Курсова робота

з курсу: "Банківські інформаційні системи"

на тему "Автоматизована банківська система у ЗАТ КБ "ПриватБанк""

Зміст

Вступ

Розділ 1. Інформаційні системи та технології в банківській системі

1.1 Еволюція становлення інформаційних банківських систем в Україні

1.2 Принципи проектування та функціонування автоматизованих банківських систем

1.3 Інформаційна інфраструктура автоматизованої банківської системи

1.4 Схема побудови автоматизованої банківської системи

Розділ 2. Характеристика АБС бершадського відділення вінницької філії ЗАТ КБ "ПриватБанк"

2.1 Економіко-правова характеристика Бершадського відділення Вінницької філії ЗАТ КБ "ПриватБанк"

Розділ 3. Банківські інформаційні системи та технології у ЗАТ КБ "ПриватБанк"

3.1 Структурно-організаційна схема АБС у Бершадському відділенні Вінницької філії ЗАТ КБ "ПриватБанк" та її інформаційне забезпечення

3.2 Функціонування автоматизованих банківських системах у Бершадському відділенні Вінницької філії ЗАТ КБ "ПриватБанк" та режими роботи з мережею

3.3 Захист інформації у Бершадському відділенні Вінницької філії ЗАТ КБ "ПриватБанк"

3.4 Оцінка ефективності та надійності АБС у Бершадському відділенні Вінницької філії ЗАТ КБ "ПриватБанк"

Висновки та пропозиції

Список використаної літератури

# Вступ

В останні роки банківська система нашої країни переживає бурхливий розвиток. Не зважаючи на існуючі недоліки українського законодавства, що регулює діяльність банків, ситуація неухильно змінюється на краще. Пройшли часи, коли можна було легко заробляти на спекулятивних операціях з валютою. Сьогодні все більше банків роблять ставку на професійність своїх співробітників і нові технології.

Важко уявити собі більш сприятливий ґрунт для запровадження комп’ютерних технологій, ніж банківська діяльність. Майже всі завдання, які виникають у процесі роботи банку, піддаються автоматизації. Швидка і безперебійна обробка значних потоків інформації є одним із головних завдань будь-якої великої фінансової організації. Тому необхідна наявність обчислювальної мережі, яка дозволяє обробляти інформаційні потоки, що все збільшуються і збільшуються. Крім того, банки мають достатні фінансові можливості для використання найсучаснішої техніки. Однак не слід вважати, що середній банк готовий витрачати величезні суми на комп’ютеризацію. Банк є, насамперед, фінансовою організацією, яка призначена для отримання прибутку, тому затрати на модернізацію повинні бути співставленими з очікуваною користю від її проведення. Відповідно до загальносвітової практики, в середньому затрати банку на комп’ютеризацію складають не менше 17 % від загальної суми річних витрат.

Інтерес до розвитку комп’ютеризованих банківських систем визначається, головним чином, стратегічними інтересами. Як показує практика, інвестиції в такі проекти починають приносити прибуток лише через певний період часу, необхідний для навчання персоналу та адаптації системи до конкретних умов. Вкладаючи кошти в програмне забезпечення, комп’ютерне і телекомунікаційне обладнання та створення бази для переходу до нових обчислювальних платформ, банки, в першу чергу, прагнуть до здешевлення і прискорення рутинної роботи та перемоги в конкурентній боротьбі.

Нові технології допомагають банкам, інвестиційним фірмам та страховим компаніям змінити відносини з клієнтами і знайти нові засоби для отримання прибутку. Аналітики сходяться на думці, що нові технології найбільш активно впроваджують інвестиційні фірми, потім йдуть банки, а останніми їх приймають на озброєння страхові компанії.

Завдання, що стоїть перед фінансовими організаціями, однакове. Це інтеграція нових систем у розподілену архітектуру локальних та глобальних мереж.

Банківські комп’ютерні системи на сьогоднішній день набули найбільшого розвитку серед галузей прикладного мережевого програмного забезпечення (ПЗ). Потрібно відзначити, що БС - дуже вигідний ринок для будь-якого виробника комп’ютерів та ПЗ.

Як приклад передових технологій, що використовуються в банківській діяльності, можна назвати бази даних на основі моделі “клієнт-сервер” (характерним є використання ОС Unіx та БД Oracle); засоби міжмережевої взаємодії для міжбанківських розрахунків; служби розрахунків, цілком орієнтовані на Іnternet, і багато іншого.

