***Запропоновано структурну модель, модель взаємодії функціональних модулів підсистеми управління доступом адміністратора баз даних, діаграма активності інформаційної системи та діаграма використання інформаційної системи з підсистемою управління доступом адміністратора баз даних для захисту від несанкціонованого доступу***

***Ключові слова: база даних, система управління, комерційна інформація, ідентифікація користувачів, несанкціонований доступ***

***Предложена структурная модель, модель взаимодействия функциональных модулей подсистемы управления доступом администратора баз данных, диаграмма активности информационной системы и диаграмма использования информационной системы с подсистемой управления правами администратора баз данных для защиты информации от несанкционированного доступа***

***Ключевые слова: база данных, система управления, коммерческая информация, идентификация пользователей, несанкционированный доступ***

УДК 004.932:519.76

# ПІДСИСТЕМА УПРАВЛІННЯ ДОСТУПОМ АДМІНІСТРАТОРА БАЗ ДАНИХ КОМЕРЦІЙНОГО ПІДПРИЄМСТВА

**І. А. Пількевич**
Доктор технічних наук, професор, завідувач кафедри*
E-mail: igor.pilkevich@mail.ru
**Н. М. Лобанчикова**
Кандидат технічних наук, доцент**
E-mail: lobanchikovanm@rambler.ru
**В. І. Котков**
Кандидат технічних наук, доцент*
E-mail: eko_univer@i.ua
*Кафедра моніторингу навколишнього природного середовища
Житомирський національний агроекологічний університет
бульвар Старий, 7, м. Житомир, Україна, 10008
**О. В. Метельський****
E-mail: sasha_metelskiy@mail.ru
**Кафедра безпеки інформаційних і комунікаційних систем
Житомирський військовий інститут ім. С. П. Корольова Національного авіаційного університету
пр. Миру, 22, м. Житомир, Україна, 10004

## 1. Вступ

Сучасні новітні технології зумовили активний розвиток системи електронних інформаційних ресурсів. Створення великих обсягів сховищ електронних даних в інформаційно-комунікаційних системах призвели до необхідності їх захисту від несанкціонованого доступу. Одним із напрямків захисту інформації є розмежування доступу до інформаційних ресурсів [1]. Для визначення доступності необхідним є класифікація документів, визначення їх доступності визначеним категоріям користувачів.

Таким чином, впровадження підсистеми розмежування доступу дозволить підвищити рівень захисту інформаційної системи від несанкціонованого доступу та користування системою. Однак, слід зазначити, що процес управління користувача інформаційно-комунікаційної системи є доволі складним та потребує великої кількості однотипних операцій від адміністратора. При додаванні користувачів та зміні їх прав доступу адміністратору необхідно внести дані у всі існуючі таблиці, а це потребує певного часу. Сучасні інформаційні технології направлені на пошук нових методів, засобів і технологій для автоматизації процесів роботи з метою мінімізації часу на виконання операцій та збільшення продуктивності праці [2, 3]. Тому розробка підсистеми управління доступом адміністратора баз даних з метою автоматизації його роботи є актуальною.

## 2. Аналіз існуючих рішень

В сучасних інформаційних системах інформація зазвичай зберігається з використанням автоматизованих бази даних [4]. Бази даних можуть бути дуже великими і можуть містити різну інформацію, що використовується організацією. Розробці підсистем управління доступом адміністратора баз даних присвячена велика кількість робіт, в тому числі [5-9]. Вагомий внесок у створення подібних систем та розвиток методів і засобів їх побудови внесли роботи таких авторів: Дж. Р. Гроффа, Пол Н. Вайнберга, А. В. Пістоліта, У. Р. Станека, А. Д. Хомоненка, В. М. Циганкова, М. І. Шлезінгера, М. М. Биченка, С. В. Кавуна, Л. Шапиро, Ф. Уоссермена, Дж. Стокмана та ін. Такі системи призначені для управління доступом адміністратора баз даних комерційного підприємства та ефективних засобів захисту інформації від несанкціонованого доступу. Запропоновані методи та засоби є окремими

рішеннями для підвищення рівня безпеки та автоматизації роботи адміністратора [10]. Тому необхідним є розробка інформаційної технології, що поєднувала б процеси автоматизації роботи адміністратора баз даних та підвищувала рівень захисту інформації від несанкціонованого доступу.

