МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кафедра Комп'ютерних систем та мереж

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

Жуков І.А.

«_____» _____ 2020 р.

ДИПЛОМНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ

"МАГІСТР"

Тема: «Корпоративна комп'ютерна мережа підприємства»

Виконавець: Мельниченко Денис Вікторович

Керівник: Дрововозов Володимир Іванович

Нормоконтролер: Андреєв Володимир Ілліч

Київ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії

Кафедра комп'ютерних систем та мереж

Спеціальність 123 «Комп'ютерна інженерія»
(шифр, найменування)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Жуков І.А.
« » жовтня 2020 р.

ЗАВДАННЯ

на виконання дипломної роботи

Мельниченка Дениса Вікторовича
(прізвище, ім'я, по батькові)

1. Тема роботи: Корпоративна комп'ютерна мережа підприємства
затверджена наказом ректора від 02. 10. 2019 р. № 2258/ст.

2. Термін виконання роботи: з 05 жовтня 2020 р. по 31 грудня 2020 р.

3. Вихідні данні до роботи: 1. Розглянути особливості побудови та функціонування корпоративної комп'ютерної мережі підприємства. 2. Визначити структуру бази даних для підприємства. 3. Розглянути корпоративну мережу для системи управлінського обліку підприємства. 4. Розглянути засоби підвищення ефективності функціонування корпоративної системи.

4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
1. Аналіз вимог до корпоративної комп'ютерної мережі підприємства. 2. Структура бази даних для підприємства. 3. Корпоративна мережа для системи управлінського обліку підприємства. 4. Засоби підвищення ефективності функціонування корпоративної системи.

5. Перелік обов'язкового графічного матеріалу: 1.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Узгодити завдання з керівником дипломної роботи	05.10.20	
2.	Вивчити науково-технічну літературу за темою дипломної роботи	05.10.20-09.10.20	
3.	Зробити аналіз вимог до корпоративної комп'ютерної мережі підприємства	10.10.20-17.10.20	
4.	Визначити структуру бази даних для підприємства	18.10.20-28.10.20	
5.	Розглянути корпоративну мережу для системи управлінського обліку підприємства	29.10.20-24.11.20	
6.	Визначити засоби підвищення ефективності функціонування корпоративної системи.	25.11.20-14.12.20	
7.	Оформити текстові і графічні матеріали дипломної роботи	07.12.20-14.12.20	
8.	Підготувати презентацію по дипломній роботі	07.12.20-14.12.20	
9.	Представити дипломну роботу на кафедру	17.12.20	

Студент _____ /Мельниченко Д.В./

Керівник дипломної роботи _____/Дрововозов В.І./

7. Дата видачі завдання 05.10.2020 р.

Керівник _____ Дрововозов В.І.
(підпис)

Завдання прийняв до виконання _____ Мельниченко Д.В.

Дата 05.10.2020 р.

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Корпоративна комп'ютерна мережа підприємства», загальним обсягом 99 с., рисунків 11, таблиць 11, джерел літератури 33.

КОРПОРАТИВНА КОМП'ЮТЕРНА МЕРЕЖА ПІДПРИЄМСТВА, УПРАВЛІНСЬКИЙ ОБЛІК, АУДИТОРСЬКА КОМПАНІЯ, КОРПОРАТИВНА СИСТЕМА УПРАВЛІНСЬКОГО ОБЛІКУ, СХОВИЩЕ ДАНИХ, МЕРЕЖЕВЕ ОБЛАДНАННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА

Актуальність теми. Задачі підвищення ефективності компонентів комп'ютерної мережі підприємства, сховища даних, мережеве обладнання, інформаційна безпека, є актуальними.

Об'єкт та предмет дослідження. Корпоративна комп'ютерна мережа підприємства управлінського обліку для аудиторської компанії. Методи та системи, що використовуються для автоматизації управлінського обліку, і які можна застосувати до аудиторської компанії, засоби та методи підвищення ефективності функціонування корпоративної комп'ютерної мережі підприємства.

Мета дипломної роботи. Вирішення проблеми автоматизації управлінського обліку аудиторської компанії через побудову інформаційно-управляючої системи підприємства та підвищення ефективності функціонування корпоративної комп'ютерної мережі підприємства, системи управлінського обліку аудиторської компанії.

Методи дослідження. Методи аналітичних оглядів і аналізів початкових даних для побудови корпоративної комп'ютерної мережі підприємства, системи управлінського обліку аудиторської компанії. Аналізи вибору структури бази даних та корпоративної мережі головного офісу підприємства та його філіалів для системи управлінського обліку, питання інформаційної безпеки корпоративної системи управлінського обліку, засоби та методи підвищення ефективності функціонування корпоративної системи.

Матеріали дипломної роботи рекомендується використовувати при розробці корпоративної комп'ютерної мережі підприємства.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

ККМП	–	Корпоративна комп’ютерна мережа підприємства
КСУОАК	–	Корпоративна система управлінського обліку аудиторської компанії
УОАК	–	Управлінський облік аудиторської компанії
СУБД	–	Система управління базами даних
БД	–	База даних
VPN (Virtual Private Network)	–	Віртуальна приватна мережа
CSMA/CD	–	*Carrier Sense Multiple Access with Collision Detection*, множинний доступ із прослуховуванням несучої й дозволом колізій
ПЗ	–	Програмне забезпечення
СОА	–	Сервіс-орієнтована архітектура
ПЗ	–	Програмне забезпечення
РООСБД	–	Розподілена об'єктно – орієнтована система баз даних
ФОЗ	–	Файловий об'єкт зберігання
УООМД	–	Узагальнена об'єктно - орієнтована модель даних

ВСТУП

Найважливішою складовою при побудові корпоративних комп’ютерних мереж є аналіз функціонування комп’ютерних мереж підприємства та висування вимог до них.

Однією зі сфер діяльності підприємств та організацій є надання аудиторських послуг. В якості даного підприємства можна розглядати аудиторську компанію.

Аудиторська діяльність – це безпосередня самостійна, систематична, на власний ризик підприємницька діяльність щодо надання аудиторських послуг із метою отримання прибутку, яка здійснюється фізичними і юридичними особами, зареєстрованими як суб'єкти підприємницької діяльності у порядку, встановленому законодавством.

Основними нормативними документами, що визначають головні засади аудиторської діяльності підприємства, є Закон України "Про аудиторську діяльність", Національні стандарти аудиту та Кодекс професійної етики аудиторів України.

Згідно з Законом України «Про аудиторську діяльність», до аудиторської діяльності належить організаційне і методичне забезпечення аудиту, практичне виконання аудиторських перевірок (аудиту) та надання інших аудиторських послуг.

Національне законодавство обмежує рамки аудиту аудитом фінансової звітності, всі інші перевірки належать до аудиторських послуг.

Згідно з Законом України "Про аудиторську діяльність", аудит — це перевірка публічної бухгалтерської звітності, обліку, первинних документів та іншої інформації щодо фінансово-господарської діяльності суб'єктів господарювання з метою визначення достовірності їхньої звітності, обліку, його повноти і відповідності чинному законодавству та встановленим нормативам. При цьому закон уточнює, що публічна бухгалтерська звітність складається з аудиторського висновку, балансу, звіту про фінансові результати, іншої звітності в межах відомостей, які не становлять комерційної таємниці й визначені законодавством для надання користувачам та публікації.

Аналогічне поняття аудиту трактується Національними стандартами аудиту. Отже, аудит, згідно з чинним національним законодавством за об'єктом дослідження зводиться до аудиту фінансової звітності, а за суб'єктом він може бути тільки зовнішнім, тобто здійснюватися незалежним аудитором або аудиторською фірмою на договірній основі. За ініціативою здійснення аудит може бути обов'язковим, проведення якого регламентується чинним законодавством, та добровільним, коли аудит проводиться з ініціативи клієнта.

Підвищення вимог до темпів та якості надання аудиторських послуг, ускладнення фінансової діяльності компаній, з якими співпрацює аудиторська фірма, а також вимоги законодавства викликають значне збільшення обсягів робіт по організації та управлінню діяльністю аудиторської фірми. При управлінні організацією актуальними є проблеми сумісності підсистем планування, поточного надання послуг, обліку та управління.

Не вирішеним є коло питань, що відносяться до автоматизації планування, ціноутворення та обліку людино-годин при наданні аудиторських послуг, а також здійснення фінансового аналізу щодо успішності діяльності аудиторської компанії. Дані процеси і є складовими частинами управлінського обліку.

Вибір засобів для удосконалення процесу автоматизації управлінського обліку саме аудиторської компанії (підприємства, організації), з притаманними даному виду діяльності особливостями є актуальною задачею. Деякі аудиторські компанії використовують самостійно розроблені продукти, деякі для розрахунків використовують *Microsoft Excel*. Звичайно, аудиторська компанія може пристосувати до своїх потреб такі комплексні програмні засоби управління діяльністю, як *Oracle Business Suite* або *SAP*, але вартість таких програм дуже висока для аудиторського бізнесу, і не зможе окупитися.

Вказані обставини визначають актуальність та практичне значення теми даної роботи, що орієнтована на комплексне вирішення проблеми автоматизації управлінського обліку аудиторської компанії.

Метою роботи є вирішення проблеми автоматизації управлінського обліку аудиторської компанії через побудову інформаційно-управляючої системи

підприємства до складу якого входить корпоративна мережа, підвищення ефективності функціонування корпоративної системи управлінського обліку аудиторської компанії. Дана система повинна спростити процеси ціноутворення та розрахунку фінансових результатів, і прибрати недоліки, пов'язані зі збором з різних облікових джерел інформації, що використовується для управлінського обліку.

Об’єктом дослідження є типова аудиторська компанія, що надає послуги з перевірки правильності ведення бухгалтерського обліку, застосування податкового та господарського законодавства, надання юридичних консультацій, ведення бухгалтерського обліку інших підприємств.

Предмет дослідження – методи та системи, що використовуються для автоматизації управлінського обліку, і які можна застосувати до аудиторської компанії.

Завдання дослідження:

1. Системний аналіз проблем автоматизації, дослідження особливостей роботи аудиторських компаній, а також структури інформаційних потоків всередині компанії.

2. Аналіз вимог до бази даних управлінського обліку з урахуванням особливостей роботи аудиторської компанії, вибір виду бази даних.

3. Вивчення особливостей побудови бази даних обраного виду, підбір оптимального програмного забезпечення для функціонування бази даних.

4. Розробка моделі корпоративної мережі для системи управлінського обліку з урахуванням вимог, що висуваються до структури мережі та обладнання програмним забезпеченням бази даних.

5. Підбір обладнання для технічної реалізації корпоративної мережі..

6. Вивчення вимог до інформаційної безпеки системи управлінського обліку, що висуваються особливостями роботи аудиторської компанії.

7. Розробка системи захисту інформації в системі управлінського обліку аудиторської компанії з метою підвищення ефективності функціонування системи.

РОЗДІЛ 1
АНАЛІЗ ВИМОГ ДО КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

1.1. Мета, основні завдання і особливості функціонування системи

Однією зі сфер діяльності підприємств та організацій є надання аудиторських послуг. В якості даного підприємства можна розглядати аудиторську компанію.

Велика частина інформації, на підставі якої щодня приймаються рішення, з'являється неформальним шляхом. Керуючий спілкується з підлеглими, розмовляє з колегами і клієнтами, читає газети і ділові періодичні видання. З цих джерел він дізнається багато корисного, але цієї інформації далеко недостатньо для прийняття рішень по управлінню справами маленькою організації. Кількість інформації, що з'являється в результаті діяльності організації і має вплив на успіх ведення справ, а також швидкість, з якої ця інформація змінюється, робить необхідним для керівництва застосування формальних методів збору і обробки інформації.

Корпоративна система управлінського обліку визначається як формальна система для видачі адміністрації інформації, необхідної для прийняття управлінських рішень. До такої інформації входить:

– інформація щодо клієнтів: їх кількість, сфера діяльності, кількість наданих послуг кожному клієнту, вартість послуги для конкретного клієнта, специфіка питань, з якими звертається клієнт;

– інформація щодо постачальників: їх кількість, види продукції та послуг, що постачаються, вартість закупленої продукції та послуг, обсяги закупівель;

– інформація щодо послуг: асортимент послуг, що надається, в цілому, а також в розрізі департаментів, вартість послуги, кількість людино-годин, що витрачається на надання послуги;

– інформація щодо персоналу: загальна кількість, кількість в розрізі департаментів, професій, оплата праці, погодинні ставки роботи для клієнта.

Загальною метою корпоративної системи управлінського обліку є полегшення ефективного виконання функцій планування, контролю діяльності з надання послуг та процесу управління в цілому. Найважливішим її завданням є видача потрібної інформації потрібним людям в потрібний час, а також розрахунок показників ефективності роботи компанії.

Необхідно відзначити, що корпоративна система управлінського обліку не є єдиною всеосяжною інтегрованою системою для задоволення всіх потреб адміністрації в інформації. Така система організації складається з низки інформаційних систем різних виробників та різного призначення, кожна з яких служить для прийняття рішень в деякій конкретної області.

Коло конкретних завдань, розв'язуваних у результаті створення сучасної системи управлінського обліку, включає:

– об'єднання в єдиний інформаційний простір територіально віддалених один від одного об'єктів і підрозділів компанії;

– високошвидкісну передачу по каналах зв'язку будь-яких видів інформаційних потоків;

– підтримку діяльності всіх підрозділів та об'єктів компанії;

– автоматизацію всіх бізнес-процесів компанії, оперативний контроль і управління процесами надання послуг, взаєморозрахунків зі споживачами і постачальниками, управління персоналом;

– створення єдиного інформаційного простору для технологічних і бізнес-систем, створення єдиної бази знань компанії;

– впровадження корпоративних стандартів і використання єдиної технології обробки інформації на всіх рівнях управління;

– впровадження систем електронного документообігу, що дозволяє раціонально організувати внутрішні і зовнішні інформаційні потоки;

– організацію чіткого персонального контролю за виконанням наказів, доручень;

– потужні засоби обробки і аналізу отриманої інформації, розрахунок планової і фактичної собівартості послуг;

– забезпечення необхідного рівня безпеки та захисту інформаційних ресурсів корпорації.

Головним підсумком впровадження корпоративної системи управлінського обліку повинно стати створення в компанії ефективного і дієвого механізму аналізу економічних показників та управління, що охоплює бізнес-процеси – планування, фінансової діяльності, роботи з клієнтами, маркетинг, кадрові. В результаті цього компанія виходить на якісно новий рівень управління і планування своєї діяльності.

Аналіз вимог до системи управлінського обліку має на меті оцінити ділову значимість інформаційно-технологічних рішень, визначити головні цілі і вибрати пріоритети для окремих частин комп'ютерної системи.

Для виконання аналізу вимог до корпоративної системи необхідно:

– визначити цілі та вигоди від корпоративної системи;

– оцінити поточний стан системи управлінського обліку та вимоги, що накладаються на систему особливостями функціонування аудиторської компанії;

– оцінити поточний стан документообігу компанії та визначитися з вимогами до його розвитку;

– визначити структуру системи управлінського обліку;

– оцінити поточний стан локальних мереж і парку комп'ютерів на підприємстві, що допоможе виявити проблеми, які потребують вирішення;

– визначитися з мережними технологіями, що будуть використані для розвитку корпоративної мережі;

– визначитися з обладнанням, яке має бути добавлено в мережу для її ефективного функціонування;

– визначитися з системою безпеки, що має бути запроваджена.

Загальні вимоги, яким повинна відповідати інформаційна система, полягають в гнучкості, інформаційній сумісності, надійності, ефективності та безпеці:

1. Гнучкість, здатність до адаптації і подальшого розвитку передбачає можливість пристосування інформаційної системи до нових умов, нових потреб підприємства. Виконання цих умов можливо, якщо на етапі розробки інформаційної системи використовуються загальноприйняті засоби і методи документування, так що по закінченні певного часу зберігається можливість розібратися в структурі системи і внести до неї відповідні зміни, навіть якщо всі розробники або їх частина з якихось причин не зможуть продовжити роботу.

2. Інформаційна сумісність передбачає взаємодію інформаційних систем, що вже існують в компанії. Сюди відноситься можливість обміну даними між системами бухгалтерського обліку, документообігу, обліку персоналу, базами даних, системою здавання електронної звітності, електронною поштою, а також можливість вивантаження інформації в формати *XML*, текстовий, електронні таблиці.

3. Надійність інформаційної системи передбачає її функціонування без спотворення інформації, втрати даних "з технічних причин". Вимога надійності забезпечується створенням резервних копій збереженої інформації, виконання операцій протоколювання, підтриманням якості каналів зв'язку і фізичних носіїв інформації, використанням сучасних програмних і апаратних засобів. Сюди ж слід віднести захист від випадкових втрат інформації внаслідок недостатньої кваліфікації персоналу.

4. Ефективність системи – її здатність вирішувати покладені на неї завдання в мінімальні терміни.

5. Безпека - властивість системи, в силу якої сторонні особи не мають доступу до інформаційних ресурсів організації, крім тих, які для них призначені. Система, яка не відповідає вимогам безпеки, може завдати шкоди інтересам замовника, насамперед майновим. Вимога безпеки забезпечується сучасними засобами

розробки інформаційних систем, сучасною апаратурою, методами захисту інформації, застосуванням паролів і протоколюванням, постійним моніторингом стану безпеки операційних систем і засобів їх захисту.

1.2. Особливості роботи аудиторської компанії. Структура інформаційних потоків

Понятійний інструментарій аудиторської діяльності за Законом України «Про аудиторську діяльність» надано на рис. 1.1.

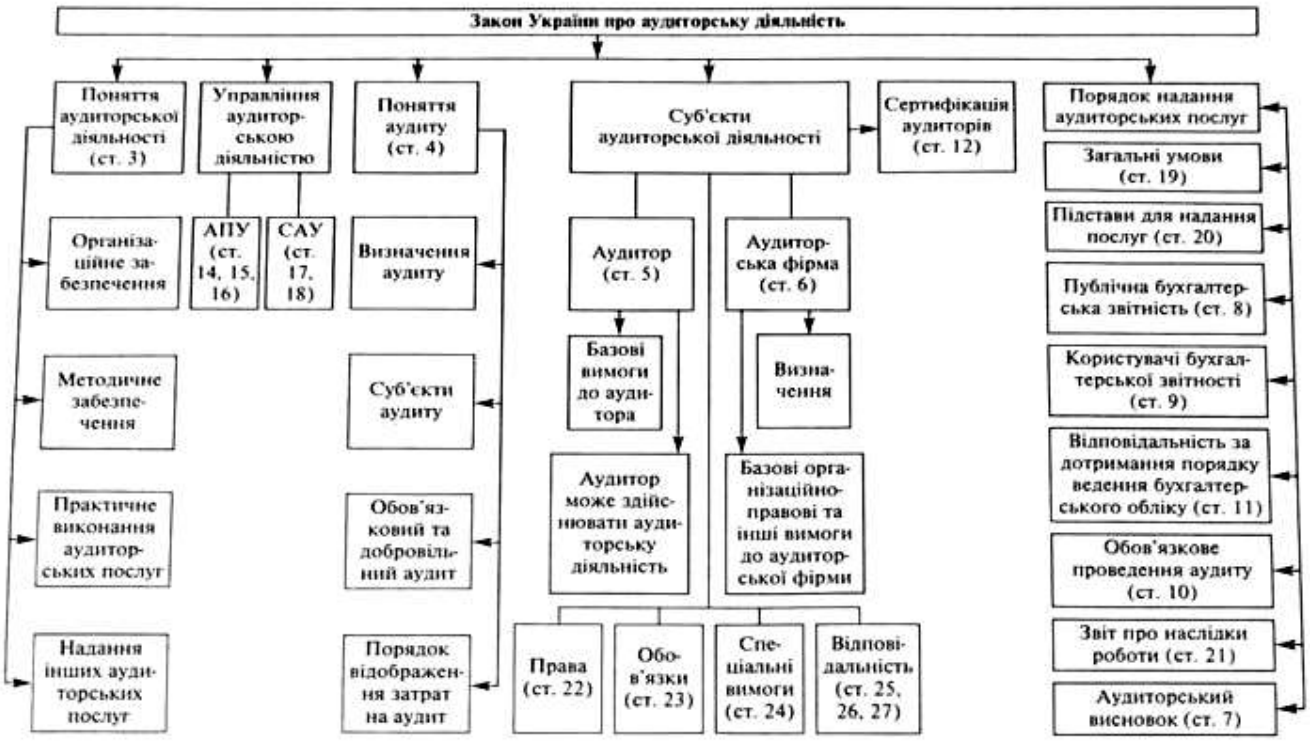

Рис. 1.1. Понятійний інструментарій аудиторської діяльності за Законом України «Про аудиторську діяльність»

Аналіз потоків інформації - найважливіший етап в раціоналізації існуючої системи управління, який повинен забезпечити виконання цільових завдань проектування інформаційної системи.

Аналіз існуючих процесів управління може бути здійснено перш всього на базі дослідження існуючої інформаційної системи підприємства, яка характеризується

наявністю існуючої схеми документообігу, системи економічних показників діяльності підприємства, структурним складом підрозділів, які беруть участь у процесі управління, і інтенсивністю потоків даних, циркулюючих між ними.

Робота аудиторської компанії полягає в наданні клієнтам таких послуг:

- аудит фінансової та податкової звітності;

- консультування з питань ведення бухгалтерського обліку;

- консультування з питань податкового законодавства;

- консультування з питань господарського та цивільного права;

- супроводження клієнта в судових справах з контрагентами та податковими органами;

- послуги ведення бухгалтерського обліку.

Для здійснення діяльності структура аудиторської компанії налічує такі департаменти:

1. Керівництво аудиторської компанії. Функції:

- визначення напрямів розвитку компанії;
- встановлення внутрішніх правил роботи;
- прийняття стратегічних та тактичних рішень, необхідність яких виникає в ході діяльності компанії.

2. Департамент аудиту. Функції:

- аудит суб'єктів виробничої діяльності (підприємства, що виробляють продукцію або надають послуги);
- аудит суб'єктів комерційної господарської діяльності (оптові та роздрібні торговельні підприємства);
- аудит суб'єктів некомерційної господарської діяльності (благодійні фонди, громадські організації);
- аудит банків;
- аудит небанківських фінансових установ (страхові компанії, ломбарди, інвестиційні фонди).

3. Департамент надання аудиторських послуг. Функції:

– інформаційно-консультаційне обслуговування суб'єктів господарської діяльності;

– інформаційно-консультаційне обслуговування банків та небанківських фінансових установ;

– навчання з питань організації та ведення бізнесу.

4. Департамент правового забезпечення. Функції:

– корпоративні відносини і договірне супроводження (складання договорів, перевірка договорів на невигідні для клієнта та неоднозначні положення);

– судово-претензійна діяльність та представництво (складання претензій, заперечень на акти податкової інспекції, судових позовів, представництво інтересів клієнта в судах);

– правові дослідження та експертизи.

5. Департамент науково-економічного забезпечення розвитку бізнесу. Функції:

– аналітика та прогнозування розвитку бізнесу;

– економічні дослідження та фінансовий менеджмент;

– наукове, методичне та організаційне забезпечення аудиту.

6. Департамент бухгалтерського обліку. Функції:

– ведення бухгалтерського обліку клієнтів, що не мають власної бухгалтерії та уклали угоду про ведення обліку з аудиторською компанією.

