

## **АРХІТЕКТУРА СИСТЕМИ ВІРТУАЛЬНИХ ЕЛЕКТРОННИХ СХОВИЩ «ВІДКРИТОГО ДОСТУПУ» ВНЗ**

**Тимофєєв В.І., Тимошин Ю.А., Ярченко В.П., Шемседінов Т.Г.**  
**Національний технічний університет України**  
**"Київський політехнічний інститут"**

*У статті приведені результати розробленої системи віртуальних електронних сховищ з відкритим доступом в середовищі корпоративної мережі НТУУ «КПІ», яка може виступати як компонент системи електронного уряду України. Система є частиною розробленого пілотного зразка центру інтегрованого доступу, обробки і архівації інформаційних ресурсів ВНЗ, включаючи використання компонентів національного освітнього GRID. Розроблена архітектура її реалізації на корпоративному рівні з урахуванням вимог безпеки і управління.*

**Ключові слова:** архів, віртуальне сховище, Web-клієнти, FTP-клієнти, інформаційні вітрини IT-архітектура

### **Вступ**

Широко відома Будапештська ініціатива відкритого доступу (Budapest Open Access Initiative-2001), яка поклала початок міжнародному проекту доступу до наукових публікацій з відкритим доступом в Інтернеті для багатьох країн світу [ 1 ].

В останні декілька років багато університетів прагнуть створювати сховища (і кіоски) даних, щоб забезпечити інформаційний попит абітурієнтів, студентів, що поступають до магістратури, майбутніх аспірантів та докторантів про умови вступу до навчального закладу. Сучасні технології таких сховищ даних спираються, перш за все, на технології ETL (extract-transform-load - <<вилучення-перетворення-завантаження>>), засоби моделювання і проектування баз даних, а також на гетерогенні системи управління реляційними базами даних [ 2 ] .

Проте дані зберігаються в розрізних системах, і для виконання запитів чи замовлень ці дані необхідно інтегрувати чи виконувати консолідацію одержаних з різних систем результатів. Потреба в інтеграції корпоративних даних послужила поштовхом до створення сховищ даних, а також кіосків даних - еквівалента сховища даних на рівні підрозділу ВНЗ чи за вузькою їх тематичною спрямованістю.

Не зникає також потреба у наданні безпечного доступу до таких ресурсів та відповідного управління ними в умовах масового доступу до ресурсів ВНЗ сторонніх користувачів при спрощеній процедурі їх реєстрації чи при її повній відсутності.

Відомо, що базовими технологіями такого доступу на цей час є використання Web-клієнтів та FTP- доступу.

### **Аналіз вимог до систем з відкритим доступом користувачів**

Система віртуальних архівів у ВНЗ може включати такий сегмент, як віртуальні електронні сховища «Відкритого доступу» для забезпечення відкритого доступу до інформації загального користування, до якої можна віднести, наприклад, інформацію для абітурієнтів, данні про керівництво університету, інформацію про магістратуру, аспірантуру та докторантуру, про наукові конференції та семінари, наукові видання закладу, тощо.

Доступ до таких систем може бути реалізовано однією з двох відомих технологій [ 3 ]:

- Без реєстрації користувача на рівні гостьового входу до системи;
- З тимчасовою реєстрацією користувача.

Окрім того до такої інформації можуть доступатися також штатні користувачі мережі ВНЗ, які мають повну реєстрацію в системі електронних архівів – співробітники, викладачі та студенти.

Клієнтами до сховищ відкритого доступу можуть бути Web- клієнти чи FTP- клієнти. Ресурси відкритого доступу можуть бути організовані з використанням різних систем:

- На SharePoint Portal Server з використанням його Web- серверу у формі створених інформаційних вітрин чи спеціалізованих електронних каталогів;
- Через використання FTP- серверів для доступу до інформаційних файлів;
- Через використання спеціального шлюзу доступу до віртуального архіву ВНЗ;
- Через систему «Абітурієнт», яку використовують декілька ВНЗ, чи подібні інші системи;
- З використанням Web-серверу ВНЗ загального доступу.