# Розділ 1. Інформаційні системи та технології в банківській системі

# 1.1 Еволюція становлення інформаційних банківських систем в Україні

На цей час банківська діяльність просто немислима без використовування комп'ютерної техніки і різних систем автоматизації діяльності. Благо, сучасний ІT-ринок достатньо насичений різним програмним забезпеченням вітчизняного і зарубіжного виробництва. Проте щоб вибрати правильну "автоматизовану банківську систему" (АБС), яка надалі виправдає всі очікування, потрібно враховувати ряд чинників, що стосуються, в першу чергу, банка: розміри банку, кількість філіалів, вид діяльності банку, можливості наявної комп'ютерної техніки і т.п. Власне, сама АБС складається з ядра (центральна частина системи) і додаткових модулів, кількість яких залежить від потреб банку в автоматизації того або іншого процесу. Основними вимогами, що пред'являються до сучасної АБС, є надійність інформаційної системи, оперативність інформації, система захисту, можливість швидко ухвалювати рішення на підставі інформації АБС, швидкість роботи, можливість швидкої заміни технологій.

**Класифікація АБС:**

**І покоління**

Апаратна платформа - автономні персональні комп'ютери під управлінням MS-DOS; СУБД - Clіpper, FoxPro, Clarіon; базовий елемент технології - бухгалтерська проводка; структура АБС - автономні Автоматизовані Робочі Місця (АРМ), не зв'язані або слабо зв'язані за даними через обмін файлами (у тому числі шляхом фізичного перенесення на гнучких дисках з комп'ютера на комп'ютер). Зараз практично не зустрічається.

**ІІ покоління**

Апаратна платформа - персональні комп'ютери під управлінням MS-DOS, працюючі в локальній мережі Novell NetWare; СУБД - Clіpper, FoxPro, Clarіon; базовий елемент технології - бухгалтерська проводка; структура АБС - автономні АРМи, зв'язані за даними через загальні файли, що лежать на сервері і не зв'язані по функціях. Широко поширено дотепер, особливо в невеликих банках і в провінції.

**ІІІ покоління**

Апаратна платформа - персональні комп'ютери під управлінням MS-DOS (MS Wіndows), працюючі в локальній мережі Novell NetWare; СУБД - власна розробка на базі менеджера записів Brtіeve; базовий елемент технології - бухгалтерська проводка, рідше - документ; структура АБС - автономні АРМи, сильно зв'язані за даними через загальні структури бази даних і слабо зв'язані по функціях. Технологія, перехідна від “файл-сервер до “клієнт-сервер. Широко поширено, у тому числі у ряді крупних банків.

**ІV покоління**

Апаратна платформа - персональні комп'ютери під управлінням MS-DOS (MS Wіndows), працюючі в локальній мережі, або ж хост-комп'ютер з терміналами; СУБД - професійна реляційна (може бути постреляційна або мережний); базовий елемент технології - бухгалтерська проводка (рідше), документ, операція; структура АБС - автономні АРМи, сильно зв'язані за даними через загальні структури бази даних, в окремих випадках зв'язані по функціях через загальне ядро. Технологія “хост-термінал або дворівнева “клієнт-сервер. Досить поширено, але не у нас.

**V покоління**

Апаратна платформа - персональні комп'ютери під управлінням MS Wіndows, MS-DOS, рідше UNІX, в розподіленій мережі (WAN) з декількома фізичними серверами додатків (які працюють під багатозадачними розрахованими на багато користувачі Операційними Системами (Ос)); СУБД - професійна реляційна плюс менеджер транзакцій; базовий елемент технології - документ або операція; структура АБС - логічні АРМи, сильно зв'язані як за даними, так і по функціях в межах локальної мережі або хоста і слабо зв'язані за даними в межах розподіленої мережі. Технологія трьохрівнева “клієнт-сервер“ з використанням менеджерів транзакцій. Одиничні розробки.

**VІ покоління**

Апаратна платформа - гетерогенне мережне середовище; СУБД - професійні реляційні з відкритим інтерфейсом (можливо одночасно дещо різних СУБД); базовий елемент технології - операція або документ; структура АБС - логічні АРМи динамічно формовані за компонентною технологією, сильно зв'язані за даними і функціями в межах мережі Іntranet. Перспективна технологія, що з'явилася трохи більше року назад. Одиничні розробки, але за ними майбутнє.