7. Департамент забезпечення діяльності фірми. Функції:

– закупівля канцтоварів, оргтехніки та інших предметів та засобів для діяльності компанії;

– організація відряджень, бронювання місць в готелях, замовлення квитків;

– ведення бухгалтерського та управлінського обліку аудиторської компанії;

– підбір персоналу.

Для створення, обробки документів та документообігу аудиторська компанія використовує такі програмні засоби:

– операційна система *Windows Server 2003* – для роботи серверів та робочих станцій департаменту бухгалтерського обліку;

− операційна система *Windows XP* – для роботи комп'ютерів персоналу всіх інших департаментів;

− *Microsoft Word* – для створення текстових документів: листів, наказів, аудиторських висновків, допоміжної аудиторської інформації;

− *Microsoft Excel* – для допоміжних аудиторських розрахунків, для підрахунку ефективності окремих бізнес-процесів, роботи з клієнтом, взагалі для підрахунку ефективності та прибутковості діяльності компанії;

− *Microsoft Outlook* – для обміну документами та інформацією як в середині компанії, так і з зовнішніми джерелами та отримувачами інформації;

− 1С:Підприємство 7.7 та 8.0 – для ведення бухгалтерського обліку клієнтів та власного бухгалтерського обліку аудиторської компанії;

− *Microsoft SQL Server* – для роботи мережних версій 1С: Підприємство;

− Ліга Закон – для отримання законодавчих та нормативних документів органів влади, а також консультацій з питань права, оподаткування та бухгалтерського обліку,

− Бест Звіт – для здавання електронної звітності в податкову інспекцію.

В документообігу аудиторської компанії беруть участь документи внутрішні та зовнішні. В табл. 1.1 показано, які департаменти та програмні засоби задіяні в процесі створення та обробки різних видів документів.

Таблиця 1.1.

Департаменти та програмні засоби, що задіяні в процесі створення та обробки документів аудиторської компанії

Вид документа	Програмний засіб, що задіяний при створенні та обробці	Використання паперових документів	Документ створюється	Документ використовується
Внутрішні документи:				
наказ	*Microsoft Word, Microsoft Outlook*	Так	керівництво	всі департаменти
розпорядження	*Microsoft Word, Microsoft Outlook*	Так	керівництво	всі департаменти
правила	*Microsoft Word*	Так	підготовка –	всі департаменти

внутрішнього розпорядку			департамент забезпечення діяльності, затвердження - керівництво	
інформаційні листи	*Microsoft Outlook*	Ні	всі департаменти	всі департаменти
документи управлінського обліку	*Microsoft Word, Microsoft Excel, Microsoft Outlook,* 1С:Підприємство	Так	департамент науково-економічного забезпечення розвитку бізнесу	Керівництво
Зовнішні вхідні документи:				
листи	*Microsoft Outlook, Microsoft Excel*	Так	зовнішні контрагенти	будь-який з департаментів, в залежності від теми листа
документи клієнтів, що надаються для ведення бухгалтерського обліку або аудиту	*Microsoft Outlook,* 1С:Підприємство	Так, надходять переважно в паперовому вигляді	зовнішні контрагенти	департаменти бухгалтерського обліку, аудиту, аудиторських послуг, правового забезпечення
договори	*Microsoft Excel,* 1С:Підприємство	Так	зовнішні контрагенти	департамент забезпечення діяльності, правовий департамент, керівництво
рахунки на оплату	*Microsoft Outlook,* 1С:Підприємство	Так	зовнішні контрагенти	департамент забезпечення діяльності, керівництво
акти виконаних робіт та накладні	1С:Підприємство	Так	зовнішні контрагенти	департамент забезпечення діяльності
Зовнішні вихідні документи:				
листи	*Microsoft Word, Microsoft Outlook*	Так	будь-який департамент	зовнішні контрагенти
бухгалтерська звітність	1С:Підприємство, Бест Звіт	Так	департамент бухгалтерсько	зовнішні контрагенти

			го обліку	
аудиторські висновки	*Microsoft Word*, *Microsoft Excel*, Ліга Закон	Так	департамент аудиту	зовнішні контрагенти
консультаційні документи	*Microsoft Word*, *Microsoft Excel*, *Microsoft Outlook*, Ліга Закон	Так	департаменти аудиторських послуг, правового забезпечення	зовнішні контрагенти
договори	*Microsoft Word*, *Microsoft Excel*, 1С:Підприємство	Так	департамент забезпечення діяльності, правових послуг, керівництво	зовнішні контрагенти
рахунки на оплату	*Microsoft Outlook*, 1С:Підприємство	Так	департамент забезпечення діяльності	зовнішні контрагенти
акти виконаних робіт	1С:Підприємство	Так	департамент забезпечення діяльності	зовнішні контрагенти

З таблиці видно, що документи переважно створюються та обробляються програмами *Microsoft Word* та *Microsoft Excel*, надсилаються отримувачам через *Microsoft Outlook*.

Для ведення бухгалтерського обліку використовуються програми 1С:Підприємство.

Дані для аналітичних розрахунків, що необхідні для управлінського обліку, частково беруться з програм 1С:Підприємство, шляхом вивантаження в *Microsoft Excel*, частково – з паперових джерел. Автоматизація управлінського обліку здійснюється лише за допомогою зв'язування електронних таблиць *Microsoft Excel* та налаштування формул.

1.3. Структура та особливості функціонування системи управлінського обліку аудиторської компанії

У складі корпоративних інформаційних систем можна виділити дві незалежні складові:

- комп'ютерна інфраструктура організації, що представляє собою сукупність мережної, телекомунікаційної, програмної, інформаційної та організаційної інфраструктури є корпоративною мережею, котра являє собою найважливішою складовою підприємства, тобто аудиторської компанії;

- взаємопов'язані функціональні підсистеми, які забезпечують вирішення завдань організації і досягнення її цілей.

Перша складова відображає системно-технічний, структурний бік будь-якої інформаційної системи. По суті, це основа для інтеграції функціональних підсистем, що повністю визначає властивості інформаційної системи, її успішну експлуатацію.

Друга складова корпоративної інформаційної системи цілком відноситься до прикладної області і в значній мірі залежить від специфіки завдань і цілей підприємства. Дана складова повністю базується на комп'ютерній інфраструктурі підприємства та визначає прикладну функціональність інформаційної системи.

Взаємозв'язки між двома зазначеними складовими інформаційної системи досить складні. З одного боку, ці дві складові в певному сенсі незалежні. Наприклад, організація мережі і протоколи, які використовуються для обміну даними між комп’ютерами, абсолютно не залежать від того, які методи і програми планується застосовувати на підприємстві для організації бухгалтерського обліку.

З іншого боку, зазначені складові все ж залежать одна від одної. Функціональні підсистеми в принципі не можуть існувати без комп'ютерної інфраструктури. В той же час комп'ютерна інфраструктура сама по собі досить обмежена, оскільки не володіє необхідною функціональністю. Неможливо експлуатувати розподілену інформаційну систему при відсутності мережевої інфраструктури. Хоча, маючи розвинену інфраструктуру, можна надати співробітникам організації ряд корисних загальносистемних служб (наприклад, електронну пошту і доступ в Інтернет), що спрощують роботу і роблять її більш ефективною (зокрема, за рахунок використання більш розвинених засобів зв'язку).

Таким чином, розробку інформаційної системи доцільно починати з побудови комп'ютерної інфраструктури (корпоративної мережі) як найбільш важливою складової, що спирається на апробовані промислові технології і гарантовано реалізованої в розумні терміни в силу високого ступеня визначеності як постановці завдання, так і в пропонованих рішень.

Функціональні підсистеми, на відміну від корпоративної мережі, мінливі по своїй природі, так як у предметній області діяльності організації постійно відбуваються більш або менш істотні зміни. Функціональність інформаційних систем сильно залежить від організаційно-управлінської структури організації, її функціональності, розподілу функцій, прийнятих в організації фінансових технологій і схем, існуючої технології документообігу і багатьох інших факторів.

Функціональна підсистема корпоративної системи управлінського обліку має будуватись на принципах, що були сформульовані академіком В.М. Глушковим:

1. Автоматизація документообігу. Визначальним при цьому є замикання більшості інформаційних потоків між окремими органами управління безпосередньо через комп'ютерну мережу.

2. Інтегральна інформаційна база. Суть даного принципу полягає в тому, що створюється єдина для всіх управлінських завдань первинна база даних з мінімумом надмірності (необхідним для підтримання збереження і цілісності бази). На цю базу замикається система обліку, що здійснює її постійну оперативну актуалізацію. У правильно побудованій системі різні управлінські завдання можуть працювати зі своїми власними локальними базами даних, але організація та підтримка таких баз не повинні вимагати ніякого додаткового введення, оскільки вони формуються і актуалізуються як вторинні бази даних безпосередньо з вихідної (первинної) інтегральної бази.

3. Одноразове введення даних. Даний принцип тісно пов'язаний з попереднім і передбачає, що будь-яка нова інформація вводиться в інтегральну базу для подальшого багаторазового використання без необхідності повторного введення.

4. Динамічна цілісність. Інтегральна база може мати як зосереджений характер, будучи реалізованої на одному сервері, так і розподілений, розміщуючись фактично

на деякій сукупність взаємозалежних серверів. Але в будь-якому випадку повинна забезпечуватися коректність модифікацій бази і взаємна відповідність її частин і локальних реалізацій. При цьому внесення тих чи інших змін у котрусь із частин інтегральної бази має автоматично ініціювати процедури відповідних змін у всіх інших, залежних від неї базах даних. В ідеальному випадку підтримка цілісності забезпечується вже на рівні відповідних програмних засобів і вимагає мінімального втручання людини.

5. Системна єдність. Створення широкої інформаційної системи вимагає обов'язкового опрацювання та узгодження всіх її елементів, в першу чергу таких, як інформаційне наповнення та формати баз даних, процедури актуалізації баз даних і внесення змін в їх структуру, склад комплексу програмних і апаратних засобів, організацію програмних засобів та взаємодія між ними, користувальницькі інтерфейси.

6. Типовість (універсальність і уніфікація). Суть цього принципу полягає в тому, що інформаційна система повинна будуватись на основі широко розповсюджених програмних засобів, щоб в подальшому не виникало проблем щодо оновлення та заміни компонентів системи.

7. Модульність. Дозволяє порівняно легко адаптувати систему до мінливих умов, проводити її помодульний розвиток і вдосконалення.

Враховуючи вищевикладені принципи, система управлінського обліку має складатись з технічних та програмних засобів, що вирішують такі завдання:

1. Об'єднання в єдину мережу головного офісу та територіально виділених підрозділів компанії.

2. Забезпечення передачі потоків інформації як у текстовому та табличному вигляді, так і мультимедійної, що накладає високі вимоги до пропускної здатності мережі.

3. Створення, читання, редагування текстових документів.

4. Сканування та зберігання електронних копій паперових документів, що надходять або створюються на підприємстві.

5. Ведення реєстрів документів, що створюються в аудиторській компанії, або надходять до неї.

6. Ведення бухгалтерського обліку аудиторської компанії.

7. Ведення обліку роботи персоналу за видами робіт, з визначенням погодинної вартості роботи для клієнта.

8. Облік кількості підготовлених аудиторських висновків, наданих консультації з визначенням собівартості кожної такої роботи.

9. Концентрація в одній програмі вартісної бухгалтерської та кількісної аудиторської інформації.

10. Виконання розрахунків ефективності та прибутковості роботи компанії.

11. Можливість переглядати текстові, табличні та скановані документи по виконаній роботі для конкретного клієнта або співробітника компанії, не виходячи з бази даних.

1.4. Висновки за розділом

При системному аналізі проблем автоматизації, дослідження особливостей роботи аудиторських компаній, а також структури інформаційних потоків всередині компанії система управлінського обліку має складатись з технічних та програмних засобів, що вирішують такі завдання: об'єднання в єдину мережу головного офісу та територіально виділених підрозділів компанії, забезпечення передачі потоків інформації як у текстовому та табличному вигляді, так і мультимедійної, що накладає високі вимоги до пропускної здатності мережі, створення, читання, редагування текстових документів, сканування та зберігання електронних копій паперових документів, що надходять або створюються на підприємстві, ведення реєстрів документів, що створюються в аудиторській компанії, або надходять до неї, ведення бухгалтерського обліку аудиторської компанії, ведення обліку роботи персоналу за видами робіт, з визначенням погодинної вартості роботи для клієнта, облік кількості підготовлених аудиторських висновків, наданих консультації з визначенням собівартості кожної такої роботи, концентрація в одній програмі вартісної бухгалтерської та кількісної аудиторської інформації, можливість

переглядати текстові, табличні та скановані документи по виконаній роботі для конкретного клієнта, не виходячи з бази даних, можливість переглядати текстові, табличні та скановані документи по виконаній роботі конкретного співробітника компанії, не виходячи з бази даних, виконання розрахунків ефективності та прибутковості роботи компанії.

РОЗДІЛ 2
СТРУКТУРА БАЗИ ДАНИХ ДЛЯ ПІДПРИЄМСТВА

2.1. Аналіз вимог до бази даних

Основні питання, що потребують вирішення при аналізі вимог:

– чи зможе нова система об'єднати існуючі програми або їх необхідно буде кардинально переробляти для спільної роботи з новою системою;

– які дані використовуються різними програмами; чи зможуть програми спільно використовувати будь-які з цих даних;

– хто буде вводити дані в базу і в якій формі; як часто будуть змінюватися дані;

Згідно аналізу діяльності аудиторської компанії та сформульованих завдань, що мають вирішуватись системою управлінського обліку, розглянуто наявність програмних засобів, за допомогою яких ці завдання планується здійснювати (табл. 2.1).

Взаємозв'язки між існуючими програмами можуть відбуватися таким чином:

1. Програми *Microsoft – Word* та *Excel*, в частині, що стосується таблиць, без проблем здійснюється перенесення інформації шляхом копіювання. Також можливе налаштування гіперпосилань між окремими документами.

2. Програми 1С:Підприємство та 1С:Зарплата та кадри – вже існують в *SQL*-форматі, можливе будь-яке вивантаження даних в іншу *SQL*-базу. Також можливе вивантаження таблиць в *Excel*, звітів – в *XML* та *DBF* формати.

Таким чином, існуюча облікова інформація може трансформуватись та використовуватись в управлінській базі даних. Також, в базу даних має окремо вводитись така інформація:

– реєстри аудиторських висновків, консультацій;

– довідник погодинних розцінок роботи аудиторів;

– дані щодо роботи над завданням (висновком або консультацією): замовник, виконавець, вид завдання, кількість витрачених людино-годин.

Таблиця 2.1.

Наявність програмних засобів для вирішення завдань управлінського обліку

№	Завдання	Вирішується існуючими програмними засобами	Програмні засоби, що мають додаватися
1	Створення, читання, редагування текстових документів	Microsoft Word	Не потрібно
2	Сканування та зберігання електронних копій паперових документів, що надходять або створюються на підприємстві	Вирішення відсутнє	Потрібно запровадження системи електронного документообігу
3	Ведення реєстрів документів, що створюються в аудиторській компанії, або надходять до неї	Microsoft Excel – ведеться лише реєстр, дані для аналізу не використовуються	Потрібно ведення в базі даних з можливістю аналізу та прикріпленням електронних копій
4	Ведення бухгалтерського обліку аудиторської компанії	1С: Підприємство	Не потрібно
5	Ведення обліку роботи персоналу за видами робіт, з визначенням погодинної вартості роботи для клієнта	1С:Зарплата та кадри – ведення нарахування та виплати заробітної плати, відпрацьованого часу	Потрібний облік кількості людино-годин на виконання кожного аудиторського завдання та розцінок на послуги, що виставляються клієнтам
6	Облік кількості підготовлених аудиторських висновків, наданих консультації з визначенням собівартості кожної такої роботи	Вирішення відсутнє, в 1С:Підприємство ведеться лише облік за актами виконаних робіт, деталізація відсутня	Потрібно ведення в базі даних з можливістю прикріплення електронних документів висновків та консультацій
7	Концентрація в одній програмі вартісної бухгалтерської та кількісної аудиторської інформації	Microsoft Excel – вводиться частково з 1С:Підприємство, частково - вручну	Потрібне автоматичне відображення в базі даних
8	Виконання розрахунків ефективності та прибутковості роботи компанії	Microsoft Excel - вручну	Потрібне автоматичне здійснення розрахунків станом на будь-який час
9	Можливість переглядати текстові, табличні та скановані документи по виконаній роботі для конкретного клієнта, не виходячи з бази даних	Вирішення відсутнє	Потрібне запровадження

10	Можливість переглядати текстові, табличні та скановані документи по виконаній роботі конкретного співробітника компанії, не виходячи з бази даних	Вирішення відсутнє	Потрібне запровадження

Такі дані можуть вводитись безпосередньо в базу за наявності відповідного інтерфейсу, або протягом певного періоду накопичуватися в *таблицях Microsoft Excel* та завантажуватися в управлінську базу.

Введені в базу дані не будуть піддаватися подальшим змінам, будуть лише накопичуватись та аналізуватись. Частота аналізу даних:

– щодо ефективності та прибутковості роботи – раз на місяць;

– щодо ціноутворення - потреба може виникати частіше, але не кожен день.

Перелік вимог до бази даних, на основі якої будується корпоративна система управлінського обліку, можна сформулювати таким чином:

– використання великих обсягів даних;

– розміщення в базі історичних даних, які в основному є статичними;

– додавання в систему нових даних відбувається відносно рідко великими блоками (наприклад, раз на місяць завантажуються дані з програм 1С:Підприємство);

– дані, додані в систему, звичайно ніколи не видаляються;

– перед завантаженням дані проходять різні процедури "очищення", пов'язані з тим, що в одну систему можуть надходити дані з багатьох джерел, які мають різні формати подання для одних і тих же понять, дані можуть бути змінені, помилкові;

– невелике число користувачів (аналітики, керівництво);

– запити для аналізу даних не носять наперед завданий та відомий характер; види запитів можуть змінюватись в залежності від економічної ситуації та сьогоденної потреби;

– база обслуговує відносно малу кількість працівників керівної ланки;

– можливість здійснення запитів не лише до даних, що зберігаються в табличному вигляді, а і до документів, формати яких відмінні від формату таблиць бази заних.

2.2. Вибір виду бази даних

2.2.1. Види організації та зберігання даних

Існують такі основні види організації та зберігання даних:

1. Реляційні бази даних.
2. Об'єктно-орієнтовані бази даних.
3. Сховища даних.

Існують також проміжні та гібридні різновиди баз та сховищ даних, але зараз розглянемо основні вищенаведені форми.

Реляційні бази даних - це сукупність відносин, що містять всю інформацію, яка повинна зберігатися в базі даних. Однак користувачі сприймають таку базу даних як сукупність двомірних пов'язаних таблиць.

Властивості таблиці реляційної бази даних:

– кожна таблиця складається з однотипних рядків і має унікальне ім'я;

– рядки мають фіксовану кількість полів і значень (множинні поля і повторювані групи неприпустимі), інакше кажучи, в кожній позиції таблиці на перетині рядка та стовпчика завжди є в точності одне значення або *NULL*;

– рядки таблиці обов'язково відрізняються один від одного хоча б єдиним значенням, що дозволяє однозначно ідентифікувати будь-який рядок;

– стовпцям таблиці присвоюються унікальні імена, і в кожному з них розміщуються однорідні значення даних (дати, прізвища, цілі числа або грошові суми);

– повний інформаційний зміст бази даних подається у вигляді явних значень даних, і такий метод подання є єдиним, зокрема, не існує будь-яких спеціальних "зв'язків" або покажчиків, що з'єднують одну таблицю з іншою;

– таблиці зв'язуються одна з одною за допомогою індексів, що являють собою вказівники на дані, розміщені в реляційній таблиці;

– управління реляційними базами даних здійснюється за допомогою спеціальних мов, найпоширенішою з яких є *SQL* (*Structured Query Language* - структурована мова запитів).

Реляційні системи управління базами даних (СУБД) залишаються одними з найбільш поширених, незважаючи на деякі властиві їм недоліки. Зараз основним предметом критики реляційних СУБД є не їхня недостатня ефективність, а також деяка обмеженість таких систем при використанні в так званих нетрадиційних областях (найбільш поширеними прикладами є системи автоматизації проектування), в яких потрібні дуже складні структури даних. Причому ця обмеженість реляційних СУБД є прямим наслідком їх простоти і проявляється лише в окремих предметних областях.

Об'єктно-орієнтовані бази даних - характерний об'єктно-орієнтований підхід, розподіл даних, наявність активного сервера баз даних, мови програмування четвертого покоління, фрагментація і паралельна обробка запитів, технології тиражування даних, багатопотокова архітектура та інші революційні досягнення в області обробки даних.

Об'єктно-орієнтований підхід має ряд переваг для розробника, з яких можна відзначити наступні:

– можливість розбити систему на сукупність незалежних сутностей (об'єктів) і провести їх сувору незалежну специфікацію;

– простота еволюції системи за рахунок таких елементів об'єктного підходу як спадкування і поліморфізм;

– можливість об'єктного моделювання системи, що дозволяє простежити поведінку реальних сутностей предметної області вже на ранніх стадіях розробки.

– можливість безпосереднього зберігання та використання об'єктів, не розкладаючи їх по таблицях;

– типи даних визначаються розробником і не обмежені набором визначених типів.

При занесенні складного об'єкта в реляційну базу обов'язкова процедура декомпозиції його даних для того, щоб розмістити їх в таблицях. При читанні об'єкта з реляційної бази він збирається з окремих елементів і тільки потім може використовуватися. У об'єктних СУБД дані об'єкту, а також методи зміни цих даних зберігаються у сховищі як єдине ціле.

Використання об'єктної моделі представлення даних (і, відповідно, об'єктно-орієнтованої СУБД) найбільш привабливо для інформаційних систем корпоративного рівня, розробка яких ведеться методами об'єктного проектування.

Сховища даних - предметно-орієнтовані, прив'язані до часу та незмінні зібрання даних для підтримки процесу прийняття управлінських рішень.

Основні риси сховищ даних:

1. Предметна орієнтованість. Інформація в сховищі даних організована у відповідності з основними аспектами діяльності підприємства (замовники, продажі, склад і т.п.); це відрізняє сховище даних від оперативної БД, де дані організовані відповідно до процесів (виписка рахунків, відвантаження товару і т.п.). Предметна організація даних у сховищі сприяє як значному спрощенню аналізу, так і підвищенню швидкості виконання аналітичних запитів.

2. Інтегрованість. Вихідні дані витягуються з оперативних БД, перевіряються, очищаються, приводяться до єдиного вигляду, в потрібному ступені агрегуються (тобто обчислюються сумарні показники) і завантажуються в сховище. Такі інтегровані дані набагато простіше аналізувати.

3. Прив'язка до часу. Дані в сховищі завжди безпосередньо пов'язані з певним періодом часу. Дані, вибрані із оперативних БД, накопичуються в сховищі у вигляді "історичних шарів", кожен з яких відноситься до конкретного періоду часу. Це дозволяє аналізувати тенденції в розвитку бізнесу.

4. Незмінність. Потрапивши в певний "історичний шар" сховища, дані вже ніколи не будуть змінені. Це також відрізняє сховище від оперативної БД, в якій дані весь час змінюються. Стабільність даних також полегшує їх аналіз.