Необхідно зазначити також існуючі обмеження безпеки та вимоги управління, що встановлюються для прикладної корпоративної мережі ВНЗ, для забезпечення яких необхідно відповідно структурувати розташування програмно-технічних засобів по зонах безпеки і забезпечити їх стійкість до несанкціонованого доступу та зовнішніх атак.

#### **Схема взаємодії компонентів віртуальних електронних сховищ**

Доступ може бути організовано через мережу загального доступу Інтернет чи через наукову мережу УРАН [ 4 ]. На період роботи приймальної комісії можуть бути тимчасово доступні відкриті ресурси через спеціалізовані точки входу Wi-Fi для мобільних користувачів. В цьому разі рекомендується використовувати технологію доступу з тимчасовою реєстрацією користувача на період сеансу.

Сервер доступу FTP- клієнтів може взаємодіяти з одним чи декількома FTP- серверами та сервером додатків, на якому можуть бути розташовані спеціалізовані додатки, наприклад, що реалізують основні механізми технології ETL (Extract-Transport-Loading) для забезпечення функціонування «вітрин» та оновлення інформації SQL- сервера порталу. В разі використання технологій Майкрософт типу MSA 2.0 чи більш сучасних, на FTP-сервері повинен бути розгорнутий IIS-сервер, який виконує функції майкрософтовського Web-сервера. Відповідно до цієї технології всі сервери і пристрої шлюзів, що забезпечують доступ до відкритих ресурсів, повинні бути розташовані в зоні Периметру прикладної корпоративної мережі ВНЗ.

Необхідно зауважити, що SharePoint Portal Server повинен бути орієнтован у зовнішній інформаційний простір за вимогою безпеки для корпоративної прикладної мережі ВНЗ. При використанні для цих цілей внутрішнього корпоративного порталу буде важче забезпечити стійку роботу зони Периметру прикладної корпоративної мережі [ 5 ].

З метою розширення функціональності такої системи відкритого доступу можна використати Exchange Server, який входить до складу забезпечуючих серверів SharePoint Portal, для надання можливості зовнішнім клієнтам поштового обміну, наприклад, з приймальною комісією чи відділом аспірантури чи підготовчим відділенням. Web-сервер порталу може відображати відкриту частину каталогу системи віртуальних архівів ВНЗ.

Ще одне зауваження – система повинна бути налаштована так, що всі клієнти відкритого доступу можуть тільки «читати» архівні данні та інформацію. Право оновлення даних та налаштування ролей доступу надано тільки адміністратору системи [6].

На Рис.1 представлено схему взаємодії компонентів системи віртуальних електронних сховищ відкритого типу.

Джерелами, що «підпитують» вище згадані сервери та системи, можуть виступати БД, сховища, довідкові системи, файли, каталоги різного рівня, включаючи каталоги та репозиторій E-library [7-8]. В свою чергу, данні оперативних БД прикладної корпоративної мережі ВНЗ та репозиторій зовнішніх інформаційних джерел та сховищ інших ВНЗ являються основними джерелами поновлення інформації для джерел віртуальних електронних сховищ «Відкритого доступу».

#### **Розробка архітектури системи віртуальних електронних сховищ**

На цій основі була розроблена відповідна архітектура системи віртуальних електронних сховищ, приклад реалізації якої показано на Рис. 2.