*Метою дослідження* є розробка підсистеми управління доступом адміністратора баз даних комерційного підприємства, що автоматизує процеси управління базою даних (БД) та підвищує рівень захисту інформаційної системи від несанкціонованого доступу. Основними завданнями роботи є: провести аналіз технологій розробки підсистеми управління доступом до бази даних, провести аналіз методів та засобів управління базами даних, провести аналіз методів ідентифікації та аутентифікації користувачів, методів управління доступом в інформаційних системах, розробити структуру підсистеми адміністрування інформаційної системи та провести практичну реалізацію запропонованих методів і заходів.

## 3. Основна частина

Проведений аналіз предметної області дослідження дозволив сформувати структурну схему функціональних модулів управління доступом адміністратора баз даних, яка представлена на рис. 1.

До структурної схеми управління доступом адміністратора баз даних входять слідуючи функціональні модулі: визначення групи доступу, реєстрації користувачів, розмежування прав доступу та аутентифікації, які взаємодіють через інтерфейс програмного продукту та базу даних інформаційної системи.

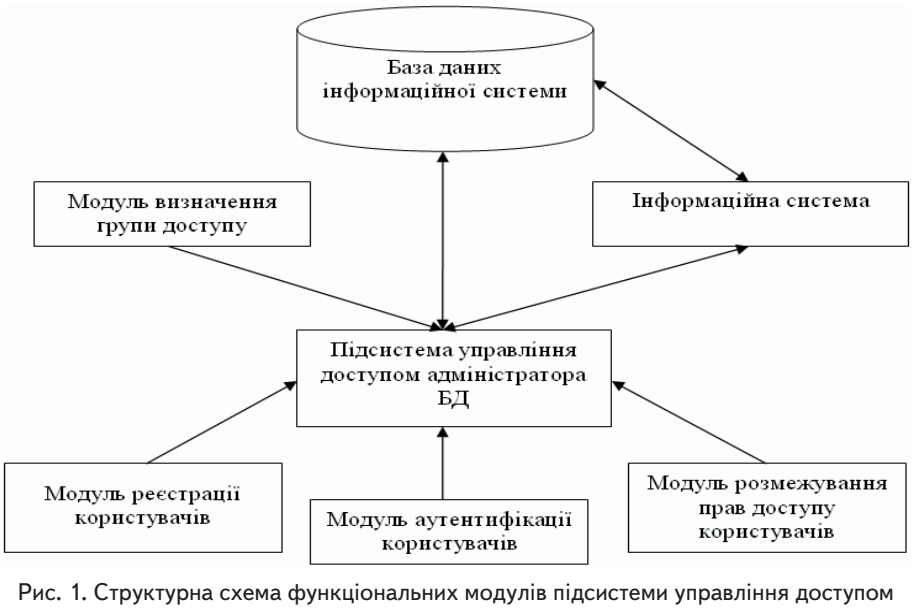


Рис. 1. Структурна схема функціональних модулів підсистеми управління доступом адміністратора баз даних

Модуль розмежування прав доступу представлено блоком вибору та налаштування групової політики безпеки.

Модуль реєстрації користувачів підсистеми призначений для додавання, видалення, перегляду користувачів інформаційної системи. В даному модулі повинно бути передбачено зміну контрольного питання та відповіді на нього, зміну групи доступу, а також зміну паролю. Модуль аутентифікації призначений для запобігання несанкціонованому доступу до інформаційної системи. Для входження в систему необхідно підключити базу даних інформаційної системи, яка включає дані про користувачів та групи доступу до інформації. Модуль аутентифікації представлено наступними функціональними блоками: введення логіну, введення паролю, здійснення входу в інформаційну систему, нагадування паролю. Після успішного проходження процедури аутентифікації, відповідно до налаштувань групової політики безпеки підсистеми аутентифікації користувачів інформаційної системи, відбувається вхід в інформаційну систему і користувач може починати роботу відповідно до встановлених прав.

Вихідними потоками даних в цьому випадку є інформаційний вектор наступного виду:

$$I = \{R,\ \text{login},\ \text{Group\_dostup}\},$$

де $R$ – бінарне рішення про надання прав доступу користувачу; $\text{login}$ – ім'я користувача; $\text{Grup\_dostup}$ – група доступу, до якої відноситься користувач системи.

Таким чином, вихідними потоками даних підсистеми аутентифікації є: права доступу користувачів, перелік користувачів системи, рішення про проходження системи аутентифікації, перелік груп доступу користувачів та перелік можливостей групи користувачів.