Дані в сховище потрапляють з оперативних систем (*OLTP*-систем), які призначені для автоматизації бізнес-процесів. Крім того, сховище може

поповнюватися за рахунок зовнішніх джерел, наприклад, статистичних звітів, різних довідників і т.д. Сховище даних крім деталізованої інформації містить у собі агрегати, тобто узагальнюючу інформацію, наприклад, суми продажів, кількість, загальні витрати і т.д.

Причини побудови сховищ даних:

– складність безпосереднього аналізу даних оперативних систем через розрізненість даних та зберігання їх у форматах різних СУБД;

– складні аналітичні запити до оперативної інформації гальмують поточну роботу компанії, надовго блокуючи таблиці і захоплюючи ресурси сервера.

Основним принципом роботи зі сховищами даних є *OLAP*.

OLAP - це *Online Analytical Processing*, тобто оперативний аналіз даних. 12 визначальних принципів *OLAP* (табл. 2.2) сформулював в 1993 р. Е. Ф. Кодд – «винахідник» реляційних БД.

Таблиця 2.2.

12 визначальних принципів *OLAP*

1	Багатовимірне представлення даних	Засоби повинні підтримувати багатомірний на концептуальному рівні погляд на дані.
2	Прозорість	Користувач не повинен знати про те, які конкретні засоби використовуються для зберігання і обробки даних, як дані організовані і звідки вони беруться.
3	Доступність	Засоби повинні самі вибирати і зв'язуватися з найкращим для формування відповіді на даний запит джерелом даних. Засоби повинні забезпечувати автоматичне відображення їх власної логічної схеми в різні гетерогенні джерела даних.
4	Узгоджена продуктивність	Продуктивність практично не повинна залежати від кількості Вимірів у запиті.
5	Підтримка архітектури клієнт-сервер	Засоби повинні працювати в архітектурі клієнт-сервер.
6	Рівність всіх вимірювань	Жодне з вимірювань не повинно бути базовим, всі вони повинні бути рівноправними (симетричними).
7	Динамічна обробка розріджених матриць	Невизначені значення повинні зберігатися та оброблятися найбільш ефективним способом.
8	Підтримка багатокористувацького режиму роботи з даними	Засоби повинні забезпечувати можливість працювати більш ніж одному користувачеві.
9	Підтримка операцій на основі різних вимірювань	Всі багатовимірні операції (наприклад Агрегація) повинні одноманітно і узгоджено застосовуватися до будь-якого числа будь-яких вимірів.

10	Простота маніпулювання даними	Засоби повинні мати максимально зручний, природний і комфортний користувальницький інтерфейс.
11	Розвинені засоби подання даних	Засоби повинні підтримувати різні способи візуалізації (подання) даних.
12	Необмежена кількість вимірювань і рівнів агрегації даних	Не повинно бути обмежень на кількість підтримуваних Вимірів.

OLAP надає зручні швидкодіючі засоби доступу, перегляду та аналізу ділової інформації. Користувач отримує природну, інтуїтивно зрозумілу модель даних, організовуючи їх у вигляді багатовимірних кубів (*Cubes*). Осями багатовимірної системи координат служать основні атрибути аналізованого бізнес-процесу. Наприклад, для аудиторських послуг це можуть бути послуга, регіон, клієнт. В якості одного з вимірювань використовується час. Одна з дуже важливих відмінностей *OLAP*-систем від *OLTP* полягає в тому, що дані з плином часу не змінюються, а накопичуються, що дозволяє проводити аналіз зміни будь-яких бізнес-параметрів у часі. На перетинанні осей - вимірів (*Dimensions*) - знаходяться дані, що кількісно характеризують процес - міри (*Measures)*. Це можуть бути обсяги наданих послуг у кількісних одиницях або в грошовому вираженні, людино-години, витрати і т. п. Користувач, що аналізує інформацію, може "розрізати" куб за різними напрямками, отримувати зведені (наприклад, по роках) або, навпаки, детальні (по тижнях) відомості та здійснювати інші дії, які йому прийдуть у голову в процесі аналізу.

2.2.2. Моделі сховищ даних

Забезпечуючи багатовимірне концептуальне подання з боку користувальницького інтерфейсу до вихідної базі даних, всі продукти *OLAP* діляться на декілька класів за типом вихідної БД. Багатомірний гіперкуб, використовуваний в *OLAP*-технології, може бути реалізований в рамках реляційної моделі або існувати як окрема база даних спеціальної багатомірної структури. Залежно від цього прийнято розрізняти багатомірний (*MOLAP*) і реляційний (*ROLAP*) підходи до побудови сховищ даних.

У *MOLAP*-моделі *(Multidimensional OLAP)* багатомірне представлення даних реалізується фізично. В спеціалізованих СУБД, заснованих на багатовимірному поданні даних, дані організовані у формі не реляційних таблиць, а в організованих багатовимірних масивах:

– гіперкуби (усі збережені в базі даних комірки повинні мати однакову розмірність, тобто перебувати у максимально повному базисі вимірювань);

– полікуби (кожна мінлива величина зберігається з власним набором вимірювань, і всі пов'язані з цим складності обробки перекладаються на внутрішні механізми системи).

Використання багатовимірних баз даних в системах оперативної аналітичної обробки має наступні переваги:

1. Висока продуктивність. У разі використання багатовимірних СУБД пошук і вибірка даних здійснюється значно швидше, ніж при багатовимірному концептуальному погляді на реляційні бази даних, так як багатовимірна база даних денормалізована, містить заздалегідь агреговані показники і забезпечує оптимізований доступ до комірок, що запитуються.

2. Багатовимірні СУБД легко справляються з завданнями включення в інформаційну модель різноманітних вбудованих функцій, тоді як об'єктивно існуючі обмеження мови *SQL* роблять виконання цих завдань на основі реляційних СУБД досить складним, а іноді і неможливим.

Недоліки *MOLAP*-моделі:

1. Багатовимірні СУБД не дозволяють працювати з великими базами даних.

2. Багатовимірні СУБД порівняно з реляційними дуже неефективно використовують зовнішню пам'ять. У переважній більшості випадків інформаційний гіперкуб є сильно розрідженим, а оскільки дані зберігаються в упорядкованому вигляді, невизначені значення вдається видалити тільки за рахунок вибору оптимального порядку сортування, що дозволяє організувати дані в максимально великі безперервні групи. Але навіть у цьому випадку проблема вирішується тільки частково. Крім того, оптимальний з точки зору зберігання розсіяних даних порядок

сортування швидше за все не буде збігатися з порядком, який найчастіше використовується в запитах.

Використання багатовимірних СУБД виправдане тільки при наступних умовах:

1. Обсяг вихідних даних для аналізу не занадто великий (не більше декількох гігабайт), тобто рівень агрегації даних досить високий.

2. Набір інформаційних вимірів стабільний (оскільки будь-яка зміна в їх структурі майже завжди вимагає повної перебудови гіперкуба).

Час відповіді системи на нерегламентовані запити є найбільш критичним параметром.

Приклади *OLAP*-серверів, які використовують *MOLAP*-архітектуру: *Oracle Express Server* фірми *Oracle, IBM Informix MetaCube, IBM DB2 OLAP, Arbor Essbase*.

ROLAP (Relational OLAP) - системи оперативної аналітичної обробки реляційних даних дозволяють представляти дані, збережені в реляційній базі, в багатомірній формі, забезпечуючи перетворення інформації в багатомірну модель через проміжний шар метаданих. У цьому випадку гіперкуб емулюється СУБД на логічному рівні.

Основними складовими структури сховищ даних є таблиця фактів (*fact table*) і таблиці вимірів (*dimension tables*).

Таблиця фактів є основною таблицею сховища даних. Як правило, вона містить відомості про об'єкти або події, сукупність яких буде надалі аналізуватися. Якщо проводити аналогію з багатовимірної моделлю, то рядок таблиці фактів відповідає комірці гіперкуба. Зазвичай говорять про чотири типи фактів, що найбільш часто зустрічаються. До них відносяться:

– факти, пов'язані з операціями (*Transaction facts*). Вони засновані на окремих подіях (типовими прикладами яких є телефонний дзвінок або зняття грошей з рахунку за допомогою банкомату);

– факти, пов'язані з "моментальними знімками" (*Snapshot facts*). Засновані на стані об'єкту (наприклад, банківського рахунку) в певні моменти часу, наприклад на

кінець дня або місяця. Типовими прикладами таких фактів є обсяг продажів за день або денна виручка;

– факти, пов'язані з елементами документа (*Line-item facts*). Засновані на тому чи іншому документі (наприклад, рахунку за товар або послуги) і містять детальну інформацію про елементи цього документа (наприклад, кількості, ціни, процент знижки);

– факти, пов'язані з подіями або станом об'єкта (*Event or state facts*). Представляють виникнення події без подробиць про нього (наприклад, просто факт продажу або факт відсутності такої без інших подробиць).

Таблиця фактів індексується по складному ключу, складеному з ключів окремих змін. При цьому як основні, так і деякі неключові поля таблиці фактів повинні відповідати майбутнім вимірам *OLAP*-куба. Крім цього таблиця містить одне або кілька числових полів, на підставі яких надалі будуть отримані агрегатні дані.

Таблиця вимірів містить незмінні або рідко змінні дані. У кожній таблиці вимірів перераховані можливі значення одного з вимірювань гіперкуба. У переважній більшості випадків ці дані представляють собою один запис для кожного члена нижнього рівня ієрархії у вимірі. Таблиці вимірів також містять як мінімум одне описове поле (зазвичай з ім'ям члена вимірювання) і, як правило, цілочисельне ключове поле (зазвичай це сурогатний ключ) для однозначної ідентифікації члена вимірювання. Кожна таблиця вимірювань повинна знаходитися у відношенні «один до багатьох» з таблицею фактів.

Дана схема організації даних названа «зіркою». Кінці зірки утворюються таблицями вимірів, а з таблицею фактів, розташованою в центрі, утворюють промені. В термінології Кодда, кожен промінь схеми зірки задає напрямок консолідації даних за відповідним виміром.

У складних задачах з багаторівневими вимірами використовуються різні розширення схеми «зірка» - схема «сніжинка». Це розширення може проявлятися у двох різновидах.

1. У разі великої кількості складних атрибутів в таблиці вимірів, деякі атрибути можуть бути деталізовані в окремих таблицях вимірів. Іншими словами, окремі виміри містяться не в одній, а декількох пов'язаних між собою таблицях. Додаткові таблиці вимірів в такій схемі, зазвичай відповідають верхнім рівням ієрархії вимірювання і знаходяться в співвідношенні «один до багатьох» з головною таблицею вимірів.

2. Інше розширення пов'язане зі створенням окремих таблиць фактів для всіх можливих сполучень рівнів узагальнення різних вимірів. Це дозволяє досягти кращої продуктивності, але часто призводить до надлишковості даних і до значних ускладнень в структурі бази даних, в якій виявляється величезна кількість таблиць фактів.

Приклади *OLAP*-серверів, які використовують *ROLAP*-архітектуру: *IBM Informix Red Brick, HighGate Project* фірми *Sybase, Microsoft SQL Server 2000 Analysis Services* фірми *Microsoft*.

Гібридні системи (Hybrid OLAP, HOLAP) розроблено з метою поєднання переваг і мінімізації недоліків, властивих попереднім класів. До цього класу відноситься *Media/MR* компанії *Speedware*. За твердженням розробників, він об'єднує аналітичну гнучкість і швидкість відповіді *MOLAP* з постійним доступом до реальних даними, властивим *ROLAP*.

Приклади *OLAP*-серверів, які використовують *HOLAP*-архітектуру: *Microsoft SQL Server 2000 Analysis Services* фірми *Microsoft, SAS Institute*.

2.2.3. Інтерфейси для рівня представлення даних

Існує багато інтерфейсів для рівня представлення даних. Розглянемо три найбільш поширених інтерфейсів *ODBC, OLE DB, ADO* і проведемо їх порівняльний аналіз.

Інтерфейс ODBC - Відкрите з'єднання з базою даних (*Open Database Connectivity*) - стратегія *Microsoft*, що надає розробникам додатків єдиний *API* (*application programming interface* – інтерфейс програмування додатків) для різних ядер баз даних, систем управління реляційними і нереляційними базами даних

(*database management system - DBMS*). *ODBC API* призначений для надання прикладним розробникам аналогічних функціональних можливостей незалежно від типу даних, до яких здійснюється доступ, - баз даних *ISAM*, текстових даних (*Excel*) або баз даних *SQL*. Ця мета досягається шляхом закріплення кожного драйверу *ODBC* за одним з визначених рівнів відповідності. Щоб вважатися драйвером *ODBC*, драйвер повинен відповідати специфікаціям ядра *ODBC*. Ці вимоги гарантують, що розробник програми завжди може розраховувати на одні і ті ж функціональні можливості незалежно від того, до яких даними відбувається звернення. Якщо формат використовуваних даних безпосередньо не підтримує основні функціональні можливості, драйвер *ODBC* повинен емулювати ці функції.

Відкритий інтерфейс доступу до баз даних являє собою бібліотеку функцій, яка дозволяє прикладній програмі звертатися до різних СУБД. Використовуючи структуровану мову запитів *SQL*, інтерфейс *ODBC* пропонує незалежний від постачальника доступ до різних СУБД. Таким чином, розробник прикладної програми може створювати програму для віртуальної бази даних і дозволити драйверу перетворити логічні дані в дані конкретної СУБД або систем, що використовуються даною прикладною програмою.

Привабливість *ODBC* обумовлена її портативністю і взаємодією з кодом прикладної програми. *ODBC* функціонує як стандартний інтерфейс для розробників прикладних програм, а також для розробників бібліотек драйверів.

Інтерфейс *OLE DB* являє собою набір інтерфейсів *OLE*, що забезпечують уніфікований доступ додатків до даних з різних джерел. Ці інтерфейси підтримують підходящий для конкретного джерела даних обсяг функціональності СУБД, що робить доступною інформацію, що зберігається в ньому.

OLE DB дозволяє розробляти програми, які працюють з різними джерелами даних. *OLE DB* полегшує додаткам доступ до даних, що зберігаються в різних СУБД і в джерелах інформації, відмінних від СУБД. В якості джерел для СУБД можуть виступати бази даних мейнфреймів, такі як *IMS* ™ і *DB2*®, серверні бази даних, наприклад *Oracle*® і *Microsoft SQL Server*, а також бази даних персональних комп'ютерів, такі як *Microsoft Access*, *Paradox* і *Microsoft FoxPro*®. До не-СУБД

джерел відносяться файлові системи, такі як *Windows NT®* і *UNIX®*, индексно-послідовні файли, електронна пошта, електронні таблиці, засоби управління проектами та багато іншого.

Концептуально *OLE DB* є багатокомпонентною СУБД. Переваги багатокомпонентних СУБД можна розглядати з двох точок зору: споживачів і компонентів доступу до даних. По-перше, потреби в тому, що стосується управління базою даних, у різних споживачів можуть сильно відрізнятися. Якщо якийсь споживач вирішує використовувати котрусь модель СУБД, це передбачає вибір конкретного диспетчера сховища, методу доступу до файлів, моделі захисту, мови запитів і сценаріїв, процесора запитів і диспетчера транзакцій. Найчастіше споживачі використовують далеко не всі функціональні можливості комерційних монолітних СУБД. Проте їм доводиться розплачуватися додатковими накладними витратами ресурсів за непотрібну їм функціональність.

По-друге, великі обсяги важливих даних зберігаються в системах, які не підпадають під визначення СУБД. Найпопулярніші *API* доступу до даних, наприклад *ODBC* (*Open Database Connectivity*), встановлюють для компонентів доступу до даних високу початкову планку, вимагаючи, щоб вони підтримували доступ до даних за допомогою *SQL*. *OLE DB* знижує початкову планку для простих компонентів доступу до табличних даних, вимагаючи реалізації лише тих функціональних можливостей, які властиві сховищу даних. У мінімальному варіанті компоненту доступу необхідні інтерфейси, що забезпечують доступ до даних, як до таблиць. Це відкриває можливості створення компонентів-процесорів запитів, наприклад процесорів географічних або *SQL* запитів, які можуть використовувати табличну інформацію будь-якого компонента, що забезпечує доступ до своїх даних за допомогою *OLE DB.*

Функціональність *OLE DB* включає доступ і оновлення даних, обробку запитів, інформацію каталогів, повідомлення, транзакції, захист і віддалений доступ до даних. Визначаючи уніфікований набір інтерфейсів доступу до даних, компоненти *OLE DB* не тільки сприяють уніфікації доступу до різних джерел інформації, але і дозволяють зменшити вимоги додатків до об'єму пам'яті, дозволяючи їм задіяти

тільки ті можливості СУБД, які дійсно необхідні. Початково *OLE DB* визначає уніфікований доступ до табличних даних.

Інтерфейс ADO - це об'єктно-орієнтований інтерфейс фірми *Microsoft* для роботи з базами даних та іншими аналогічними джерелами даних - об'єктами даних *ActiveX* (*ActiveX Data Object - ADO*). *ADO* містить опис об'єктів, які можна використовувати для роботи з даними багатьох різних типів додатків. *ADO* спирається на інтерфейс *Common Object Model* (*COM*), що містить об'єкти, доступні для широкого спектру мов програмування, включаючи *Visual C++*, *Visual Basic*, *Visual Basic for Applications* (*VBA*), *VBScript* і *JavaScript*. *ADO* також можна використовувати в серверних або додатках проміжного типу, особливо при роботі з *Active Server Page* компанії *Microsoft*.

ADO містить тільки опис різних використовуваних об'єктів і не забезпечує їх спеціальної реалізації. Компанія *Microsoft* включила реалізацію *ADO* для доступу до будь-яких наявних джерел даних *OLE DB*, включаючи новий провайдер *Active Directory*, який реалізує інтерфейс *OLE DB* для роботи з файловими системами. Ця реалізація *ADO* для *OLE DB* отримала назву *ADODB*.

ADODB також може використовуватися для доступу до провайдера *Microsoft OLE DB* (*MSDASQL*), що забезпечує, в свою чергу, доступ до будь-яких наявних джерел даних *ODBC*.

Архітектура *ADO* представлена на рис. 2.1.

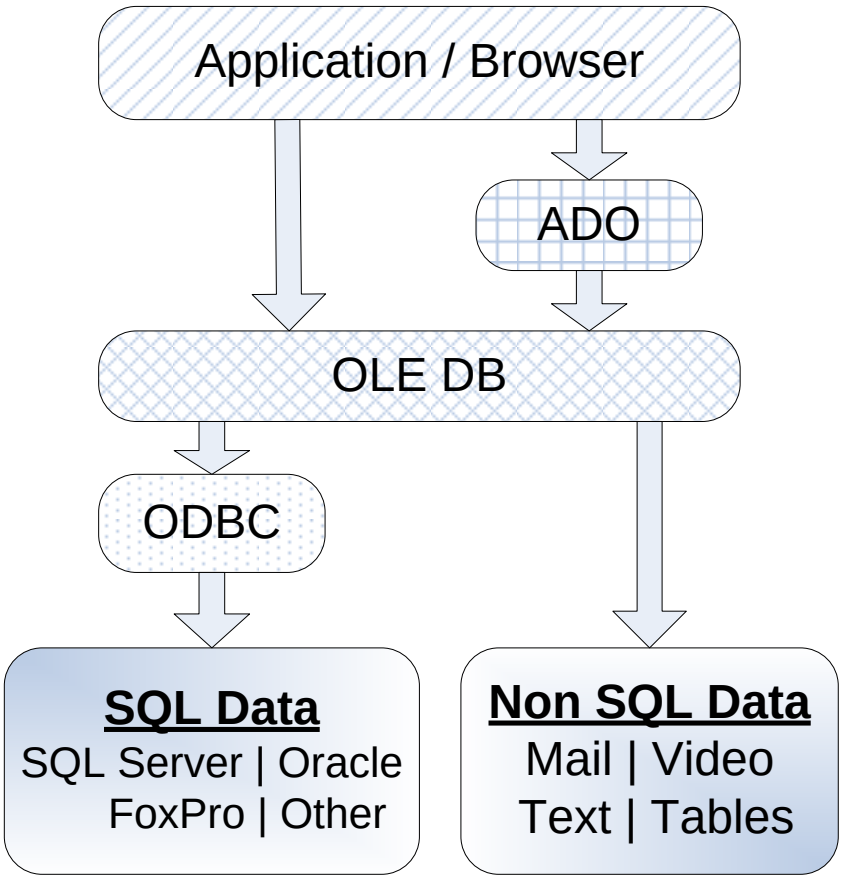

Рис. 2.1. Архітектура *ADO*

В основу інтерфейсу *ADO* покладено набір об'єктів, набагато більш простих у використанні, ніж об'єкти *OLE DB*. Хоча структура об'єктів *ADO* аналогічна *OLE DB*, об'єкти *ADO* не настільки є залежними від їх ієрархії. У більшості випадків можна просто створити і використовувати лише об'єкти, необхідні для роботи, і не піклуватися про створення багатьох інших зайвих "батьківських" об'єктів.

В табл. 2.3 представлено порівняння розглянутих вище інтерфейсів представлення даних.

Таблиця 2.3.

Порівняльні характеристики інтерфейсів представлення даних

Порівняльні характеристики	ODBC	OLE DB	ADO
1. Підтримка інтерфейсу багатьма СУБД	+	+	+
2. Єдиний API для різних джерел даних	+	+	+
3. Джерело даних може не підтримувати SQL	-	+	+
4. Підтримка не реляційних джерел даних	-	+	+
5. Зручність використання інтерфейсу	+	-	+
6. Можливість застосування інтерфейсу для зв’язку	-	-	+

БД с WWW			
Результати (в балах)	3	4	6

За результатами порівняння інтерфейсів можна визначити, що *ADO*-інтерфейс, який зібрав у собі переваги інтерфейсу *OLE DB* і зручність програмування, є найбільш відповідним інтерфейсом для роботи зі сховищами даних.

2.3. Вибір програмного забезпечення для організації сховища даних

Кількість постачальників існуючих на ринку *OLAP*-продуктів досить велика. Такими постачальниками є: *Microsoft, Oracle, Sybase, Informix, IBM, Targit, Next Action Technology, Cartesis, Hyperion Solutions, Cristal Decisions, Knosys, Cognos, Brio Technology, Arbor Systems, SAS Institute, IQ Software, Business Objects* та інші. Через досить велику кількість постачальників, коло порівнюваних продуктів було звужене до найбільш відомих і таких, що довго знаходяться на ринку. Для аналізу вибрані наступні постачальники: *Microsoft, Sybase, IBM, Oracle, Informix* (табл. 2.4). Кожна з цих фірм відома своїми досягненнями в області СУБД і має у ряді своїх продуктів і *OLAP*-засоби.

Таблиця 2.4.

Порівнювані *OLAP*-продукти

Компанія-виробник	Назва OLAP-продукту
Microsoft	OLAP Services
Sybase	Adaptive Server IQ Multiplex
IBM	DB2 OLAP Server
Oracle	Express
Informix	MetaCube

2.3.1. Критерії порівняння *OLAP*-продуктів

Розглянувши описи вибраних 5 продуктів, можна визначити критерії, за якими порівнюються *OLAP*-продукти і визначається найбільш підходящий для цілей даної роботи продукт. Завдання полягає у виборі швидкого, зручного, надійного та недорого *OLAP*-продукту, що дозволяє створити невелике сховище даних, призначене для розробки корпоративної системи управлінського обліку. Отже,

продукт не повинен вимагати великих системних ресурсів. Критерії порівняння *OLAP*-продуктів наступні:

1. Підтримка *ODBC*-протоколу.