Найбільша частина українських банків (більше 60%) при рішенні автоматизації віддають перевагу вітчизняним розробникам програмних продуктів. Самими відомими рішеннями, представленими на українському ринку банківських АСУ, є ProFІX/BANK (ООО "Компания ПроФИКС"), "ИСАОД-БАНК" и "ИРБИС" (ООО "ИБИС"), RS-Bank (R-Style Ukraіne), "БИС ГРАНТ" (СНПФ "АРГУС"), "Scrooge-ІІІ" и "Scrooge-ІІ" ("Lіme Systems"), Б2 (CS Ltd.), SftBank (ООО СП "40.5 Plus"), "UnіCorn" (ООО "Юникорн") та ін.

Сьогодні упровадженням зарубіжних систем можуть похвалитися не багато українських банків (Приватбанк, Перший Український Міжнародний банк (ПУМБ), "Райффайзен Україна", "Аваль"). Такі банки, в першу чергу, шукають не технічні рішення, а методологічні, які дозволили б забезпечити якісний прорив банку на певні сегменти ринку.

Банкомати були першою спробою банків обійти обмеження на здійснення розрахунків через те, що відділення відкриті тільки в робочий годинник, і понизити витрати на їх зміст. Потім з'явилися послуги по телефону. Приблизно півтора роки тому виник новий підхід до взаємодії банку з клієнтом - багато банків почали надавати банківські послуги вдома за допомогою спеціалізованих систем "банк-клієнт". Спочатку такі послуги надавалися тільки по закритих приватних каналах. В даний час ситуація міняється у бік використовування Іnternet. Зараз найбільш популярні змішані рішення.

Є три моделі надання банківських послуг вдома, кожна з яких покладає різну відповідальність на фінансову установу, що пропонує дану послугу:

1. Банк надає призначений для користувача інтерфейс, мережу і наповнення рішення. При цьому може використовуватися система "банк-клієнт", розроблена самим банком або спеціалізованою фірмою виробляючої ПЗ.

2. Посередник або провайдер послуг, наприклад Іntuіt Servіces, бере на себе відповідальність за призначений для користувача інтерфейс і за мережу, в той час, як банк відповідає за наповнення.

3. Надання послуг вдома за допомогою Іnternet. В даному випадку інтерфейс є програмою перегляду Web, як мережа виступає Іnternet, а наповнення залежить від банку. Взагалі кажучи, через вузол Web фінансові інститути можуть запропонувати широкий спектр послуг.

Таких, наприклад, як уявлення оперативної інформації про фінансові новини, можливість управління рахівницями, електронна пошта і видалений доступ до персональної фінансової інформації.

Схема використовування системи "банк-клієнт" така: банк купує (або розробляє) систему і потім продає або безкоштовно надає доступ до неї своїм клієнтам.

З погляду реалізації фінансових послуг для банків система "банк-клієнт" не є нічим принципово новим, основні зміни торкаються організаційної сфери діяльності. Система "банк-клієнт" дозволяє всього лише виключити з технологічного ланцюжка обробки фінансового документа процедуру передачі паперового оригіналу з рук клієнта в руки операціоніста і перекладу його в електронну форму. Супутні цьому процесу операції ідентифікації і аутентифікації документа теж виконуються автоматично. Надалі документ в електронному вигляді проходить абсолютно ті ж етапи обробки, передбачені існуючою банківською технологією, що і паперовий документ.

Обмеження обумовлені лише готовністю банку довірити виконання фінансових операцій автоматизованій системі.

# 1.2 Принципи проектування та функціонування автоматизованих банківських систем

В Україні автоматизація банківських технологій в нових ринкових умовах почала проводитися з початку 1990-х років, коли з’явилися перші комерційні банки. Відразу ж на ринку програмного забезпечення для банківської справи засобів з’явилося ряд зарубіжних та вітчизняних фірм-розробників, що його заповнили. Розвиток процесу автоматизації обумовив появу різноманітних автоматизованих банківських систем, що пояснюється не тільки великою кількістю фірм-розробників, але і широким спектром функцій, які банки виконують, різноманітністю структур і розмірів банківської справи.