Проведений аналіз призначення і задач кожного функціонального модулю системи дозволяє визначити вимоги до функцій системи. Для виконання поставлених задач та належного функціонування системи необхідно, щоб система могла: дозволяти роботу з системою зареєстрованим користувачам, забезпечувати гнучку адаптацію доступності процедур системи для кожного окремого користувача, забезпечувати збереження інформації в базі даних системи про проведену оцінку документів і користувачів системи.

Для вирішення поставлених задач необхідно провести проектування бази даних користувачів інформаційної системи, визначити групи користувачів і права доступу кожної групи до інформаційних ресурсів та дії, що може виконувати дана група користувачів.

Розроблена система є інтегрованою інформаційною підсистемою, тому доповнення існуючої бази даних інформаційної системи підприємства проводимо за допомогою додаткових таблиць, що забезпечать роботу підсистеми.

В системі визначено три групи користувачів: G1 – доступ до перегляду та редагування таблиць з доку-

ментами; G2 – доступ та редагування форм оцінювання документів; G3 – повний доступ.

Спеціалістом з обслуговування бази даних інформаційної системи є адміністратор, якому надані повні права доступу до даного програмного продукту (група доступу G3). Він проводить налагодження системи, підтримує працездатність системи, проводить налагодження баз даних, реєструє користувачів і проводить налагодження їх логіну. Права адміністратора включають права інших користувачів системи, а саме: експерта з питань безпеки інформації та спеціаліста. Права інших користувачів розмежовуються. Так, експерту в системі надаються права доступу та редагування форм оцінювання документів (група доступу G2). Таким чином він може проводити оцінку документів і проводити налаштування критеріїв оцінювання. Спеціаліст має право переглядати документи, які пройшли оцінку на наявність інформації, що містить комерційну таємницю, та додавати документи. В системі передбачено ряд загальнодоступних функцій користувачів. Це, наприклад, під'єднання та від'єднання бази даних, перегляд звітності у системі, а також перегляд таблиці з документами.

Діаграма використання системи представлена на рис. 2.

Діаграма активності інформаційної системи з підсистемою управління доступом адміністратора баз даних заключається в наступному. Для того, щоб почати роботу з системою, в першу чергу, потрібно ввімкнути систему. Після чого йде запит на вибір та підключення БД інформаційної системи (БД ІС). При правильному підключенні бази даних завантажується інтерфейс системи. Користувач повинен ввести свій логін та пароль.

При коректному введенні логіну та паролю відбувається розблокування входу в інформаційну систему, проводиться аналіз групи доступу до інформаційних ресурсів системи, розблоковуються визначені для цього типу користувача системи функції. Користувач вибирає дії в залежності від налаштованих прав, а інші є недоступними. По закінченню роботи авторизованого користувача відбувається збереження модифікованих даних, відбувається відключення бази даних та вихід із системи. Адміністратор може надавати права користувачам, додавати, редагувати їхні дані, переглядати та редагувати дані, що знаходяться на сервері. При неправильному введенні логіну або (та) паролю відбувається блокування входу в систему і далі користувачу пропонується або здійснити повторний вхід в систему, відновити пароль, або вийти з системи. При повторному входженні необхідно ввести коректний логін та пароль зареєстрованим користувачам, а при виході відбувається від'єднання БД ІС та вихід з програмного комплексу. Підсистема базується на використанні парольного доступу та рольового управління роботою в інформаційній системі.

В результаті проведених досліджень було розроблено інтерфейс користувачів підсистеми управління доступом адміністратора баз даних. Так як підсистема управління доступом є інтегрованою в інформаційну систему, то відповідно головна форма системи має вигляд, що представлений на рис. 3.

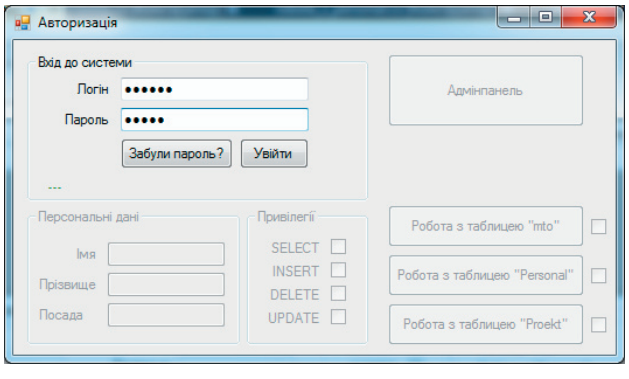


Рис. 3. Вигляд головної форми в момент введення логіну та паролю користувача

Як видно з рис. 3, користувачу пропонується введення логіну та паролю. На головній формі „Авторизація активними є кнопки „Увійти" та „Забули пароль ?". Після введення коректного логіну та паролю,