*Я*кщо *OLAP*-продукт підтримує цей протокол, це автоматично означає, що дані в сховище даних можуть завантажуватися з великої кількості різних СУБД і електронних таблиць, для яких існує драйвер *ODBC*.

2. Підтримка доступу до нереляційних джерел даних.

Мається на увазі можливість *OLAP*-продукту здійснювати доступ не тільки до СУБД через *ODBC*, але і до інших джерел даних. Такими джерелами можуть бути текстові та графічні файли, файлові системи, такі як *Windows* і *UNIX*, індексно-послідовні файли, електронна пошта, електронні таблиці, засоби управління проектами та багато іншого. Прикладом протоколу, що дозволяє здійснювати доступ до нереляційних джерел даних є *OLE DB.*

3. Можливість зберігання даних у формі *MOLAP* і *HOLAP*.

Більшість *OLAP*-продуктів дозволяють зберігати дані тільки в реляційній формі, тобто, *ROLAP*. У цього способу є свої переваги і свої недоліки. Перевагою є можливість практично необмеженого масштабування (в межах апаратних засобів), недоліком є більш низька, порівняно з *MOLAP*, швидкість роботи. Обсяги даних, збережених у формі *MOLAP* в реальних додатках на сьогоднішній день обмежені 10-20 гігабайт, причому за рахунок денормалізації та попередньо виконаної агрегації 20 гігабайт в багатомірній базі, в кращому разі, еквівалентні не більш ніж 1 гігабайту вихідних даних. *HOLAP* поєднує в собі переваги обох підходів, вірніше, при цьому використовуються обидві архітектури - поєднуючи високу продуктивність і масштабованість.

4. Тимчасове зберігання багатовимірних даних на клієнтських комп’ютерах.

Можливість збереження на клієнтському комп'ютері частини багатовимірної БД дозволяє виконувати аналіз даних без безпосереднього з'єднання з *OLAP*-сервером. Це надає дві істотні переваги: по-перше, скорочується кількість і обсяг передачі інформації через мережу, по-друге, з'являється можливість повністю працювати без підключення до *OLAP*-серверу.

5. Можливість створення обчислюваних міток.

Обчислювані мітки не зберігаються на диску і не завантажуються в багатомірну базу з джерела даних. Використовуючи обчислювані мітки, можна включити в багатомірну базу вимірювання та заходи, яких немає у вихідних даних.

6. Спільна робота з декількома кубами.

Це дозволяє проводити дослідження за кількома кубами одночасно. Куби можуть перебувати на одному або декількох серверах. Важливість цього критерію полягає в тому, що є можливість спільного використання даних, що відносяться до різних областей аналізу. Наприклад, якщо в одному кубі зберігаються дані про надані послуги, а в другому - дані про співробітників, то можна аналізувати обсяг наданих послуг кожним співробітником.

7. Масштабованість.

Цей критерій передбачає можливість *OLAP*-продукту працювати з обсягами даних в широких межах (від дуже маленьких до дуже великих) без зміни складу програмного продукту. Практично всі *OLAP*-продукти задовольняють цим критерієм.

8. Оптимізація схеми агрегування.

Мається на увазі можливість зміни кількості обчислених заздалегідь агрегатів. Чим більше агрегатів зберігається в готовому вигляді, тим вище продуктивність системи і тим менше середній час відповіді на запит. В той же час, збільшення кількості збережених агрегатів призводить до збільшення обсягу даних, що зберігаються. Можливість зберігати тільки ті агрегати, які найбільш часто використовуються в запитах користувачів, дозволяє отримати найменший обсяг сховища даних при максимальній продуктивності для найбільш популярних запитів до БД. Тому даний критерій досить важливим при виборі оптимального *OLAP*-продукту.

9. Зручні засоби адміністрування.

Від зручності побудови засобів адміністрування залежить продуктивність праці адміністратора *OLAP*-продукту. Засоби адміністрування повинні мати графічний інтерфейс користувача, вбудовані засоби навчання і всеосяжні засоби допомоги.

10. Рішення проблеми "вибуху даних".

Як вже зазначалося, для більшості *OLAP*-продуктів попереднє обчислення агрегатів - це основна стратегія, що забезпечує виграш в продуктивності. В той же час попередня агрегація пов'язана зі значними витратами: число агрегатів легко може перевищити кількість вихідних точок з детальною інформацією, що призводить до різкого зростання обсягу даних, що зберігаються. Ефект «вибуху даних» проявляється при попередньому підрахунку агрегатів. Синдром вибуху може призвести до ще більших проблем при розрідженому розподілі вихідних даних по багатомірному кубу. Відсутні або неправильні значення даних створюють розрідження в моделі даних *OLAP*. Найбільш вдалі *OLAP*-продукти борються з цією проблемою, не зберігаючи порожні значення, таким чином, навіть погано заповнені куби не роздуваються в обсязі.

11. Багатокористувацький доступ до *OLAP*-серверу.

Прийняттям управлінських рішень зазвичай займається не одна людина, а група. У випадку аудиторської компанії фінансовим аналізом займається департамент науково-економічного забезпечення розвитку бізнесу; департаменти аудиту, аудиторських послуг та правовий повинні також мати доступ для внесення своїх кількісних та вартісних даних, а також готових документів. Керівник отримує узагальнену інформацію, керує ціновою політикою. Крім того, *OLAP*-продукти дуже дорогі і використання їх в режимі одного вкрай недоцільно. Таким чином, *OLAP*-продукт обов'язково повинен підтримувати роботу в багатокористувацькому режимі.

12. Можливість попереднього обчислення агрегатів.

OLAP-продукт повинен працювати однаково з великою швидкістю і з маленькими і з великими об'ємами даних, так як основний принцип *OLAP* - це швидка обробка запитів. Висока швидкість визначається в першу чергу тим, чи зберігаються в багатомірній базі даних заздалегідь обчислені агрегати, або вони обчислюються в процесі відповіді на запит користувача.

13. Безпека на рівні комірки інформації.

Сховища даних зазвичай зберігають інформацію про всі аспекти діяльності підприємства. Крім позитивних сторін у сховище даних є негативна - у разі, якщо інформація потрапить до неавторизированого користувача. Тому забезпечення захисту даних має дуже високу важливість. Найкращим рівнем захисту є обмеження доступу не тільки на рівні таблиць, але і на рівні записів у таблицях, тобто безпеку на рівні комірки інформації.

14. Кросплатформеність.

Для більшості *OLAP*-продуктів існують версії під різні апаратні і програмні платформи. Серед порівнюваних продуктів тільки *OLAP Services* фірми *Microsoft* підтримує роботу на одній платформі *Windows*. Але так як *Windows* є найбільш дешевою операційною системою, це не дуже критичний критерій.

15. Ціна *OLAP*-сервера і ліцензії на 5 осіб.

Для порівняння взято вартість набору з *OLAP*-сервера і ліцензії на 5 робочих місць. Це є достатнім для створення системи управлінського обліку невеликої за масштабом аудиторської компанії.

2.3.2. Порівняння *OLAP*-продуктів

Згідно з обраними вище критеріями складено наступну таблицю порівняння різних *OLAP*-продуктів (табл. 2.5).

Таблиця 2.5.

Порівняння *OLAP*-продуктів різних виробників

Критерій\Продукт		Microsoft OLAP Services	Sybase Adaptive Server IQ Multiplex	IBM DB2 OLAP Server	Oracle Express	Informix MetaCube
1	Підтримка ODBC-протоколу	+	+	-	+	+
2	Підтримка доступу до нереляційних джерел даних	+	-	-	-	-
3	Можливість зберігання даних у формі MOLAP і HOLAP	+	-	-	+	-
4	Тимчасове зберігання багатовимірних даних на клієнтських комп’ютерах	+	-	-	-	-
5	Можливість створення	+	+	+	+	+

	обчислюваних міток					
6	Спільна робота з декількома кубами	+	-	-	+	-
7	Масштабованість	+	+	+	+	+
8	Оптимізація схеми агрегування	+	-	-	-	+
9	Зручні засоби адміністрування	+	-	+	+	+
10	Рішення проблеми "вибуху даних"	+	+	+	+	+
11	Багатокористувацький доступ до OLAP-серверу	+	+	+	+	+
12	Можливість попереднього обчислення агрегатів	+	-	+	-	+
13	Безпека на рівні комірки інформації	-	-	-	+	+
14	Кросплатформеність	-	+	+	+	+
15	Ціна OLAP-сервера і ліцензії на 5 осіб	+ (1575)	- (25975)	- (29425)	+ (4570)	- (100000)
Результати порівняння + -		13 2	6 9	7 8	11 4	10 5

В результаті проведеного порівняння п'яти перерахованих раніше *OLAP*-продуктів, найбільш підходящим до вимог виявився продукт *OLAP Services* фірми *Microsoft*. *OLAP Services* набрав найбільшу кількість позитивних оцінок. Найближчим конкурентом є продукт *Express* фірми *Oracle*. Продукт *Microsoft* має найменшу ціну серед всіх порівнюваних продуктів завдяки тому, що він входить до складу *MS SQL Server*. Решта з порівнюваних мною *OLAP*-продуктів мають занадто завищену ціну, хоча їх можливості більш обмежені. Використання *OLAP*-серверів фірм *Informix*, *IBM* і *Sybase* може бути доцільно лише в разі наявності інфраструктури, заснованої на БД цих фірм. У всіх інших випадках, на мою думку, доцільно використовувати продукти *Microsoft* або *Oracle*.

2.4. Визначення структури багатовимірної бази даних

Тепер необхідно визначити структуру багатовимірної БД, тобто визначити конкретні Виміри і Факти, їх взаємозв'язки і рівні агрегації збережених даних.

Факти - це елементи, які можуть бути виміряні та проаналізовані. Факти можуть бути числовими і адитивними. Числові факти - це кількісні величини. Над

числовими фактами допускається виконання різних математичних операцій, їх легко виміряти.

Фактом, представленим послідовним рядом значень (*continuously valued*), може бути будь-яка з набору величин; зазвичай вона часто змінюється. Факти, представлені послідовно вибраними значеннями, корисні, оскільки завжди містять нову інформацію.

Адитивний факт може сумуватися за всіма вимірами. За допомогою адитивних фактів можна отримати компактні набори результатів. Кількість записів, що переглядаються за запитами до історичної базі даних, може досягати декількох тисяч, так що підсумувати їх вміст - цінна можливість.

Числові, представлені послідовним рядом значень, і адитивні елементи майже завжди зберігаються в таблиці фактів, але не всі факти обов'язково повинні відповідати цим критеріям.

Деякі факти напівадитивні (*semiadditive*). Їх можна коректно підсумувати за одним з вимірів, але не можна за іншим. Наприклад, має сенс підсумувати складські запаси продуктів по регіонах, але не за часом. Напівадитивні факти не можна підсумувати по всім тестам, але їх можна оцінювати іншими способами. Середня величина складських запасів у часі має сенс, як і максимальний і мінімальний рівень запасів, і деякі інші статистичні показники.

Існують неадитивні (*nonadditive*) факти. Ці факти неможливо підсумувати ні по одному з вимірів. Приклад числового неадитивного факту - відношення. Неадитивні факти не можна підсумувати, але їх можна порахувати, тому вони вимірювані. Неадитивні факти частіше групуються з вимірюваннями.

Факти багатовимірної БД для управлінського обліку аудиторської компанії:

- кількість клієнтів;
- загальна сума наданих послуг;
- кількість витрачених людино-годин роботи персоналу.

Виміри - це описові атрибути, що служать як обмежувачі при запитах або заголовки рядів у звітах. Виміри, як правило, текстові, статичні і неадитивні.

Приклади вимірів - ім'я співробітника і реєстраційний номер в системі соціального страхування. Людина може змінити ім'я, але часті зміни малоймовірні, і цей елемент зазвичай не відноситься до числа вимірюваних. Замість цього він несе інформацію про вимірюваної величини в таблиці фактів, такий, наприклад, як підвищення оплати праці службовців.

Не завжди можна легко відрізнити факти від вимірів. Іноді у вимірах можуть міститися числові, адитивні елементи, такі, як ціна одиниці товару. А іноді статичні і неадитивні елементи зручно розмістити в таблиці фактів. Все залежить від конкретного призначення бази даних.

Виміри багатовимірної БД для управлінського обліку аудиторської компанії: час, клієнти, послуги.

Перш ніж завантажити дані в сховище даних, необхідно організувати базу даних у вигляді схеми зірка або сніжинка (рис. 2.2). Як було сказано вище, схема сніжинки дозволяє зменшити вимоги до обсягу даних, так як повторювані дані виносяться в окрему таблицю.

Загальна структура вимірів надана у вигляді таблиці (табл. 2.6).

Таблиця 2.6.

Загальна структура вимірів БД управлінського обліку

Час	Послуги	Клієнти	Персонал	Посади	Документи
Місяць	Назва	Назва	Код	Назва	Назва
Квартал	Тип	Код	ПІБ	Департамент	Тип
Рік	Частота надання	Адреса	Посада	Вартість людино-години	
		Контактна особа	Зарплата		
		E-mail			
		Телефон			

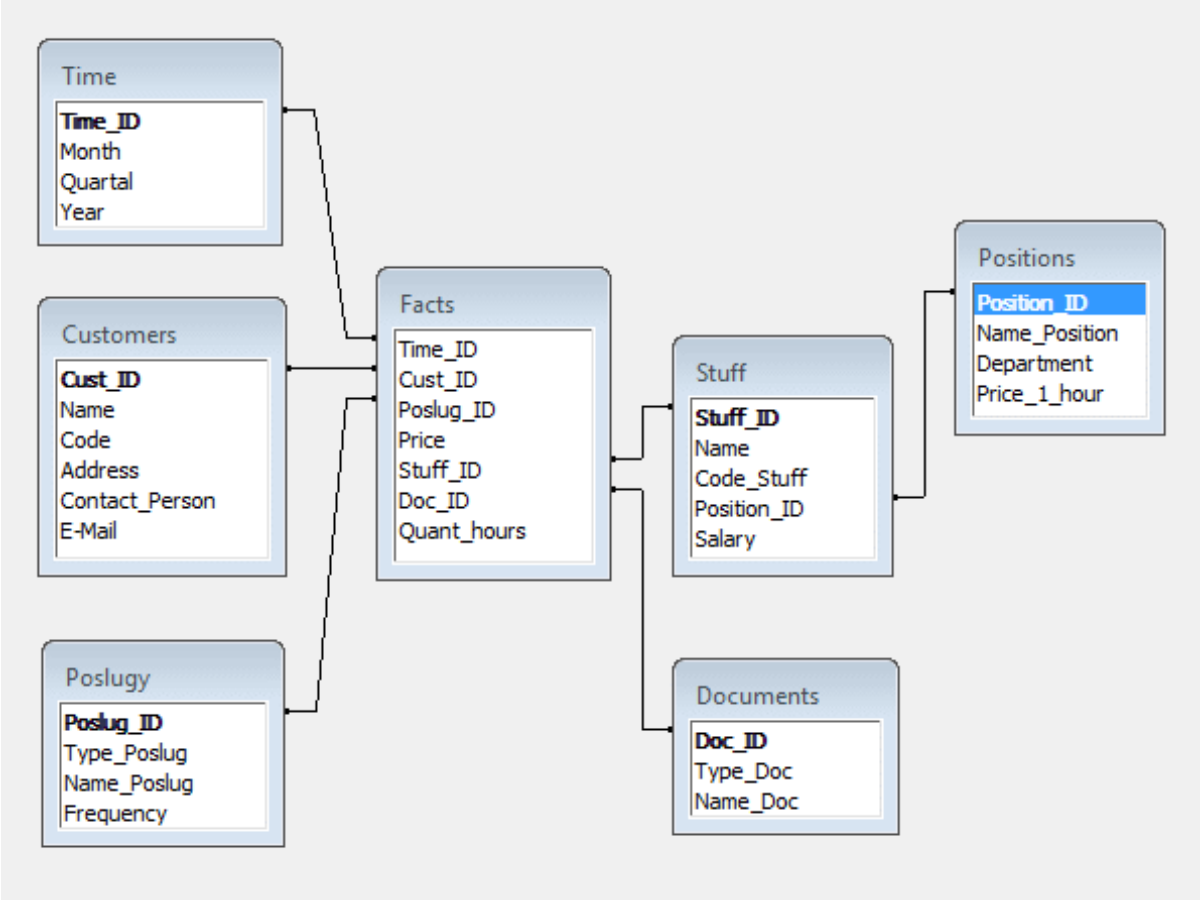

Рис. 2.2. Структура бази даних

Таким чином, багатовимірну БД для реалізації її в корпоративній системі управлінського обліку пропонується будувати за схемою:

1. Використання сховища даних з архітектурою *HOLAP (Hybrid OLAP - Гібридні системи)*, яка поєднує переваги компактності побудови реляційних баз даних із швидкістю доступу до даних, що забезпечується в *OLAP*-кубах.

2. Використання для сховища даних інтерфейсу рівня представлення даних *ADO* (*ActiveX Data Object*), який забезпечує доступ до даних в сховищі, які зберігаються як в *SQL*-форматі, так і в форматах тестових, табличних, мультимедійних файлів. Також даний інтерфейс забезпечує підтримку більшості мов програмування високого рівня в разі виникнення необхідності написання спеціального додатку для роботи зі сховищем даних.

3. Вибір *OLAP*-продукту для створення сховища даних - *OLAP Services* фірми *Microsoft*, який входить до складу *MS SQL Server*. Переваги продукту – демократична ціна, підтримка архітектури сховища даних *HOLAP*, інтерфейсу

представлення даних *ADO*, можливість використання в якості додатку для роботи зі сховищем даних таких продуктів *Microsoft*, як *Excel*, *Acceess*, а також будь-якого *web*-броузера.

2.5. Висновки за розділом

У результаті аналізу вимог до бази даних зроблено висновок, що вона в корпоративній системі управлінського обліку будується за схемою: використання сховища даних з архітектурою *HOLAP;* використання для сховища даних інтерфейсу рівня представлення даних *ADO*; вибір *OLAP*-продукту для створення сховища даних - *OLAP Services* фірми *Microsoft*, який входить до складу *MS SQL Server*. Перевагами цього продукту є: підтримка архітектури сховища даних *HOLAP*, інтерфейсу представлення даних *ADO*, можливість використання в якості додатку для роботи зі сховищем даних таких продуктів *Microsoft*, як *Excel*, *Acceess*, а також будь-якого *web*-броузера.

РОЗДІЛ 3
КОРПОРАТИВНА МЕРЕЖА ДЛЯ СИСТЕМИ УПРАВЛІНСЬКОГО ОБЛІКУ ПІДПРИЄМСТВА

Після розробки моделі системи управлінського обліку і визначення того, які процедури вимагають зміни або поліпшення, необхідно побудувати технічну модель мережі. Технічна модель описує, яке комп'ютерне обладнання потрібно використовувати, щоб досягти цілей, визначених у бізнес-моделі. Для побудуви технічної моделі, потрібно проаналізувати існуюче обладнання, визначити системні вимоги.

3.1. Аналіз існуючої комп'ютерної мережі підприємства

Офіс аудиторської компанії знаходиться в офісній будівлі, займає один поверх. Компанія має дві філії в інших містах, які повинні бути включені в корпоративну мережу. На даний момент обмін даними з філіями здійснюється електронною поштою, що має ряд серйозних недоліків, таких, як ризик втрати конфіденційних даних, втрати часу на формування та пересилання необхідної інформації.

В результаті інвентаризації існуючого комп'ютерного та мережевого обладнання встановлено наступне.

Комп'ютерна мережа головного офісу компанії має клієнт - серверну архітектуру з доменною організацією. Виконана за стандартом *Ethernet IEEE 802.3 і 100VG ANY LAN IEEE 802.12.* Як основне середовище для передачі інформації використовується *10Base-T* - неекранована вита пара (*Unshielded twisted pair, UTP*) і оптоволоконний кабель. Канали зв'язку організовані з використанням комутаторів мережевого устаткування *HP ProCurve Switch 2424M і HUB*-ів різних фірм.

Така організація мережі обумовлена тим, що дозволяє легко міняти конфігурацію системи, переміщати комп'ютери, виявляти і усувати неполадки. При виході з ладу однієї кабельної ділянки припиняється робота тільки одного мережевого комп’ютера, решта комп'ютерів продовжує функціонувати нормально.

У департаментах аудиту та правового забезпечення розташовано по одному комутатору *HP ProCurve Switch 2424M*. Комутатори *HP ProCurve Switch 2424M* мають 24 порти і можуть працювати в режимі автоматичного переключення між швидкостями передачі даних 10 та 100 МБіт/с. Департамент бухгалтерського обліку підключений до мережі через комутатор *3Com SuperStack II Switch 1000*, який налічує 12 портів. Всі інші департаменти підключені до комутаторів *HP ProCurve Switch 2424M*. Комутатори *HP ProCurve Switch 2424M* об'єднані між собою двома лініями оптоволоконного кабелю. Таким чином, для всіх департаментів, крім бухгалтерії, утворюється вузол комутації на 48 портів, а в бухгалтерському департаменті всього на 12 портів, що потребує термінового розширення.

Вся мережа головного офісу шляхом програмування комутаторів розбита на 2 віртуальних мережі (*Virtual Local Area Network VLAN*). Перша та найбільша з цих мереж охоплює всі департаменти компанії. Використовується для зберігання робочих документів користувачів, аудиторської інформації, сумісної роботи над документами. У даній мережі використовуються всі порти комутаторів *HP ProCurve Switch 2424M*. Від портів комутаторів прокладені лінії до кінцевих користувачів. Так як кінцева кількість користувачів мережі може з часом змінюватись, то лінії прокладалися за принципом: у кожному крилі, з обох сторін коридору розташовано по *HUB-у*. При збільшенні кількості користувачів мережі, знадобиться тільки протягнути дріт до найближчого *HUB-у*. Друга віртуальна мережа є мережею бухгалтерії. Використовується для клієнт-серверної версії програми 1С:Підприємство. Вона займає всі 12 портів комутатора *3Com SuperStack II Switch 1000*. Мостом між цими двома мережами є сервер *Work*. Але перехід з однієї мережі в іншу на цьому сервері заборонений на фізичному рівні - це зроблено з міркувань безпеки мережі. Сервер *Work* використовується як сервер *Internet* для обох підмереж. Схема існуючої корпоративної мережі підприємства надана на рис. 3.1.