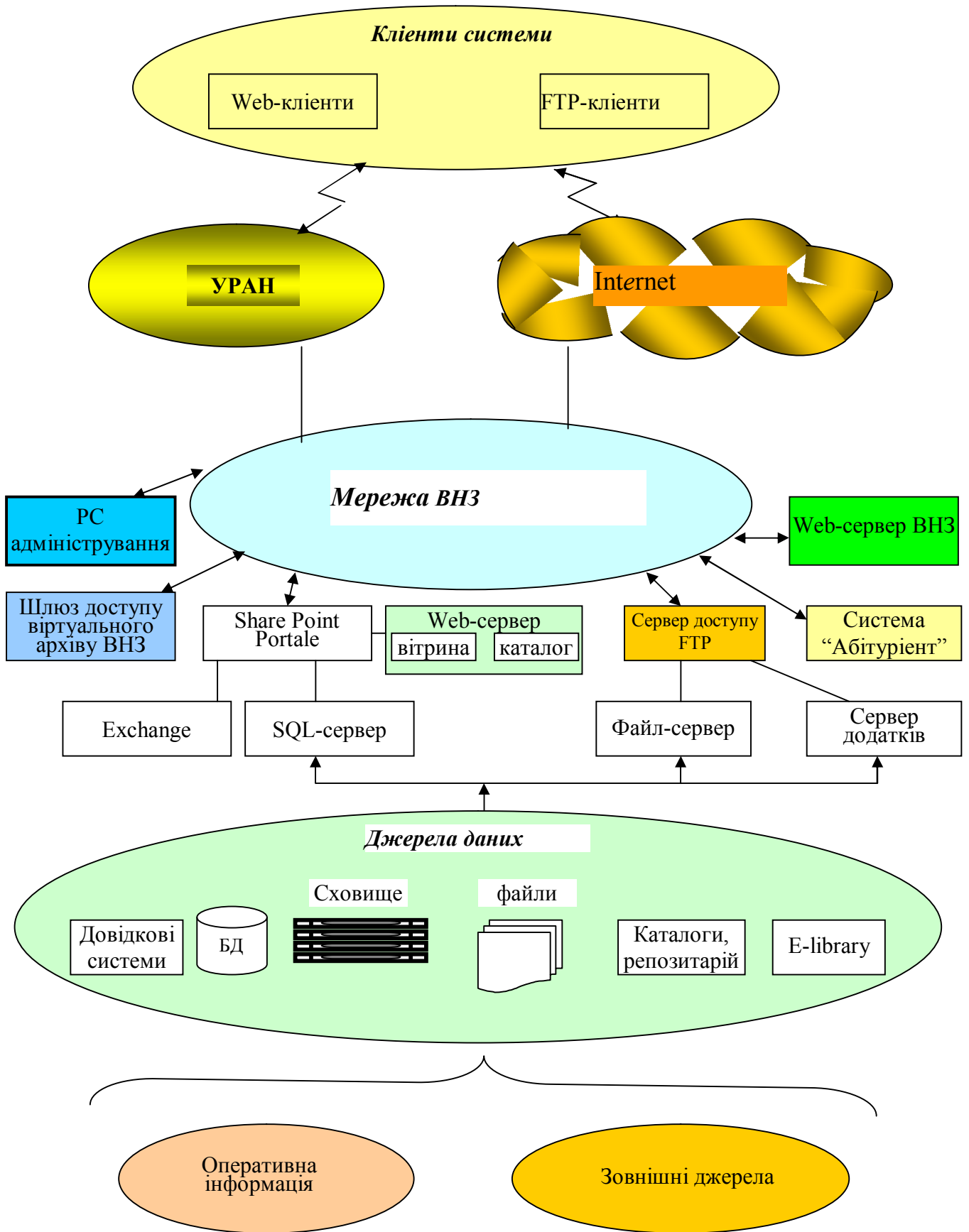


Рисунок 1 Схема взаємодії компонентів віртуальних електронних сховищ «відкритого доступу»

