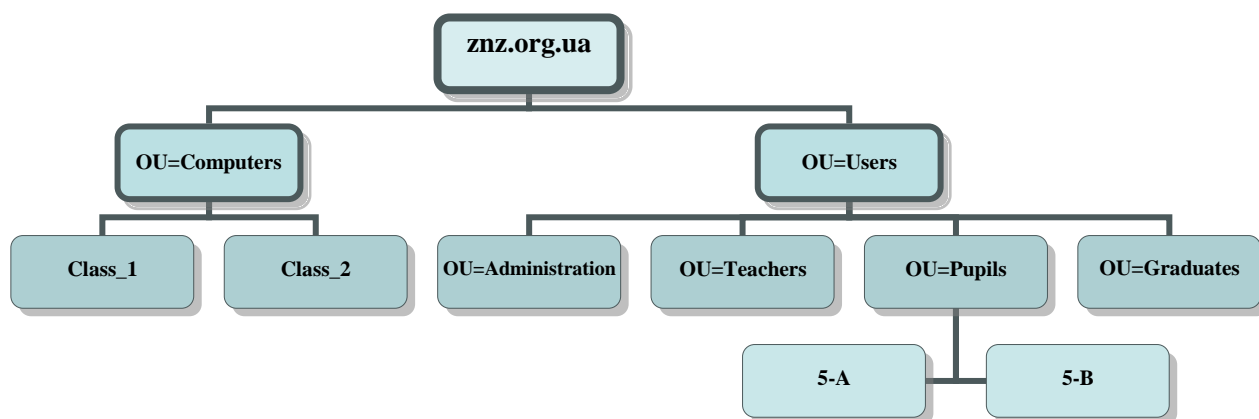


Рис. 1. Структура пропонованого каталогу LDAP

Слід звернути увагу, що у каталозі зберігаються облікові записи як користувачів, так і комп'ютерів. Такий підхід дає можливість за допомогою запитів формувати фільтри для визначення атрибутів об'єктів каталогу. Поряд з контейнером *Учні (Pupils)*, пропонуємо використовувати контейнер *Випускники (Graduates)*. Тобто після закінчення школи, облікові записи учнів слід переносити у цей контейнер, у такий спосіб надавши їм можливість не полишати освітній простір школи.

Атрибути облікового запису (таблиця 1) як об'єкта каталогу LDAP дають можливість здійснити автентифікацію.

Таблиця 1

Атрибут	Значення	Опис
objectClass	Person	клас даного об'єкта (особа)
Description	2007_2018	опис даного об'єкта (рік початку навчання, рік закінчення)
distinguishedName	CN=Petrenko,OU=Pupils,OU=Users,DC=znz,DC=org,DC=ua	місцезнаходження об'єкта в дереві каталогів LDAP
displayName	Петренко Іван Миколайович	ім'я користувача
homeDirectory	\\Server\Users\Pupils\2017\petrenko_im	шлях до домашньої папки
sAMAccountName	petrenko_im	ім'я облікового запису
mail	petrenko_im@znz.org.ua	електронна пошта користувача

З точки зору безпеки сервер OpenLDAP не повинен виконувати анонімні запити. Тому у каталозі слід створити окремий обліковий запис користувача, від імені якого здійснюватиметься зчитування даних.

Слід зазначити, що усі програмні засоби, які були згадані вище є вільно поширюваними, а тому їх використання є легальним. Крім цього для кожного з них реалізовані додаткові модулі, які дозволяють виконувати автентифікацію користувачів на основі каталогу LDAP. Зазначені модулі слід встановити та сконфігурувати як складові сервера школи. Незважаючи на те, що кожен сервіс має власні особливості конфігурування наведемо спільні параметри, які слід використати 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 сервісів. На нашу думку, у випадку формування освітнього простору школи слід дотримуватись правила, за яким облікові записи користувачів створює адміністратор у каталозі LDAP.

Перспективним напрямом удосконалення запропонованої системи автентифікації є забезпечення можливості роботи користувачів з єдиними атрибутами доступу до різних освітніх ресурсів за принципом однократного введення паролю (так звана технологія єдиного входу (Single Sign-On)). Такий підхід реалізовано на основі технології pubcookie та каталозі LDAP у Українському інституті інформаційних технологій в освіті Національного Технічного Університету України "КПІ" [5].

Впровадження описаних підходів можливе кваліфікованими фахівцями у галузі адміністрування комп'ютерних мереж і систем. Розв'язання цієї

проблеми бачимо у відповідній підготовці вчителів інформатики або із залученням сторонніх організацій, наприклад науково-дослідних чи комерційних.

## ЛІТЕРАТУРА

1. Биков В. Ю. Доменно-фреймова модель педагогічної системи. [Електронний ресурс]. — Режим доступу [http://www.ime.edu-ua.net/cont/Bykov8.doc](http://www.ime.edu.ua.net/cont/Bykov8.doc).
2. Засоби інформаційно-комунікаційних технологій єдиного інформаційного простору системи освіти України. / [В.В. Лапінський, А.Ю. Пилипчук, М.П. Шишкіна та ін]: за наук. ред.. проф.. В.Ю. Бикова. — К.: Педагогічна думка, 2010. — 160 с.
3. Постанова про затвердження Державної цільової програми впровадження у навчально-виховний процес загальноосвітніх навчальних закладів інформаційно-комунікаційних технологій "Сто відсотків" на період до 2015 року. [Електронний ресурс]. — Режим доступу <http://zakon2.rada.gov.ua/laws/show/494-2011-%D0%BF>.
4. Рамський Ю. С., Формування інформаційної культури майбутніх учителів математики та інформатики у процесі підготовки їх до розробки освітніх ресурсів. / Юрій Рамський, Василь Олексюк // Науковий часопис НПУ ім. М.П. Драгоманова, серія 2. Комп'ютерно-орієнтовані системи навчання.— К.:НПУ імені М.П. Драгоманова, 2010. — №8(15). — с.65-68.
5. Створення освітнього web-простору для навчання. [Електронний ресурс]. / В. М. Валуйський, М.В.Гончаренко, А.А.Павловський, А.О.Новацький. — Режим доступу [http://uiite.kpi.ua/fileadmin/\\_wfqbe/1245139683\\_web](http://uiite.kpi.ua/fileadmin/_wfqbe/1245139683_web).
6. Liferay Portal Enterprise Intranets: A practical guide to building a complete corporate intranet with Liferay.— Packt Publishing, 2008. — 386 p.
7. Gerald Carter. LDAP System Administration. — O'Reilly, 2003.— 308 p.