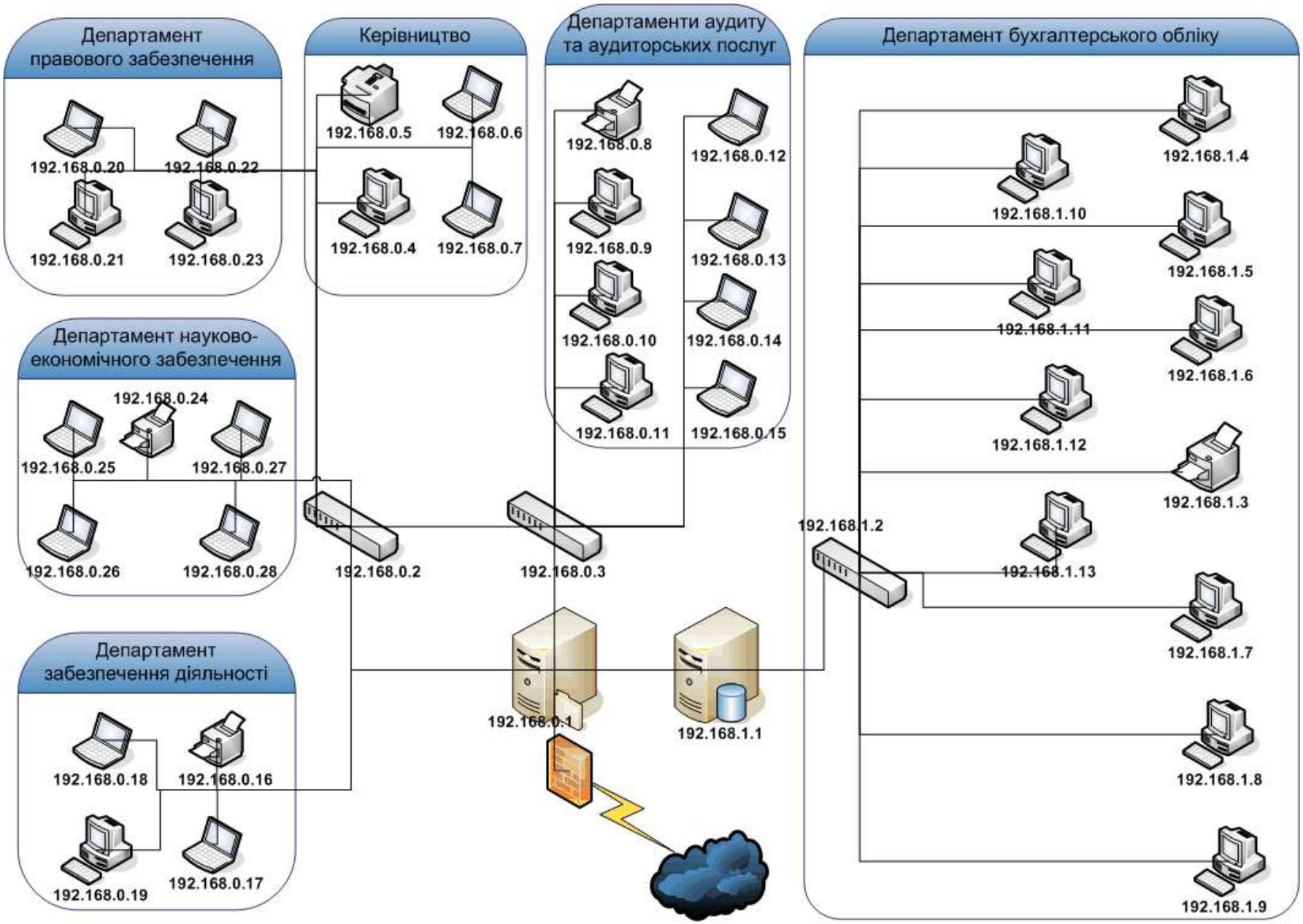

Рис. 3.1. Схема існуючої корпоративної мережі підприємства

3.2. Визначення системних вимог для побудови комп’ютерної мережі

Вимоги до сучасних обчислювальних мереж полягають в наступному:

1. Продуктивність.

Існує кілька основних характеристик продуктивності мережі:

– час реакції як інтервал часу між виникненням запиту користувача до будь-якої мережевої служби і отриманням відповіді на цей запит;

– пропускна здатність - обмежує обсяг даних, переданих мережею або її частиною в одиницю часу;

– затримка передачі визначається як затримка між моментом надходження пакета на вхід будь-якого мережевого пристрою або частини мережі і моментом появи його на виході цього пристрою.

2. Надійність і безпека.

Для оцінки надійності використовується коефіцієнт готовності, який означає частку часу, протягом якої система може бути використана.

Іншим аспектом загальної надійності є безпека, тобто здатність системи захистити дані від несанкціонованого доступу.

Ще однією характеристикою надійності є відмовостійкість. У мережах під відмовостійкістю розуміється здатність системи сховати від користувача відмову окремих її елементів. У відмовостійкій системі відмова одного з її елементів призводить до деякого зниження якості її роботи, а не до повної зупинки.

3. Розширюваність і масштабованість.

Розширюваність означає можливість порівняно легкого додавання окремих елементів мережі (користувачів комп'ютерів, доповнень, служб), нарощування довжини сегментів мережі і заміни існуючої апаратури на більш потужну.

Масштабованість (*scalability*) означає, що мережа дозволяє нарощувати кількість вузлів і довжину зв'язків в дуже широких межах, при цьому продуктивність мережі не погіршується.

4. Прозорість.

Прозорість мережі досягається в тому випадку, коли мережа видається користувачам не як безліч окремих комп'ютерів, пов'язаних між собою складною системою кабелів, а як єдина традиційна обчислювальна машина з системою розподілу часу.

5. Керованість.

Керованість мережі передбачає можливість централізовано контролювати стан основних елементів мережі, виявляти і вирішувати проблеми, які виникають при роботі мережі, виконувати аналіз продуктивності і планувати розвиток мережі.

6. Сумісність.

Сумісність означає, що мережа здатна містити в собі найрізноманітніше програмне і апаратне забезпечення, тобто в ній можуть співіснувати різні операційні системи, які підтримують різні стеки комунікаційних протоколів, і працювати апаратні засоби та додатки від різних виробників.

В нашому випадку, крім вищенаведених загальних вимог до мережі, існують спеціальні вимоги до мережевого обладнання, обумовлені потребами функціонування системи управлінського обліку:

1. Забезпечення безперебійної роботи сховища даних на базі *Microsoft OLAP Services*. Оскільки *Microsoft OLAP Services* є складовою частиною *Microsoft SQL Server*, то системні вимоги до обладнання мережі повинні задовольняти вимогам до даного програмного забезпечення, а також залишати можливість для модернізації.

Системні вимоги до *Microsoft SQL Server R2 Enterprise IA64* надані у табл. 3.1.

Таблиця 3.1.

Системні вимоги до *Microsoft SQL Server R2 Enterprise IA64*

Компонент	Вимога
Процесор	Тип процесора: • Процесор Itanium або більш потужний Швидкодія процесора: • Рекомендується: 1,0 ГГц і вище
Оперативна пам'ять	ОЗУ: • Не менш: 4 ГБ • Рекомендується: 16 ГБ та більше

	• 4 ТБ (максимальний обсяг ОЗУ, що підтримується випуском SQL Server Enterprise, дорівнює 4 ТБ або максимальному обсягу пам'яті ОС, в залежності від того, яке значення менше).

2. Об'єднання в одну локальну мережу головного офісу та філій в інших містах за допомогою *VPN (Virtual Private Network)* – технології віртуальної приватної мережі.

3. Забезпечення пропускної здатності мережі для обміну мультимедійною інформацією в режимі реального часу, наприклад, проведення відеоконференцій, а також *IP*-телефонії.

3.3. Технічна модель корпоративної мережі

Після визначення системних вимог можна описати технічну модель корпоративної мережі. На цьому етапі потрібно визначити, яким чином передбачається задовольнити виробничі вимоги з технічної точки зору.

Що отримає компанія при створенні корпоративної мережі:

– єдиний інформаційний простір;

– оперативність отримання інформації і можливість формування консолідованих звітів рівня підприємства;

– централізовані фінансові та інформаційні потоки даних;

– можливість оперативного збору та обробки інформації;

– зниження витрат при використанні серверних рішень;

– перехід від рішень для робочих груп на рішення рівня підприємства;

– можливість обробки мультимедіа потоків даних між головним офісом та філіями;

– зниження витрат на зв'язок між підрозділами компанії, організація єдиного номерного простору;

– створення єдиного середовища передачі інформації різного характеру.

Загальний принцип при побудові корпоративної мережі - єдине управління, загальна політика безпеки, доступність і продуктивність системи.

3.3.1. Рівні розвитку мережі

Виділяється п'ять рівнів розвитку корпоративної мережі:

1. Базовий обмежений - включає в себе мережу передачі даних для забезпечення роботи впроваджуваних бізнес-додатків.

2. Базовий розширюваний являє собою мережу передачі даних, побудовану з урахуванням майбутніх потреб у інформатизації.

3. *VoIP* припускає наявність універсальних (мультисервісних) каналів для передачі даних і голосу (телефонії) у філіальній мережі.

4. Конвергентний - передбачає мультисервісну корпоративну мережу з IP-телефонією та відео-конференцзв'язком.

5. *Unified Communications* включає інтегровану мережу з об'єднанням "простору програм" і "простору зв'язку", в якій застосовуються рішення *Unified Messaging, Rich Media Conferencing, Presence*, сервіси для *IP*-телефонії (рис. 3.2).

Зупинимося детальніше на останніх двох пунктах. Можливості конвергентного рівня розвитку мережі, такі, як *IP*-телефонія та конференцзв'язок, потрібні аудиторській компанії вже зараз. Але немає сенсу запроваджувати поточні технології, коли вже у повній мірі розвивається наступний етап. Тому *Unified Communications* повинен стати нашим вибором, і саме під його системні вимоги повинна оновлюватися мережа аудиторської компанії.

Unified Communications (Уніфіковані або Об'єднані Комунікації) - це набір засобів, призначених для міжособистісного, групового і / або корпоративного спілкування, зібраний в єдину оболонку. Вірніше, в єдину серверну платформу і невелику кількість клієнтів, різних за способом доступу до сервера, але однакових по інтерфейсу.

Ключові компоненти *UC*:

1. Голосові комунікації - стаціонарні, мобільні та програмні телефони. Можуть працювати як в середині будівель, так і за допомогою віддаленого доступу.

2. Конференції - аудіо, відео, і веб-конференції.

3. Електронна пошта, а також голосова пошта, календарі із загальним доступом.

4. Миттєві повідомлення / інформація про доступність - обмін миттєвими повідомленнями та інформацією про доступність. Інформація про доступність агрегується, тобто статус користувача повинен відображатися після обробки інформації з різних джерел.

5. Клієнти - товсті клієнти, тонкі веб-клієнти і мобільні клієнти. Так само може включати клієнти, що вбудовуються в різні програми.

6. Додатки - сюди відносяться програми з інтегрованими функціями взаємодії. Ключові програми - це: об'єднані інструменти адміністрування, програми, які використовуються для взаємодії і повідомлень, мобільні додатки, контакт-центри, інші додатки, в які вбудовані функції комунікацій.

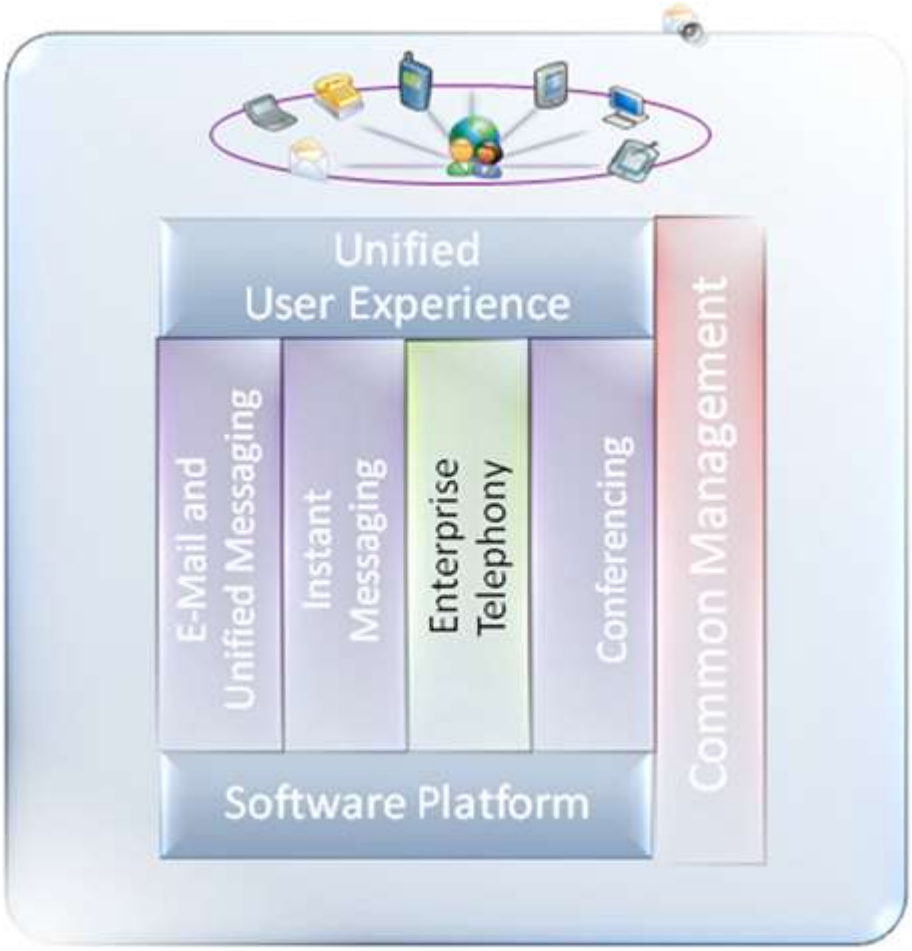

Рис. 3.2. Складові *Unified Communications*

Виробники *UC*.

Останнім часом дуже багато виробників намагаються позиціонувати свої продукти як рішення для об'єднаних комунікацій. Проте всі ці компанії можна

розділити на дві категорії: виробники, що прийшли з телефонії і виробники програмного забезпечення.

Лідером у першій категорії є *Cisco Sistems*. Компанія *Cisco*, оцінивши тенденцію, перейменувала свою автоматичну телефонну станцію *Cisco Call Manger* в *Cisco Unified Communications*, придбала компанію *WebEX* (лідера на ринку веб-конференцій) і ще ряд компаній, розробила нового клієнта *Cisco Personal Communicator*.

Лідером у другій категорії є *Microsoft*. Компанія придбала *Groove Networks* (отримавши продукт для взаємодії невеликих груп) та *Porlano* (отримавши груповий чат зі збереженням історії листування), уклала альянс в області *UC* з *Nortel* (а тепер і з *HP*). Тепер *Microsoft* вбудовує куплені технології в свої продукти і повсюдно впроваджує голосові можливості. Наступна версія продукту *Office Communications Server* вже зараз позиціонується як замінник традиційної телефонії.

3.3.2. *VPN* - Віртуальні приватні мережі

Для забезпечення включення філій в єдину мережу аудиторської компанії, а також для забезпечення доступу до корпоративної мережі співробітників, що працюють віддалено (наприклад, у відрядженнях), використовується технологія *VPN*, на основі якої і з'єднуються всі підрозділи та філії, що забезпечує достатню гнучкість і одночасно високу безпеку мережі, а також істотну економію витрат.

Віртуальна приватна мережа (*VPN - Virtual Private Network*) створюється на базі загальнодоступної мережі Інтернет. І якщо зв’язок через Інтернет має свої недоліки, головним з яких є схильність до потенційних порушень захисту та конфіденційності, то *VPN* можуть гарантувати, що трафік, який спрямовується через Інтернет, так само захищений, як і передача усередині локальної мережі. Структура *VPN* включає в себе канали глобальної мережі, захищені протоколи і маршрутизатори.

VPN-технологія діє за наступними принципами.

VPN-пристрій розташовується між внутрішньою мережею та Інтернет на кожному кінці з'єднання. Коли дані передаються через *VPN*, вони зникають "з

поверхні" в пункті відправлення і знову з'являються тільки в пункті призначення. Цей процес прийнято називати "тунелювання". Це означає створення логічного тунелю в мережі Інтернет, який з'єднує дві крайні точки. Завдяки тунелюванню приватна інформація стає невидимою для інших користувачів Інтернету. Перш ніж потрапити в інтернет-тунель, дані шифруються, що забезпечує їх додатковий захист. Протоколи шифрування бувають різні. Все залежить від того, який протокол тунелювання підтримується тим або іншим *VPN*-рішенням. Ще однією важливою характеристикою *VPN*-рішень є діапазон підтримуваних протоколів аутентифікації. Більшість популярних продуктів працюють зі стандартами, заснованими на використанні відкритого ключа, такими як *X.509*. Це означає, що, підсиливши свою віртуальну приватну мережу відповідним протоколом аутентифікації, можна гарантувати, що доступ до захищених тунелів отримають тільки відомі люди.

У дипломній роботі розглянуто використання *VPN* для об'єднання двох офісних мереж (рис. 3.3).

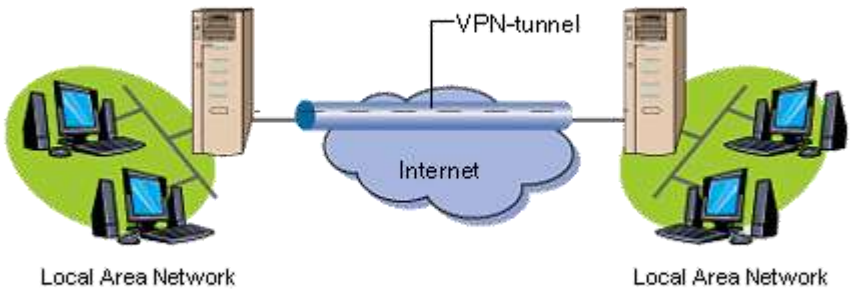

Рис. 3.3. Використання *VPN* для об'єднання двох офісних мереж

У випадку зі співробітниками, що працюють віддалено – їм достатньо скористуватися послугами найближчого інтернет-провайдера. При цьому на ноутбуках співробітників повинно бути встановлене програмне забезпечення для *VPN*-зв'язку.

У дипломній роботі розглянуто використання *VPN* для мобільних клієнтів

(рис. 3.4).

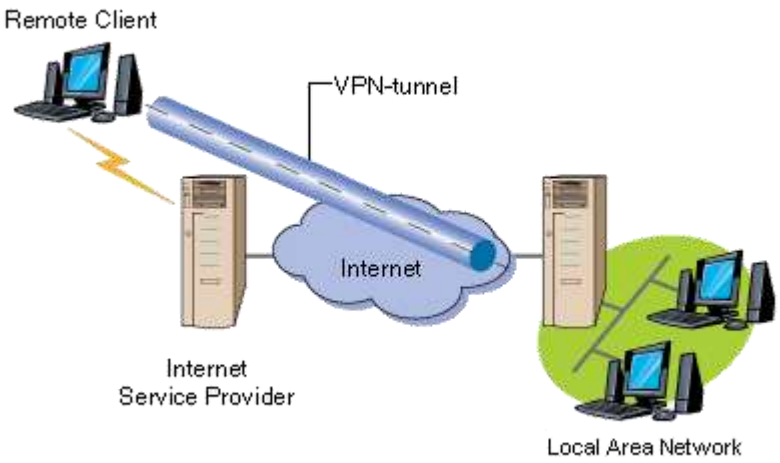

Рис. 3.4. Використання *VPN* для мобільних клієнтів

Протокол *VPN* визначає, яким чином система *VPN* взаємодіє з іншими системами в інтернеті, а також рівень захищеності трафіку. Протокол *VPN* впливає на загальний рівень безпеки системи. Причиною цього є той факт, що протокол *VPN* використовується для обміну ключами шифрування між двома кінцевими вузлами. Якщо цей обмін не захищений, зловмисник може перехопити ключі і потім розшифрувати трафік, звівши нанівець всі переваги *VPN*.

Для того, щоб була можливість створення *VPN* на базі обладнання і програмного забезпечення від різних виробників, необхідний певний стандартний механізм. Таким механізмом побудови *VPN* є протокол *Internet Protocol Security (IPSec)*. *IPSec* описує всі стандартні методи *VPN*. Цей протокол визначає методи ідентифікації при ініціалізації тунелю, методи шифрування, що використовуються кінцевими точками тунелю і механізми обміну та управління ключами шифрування між цими точками. З недоліків цього протоколу можна відзначити те, що він орієнтований на *IP*.

Іншими протоколами побудови *VPN* є протоколи *PPTP* (*Point-to-Point Tunneling Protocol*), розроблений компаніями *Ascend Communications* і *3Com*, *L2F* (*Layer-2 Forwarding*) - компанії *Cisco Systems і L2TP* (*Layer-2 Tunneling Protocol*), що об'єднав

обидва вищеназваних протоколів. Однак ці протоколи, на відміну від *IPSec*, не є повнофункціональними (наприклад, *PPTP* не визначає метод шифрування).

Кажучи про *IPSec*, не можна забувати про протокол *IKE* (*Internet Key Exchange*), що дозволяє забезпечити передачу інформації по тунелю, виключаючи втручання ззовні. Цей протокол вирішує завдання безпечного управління та обміну криптографічними ключами між віддаленими пристроями, в той час, як *IPSec* кодує і підписує пакети. *IKE* автоматизує процес передачі ключів, використовуючи механізм шифрування відкритим ключем, для встановлення безпечного з'єднання. Крім цього, *IKE* дозволяє здійснювати зміна ключа для вже встановленого з'єднання, що значно підвищує конфіденційність інформації, що передається.

Для технічної реалізації *VPN*, крім стандартного мережевого обладнання, нам необхідний шлюз *VPN* (*VPN Gateway*). Він виконує всі функції по формуванню тунелів, захист інформації, контролю трафіку, а нерідко і функції централізованого управління.

У нашому випадку достатньо придбати у однієї з фірм-виробників повністю готове до роботи обладнання, що вимагає для початку роботи лише підключення до локальної мережі, Інтернету і, можливо, мінімального конфігурування.

Для невеликих мереж і адміністраторів, які не володіють великим досвідом роботи з *VPN*, це рішення є найбільш зручним і ефективним.

3.3.3. Технологія мережі *Gigabit Ethernet*

При організації взаємодії вузлів в локальних мережах основна роль відводиться протоколу канального рівня. Однак для того, щоб канальний рівень міг впоратися з цим завданням, структура локальних мереж повинна бути цілком визначеною, так, наприклад, найбільш популярний протокол канального рівня - *Ethernet* - розрахований на паралельне підключення всіх вузлів мережі до загальної для них шини - відрізку коаксіального кабелю. Подібний підхід, що полягає у використанні простих структур кабельних з'єднань між комп'ютерами локальної мережі, відповідав основній мети, яку ставили перед собою розробники перших локальних мереж у другій половині 70-х років. Ця мета полягала в знаходженні простого і

дешевого рішення для об'єднання декількох десятків комп'ютерів, що знаходяться в межах одного приміщення в обчислювальну мережу.

Дана технологія втратила свою практичність, так як зараз в локальні мережі об'єднуються не десятки, а сотні комп'ютерів, що знаходяться не тільки в різних будівлях, але і в різних містах. Тому вибираємо більш високу швидкість і надійність передачі інформації. Ці вимоги виконуються технологією *Gigabit Ethernet 1000 Base-T*.

Gigabit Ethernet 1000Base-T, заснована на крученій парі і волоконно-оптичному кабелі. Оскільки технологія *Gigabit Ethernet* сумісна з *10 Mbps* і *100Mbps Ethernet*, можливий легкий перехід на дану технологію без інвестування великих коштів в програмне забезпечення, кабельну структуру і навчання персоналу.

Технологія *Gigabit Ethernet* - це розширення *IEEE 802.3 Ethernet*, що використовує таку ж структуру пакетів, формат та підтримку протоколу *CSMA/CD*, повного дуплексу, контролю потоку та інше, але при цьому надаючи теоретично десятиразове збільшення продуктивності.

CSMA/CD (Carrier Sense-Multiple Access with Collision Detection - множинний доступ з контролем несучої і виявленням колізій) - технологія множинного доступу до загального передаючого середовища в локальної комп'ютерної мережі з контролем колізій. *CSMA/CD* відноситься до децентралізованих випадкових методів. Він використовується як у звичайних мережах типу *Ethernet*, так і в високошвидкісних мережах (*Fast Ethernet, Gigabit Ethernet*).