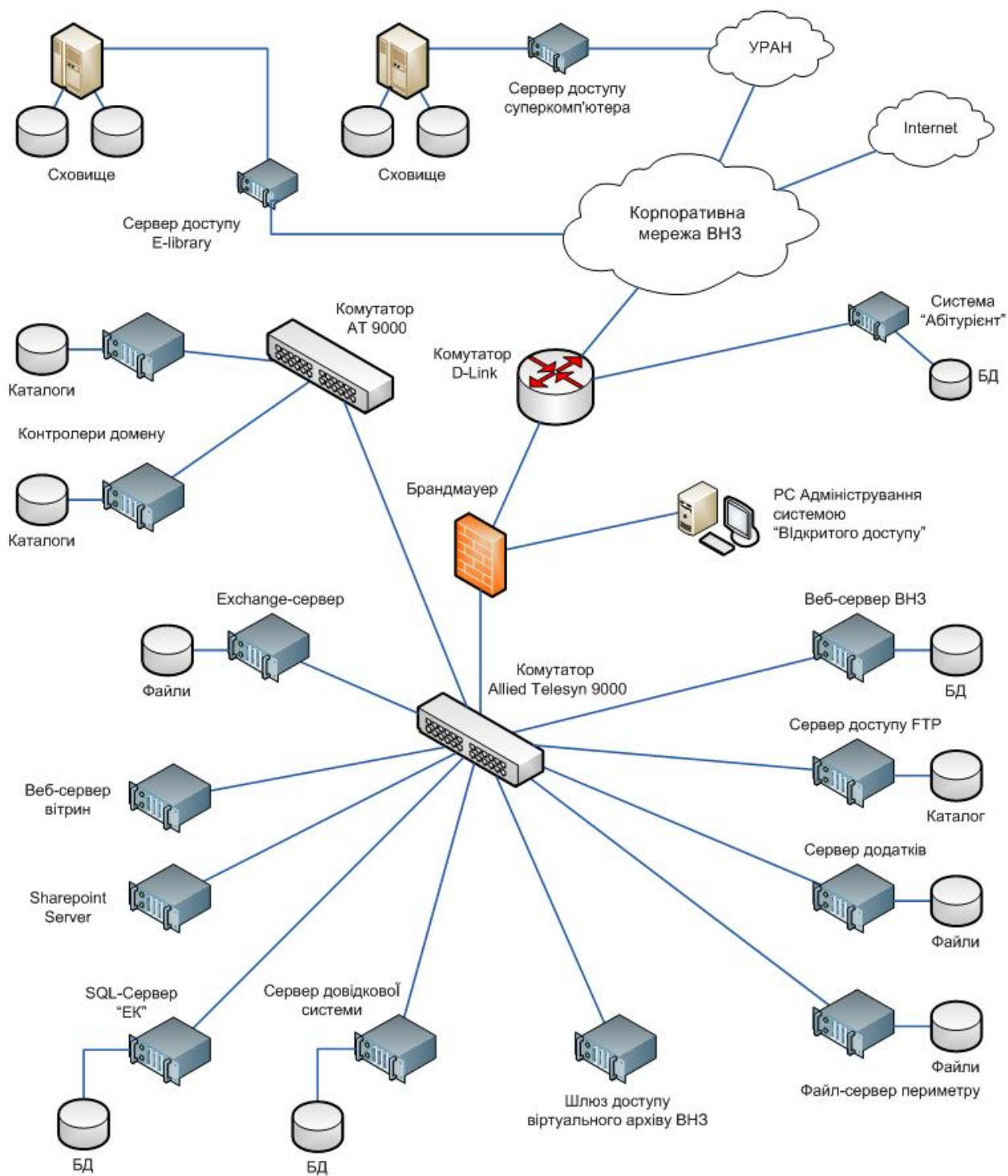


Рисунок 2 Архітектура системи віртуальних електронних сховищ «відкритого доступу»

Особливістю цієї архітектури є те, що практично всі сервери розташовано в зоні Периметру прикладної мережі ВНЗ, яка повинна бути захищена від несанкціонованого доступу засобами типу брандмауера та комутатора, які фільтрують не тільки пакети, а й запити до ресурсів з боку користувачів системи та дані, що поступають з систем віртуального архіву. У відкритій частині мережі знаходяться ресурси суперкомп'ютера, E-library та системи «Абітурієнт», а також інших джерел інформації, що мають свої засоби управління доступом до їх ресурсів та встановлені відповідні обмеження.

Web- сервер ВНЗ може знаходитися поза брандмауером тому, що обслуговує доступ до своїх ресурсів через стандартні браузері, або знаходиться під захистом брандмауера в більш захищеній зоні. Комутатор, до якого підключені захищені сервери системи, за винятком контролерів домену, повинен підключатися до портів «демільтаризованої зони» брандмауера.