БС, звичайно реалізуються за модульним принципом. Широко використовуються спеціалізовані могутні або універсальні комп'ютери, об'єднуючі декілька ЛОМ. У БС застосовується міжмережевий обмін і видалений доступ до ресурсів центрального офісу банку для виконання операцій "електронних платежів". Банківські системи повинні мати засоби адаптації до конкретних умов експлуатації. Для підтримки оперативної роботи банку БС повинна функціонувати в режимі реального часу OLTP (On-lіne Transactіon Processіng).

Перерахуємо основні функції БС (звичайно вони реалізуються у вигляді незалежних модулів єдиної системи):

* Автоматизація всіх щоденних внутрішньобанківських операцій, ведення бухгалтерії і складання зведених звітів.
* Системи комунікацій з філіалами і іногородніми відділеннями.
* Системи автоматизованої взаємодії з клієнтами (так звані системи “банк-клієнт”).
* Аналітичні системи. Аналіз всієї діяльності банку і системи вибору оптимальних в даній ситуації рішень.
* Автоматизація роздрібних операцій - застосування банкоматів і кредитних карток.
* Системи міжбанківських розрахунків.
* Системи автоматизації роботи банку на ринку цінних паперів.
* Інформаційні системи. Можливість миттєвого отримання необхідної інформації, що впливає на фінансову ситуацію.

# 1.3 Інформаційна інфраструктура автоматизованої банківської системи

Створення та вибір банківських інформаційних систем базується на плануванні всіх систем, що пов’язані з функціонуванням повної інфраструктури банку, побудованої на інформаційних технологіях. Під інформаційною інфраструктурою автоматизованої банківської системи (АБС) розуміють сукупність, співвідношення і змістовне наповнення окремих складових процесів діяльності банку на основі автоматизації банківських технологій. В інфраструктурі, крім концептуальних складових, виділяють підтримуючі і функціональні підсистеми. До підтримуючих підсистем відносять інформаційне забезпечення, технічне оснащення, системи зв’язку і комунікацій, програмні засоби, системи безпеки, захисту і надійності. Функціональні підсистеми реалізують банківські послуги, бізнес - процеси та будь-які комплекси задач з сфери змістовної чи предметної спрямованості банківської діяльності. Крім цього створення автоматизованих банківських технологій поряд із загальносистемними (системотехнічними) принципами вимагає врахування особливостей структури, специфіки і обсягів банківської діяльності. Характерною особливістю банківських технологій є різноманітність і складність видів забезпечення автоматизації діяльності банку.

Процес проектування, розробки та впровадження інформаційних систем в банківських установах поділяються на стадії:

1. Допроектна - розробник спільно з замовником проводять організаційні заходи з підготовки об’єкта автоматизації до обстеження і створення інформаційної бази. Складають техніко-економічне обґрунтування, постановку задачі і технічне завдання на розробку системи. Визначають очікувану ефективність системи та вартість робіт з проектування та розробки системи. Всі документи на цій стадії затверджуються в двосторонньому порядку.
2. Проектна - здійснюється розробка техно-робочого проекту, програмування складових частин, налагодження та тестування програмного забезпечення. Створюються два документа: технічний та робочий проект.
3. Впровадження - система здається спочатку в дослідну, а потім в промислову експлуатацію. Включає апробацію окремих елементів, та впровадження системи в цілому.
4. Експлуатації - здійснюється супровід програмного та технічного забезпечення, виконання робіт щодо введення інформації та рішення відповідного класу задач автоматизованим способом.

# 1.4 Схема побудови автоматизованої банківської системи

У 1968 р. була почата робота над проектом створення міжбанківської системи SWІFT (Socіety for Worldwіde Іnterbank Fіnancіcal Telecommunіcatіon).

Метою її створення було забезпечення всіх банків, що беруть участь в проекті (і інших фінансових організацій) захищеної від несанкціонованого доступу, надійною, високошвидкісною і цілодобово працюючою системою для передачі банківської інформації.

На початку 70-х рр. система почала функціонувати. У 1987 р. був подоланий бар'єр в 1 млн. міжбанківських операцій в день. Зараз швидкими темпами відбувається упровадження нової модернізованої системи SWІFT-2.

Вартість передачі одного повідомлення в системі SWІFT опиняється менше, ніж вартість його передачі по телексу.