Так само називають мережевий протокол, в якому використовується схема *CSMA/CD*. Протокол *CSMA/CD* працює на канальному рівні моделі *OSI*.

Характеристики і області застосування цих популярних на практиці мереж пов'язані саме з особливостями використовуваного методу доступу. *CSMA/CD* є модифікацією "чистого" *Carrier Sense Multiple Access (CSMA)*.

Якщо під час передачі кадру робоча станція виявляє інший сигнал, що займає передавальну середу, вона зупиняє передачу, посилає jam signal і чекає протягом випадкового проміжку часу (відомого як "*backoff delay*" і находимого з допомогою алгоритму *truncared binary exponential backoff*), перед тим, як знову відправити кадр.

Виявлення колізій використовується для поліпшення продуктивності *CSMA* з допомогою переривання передачі відразу після виявлення колізії і зниження ймовірності другий колізії під час повторної передачі.

Методи виявлення колізій залежать від використовуваного устаткування, але на електричних шинах, таких як *Ethernet*, колізії можуть бути виявлені порівнянням переданої та отриманої інформації. Якщо вона відрізняється, то інша передача накладається на поточну (виникла колізія) і передача переривається негайно. Надсилається *jam signal*, що викликає затримку передачі всіх передавачів на довільний інтервал часу, знижуючи ймовірність колізії під час повторної спроби.

3.4. Апаратне забезпечення локальної мережі аудиторської компанії

Вибору апаратного забезпечення потрібно приділити особливу увагу, чималу роль відіграє можливість розширення системи і простота її модернізації, оскільки саме це дозволяє забезпечити необхідну продуктивність не тільки на поточний момент часу, але і в майбутньому.

Враховуючи вимоги до мережевих технологій, наведені в попередніх підрозділах, перелік обладнання надано в зведеному вигляді (табл. 3.2).

Таблиця 3.2.

Звід мережевого обладнання

Топологія	Зірка
Мережева технологія	*Gigabit Ethernet*
Тип кабелю	Оптоволокно, STP категорії 5e
Базова операційна система	*Windows Server*
Протоколи	*TCP/IP, FTP*
Додаткові технології	*VPN, Unified Communications*

3.4.1. Серверне обладнання

При виборі сервера найбільший інтерес представляє максимальний об'єм оперативної пам'яті, який можна використовувати на даному сервері, можливість

встановлення потужного процесора, а також другого процесора (якщо планується використання операційної системи, що підтримує двухпроцесорну конфігурацію). Важливим так само залишається питання про те, яку конфігурацію дискової підсистеми можна використовувати на даному сервері, в першу чергу, який обсяг дисків, максимальна їх кількість.

Висока надійність серверів досягається шляхом реалізації комплексу заходів, що стосуються як забезпечення необхідного теплообміну в корпусі, контролю температури найважливіших компонентів, спостереження за низкою інших параметрів, так і повного або часткового дублювання підсистем.

В локальній мережі аудиторської компанії повинен бути сервер, що забезпечує роботу з файлами, базами даних, електронною поштою, інтернетом. В зв'язку з високими апаратними вимогами до обробки сховища даних, а також мультимедійної інформації, потрібне додавання в систему ще одного сервера.

3.4.2. Пасивне мережне устаткування

Пасивне обладнання становить фізичну інфраструктуру мереж (комутаційні панелі, розетки, стійки, шафи монтажні, кабелі, кабель-канали, лотки і т.п.). Від якості виконання кабельної системи багато в чому залежить пропускна здатність і якість каналів зв'язку, тому для тестування фізичних носіїв даних повинне застосовуватися складне і дороге обладнання під управлінням кваліфікованого персоналу в цій області.

3.4.3. Обладнання для *Unified Communications*

1. Обладнання *Microsoft.*

Microsoft Office Communications Server (OCS) - комунікаційна платформа, що надає всі види корпоративних комунікацій: *VoIP*-телефонію, аудіо- і відео конференції, обмін миттєвими повідомленнями, віддалене читання презентацій, спільна дистанційна робота в додатках і т.д.

Глибока інтеграція з іншими продуктами *Microsoft* робить *OCS* безпрецедентно зручним комунікаційним середовищем. Наприклад, можна зробити дзвінок

безпосередньо з відкритої програми (наприклад з *Power Point* автору презентації) одним кліком, при цьому телефонний номер абонента береться з *Active Directory*.

Устаткування для *OCS* можна розділити на дві категорії: *VoIP* шлюзи (media gateways) з підтримкою *OCS* для сполучення з телефонними мережами і абонентські термінали - телефонні апарати та інші пристрої з *OCS*-функціональністю.

Media gateways необхідні для інтеграції *OCS* з існуючими телефонними мережами - як корпоративними *PBX*, так і *PSTN*.

Office Communications Server підтримує три типи *media gateways*:

- *Basic Media Gateway* - вимагає наявності *Mediation Server*, що є частиною програмної архітектури *Microsoft OCS*, для здійснення дзвінків між *PSTN* і корпоративної *VoIP*-мережею під управлінням *Microsoft OCS*;

- *Advanced Media Gateway* - поєднує в собі функціональність *Basic Media Gateway* і *Mediation Server*. При використанні *Advanced Media Gateway* немає потреби в окремому *Mediation Server*;

- *Basic Hybrid Media Gateway* - сервер під керуванням *Windows Server*, що містить у собі *Mediation Server* і функціональність *Basic Media Gateway*. Він знижує витрати по установці й адмініструванню системи порівняно з установкою окремо *Basic Media Gateway* і *Mediation Server* на різних серверах.

Mediation Server

Будучи частиною *Office Communications Server*, *Mediation Server* (рис. 3.5) здійснює трансляцію сигналу та медіа між *VoIP*-інфраструктурою і *Basic Media Gateway*. *Mediation Server* також пов'язує *OCS* з *PBX* як на рівні розділеного впровадження, так і в топології *PBX*-інтеграції. *Mediation Server* встановлюється як окремий додаток за міжмережевим екраном (*firewall*).

Основні функції *Mediation Server*:

- кодування і декодування *SRTP* (*Secure-Real time Transport Protocol*) на стороні *Office Communications Server* (рис. 3.6);

- трансляція *media*-потоків між *OCS* і *media gateway*;

- підключення клієнтів, що знаходяться за межами мережі до внутрішніх *ICE* (*Interactive Connectivity Establishment*) компонентів для забезпечення проходження media через *NAT* і *firewall*;

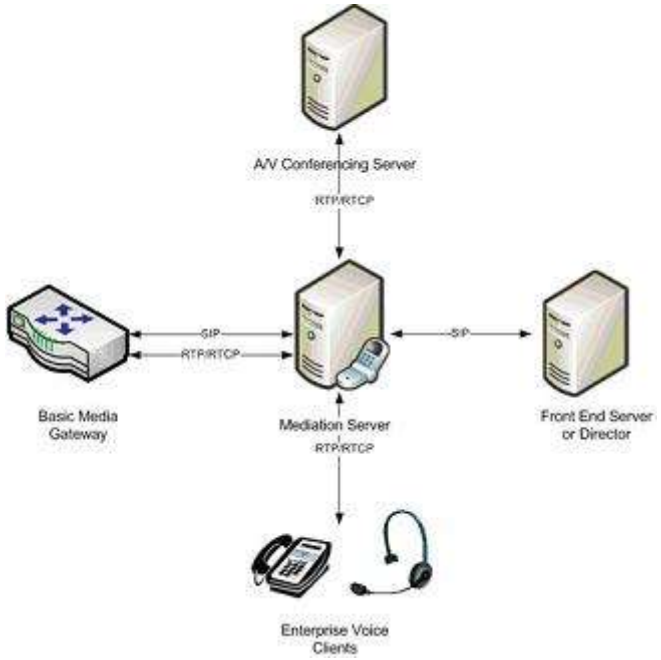

Рис. 3.5. Робота *Microsoft Mediation Server*

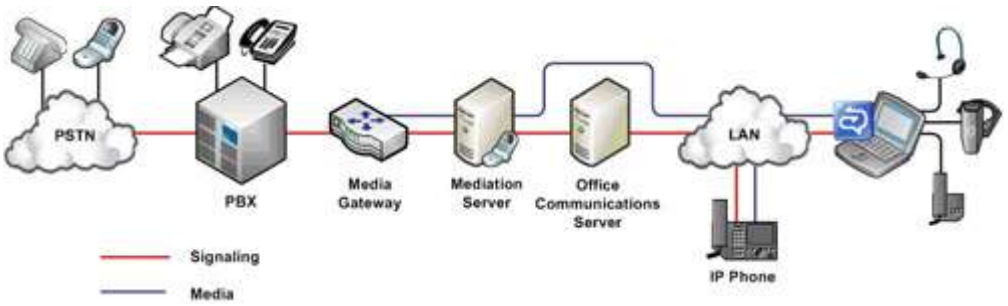

Рис. 3.6. Інформаційні потоки *Microsoft Office Communications Server*

2. Обладнання *Cisco*.

Cisco Unified Communications Manager Business Edition - це набір програм *Unified Communications* для підприємств середнього розміру (від 100 до 500 співробітників) на єдиній платформі з загальними системами активації і управління. В продукт *Cisco Unified Communcations 500 Series* входять наступні компоненти:

Cisco Unified Communication Manager Express. *IP* АТС, що відповідає за комутацію викликів, за управління телефонами і за додаткові функції телефонного зв'язку (конференції, переадресація, переведення виклику та інше).

Cisco Unity Express. Модуль, що відповідає за функції голосової пошти та автосекретаря.

Комутатор *Ethernet*. Вбудований 8-мі портовий 10/100 Mb/s комутатор *Ethernet* з підтримкою *PoE* (*Power Over Ethernet*), що дозволяє підключати *IP* телефони та офісні комп'ютери.

Модуль безпеки. Забезпечує функції безпеки завдяки використанню *Cisco IOS Firewall*, який захищає мережу від атак з назовні. *VPN* концентратор, що підтримує 10 одночасних сесій з апаратним шифруванням для забезпечення віддаленого доступу до внутрішньоофісних мережевих ресурсів мобільним користувачам.

WLAN (Wi-Fi). Вбудована або зовнішня точка доступу для забезпечення бездротового з'єднання (*WLAN*) мобільним користувачам всередині офісу.

Так само *Cisco Unified Communications* Серії 500 підтримує додаткові компоненти (постачаються окремо):

IP телефони. Широкий вибір *IP* телефонів для керівного складу, менеджерів середньої ланки і звичайних працівників компанії, включаючи бездротові телефони і телефони, що підтримують протокол *SIP*.

Програми *Cisco Unified callconnector*. Програма програми *Cisco Unified callconnector* дозволить розширити функціональність телефонного зв'язку, забезпечуючи інтеграцію *Microsoft Outlook, Internet Explorer, Microsoft Dynamics CRM* в офісну телефонну мережу.

Комутатор *Ethernet серії Cisco Catalyst® Express 520*. При необхідності можна розширити базову кількість робочих місць, додавши до комплексу *Cisco Unified Communcations 520 Series* додатковий комутатор *Ethernet*, з кількістю портів від 8 до 24.

3.5. Технічна модель та структура комп’ютерної мережі для системи управлінського обліку підприємства

Для корпоративної мережі аудиторської компанії плануються заходи:

1. Зв’язок мережі головного офісу з філіями через *VPN*-з’єднання, додавання в мережу необхідного обладнання.

2. Використання розширених мультимедійних можливостей, що забезпечуються концепцією мережі *Unified Comunications*.

3. Заміна кабельної складової мережі на кабелі з пропускною здатністю стандарту *Gigabit Ethernet*, додавання в систему маршрутизаторів відповідного стандарту.

4. Додавання в мережу серверу для роботи зі сховищем даних, а також зберігання мультимедійної інформації.

Корпоративна мережа аудиторської компанії дозволить забезпечувати швидкий та надійний зв’язок з усіма підрозділами та співробітниками, накопичувати та надійно зберігати інформацію в сховищі даних, а також використовувати дані можливості для управлінського аналізу та прийняття ефективних управлінських рішень.

Згідно визначеним вимогам та особливостям функціонування підприємства пропонована схема корпоративної мережі підприємства, яка надана на рис. 3.7.

3.6. Висновки за розділом

У результаті розробки моделі системи управлінського обліку і визначення того, які процедури вимагають зміни або поліпшення, аналізу існуючого обладнання, визначення системних вимог побудована технічна модель мережі, обґрунтовано вибір комп'ютерного обладнання, яке потрібно використовувати, щоб досягти цілей, визначених у бізнес-моделі.

Корпоративна мережа аудиторської компанії дозволить забезпечувати швидкий та надійний зв’язок з усіма підрозділами та співробітниками, накопичувати та надійно зберігати інформацію в сховищі даних, а також використовувати дані можливості для управлінського аналізу та прийняття ефективних управлінських рішень.

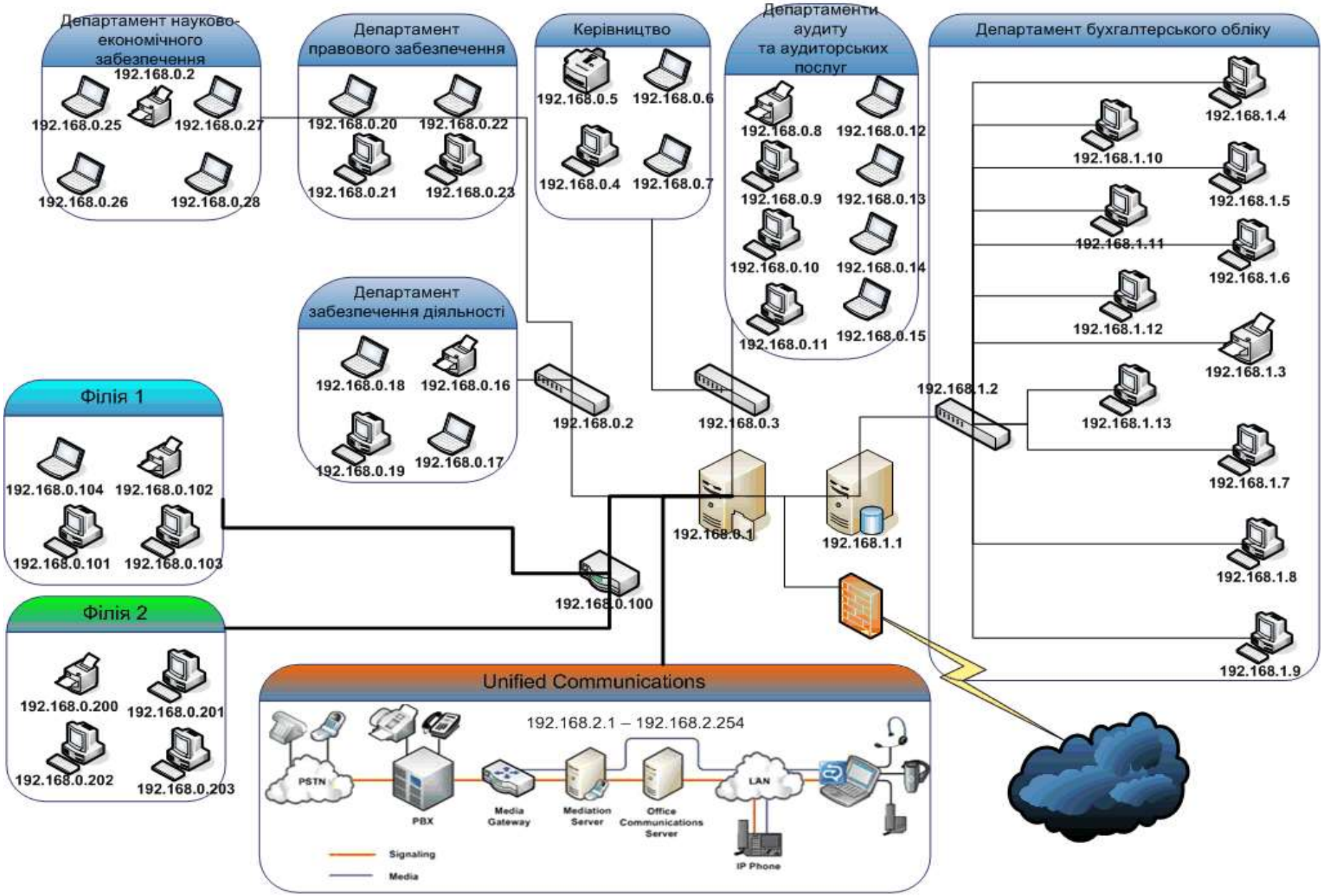

Рис. 3.7. Схема корпоративної мережі

РОЗДІЛ 4
ЗАСОБИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ КОРПОРАТИВНОЇ СИСТЕМИ

4.1. Підвищення ефективності функціонування корпоративної системи організацією інформаційної безпеки системи управлінського обліку

4.1.1. Поняття інформаційної безпеки стосовно системи управлінського обліку

Під інформаційною безпекою розуміється захищеність інформації від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самій інформації, її власникам або підтримуючій інфраструктурі.

Інформаційна безпека організації - стан захищеності інформаційного середовища організації, що забезпечує її формування, використання і розвиток.

В якості стандартної моделі безпеки можна використати модель з трьох категорій:

- конфіденційність - стан, при якому доступ до інформації здійснюють тільки суб'єкти, які мають на неї право;
- цілісність - запобігання несанкціонованої модифікації інформації;
- доступність - уникнення тимчасового або постійного приховування інформації від користувачів, які отримали права доступу.

Інформаційна безпека аудиторської компанії характеризується більш жорсткими вимогами порівняно з іншими видами консультаційного бізнесу.

Причини:

1. Конфіденційний характер діяльності – сторонні особи не повинні отримувати інформацію щодо клієнтів компанії та питань, з якими вони звертаються.

2. Зберігання великої кількості інформації та документів, які становлять комерційну таємницю як самої аудиторської компанії, так і її клієнтів.

Дії, які можуть завдати шкоди інформаційній безпеці організації, можна розділити на декілька категорій:

1. Дії, які здійснюються авторизованими користувачами. У цю категорію потрапляють: цілеспрямована крадіжка або знищення даних на робочій станції або сервері; пошкодження даних користувачів в результаті необережних дій.

2. Злочинні дії, здійснювані хакерами. Під хакерами розуміються люди, які займаються комп'ютерними злочинами як професійно (у тому числі в рамках конкурентної боротьби), так і просто з цікавості. До таких методів належать: несанкціоноване проникнення в комп'ютерні мережі (з метою знищення даних, крадіжки конфіденційної інформації, використання мережевої інфраструктури для організації атак на сайти третіх фірм, крадіжка коштів з рахунків); *DOS_атаки* (*Denial of Service* - "відмова в обслуговуванні"- це зовнішня атака на вузли мережі підприємства, що відповідають за її безпечну і ефективну роботу (файлові, поштові сервера) з метою їх перевантаження та на якийсь час виведення з ладу).

3. Комп'ютерні віруси. Окрема категорія електронних методів впливу - комп'ютерні віруси та інші шкідливі програми. Проникнення вірусу на вузли корпоративної мережі може призвести до порушення їх функціонування, втрат робочого часу, втрат даних, крадіжки конфіденційної інформації і навіть прямого розкрадання фінансових коштів. Вірусна програма, що проникла в корпоративну мережу, може надати зловмисникам частковий або повний контроль над діяльністю компанії.

4. Спам. Всього за кілька років спам з незначного дратівного фактору перетворився в одну з найсерйозніших загроз: електронна пошта останнім часом стала головним каналом розповсюдження шкідливих програм; спам забирає багато часу на перегляд і подальше видалення повідомлень, викликає у співробітників почуття психологічного дискомфорту; як приватні особи, так і організації стають жертвами шахрайських схем, що реалізуються спамерами; разом зі спамом нерідко

видаляється важлива кореспонденція, що може призвести до втрати клієнтів, зриву контрактів та інших неприємних наслідків; небезпека втрати кореспонденції особливо зростає при використанні чорних списків *RBL* та інших грубих методів фільтрації спаму.

5. Матеріальні фактори: неправильне зберігання, крадіжка комп'ютерів і носіїв, форс-мажорні обставини.

4.1.2. Загрози для інформаційної безпеки через некомпетентні дії персоналу, та їх наслідки

1. Багатопотокове завантаження.

Сценарій. Співробітник завантажує з Інтернету утиліту для багатопотокового збереження контенту вказаних сайтів. Вказавши кілька сайтів, він запускає утиліту у фоновому режимі. В результаті збою утиліта починає видавати 500-700 запитів в секунду в безперервному циклі, що призводить до ситуації *DoS* на корпоративному проксі-сервері.

Аналіз. В даному випадку злий умисел з боку співробітника відсутній, однак аналіз ситуації показав, що застосування даної утиліти не потрібно для вирішення виробничих завдань. Крім того, утиліта не проходила ніяких тестів з боку адміністраторів мережі і її застосування не було погоджено з ними, що, власне, і призвело до даної ситуації.

Рішення проблеми. У корпоративній політиці безпеки вводиться заборона на установку програмного забезпечення, що активно взаємодіє з Інтернетом, без узгодження з адміністраторами та службою безпеки. Після цього проводяться технічні заходи для пошуку і видалення подібних програм і блокування їх подальшої установки.

2. Електронна пошта.

Сценарій. Бажаючи привітати з Новим роком колег, співробітник встановлює базу розсилки з 1500 адрес, після чого створює лист з *Flash*-мультфільмом розміром 1,5 Мбайт і запускає розсилку. Подібні операції роблять також його колеги, розсилаючи вітальні листи з вкладеними картинками, *Flash*-роликами і звуковими

файлами. В результаті створюється ситуація *DoS* на поштовому сервері і блокується прийом-відправка ділової кореспонденції.

Аналіз. Це типовий приклад нецільового використання корпоративної електронної пошти, зазвичай подібні проблеми виникають перед святами. Найбільш характерна дана ситуація проявляється у великих мережах (більше 500 користувачів).

Рішення проблеми. Технічно вирішити цю проблему дуже складно, оскільки обмеження на обсяг листа і кількість листів в одиницю часу не завжди прийнятні і малоефективні при великій кількості користувачів. Найбільш ефективна міра - розробка правил використання корпоративного поштового сервера і доведення цих правил до відома всіх користувачів.

3. Засоби аналізу мережі.

Сценарій. Нещодавно прийнятий на роботу молодий програміст для самоосвіти завантажує з Інтернету сканер мережевої безпеки XSpider. Для вивчення його роботи він виставляє налаштування по максимуму і в якості мети вказує адресу одного з корпоративних серверів. В результаті засоби захисту сервера реєструють атаку, сповільнюється час реакції серверу на запити користувачів.

Аналіз. В даному випадку злий умисел відсутній, так як користувач, що встановив цю програму мережі, не мав чіткого уявлення про можливі наслідки.

Рішення проблеми. У корпоративній політиці безпеки вводиться розділ, що категорично забороняє встановлення і використання на робочих місцях користувачів засобів активного і пасивного дослідження мережі, генераторів мережевих пакетів, сканерів безпеки і інших засобів. Згідно з цим положенням застосування подібних інструментів дозволяється лише адміністраторам мережі і фахівцям із захисту інформації.

4. Поштовий вірус.