В наведеній архітектурі присутні два контролери домену (відповідно технології MSA Майкрософт) – один з яких відповідає за управління серверами та програмними засобами пристроїв Периметру, а інший – за доступ до ресурсів цих серверів з боку користувачів. Управління цими контролерами здійснюється через сервер Active Directory, що розташований у зоні Дата-центру.

Сервер додатків зберігає файли додатків, що необхідні для функціонування зображених серверів, їх взаємодію між собою та з серверами інших систем поза Периметром, в першу чергу з відповідними серверами Дата-центру та віртуального архіву ВНЗ через спеціальний шлюз доступу.

Наступні сервери – SharePoint Server, Exchange Server, SQL-server та Web-сервер складають групу серверів порталу [ 9 ].

Сервер доступу FTP підтримує каталог файлових ресурсів, які доступні для відкритого використання.

Брандмауер може бути програмним чи апаратним. Комутатори 3-го рівня AT 9000 забезпечують сполучення відповідних серверів системи та фільтрацію даних на рівні портів.

Керування системою віртуальних електронних сховищ «Відкритого доступу» ВНЗ та підтримку і управління пристроями цієї системи здійснює відповідний адміністратор. Він же відповідає за відновлення даних та образів цих серверів через Backup, а також узгоджує з іншими адміністраторами прикладної мережі реплікації даних для відповідних СУБД та налаштування шлюзів доступу в інші системи – до ресурсів суперкомп'ютера чи електронної бібліотеки.

### **Висновки**

Проведений аналіз вимог до систем з відкритим доступом користувачів відкритого доступу та засобів їх реалізації дозволив визначити основні обмеження та вимоги до створення таких систем, як сегменту прикладної корпоративної мережі ВНЗ.

Найбільш поширеним засобом доступу до більшості ресурсів залишається використання Web-застосунків, як єдиного механізму доступу користувачів до ресурсів відкритого користування. Використання FTP- механізмів доступу потребують тимчасової реєстрації користувачів для їх безпечного доступу та забезпечення стійкості системи щодо несанкціонованого доступу до відкритих ресурсів корпоративної мережі.

Було визначено основні компоненти такої системи та схема їх взаємодії, на основі чого була розроблена архітектура системи віртуальних електронних сховищ «Відкритого доступу», що забезпечує багатоаспектний доступ до інформаційних ресурсів ВНЗ широкого кола користувачів – від абітурієнтів до майбутніх аспірантів і докторантів.

Показано, що така система може бути компонентом системи електронного урядування, що створюється в Україні, в межах підпорядкованості МОН України.

### **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Guide to Business Planning for Converting a Subscription based Journal to Open Access/v.3 (Last Update\$ Feb/3, 2004)

2. У. Куль. Консолидація серверов и систем хранения данных. -М. У ж. "Системи баз даних" № 3, 2007.
3. Открытая Инициатива Архивов <http://www.openarchives.org/>
4. Тимофєєв В.І., Тимошин Ю.А., Ярченко В.П., Шемседінов Т.Г., інші – К., НТУУ «КПІ», № держреєстрації 0104U005967, Заключний звіт по темі IT/550-2009, 2010р., стор.127
5. Еталонні архітектури MSA.- К.: Майкрософт Україна; К.: Видавнича група BHV, 2005.-352 с.
6. D. Pyle. Data Preparation for Data Mining, Morgan Kaufmann Publishers, 1999.
7. W. Kim. "I/O Problems in Preparing Data for Data Warehousing and Data Mining - Part 1", Journal of Object-Oriented Programming, 101 Communications, 1999. Feb.
8. W. Kim, E. Hong, K. Kim, D. Lee. "A Component-Based Architecture for Preparing Data in Data Warehousing", Journal of Object-Oriented Programming, 2000 March/April.
9. [http://www.microsoft.ru/msdn/Experts/SQLServer/SQL7\\_dwa.htm](http://www.microsoft.ru/msdn/Experts/SQLServer/SQL7_dwa.htm) , Юлія Граванова . Сnews