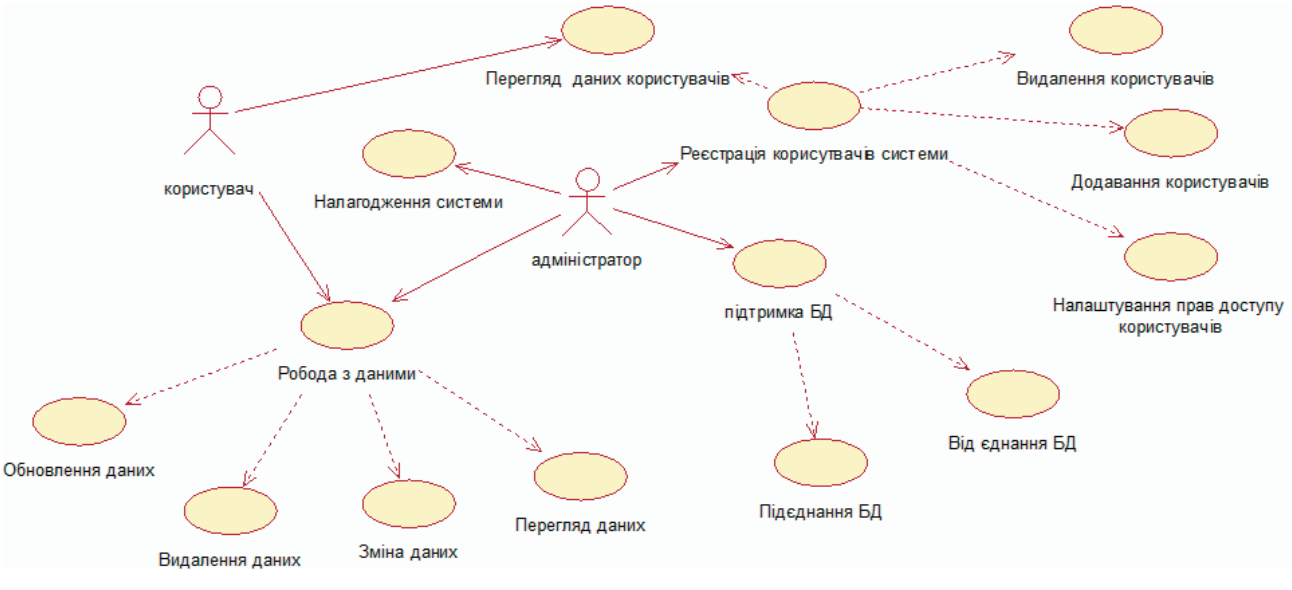


Рис. 2. Діаграма використання інформаційної системи з підсистемою управління доступом адміністратора баз даних

необхідно натиснути кнопку „Увійти”. Як видно з рис. 4, головна форма активізувалась в адмін-режимі.

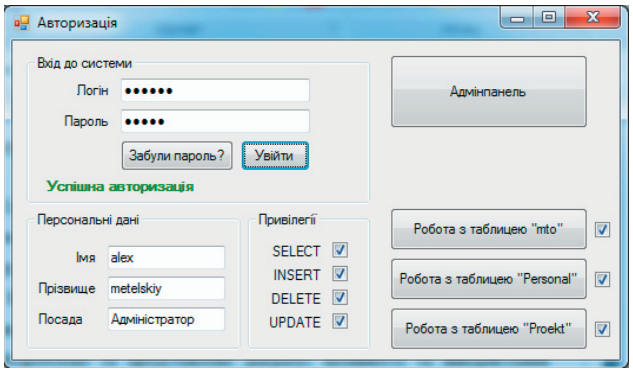


Рис. 4. Вигляд головної форми для адміністратора

Основна форма доповнилась фунціями „Адмінпанель”, „Робота з таблицею mto”, „Робота з таблицею Personal” та „Робота з таблицею Proekt”. Також висвітилось привілеї, що надаються адміністратору, та його персональні дані. Під час запуску роботи з таблицями відкривається вибрана таблиця (рис. 5).