Сценарій. Користувач отримує лист, що містить явні аномалії (відправником і одержувачем листа є сам користувач, текст листа не відповідає діловій переписці або відсутній). До листа прикладений архів з якимсь додатком. Незважаючи на

інструктаж, цікавість виявляється сильніше, користувач зберігає архів на диск, розпаковує і запускає файл, який виявляється новим різновидом поштового черв'яка.

Аналіз. Технічні заходи в даному випадку марні. Той факт, що користувач отримав лист, свідчить про те, що застосовуваний поштовий антивірус і антивірус на ПК користувача не виявляють даний різновид вірусу.

Рішення проблеми. Навчання користувачів та розробка планів проведення заходів у разі появи в корпоративній мережі поштового віруса або черв'яка.

5. Несанкціоноване підключення модему.

Сценарій. Користувач несанкціоновано підключає до свого комп'ютера стільниковий телефон і виходить в Інтернет через *GPRS*-з'єднання. В ході роботи в Інтернеті на його комп'ютер проникає мережевий черв'як, який надалі намагається заразити інші комп'ютери в рамках локальної мережі.

Аналіз. Стільникові телефони з *GPRS* дуже поширені, тому організувати точку несанкціонованого підключення не становить зусиль. Небезпека такого підключення дуже велика, оскільки воно не контролюється адміністраторами і не захищено корпоративним брандмауером.

Рішення проблеми. У цієї проблеми є два рішення: технічне та адміністративне. Для ефективного захисту необхідно застосовувати обидва: з одного боку, корпоративна політика безпеки має суворо забороняти користувачам підключення модемів або стільникових телефонів для виходу в Інтернет, а з іншого - необхідно вживати технічні заходи для блокування такої можливості (привілеї і політики безпеки, засоби моніторингу).

6. Заражений ноутбук.

Сценарій. Користувачеві видається службовий ноутбук, який він бере з собою у відрядження. Там він підключається до мережі, і його комп'ютер заражається мережевим вірусом. Після повернення він підключається до локальної мережі, і його ноутбук стає джерелом зараження.

Аналіз. Дана ситуація досить поширена, тобто в цьому випадку вірус проникає в мережу шляхом підключення до мережі зараженого мобільного комп'ютера

(ноутбука, КПК). Проблема посилюється наявністю в сучасних ноутбуках *Wi-Fi*-адаптерів.

Рішення проблеми. Дана проблема не має однозначного рішення. Гарні результати досягаються у випадку встановлення на ноутбук антивіруса і брандмауера, причому установка проводиться адміністраторами, а користувачеві суворо забороняється їх відключати або переконфігуровувати.

7. Робота з електронною поштою в обхід корпоративного поштового сервера.

Сценарій. Користувач заводить один або декілька поштових скриньок в Інтернеті і використовує їх в обхід корпоративного поштового сервера. У результаті він отримує лист з вірусом, і його комп'ютер надалі стає джерелом зараження мережі.

Аналіз. Це досить поширена ситуація. Корпоративний сервер досить легко захистити, встановивши на ньому систему поштових фільтрів і антивірус (як варіант - кілька антивірусів). Робота в обхід поштового сервера відкриває неконтрольований адміністраторами пробій у захисті мережі. Вищесказане відноситься також до засобів онлайнових комунікацій типу *ICQ, MSN Messanger* та їх аналогів.

Рішення проблеми. Найбільш ефективне рішення - заборона для співробітників компанії на використання сторонніх поштових скриньок. З одного боку, даний крок здається драконівською мірою, з іншого - закриває канал витоку інформації і усуває одне з основних джерел проникнення шкідливих програм у мережу.

4.1.3. Методика оцінки системи інформаційної безпеки

Існують дві системи оцінки поточної ситуації в області інформаційної безпеки на підприємстві. Вони отримали образні назви «дослідження знизу вгору» і «дослідження зверху вниз».

Перший метод досить простий, вимагає набагато менших капітальних вкладень, але і володіє меншими можливостями. Він заснований на схемі : «Ви - зловмисник. Ваші дії?». Тобто служба інформаційної безпеки, ґрунтуючись на даних про всі відомі види атак, намагається застосувати їх на практиці з метою перевірки, а чи можлива така атака з боку реального зловмисника.

Метод «зверху вниз» являє собою, навпаки, детальний аналіз всієї існуючої схеми зберігання і обробки інформації. Першим етапом цього методу є визначення, які інформаційні об'єкти і потоки необхідно захищати. Далі слідує вивчення поточного стану системи інформаційної безпеки з метою визначення, що з класичних методів захисту інформації вже реалізовано, у якому обсязі і на якому рівні. На третьому етапі проводиться класифікація всіх інформаційних об'єктів на класи згідно з їх конфіденційністю та вимогами до надійності і цілісності (незмінності).

Далі йде з'ясування, наскільки серйозний збиток може принести фірмі розкриття або інша атака на кожен конкретний інформаційний об'єкт. Цей етап носить назву «обчислення ризиків». У першому наближенні ризиком називається добуток «можливого збитку від атаки» на «вірогідність такої атаки». Збиток від атаки може бути представлений як від'ємне значення числа у відповідності з табл. 4.1.

Таблиця 4.1.

Ймовірність появи та наслідки ризиків інформаційної безпеки

Ймовірність / Розмір збитку	0 - відсутній	1 – рідше, ніж раз на рік	2 – близько 1 разу на рік	3 – близько 1 разу на місяць	4 – близько 1 разу на тиждень	5 – практично щодня
0 Розкриття інформації не принесе морального і фінансового збитку фірмі						
1 Збиток від атаки є, але він незначний, основні фінансові операції та стан фірми на ринку не порушені						
2 Фінансові операції не ведуться протягом деякого часу, за цей час фірма терпить збитки, але її положення на ринку і кількість клієнтів змінюються мінімально						
3 Значні втрати на ринку і в прибутку. Від фірми йде відчутна частина клієнтів						
4 Втрати дуже значні, фірма						

на період до року втрачає позиції на ринку. Для відновлення положення потрібні великі фінансові позики						
5 Фірма припиняє існування						

Наступним етапом складається таблиця ризиків підприємства (табл. 4.2).

Таблиця 4.2.

Таблиця ризиків підприємства

Опис атаки	Збиток	Ймовірність	Ризик (=Збиток*Ймовірність)

На етапі аналізу таблиці ризиків приймається значення деякого максимально допустимого ризику, наприклад, значення 7 балів. Спочатку перевіряється кожен рядок таблиці на неперевищення ризику цього значення. Якщо таке перевищення має місце, значить, цей рядок - одна з першочергових цілей розробки політики безпеки. Потім проводиться порівняння подвоєного значення (в нашому випадку 7*2=14) з інтегральним ризиком (комірка «Усього»). Якщо інтегральний ризик перевищує допустиме значення, значить, у системі набирається безліч дрібних погрішностей в системі безпеки, які в сумі не дадуть підприємству ефективно працювати. У цьому випадку з рядків вибираються ті, які дають найбільш значний внесок у значення інтегрального ризику і здійснюється спроба їх зменшити або усунути повністю.

На самому відповідальному етапі проводиться власне розробка політики безпеки підприємства, яка забезпечить належні мінімальні рівні як окремих ризиків, так і інтегрального ризику. При її розробці необхідно, однак, враховувати об'єктивні проблеми, які можуть встати на шляху реалізації політики безпеки. Такими проблемами можуть стати закони країни і міжнародного співтовариства, внутрішні вимоги корпорації, етичні норми суспільства.

Після опису всіх технічних і адміністративних заходів, запланованих до реалізації, проводиться розрахунок економічної вартості даної програми. У тому випадку, коли фінансові вкладення в програму безпеки є неприйнятними або просто економічно невигідними порівняно з потенційним збитком від атак, здійснюється повернення на рівень, де задавалося значення максимально допустимого ризику 7 балів і збільшення його на один або два пункти.

Завершується розробка політики безпеки її затвердженням у керівництва фірми і детальним документуванням. За цим повинна слідувати активна реалізація всіх зазначених у плані компонентів. Перерахунок таблиці ризиків і, як наслідок, модифікація політики безпеки фірми найчастіше проводиться раз на два роки.

4.1.4. Організація захисту інформації в системі управлінського обліку аудиторської компанії

Для вирішення проблеми захисту інформації аудиторської компанії, інформація якої пов'язана з підвищеною конфіденційністю, необхідно використовувати комплекс заходів, який складається з таких елементів (рис. 4.1):

1. Перешкода - фізично блокує зловмисникові шлях до інформації, що має бути захищена (на територію і в приміщення з апаратурою, носіїв інформації).

2. Управління доступом - спосіб захисту інформації регулюванням використання всіх ресурсів системи (технічних, програмних засобів, елементів даних).

Управління доступом включає наступні функції захисту:

- ідентифікацію користувачів, персоналу і ресурсів системи, причому під ідентифікацією розуміється присвоєння кожному об'єкту персонального імені, коду, паролю і упізнання суб'єкта або об'єкта по наданим їм ідентифікаторам;
- перевірку повноважень, що полягає у перевірці відповідності дня тижня, часу доби, а також потрібних ресурсів і процедур встановленому регламенту;
- дозвіл і створення умов роботи в межах встановленого регламенту;
- реєстрацію звернень до захищених ресурсів;

- реагування (затримка робіт, відмова, відключення, сигналізація) при спробах несанкціонованих дій.

3. Маскування - спосіб захисту інформації шляхом її криптографічного кодування. При передачі інформації по лініях зв'язку великої протяжності криптографічне закриття є єдиним способом надійного захисту.

4. Регламентація - полягає в розробці і реалізації комплексів заходів, що створюють такі умови автоматизованої обробки і зберігання в важливої інформації, при яких можливості несанкціонованого доступу до неї зводилися б до мінімуму. Для ефективного захисту необхідно чітко регламентувати структурну побудову локальної мережі (архітектура будівель, обладнання приміщень, розміщення апаратури), організацію та забезпечення роботи всього персоналу, зайнятого обробкою інформації.

5. Примус - користувачі та персонал змушені дотримуватися правил обробки і використання важливої інформації під загрозою матеріальної, адміністративної або кримінальної відповідальності.

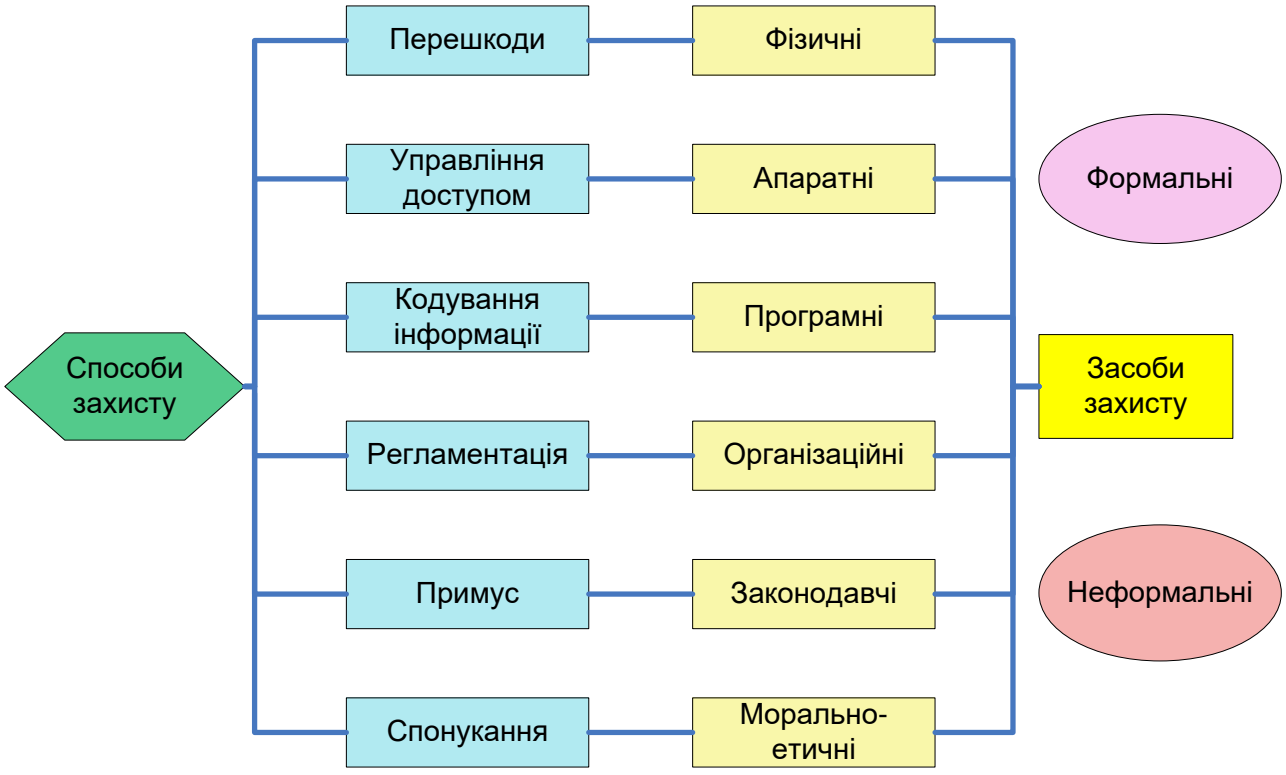

Рис. 4.1. Заходи захисту інформації

Розглянемо захист інформації шляхом створення перешкод для зловмисників.

Існує великий арсенал методів забезпечення інформаційної безпеки:

- міжмережеві екрани;
- віртуальні приватні мережі;
- засоби контентної фільтрації;
- інструменти перевірки цілісності вмісту дисків;
- засоби антивірусного захисту;
- системи виявлення вразливостей мереж і аналізатори мережевих атак.

Кожен з перерахованих засобів може бути використано як самостійно, так і в інтеграції з іншими. Це робить можливим створення систем інформаційної захисту для мереж будь-якої складності і конфігурації, не залежних від використовуваних платформ.

Міжмережевий екран являє собою систему або комбінацію систем, що утворюють між двома або більше мережами захисний бар'єр, який оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних.

Основний принцип дії міжмережевих екранів - перевірка кожного пакета даних на відповідність вхідної та вихідної *IP*-адреси базі дозволених веб-сайтів. Таким чином, міжмережеві екрани значно розширюють можливості сегментування інформаційних мереж і контролю за циркулюванням даних.

Говорячи про міжмережеві екрани, слід згадати про захищені віртуальні приватні мережі *VPN*. Їх використання дозволяє вирішити проблеми конфіденційності та цілісності даних при їх передачі по відкритим комунікаційним каналам. Використання *VPN* можна звести до вирішення трьох основних завдань:

1) захист інформаційних потоків між різними офісами компанії (шифрування інформації проводиться тільки на виході у зовнішню мережу);

2) захищений доступ віддалених користувачів мережі до інформаційних ресурсів компанії, здійснюваний через інтернет;

3) захист інформаційних потоків між окремими програмами корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється з внутрішніх мереж).

Захист інформації в розумінні *VPN* включає в себе кодування, підтвердження автентичності і контроль доступу. Кодування передбачає шифрування інформації, що передається через *VPN*. Прочитати отримані дані може лише власник ключа до шифру.

Контроль трафіку передбачає визначення та керування пріоритетами використання пропускної смуги *VPN*. З його допомогою ми можемо встановити різні пропускні смуги для мережних додатків і сервісів залежно від ступеня їх важливості.

Ефективний засіб захисту від втрати конфіденційної інформації - фільтрація вмісту вхідної та вихідної електронної пошти. Перевірка самих поштових повідомлень і вкладень у них на основі правил, встановлених в організації, дозволяє також убезпечити компанію від відповідальності за судовими позовами і захистити їх співробітників від спаму. Засоби контентної фільтрації перевіряють файли всіх поширених форматів, у тому числі стиснуті та графічні. При цьому пропускна здатність мережі практично не змінюється.

Всі зміни на робочій станції або на сервері можуть бути відстеженні адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диска *(integrity checking)*. Це дозволяє виявляти будь-які дії з файлами (зміна, видалення або ж просто відкриття) і ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (*CRC*_сум).

Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілих файлів із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти нові вірусні програми. Виявлені об'єкти можуть піддаватися лікуванню, ізолюватися (міститися в карантин) або видалятися. Захист від вірусів може бути встановлений на робочі станції, файлові і поштові сервера, міжмережеві екрани, що працюють під практично будь-якою з поширених

операційних систем (*Windows*, *Unix* і *Linux*-системи, *Novell*) на процесорах різних типів.

Фільтри спаму значно зменшують непродуктивні витрати, пов'язані з розбором спаму, знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників компанії в шахрайські операції. Крім того, фільтри спаму зменшують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси (які навіть ще не увійшли до бази антивірусних програм) часто мають ознаки спаму і фільтруються. Правда, позитивний ефект від фільтрації спаму може бути перекреслений, якщо фільтр поряд зі сміттєвими видаляє або позначає як спам і корисні повідомлення, ділові або особисті.

Для протидії природним загрозам інформаційної безпеки в компанії має бути розроблений і реалізований набір процедур щодо запобігання надзвичайним ситуаціям (наприклад, щодо забезпечення фізичного захисту даних від пожежі) і мінімізації збитку в тому випадку, якщо така ситуація все-таки виникне. Один з основних методів захисту від втрати даних - резервне копіювання з чітким дотриманням встановлених процедур (регулярність, типи носіїв, методи зберігання копій тощо.)

Розглянемо криптографічний захист інформації.

Криптографія - це наука про забезпечення безпеки даних. Вона займається пошуками рішень чотирьох важливих проблем безпеки - конфіденційності, аутентифікації, цілісності та контролю учасників взаємодії. Шифрування - це перетворення даних у нечитабельну форму, використовуючи ключі шифрування-розшифровки. Шифрування дозволяє забезпечити конфіденційність, зберігаючи інформацію в таємниці від того, кому вона не призначена.

Криптосистема складається з одного або більше алгоритмів шифрування (математичних формул); ключів, які використовуються цими алгоритмами шифрування; системи керування ключами; нешифрованого тексту; зашифрованого тексту.

У цієї методології алгоритм шифрування об'єднує ключ з текстом для створення шифротексту. Безпека систем шифрування такого типу залежить від конфіденційності ключа, який використовується в алгоритмі шифрування, а не від зберігання в таємниці самого алгоритму. Багато алгоритмів шифрування є загальнодоступними і були добре перевірені завдяки цьому.

Існують дві методології з використанням ключів - симетрична (із секретним ключем) і асиметрична (з відкритим ключем). Кожна методологія використовує свої власні процедури, свої способи розподілу ключів, типи ключів і алгоритми шифрування і розшифровки ключів.

Апаратне шифрування.

Більшість засобів криптографічного захисту даних реалізовано у вигляді спеціальних апаратних пристроїв. Ці пристрої вбудовуються в лінію зв'язку і здійснюють шифрування всієї переданої ними інформації. Переважання апаратного шифрування над програмним обумовлено декількома причинами:

1) Для апаратного шифрування характерна більша швидкість. Криптографічні алгоритми складаються з великої кількості складних операцій, що виконуються над бітами відкритого тексту. Сучасні універсальні комп'ютери погано пристосовані для ефективного виконання цих операцій. Спеціалізоване обладнання вміє робити їх набагато швидше.

2) Апаратуру легше фізично захистити від проникнення ззовні. Програма, запущена на персональному комп'ютері, практично беззахисна. Озброївшись відладчиком, зловмисник може таємно внести в неї зміни, щоб зменшити стійкість використовуваного криптографічного алгоритму, і ніхто нічого не помітить. Що ж стосується апаратури, то вона зазвичай розташовується в спеціальних контейнерах, які роблять неможливим зміну схеми її функціонування. Чіп покривається зверху спеціальним хімічним складом, і в результаті будь-яка спроба подолати захисний шар цього чіпа призводить до самознищення його внутрішньої логічної структури.

3) Апаратура шифрування більш проста в установці. Дуже часто шифрування потрібно там, де додаткове комп'ютерне обладнання є зайвим. Телефони, факси та

модеми значно дешевше обладнати пристроями апаратного шифрування, ніж вбудовувати в них мікрокомп'ютери з відповідним програмним забезпеченням.

Програмне шифрування.

Будь-який криптографічний алгоритм може бути реалізований у вигляді відповідної програми. Переваги такої реалізації очевидні: програмні засоби шифрування легко копіюються, вони прості у використанні, їх неважко модифікувати у відповідності з конкретними потребами.

У всіх розповсюджених операційних системах є вбудовані засоби шифрування файлів. Зазвичай вони призначені для шифрування окремих файлів, і робота з ключами цілком покладається на користувача. Тому застосування цих засобів вимагає особливої уваги: по-перше, у жодному разі не можна зберігати ключі на диску разом із зашифрованими з їх допомогою файлами, а по-друге, незашифровані копії файлів необхідно стерти відразу ж після шифрування.

Методологія криптографічного захисту інформації використовується для створення електронного цифрового підпису.

Електронний цифровий підпис - засіб, що дозволяє на основі криптографічних методів надійно встановити авторство і справжність документа.

Електронний цифровий підпис дозволяє замінити при безпаперовому документообігу традиційні печатку і підпис. Цифровий підпис не має нічого спільного з послідовністю символів, відповідних друку або підпису. При побудові цифрового підпису замість звичайного зв'язку між печаткою або рукописної підписом і аркушем паперу виступає складна математична залежність між документом, секретним і загальнодоступним ключами, а також цифровим підписом. Неможливість підробки електронного цифрового підпису спирається на дуже великий обсяг необхідних математичних обчислень.

Кожен абонент, що володіє правом підпису, самостійно на автономному комп'ютері формує два ключа підпису: секретний і відкритий.

Секретний ключ використовується для вироблення підпису. Тільки секретний ключ гарантує неможливість підробки зловмисником документа і цифрового

підпису від імені, що завірене. Кожен користувач системи цифрового підпису повинен забезпечити збереження в таємниці свого секретного ключа.

Відкритий ключ обчислюється як значення деякої функції від секретного, але знання відкритого ключа не дає можливості визначити секретний ключ. Відкритий ключ може бути опублікований і використовується для автентифікації документа і цифрового підпису, а також для попередження шахрайства з боку особи, що завіряє, у вигляді її відмови від підпису документу. Відкритим ключем можна користуватися тільки в тому випадку, якщо відомі його справжність і авторство, що підтверджується сертифікатом.

В роботі аудиторської компанії широко використовується електронний цифровий підпис, насамперед, при поданні звітності до податкової інспекції та інших контролюючих органів, а також при здійсненні банківських платежів.

Інші види шифрування використовуються для зберігання конфіденційної електронної інформації, для обміну даними з підрозділами та співробітниками, що працюють віддалено.

В даних випадках найбільшу важливість становить таке зберігання секретних ключів, яке б повністю виключило можливість їх потрапляння до сторонніх осіб.

Розглянемо захист інформації шляхом розробки регламентуючих документів.

При цьому поєднуються елементи регламентації та примусу. Заходи примусу використовуються при порушеннях затверджених регламентуючих документів.

Основними регламентуючими документами є положення про комерційну таємницю і положення про захист інформації.

Положення про комерційну таємницю є основним документом, в якому вказано, яка інформація вважається комерційною таємницею фірми. Даний документ містить кілька типових розділів:

- загальні положення - тут розміщуються вступна частина і посилання на закони, на яких засновано дане положення;
- основні поняття комерційної таємниці - докладні тлумачення всіх термінів і понять, зокрема інформації, що становить комерційну таємницю, ноу-хау, режиму комерційної таємниці, носіїв комерційної таємниці;

- захист комерційної таємниці - це зведення заходів і методик, які застосовуються або можуть застосовуватися організацією для захисту комерційної таємниці. В цьому розділі, як правило, описується порядок отримання доступу до комерційної таємниці і покарання за її розголошення;

- перелік відомостей, що становлять комерційну таємницю;

- спеціальні обов'язки осіб, допущених до комерційної таємниці і відповідальних за захист комерційної таємниці.

З точки зору захисту корпоративної мережі інтерес представляють останні два пункти. По-перше, все, що стосується структури локальної мережі, застосовуваних засобів захисту і конфігурації цих засобів, має бути оголошено інформацією категорії «конфіденційно». Відповідно в розділі про обов'язки осіб, допущених до комерційної таємниці, повинна бути описана процедура підключення користувача до ресурсів, що містять інформацію, що становить комерційну таємницю. Ідеальним варіантом є розробка уніфікованої заявки на підключення, яка затверджується службою безпеки і безпосереднім керівництвом користувача. У цій заявці можна передбачити графу, що заповнюється IT-спеціалістом з відміткою про дату подання доступу. Ведення подібних заявок з їх реєстрацією і нумерацією дозволяє встановити жорсткий порядок надання доступу до інформації.

Розробка Положення про захист інформації повинна проводитися IT-фахівцями (або фахівцями служби безпеки за участю IT-фахівців). Цей документ регламентує порядок роботи користувачів корпоративної мережі та встановлює їх права та обов'язки. Ідеологічно положення про захист інформації спирається на положення про комерційну таємницю. Типове положення про захист інформації містить чотири основні пункти:

- загальні положення, в яких описані призначення документа і його складу;

- вимоги до процесу розробки та впровадження програмного забезпечення власної розробки - регламентують відносини розробників ПЗ і адміністраторів і описують вимоги до програмного забезпечення в плані інформаційної безпеки;

- вимоги до сторонніх розробників - тут, крім власне вимог, необхідний опис процедури експертизи та порядку її проведення;

- обов'язки персоналу щодо забезпечення режиму інформаційної безпеки при експлуатації засобів обчислювальної техніки, мережевих комунікацій і програмного забезпечення - це основний розділ, в якому детально регламентуються всі правила поведінки користувача в мережі, порядок використання програмних і апаратних засобів. Крім того, у цьому розділі регламентується взаємодія між користувачем і адміністраторами;

- дії посадових осіб у разі порушення режиму інформаційної безпеки - розділ містить детальну схему, описує порядок дій у разі виникнення нештатних ситуацій або порушень режиму безпеки. Крім того, в цьому розділі описується порядок відключення користувача від наданих йому ресурсів мережі у разі порушень.

Після розробки положення про захист інформації воно доводиться до всіх співробітників під розписку і призначаються працівники, відповідальні за контроль над дотриманням затвердженого положення.

Таким чином, через специфіку аудиторської діяльності, а саме через підвищені вимоги до збереження комерційної таємниці, в корпоративній мережі компанії необхідно використовувати повний комплекс заходів забезпечення інформаційної безпеки.

4.2. Підвищення ефективності функціонування бази даних корпоративної системи

Розглянемо підвищення ефективності функціонування корпоративної системи використанням бази даних з розподілом даних на основі фаз. Системні обчислення ґрунтуються на фазах, які можуть бути роз'єднаними і виконуються одночасно. Кожна фаза генерує значне число вихідних файлів, розкиданих по усій площі розподіленої комп'ютерної бази даних. Ці файли мають бути пересобраны між фазами для того, щоб викликати наступне введення.

Сервіс-орієнтована архітектура COA, киберінфраструктура (*SOAC*) розроблені для виконання обчислень такого плану.

Розглянемо опис метаданих і алгоритмів управління ними, необхідних для управління розподіленим виконанням завдань, що є частиною багатофазних потоків,

у тому числі перерозподіл даних між фазами. Метадані - це облікова інформація про використання системних ресурсів даними. Замість посилальних списків, чиї елементи вказують на фактичні дані, метадані використовуються для того, щоб забезпечити структуру більшою динамікою і економічністю. У традиційних, сильносвязанных паралельних системах параметри доменів безпосередньо присоеденены до вузлів і метадані зазвичай прості. Проте, в розподілених мережах, специфічні ресурси абстрактні, пряма відповідність між доменами і ресурсами втрачається, тому використання ретельно розроблених метаданих являється, в даному випадку найбільш раціональним виходом.

Введення метаданих є вирішальним в розробці системи, що вимагає підтримки одночасного виконання і роботи системи в розподіленому різнотипному середовищі.

Для підтримки ресурсів загального доступу метадані повинні включати набір семафорів. Один семафор включається в дискриптор проекту. Для кожного прийому даних потрібний власний семафор. Отже, існують семафори метаданных, що відносяться до кожного *l* завдання, включаючи і проект. Кожен з цих семафорів, управляє доступом до відповідного завдання і завдання даних.

Дуже важливо зберігати метадані в центральній базі даних з моменту, коли управління проектом починає оперувати з кэшированной копією прийому проекту. Вследствии цього, додатково до семафора при кожній операції прийому і в дескрипторі проекту включається лічильник. Лічильники рахують число змін, але заздалегідь контролюється операція прийому і тестується дескриптор проекту тестуються.

Для перевірки послідовності кешированной доставки досить просто порівняти стан лічильника у базі даних з кешированной копією. Доступ до семафора здійснюється шляхом його повороту. Гарантія послідовності забезпечується механізмом блокування даних, який доступний на сервері бази даних.

Для передачі прийнятої інформації з сервера на сервер і зберігання у базі даних треба конвертувати отримані дані в деякий формат, що відрізняється від *java класу.* Для цієї мети використуємо *XML*. Бібліотека надає можливість зберігання вмісту атрибутів *java* класу у вигляді *XML* файлу. Структура *XML* файлу ієрархічної

структури початкового java класу співпадає з кожним *XML* тегом, пов'язаним з відповідним атрибутом класу. Далі *XML* файл може бути переданий або збережений у базі даних. Бібліотека також надає можливість зворотної конвертації знову в *java* для подальшої обробки.

У базі даних зберігається дискриптор проекту зберігатися у базі даних, включаючи усі прикріплені дані і важливі метадані. Цим забезпечується можливість збереження даних для їх застосування при отриманні наступних даних. В основному розглядаються метадані, спрямовані на розподілене виконання, спільний контроль і управління проектами в розподілених середовищах.

У структурі корпоративної системи УОАК передбачається використання розподіленої об'єктно - орієнтованої система баз даних (РООСБД)

Основною властивістю цієї архітектури є використання працюючих спільно агентів для виконання запитів і транзакцій бази даних, використання механізму видаленого об'єкту для спільного обміну інформацією між агентами багаторівневих транзакцій.

Для працездатності бази даних і виконання концепції багаторівневих транзакцій стосовно об'єктів рекомендується використання безлічі рівнів. Представлена система використовує гібридний багаторівневий паралельний протокол *FoPL,* який об'єднаний з багаторівневою системою відновлення, заснованої на використанні системи *ARIES*.

Доцільним вважається створення системи на основі застосування базової об'єктно-орієнтованої моделі. Однією з її переваг, по порівнянню, з моделлю *ODMG's* являється її математична суворість. По суті пропонована система, як і усі сучасні бази даних має багаторівневу внутрішню архітектуру. База даних може бути представлена як сукупність фізичних об'єктів, що зберігаються в постійному пристрої, що запам'ятовує. Доступ до цих об'єктів можливий за допомогою засобів облаштувань управління пам'яттю. Система має справу з дисковим простором і підтримує високий рівень доступу до фізичних об'єктів. Модуль кеширования окрім управління сторінкою в головній пам'яті підтримує принцип записів. Записи, які використовуються у більшості випадків, відображаються разом на одній сторінці

(якщо це можливо). З того моменту, коли безліч записів занесені на одну сторінку, протоколи операцій мають бути синхронізовані. Це досягається шляхом використання короткочасних регістрів-клямок. Модуль кеширования має два чітко визначених інтерфейсу: інтерфейс сторінки і інтерфейс запису. Інтерфейс сторінки доступний усім вищим рівням. Серед інших він використовується для зберігання оперативних, організаційних і допоміжних даних. Інтерфейс запису використовується для усіх запитів даних. Він доступний тільки модулю на наступному високому рівні- файловому об'єкту зберігання (ФОЗ), який робить можливим інший рівень абстракції по засобах підтримки зберігання об'єктів.

Об'єкт в пам'яті конструюється із записів і має унікальний ідентифікатор об'єкту. ФОЗ підтримує прямі фізичні посилання між об'єктами, що зберігаються, і пропонує пов'язаний з об'єктом асоціативний і навігаційний доступ до об'єктів. Доступ використовує зв'язок між об'єктами в пам'яті так, щоб очуществить реконструкцію об'єктів складнішої структури.

Доступ, пов'язаний з об'єктом, використовує прямий доступ до об'єкту, використовуючи ідентифікатори об'єкту. Асоціативний доступ забезпечує добре відомий доступ через ключові значення. Навігаційний доступ пов'язаний з передачею даних по фізичних посиланнях.

Движок оцінки запитів постійно знаходиться на вершині ФОЗ. Цей елемент виконує запити клієнтських застосувань, як тільки вони передаються з вищих рівнів. Движок оцінки запитів використовує велику кількість агентів, які об'єднуються, всякий раз, коли це можливо, і виконує роботу, потрібну додатками.

Агенти можуть реалізовуватися як потоки. Сукупність агентів, яка працює спільно за запитом додатка, на окремому вузлі РООСБД належить до одного і тому ж процесу. У рамках процесу агенти класифікуються залежно від їх ролей (т. е. *Master або slave*) і у відповідності від їх виду (локальний або розподілений). Агенти з розподіленим відображенням мають здатність розподіляти запити по видалених вузлах РООСБД, оскільки, вони обладнані механізмом видаленого виклику об'єкту. Агенти з локальним відображенням використовуються для виконання под-запросов, які включають тільки об'єкти локальних даних. Об'єкти локальних даних можуть

буть витягнуті тільки за допомогою агентів з локальним відображенням. Таким чином, на локальному або будь-якому видаленому вузлі РООСБД агенти з розподіленим відображенням мають об'єднання, принаймні, з одним локальним агентом. Як результат, движок оцінки запитів є нижчим рівнем в системі бази даних.

Агенти оптимізуються для виконання запитів (запит алгебри операцій, методи, призначені класам і так далі) окремих типів об'єктів, що відповідають їх відображенню. Агенти з розподіленим відображенням виконують запити для складніших об'єктів, які включають об'єкти, що зберігаються в пам'яті локально і видалено. Вони використовують розподіл, паралелізм, багатопоточність і підтримують концепцію транзакцій. Агенти з локальним відображенням використовують паралелізм і багатопоточність для поліпшення виконання запитів локальних об'єктів, які містять тільки об'єкти, що зберігаються локально. Маючи безліч рівнів об'єктів надається можливість використання більше вдосконаленої системи управління транзакціями, заснованою на багаторівневій моделі транзакцій.

Система управління транзакціями управляє і контролює виконання операцій, що виконуються движком оцінки запитів і файловим об'єктом зберігання. Отже, система забезпечує локальний і глобальний сериализм. Система складається з двох компонентів: менеджер транзакцій і менеджер відновлення. Менеджер транзакцій має перевагу виявлення псевдоконфліктів (конфліктів, які не походять з конфлікту високого рівня) і що можливості планування багаторівневого сериализма за допомогою сериализации конкретних операцій (підтранзакцій) рівень за рівнем. Внаслідок цього можуть бути використані різні протоколи специфічних рівнів. Нині підтримується певний двофазний блокувальний протокол *str - 2PL* і гібридний *FoPL.* Їх можна використовувати в усіх можливих комбінаціях на відповідному рівні залежно від вірогідності конфлікту. Менеджер відновлення гарантує атомарність, стійкість і послідовність даних. Це досягається за допомогою підтримки локальних записів, що відбивають оновлення об'єктів на усіх рівнях, підтримка повних і часткових поворотних операцій (підтранзакцій, повторно виконуваних операцій підтранзакцій, відновлення після збоя і так далі). Для їх функціонування

використовується поновлюючий *ARIES/ML* механізм. Він є розширенням добре відомого алгоритму відновлення *ARIES* для багаторівневих систем.

На логічному рівні дані відображаються в термінах моделі даних. Представлена система заснована на узагальненої об'єктно - орієнтованої моделі даних (УООМД). Ця модель розглядає об'єкти, як абстракції об'єктів реального світу. УООМД розрізняє величини і об'єкти. Кожен об'єкт складається з унікального постійного ідентифікатора, набору (тип, значення) пар, набору (властивість, об'єкт) пар і набору методів. УООМД грунтується на довільному типі будь-якої базової системи. Типи використовуються для структуризації значень. Класи служать структурованими базовими елементами для об'єктів, що мають однакову структуру і принцип роботи. Операції, що забезпечуються системою приведеного нижче типу, з одиничним оператор приєднання дозволяють визначити відповідний узагальнений запит алгебри, що породжує. Для того, щоб здійснити розподіл, застосовується певна техніка фрагментації. Це розбиття горизонтальної і вертикальної фрагментації. Для виконання цих завдань використовуються класи. Кожен клас призначається для певного РООСБД вузла, а у разі реплікації декількох РООСБД вузлів, вони об'єднуються в мережу. Отже, фрагментація розбиває на складові частини, (декілька локальних об'єктів) глобальні об'єкти, які відповідають фрагментованій схемі. Зробивши фрагментацію і відношення клас/вузол, необхідно розподілити фрагменти, включаючи фрагментовані методи, по відповідних вузлах РООСБД.

Об'єкти, утворені в результаті фрагментації, прямо не відповідають об'єктам, що обробляються агентами движка оцінки запитів. Крім того, запити високого рівня, транзакції, об'єктні методи і так далі мають бути переведені в код, який може бути интерпритирован цими агентами. Концептуальний інтервал між логічним УООМД рівнем і движком оцінки запитів сполучений мостом з модулем віддзеркалення. Макромова формулює транзакції високого рівня(наприклад, загальні операції оновлень і алгебра високого рівня). Модуль обробки запитів підтримує УООМД, фрагментацію і розподіл. Крім того, використовується оптимізатор запитів, який формує план виконання для оцінки запиту користувача. План виконання використовується модулем віддзеркалення, в якому конструкції високого рівня

заміщаються макросами. Далі движок оцінки запитів використовуватиме план виконання з макросами для визначення кількості запитів користувача.

Внутрішнє представлення об'єктів, копіювання, розподіл даних і т. д. приховано від користувача. Це здійснюється за допомогою призначеного для користувача інтерфейсу. Разом з цим, інтерфейс надає діалогові інтерфейси, засновані на діалогових об'єктах, які визначаються розширеними оглядачами. Ці діалогові об'єкти можуть бути створені у будь-якому сегменті мережі. Виклик операції, пов'язаної з таким діалоговим об'єктом, створить основного агента і приступить до виконання транзакції високого рівня (запит користувача).

Кластери і грати робочих станцій надають ресурси, доступні для роботи з даними. Для використання цих ресурсів потрібні нові алгоритми і детальна розробка способу розподілу даних і подальшого використання цього розподілу. Розглядається дубльований алгоритм послідовної кластеризації. Основною ознакою інтелектуального розподілу є максимальна однотипність розділених фрагментів. Ця ознака дозволяє паралелізувати завдання, що зазвичай зустрічається у базі даних.

Кластеризація - це процес розподілу даних на окремі групи (кластери) таким чином, що об'єкти усередині одного і того ж кластера подібні, але не подібні до об'єктів з інших кластерів.

При кластеризації використовуються ієрархічні методи, що спочатку передбачають розподіл кластерів унікальних типів і здійснюючі об'єднання з сусідніми кластерами до тих пір, поки не зустрінеться завершуюча умова.

Методи розподілу спочатку розглядають розподіл з одним кластером, який що містить в собі усі екземпляри класу, і кластерів, що здійснюють повторне переміщення, до завершення. Загальний ітеративний алгоритм послідовної розподіленої кластеризації призводить до глобального розподілу бази даних, шляхом прив'язки двох розділених частин на кожному повторенні.

4.3. Висновки за розділом

Для вирішення проблеми захисту інформації аудиторської компанії, інформація якої пов'язана з підвищеною конфіденційністю, необхідно використовувати комплекс заходів, який складається з таких елементів: перешкода - фізично блокує зловмисникові шлях до інформації, що має бути захищена (на територію і в приміщення з апаратурою, носіїв інформації), управління доступом - спосіб захисту інформації регулюванням використання всіх ресурсів системи (технічних, програмних засобів, елементів даних), маскування - спосіб захисту інформації шляхом її криптографічного кодування. При передачі інформації по лініях зв'язку великої протяжності криптографічне закриття є єдиним способом надійного захисту, регламентація - полягає в розробці і реалізації комплексів заходів, що створюють такі умови автоматизованої обробки і зберігання в важливої інформації, при яких можливості несанкціонованого доступу до неї зводилися б до мінімуму. Для ефективного захисту необхідно чітко регламентувати структурну побудову локальної мережі (архітектура будівель, обладнання приміщень, розміщення апаратури), організацію та забезпечення роботи всього персоналу, зайнятого обробкою інформації, примус - користувачі та персонал змушені дотримуватися правил обробки і використання важливої інформації під загрозою матеріальної, адміністративної або кримінальної відповідальності.

Розподілена обєктно-орієнтована система баз даних є перспективним напрямом, що розвивається, за рахунок загального використання агентів, які управляють транзакціями у базах даних. Це забезпечує підвищення ефективності функціонування корпоративної системи.

Загальний алгоритм послідовної розподіленої кластеризації забезпечує якісний результат, такий же як і збільшення швидкості системи шляхом підвищення паралельних і розподілених обчислень. При цьому підвищується рівень складності і коефіцієнт посилення в завданні асоціативних правил. Фаза кластеризації повинна розподілятися і виконуватися швидко, щоб не було зниження загального часу системного виконання.

ВИСНОВКИ

Запровадження корпоративної комп’ютерної мережі системи управлінського обліку підприємства варто здійснювати поступово, починаючи з найбільш важливої ланки: побудови сховища даних, що дозволить швидко одержати позитивний ефект у вигляді більшої керованості компанією.

Важливим етапом розвитку системи управлінського обліку є підключення до корпоративної мережі віддалених філій компанії. Це дозволить обмін інформацією в режимі реального часу, а також потрапляння інформації від філій в сховище даних без викривлень та втрат, що можливі при пересиланні даних електронною поштою.

Впровадження в корпоративну мережу мультимедійних технологій *Unified Communications* можна здійснювати поступово. Для цього потрібно підготувати мережу та приймально-передавальне обладнання, що забезпечить швидку передачу даних великого обсягу. До того ж, дане обладнання має досить високу вартість, і впровадження доцільно розпочати з одного підрозділу, оцінити ефективність, та з відповідними коригуваннями розповсюдити на всю компанію. У ході впровадження обов'язково потрібно організувати тренінги та консультації для співробітників підприємства з організації переходу на більш сучасні форми обміну інформацією.

Згідно сучасним вимогам до корпоративних мереж складних систем, проведеному аналізу особливостей корпоративної системи управлінського обліку в аудиторській компанії у дипломній роботі були розроблені структура корпоративної мережі головного офісу та філій виконано вибір мережного устаткування, програмного забезпечення для бази даних. Розроблена структура сховища даних. Розподілена об’єктно-орієнтована система баз даних є перспективним напрямом, що розвивається, за рахунок загального використання агентів, які управляють транзакціями в базах даних. Це забезпечує підвищення ефективності функціонування корпоративної системи.

Для вирішення проблеми захисту інформації аудиторської компанії, інформація якої пов'язана з підвищеною конфіденційністю, необхідно використовувати комплекс заходів, який складається з таких елементів: перешкода - фізично блокує зловмисникові шлях до інформації, що має бути захищена (на територію і в

приміщення з апаратурою, носіїв інформації), управління доступом - спосіб захисту інформації регулюванням використання всіх ресурсів системи (технічних, програмних засобів, елементів даних), маскування - спосіб захисту інформації шляхом її криптографічного кодування. При передачі інформації по лініях зв'язку великої протяжності криптографічне закриття є єдиним способом надійного захисту, регламентація - полягає в розробці і реалізації комплексів заходів, що створюють такі умови автоматизованої обробки і зберігання в важливої інформації, при яких можливості несанкціонованого доступу до неї зводилися б до мінімуму. Для ефективного захисту необхідно чітко регламентувати структурну побудову локальної мережі (архітектура будівель, обладнання приміщень, розміщення апаратури), організацію та забезпечення роботи всього персоналу, зайнятого обробкою інформації, примус - користувачі та персонал змушені дотримуватися правил обробки і використання важливої інформації під загрозою матеріальної, адміністративної або кримінальної відповідальності.

Розподілена об’єктно-орієнтована система баз даних є перспективним напрямом, що розвивається, за рахунок загального використання агентів, які управляють транзакціями у базах даних. Це забезпечує підвищення ефективності функціонування корпоративної системи.

Загальний алгоритм послідовної розподіленої кластеризації забезпечує якісний результат, такий же як і збільшення швидкості системи шляхом підвищення паралельних і розподілених обчислень. При цьому підвищується рівень складності і коефіцієнт посилення в завданні асоціативних правил. Фаза кластеризації повинна розподілятися і виконуватися швидко, щоб не було зниження загального часу системного виконання.

Матеріали дипломної роботи рекомендується використовувати при розробці корпоративної комп’ютерної мережі підприємства.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бойцев О. Защити свой компьютер от вирусов и хакеров. – СПб.: Питер, 2008, 288 с.

2. Бигелоу С. Сети: поиск неисправностей, поддержка и восстановление. – СПб.: БХВ-Петербург, 2005, 1200 с.

3. Ватаманюк А. Создание и обслуживание локальных сетей.– СПб.: Питер, 2008. – 302 с.

4. Вишневский В.М. Теоретические основы проектирования компьютерных сетей . – М.: Техносфера, 2003. – 512 с.

5. Гектор Гарсиа-Молина, Джеффри Ульман, Дженнифер Уидом. Системы баз данных. Полный курс. – М.: Вильямс, 2003, 1088 с.

6. Жуков І.А., Гуменюк В.О., Альтман І.Є. Комп'ютерні мережі та технології: Навч. посібник. – К.: НАУ, 2004. – 276 с.

7. Костров Б.В. Телекоммуникационные системы и вычислительные сети. — М.: «ТЕХБУК», 2006. — 256 с.

8. Коханович Г.Ф., Чуприн В.М. Сети передачи пакетных данных. — К.: «МК-Пресс», 2006. — 272 с.

9. Кренке Д. Теория и практика построения баз данных. – СПб.: Питер, 2005, 800 с.

10. Кульгин М.В. Компьютерные сети. Практика построения. Для профессионалов. 2-е изд./– СПб.: Питер, 2003. – 462 с.

11. Мелехин В.Ф., Павловский В.Г. Вычислительные машины, системы и сети. – М.: Академия, 2007, 560 с.

12. Жуков І.А. Експлуатація комп'ютерних систем та мереж. / І.А. Жуков, В.І. Дрововозов, Б.Г. Масловський // Навч. Посібник. – К.: НАУ, 2007. – 368 с.

13. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принипы, технологии, протоколы : Учебник для вузов. 4-е изд. – СПб.: Питер, 2010.- 944 с.

14. Паркер Т., Сиян К. TCP/IP. Для профессионалов. 3-е изд. – СПб.: Питер, 2004.- 859 с.