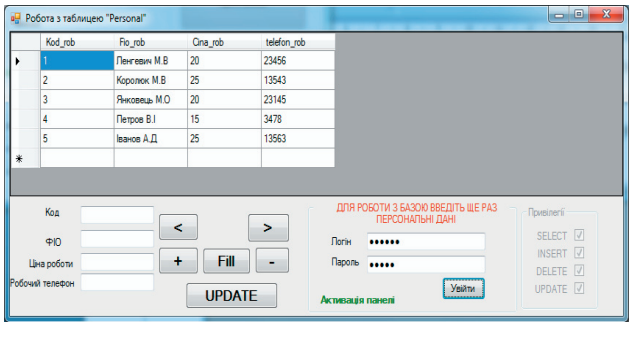


Рис. 5. Вигляд вікна „Робота” з таблицею „Persona”l

Якщо необхідно увійти до „Адмінпанелі”, то відкривається вікно, в якому адміністратор може реєструвати користувачів, надавати їм привілеї та можливість роботи з таблицями. Також адміністратор може видаляти користувачів або змінювати їх персональні дані та привілеї. Зовнішній вигляд „Адмінпанелі” представлений на рис. 6.

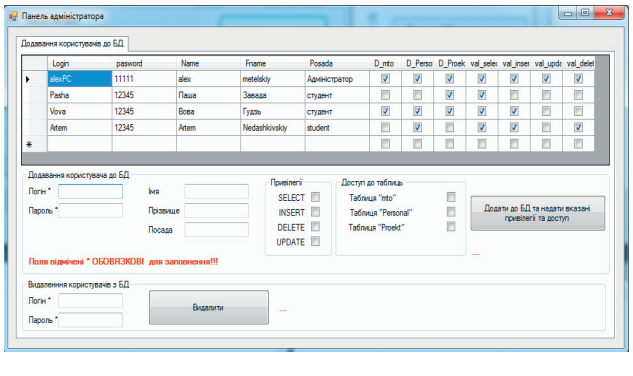


Рис. 6. Вигляд форми „Панель адміністратора”

При заповнені обов’язкових і додаткових полів та при натисканні на „Додати до БД та надати вказані привілеї та доступ”, користувач автоматично додається до БД з вказаними привілеями, доступом і власними даними користувача. При вводі логіна та пароля в полі „Видалення користувача з БД” та натисненні кнопки „Видалити”, користувач автоматично видаляється з даної БД, що значно автоматизує процес роботи адміністратора.

Якщо необхідно увійти в систему з доступом звичайного користувача, то кнопка „Адмінпанель” блокується, а інші, в залежності від привілеїв доступу, відкриваються. Також в системі можна переглянути особисті дані користувача (рис. 7).

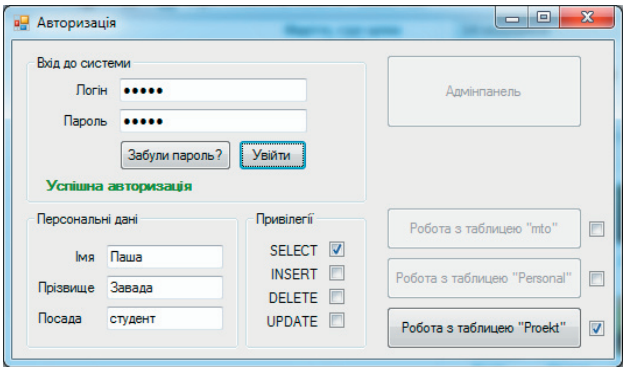


Рис. 7. Вигляд форми „Панель користувача”

В системі передбачена можливість відновлення паролю, якщо користувач випадково його забув. Для цього на головному вікні було створено кнопку „Забули пароль ?”. При натисненні на неї відбувається перехід в діалогове вікно, в якому потрібно ввести дані про користувача. При коректному введені даних на екран виведеться пароль користувача. Вигляд цієї форми показано на рис. 8.

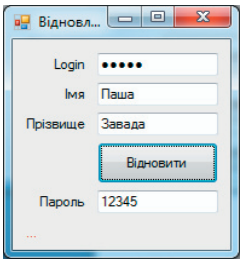


Рис. 8. Вигляд форми відновлення пароля при коректному введенні даних

У випадку, якщо хоч якісь дані про користувача були введені невірні, то пароль не висвітиться, а на формі з’явиться відповідний запис (рис. 9).

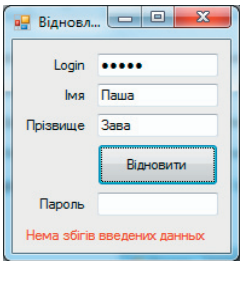


Рис. 9. Вигляд форми відновлення пароля при невірному введенні даних

Одним з найголовніших перевірок працездатності системи – це перевірка налаштувань в самій базі даних (рис. 10).

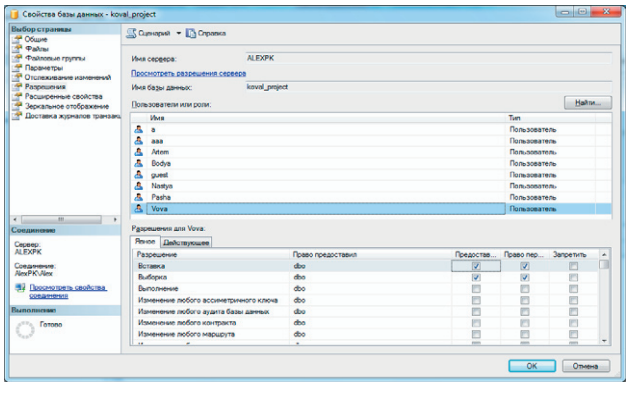

Рис. 10. Перевірка працездатності системи в самій БД

З опису системи видно, що запропонована інформаційна технологія призначена для автоматизації роботи адміністратора щодо управління користувачами інформаційної системи, яка дозволяє легко додавати та видаляти користувачів, змінювати права їх доступу не виконуючи при цьому численні дії в командному рядку.

## 4. Висновки

В результаті досліджень було проведено аналіз технології розробки підсистеми управління доступом адміністратора баз даних, в результаті якого визначено особливості побудови такого роду систем та технології реалізації підсистем управління. Було запропоновано засоби авторизації контролю доступу легальних користувачів до ресурсів системи, надаючи кожному з них саме ті права, які були визначені адміністратором, а також контроль можливостей виконання користувачем різних системних функцій. Реалізовано прототип системи із використання системи управління базою даних SQL Microsoft Server 2008 та Microsoft Visual Studio 2010. Розроблено форми для процедури ідентифікації користувачів підсистеми управління доступом адміністратора баз даних. Проведено налаштування прав доступу користувачів до інформаційних ресурсів інформаційної системи.

Література


1. Корченко, О. Г. Системи захисту інформації [Текст] : монографія / О. Г. Корченко. – К. : НАУ, 2004. – 264 с.
2. Chen, P. P. The Entity-Relationship Model: Toward a Unified View of Data / P. P. Chen // ACM Trans. On Database Syst. – 1976. – V.1, №1. – P. 9-36.
3. Codd, E. F. A relational model of data large shared data banks / E. F. Codd // Comm. ACM. – 1970. – V.13, №6. – P. 377-387.
4. Кавун, С. В. Информационная безопасность в бизнесе [Текст] : научное издание / С. В. Кавун. – Харьков: ХНЭУ, 2007. – 408 с.
5. Коннолли, Т. Базы данных. Проектирование, реализация и сопровождение. Теория и практика [Текст] : пер. с англ. / Т. Коннолли, К. Бегг. – 3-е изд. – М. : Изд. дом „Вильямс, 2003. – 1440 с.
6. Дейт, К. Дж. Введение в системы баз данных [Текст] : пер. с англ. / К. Дж. Дейт. – 8-е изд. – М. : Изд. дом „Вильямс, 2005. – 1328 с.
7. Хомоненко, А. Д. Базы данных [Текст] : учебник для высш. учеб. заведений / А. Д. Хомоненко, В. М. Цыганков, М. Г. Мальцев; под ред. проф. А. Д. Хомоненко. – 4-е изд., доп. и перераб. – СПб. : Изд. дом „КОРОНА-принт”, 2004. – 736 с.
8. Харрингтон, Дж. Л. Проектирование реляционных баз данных [Текст] / Дж. Л. Харрингтон. – М.: Изд-во „Лори, 2006. – 232 с.
9. Поповский, В. В. Защита информации в телекоммуникационных системах [Текст]: ученик в 2-х томах / В. В. Поповский, А. В. Персиков. – Харьков: ООО „Компания СМИТ, 2006. – Т.2. – 292 с.
10. Грибунин, В. Г. Комплексная система зашиты информации на предприятии [Текст] : учеб. пособие для студ. высш. учеб. заведений / В. Г. Грибунин, В. В. Чудовский. – М.: Изд. центр „Академия, 2009. – 416 с.