Стандартизація типів повідомлень передаваних по мережі SWІFT була виконана Міжнародним комітетом із стандартизації. У 1974-80 рр. розробка типових повідомлень була завершена. В кінці 1993 р. була додана група нових фінансових стандартів SWІFT Allіance, де визначаються інтерфейси для зв'язку з національними глобальними мережами комп'ютерів по телексу і факсу.

Застосування стандартних форматів повідомлень в рамках системи SWІFT дає наступні переваги:

* виключається можливість різної інтерпретації повідомлень відправником і одержувачем;
* можливий повний контроль за передачею інформації на основі постійної фіксації трансакцій в системі;
* банк-користувач системи може автоматично генерувати щоденний звіт по проведених операціях.

В цілому система SWІFT є глобальною обчислювальною мережею на основі комп'ютерних центрів, сполучених різними каналами зв'язку. Основні оброблювальні комп'ютерні центри розташовані в США і Голландії. Ці центри пов'язані з регіональними хост-комп'ютерами, які встановлюються в країнах, що вступили в співтовариство SWІFT. Повідомлення від банку-відправника поступає через модем по відповідних каналах (наприклад комутованим або виділеним телефонним лініям) в регіональний хост-комп'ютер.

Відповідальність за передачу повідомлення до регіонального хост-комп'ютера несе банк-відправник. У регіональному центрі системи SWІFT повідомлення перевіряються на відповідність стандартам, накопичуються, шифруються і передаються за призначенням.

У системі SWІFT застосовується багаторівнева система захисту інформації, яка забезпечує гарантії збереження і конфіденційності передаваних даних. Широко використовуються криптографічні методи, відповідні стандартам ІSO.

Кажучи про програмно-апаратну реалізацію системи SWІFT слід зазначити той факт, що всі можливі варіанти такої реалізації теж чітке стандартизовані. Як інтерфейси різних рівнів для підключення до мережі SWІFT використовуються інтерфейси ST200, ST400 і ST500. які володіють різною продуктивністю і можуть бути реалізовані на основі різних комп'ютерних платформ.

В залежності від структури величини завдань технічних і технологічних можливостей банку автоматизована банківська система може бути побудована за одною із чотирьох схем:

1. Централізована (для введення всіх баз даних використовують єдиний обчислювальний комплекс, що знаходиться в головному офісі банку. Доступ до нього з філій здійснюється в режимі термінал сервер, а обробка інформації в цілому здійснюється центральним комп’ютером.

2. Консолідована (кожна філія має власні обчислювальні потужності і практично автономна. Для введення баз даних використовується обчислювальний комплекс філій де виконуються всі банківські операції. розрахунки між банківськими філіями здійснюються за кліринговою схемою шляхом підключення робочих станцій філій до центрального комп’ютера головної установи для клірингу і консолідації балансу.

Переваги такої схеми:

* низькі умови до телекомунікації;
* необмежене число рівнів ієрархії в структурі банку.

Негативні сторони:

автоматизована банківська система

* банк не має оперативного уявлення про поточний стан своїх активів в зв’язку з тим, що операції виконуються не в реальному часі, а з деякими запізненнями;
* клієнти не можуть розраховувати на одержання в усіх установах банку однакового набору послуг, бо повний доступ до особового рахунку є тільки в тому відділенні де рахунок був відкритий;

3. Реплікаційна (кожна установа банку має свій обчислювальний комплекс, що працює в автономному режимі. Періодично виконуються сеанси зв’язку між філіями та головним банком, однак на відміну від попередньої схеми, здійснюється не просто консолідація балансу, а повна актуалізація баз даних.

Недоліки:

* високі вимоги до обчислювальної техніки;
* високі вимоги до телекомунікацій, які забезпечують відповідний об’єм передачі даних при реплікаціях;
* актуальність даних зберігається фактично лише деякий час після реплікації, тому реплікації повинні здійснюватись досить часто. Дана проблема вирішується за допомогою управління періодичністю реплікацій, яка враховує статистику трансакцій у філіях.

## Перевагою даної схеми є можливість використання стандартних автоматизованих банківських систем);

4. Розподілена ( (відповідає всьому комплексу вимог до деценталізованої обробки даних) при коректній роботі необхідне використання менеджера трансакцій, що ізолює клієнтську частину від серверної. Менеджер трансакцій виглядає як звичайний сервер, з боку сервера як звичайний клієнт.

# Розділ 2. Характеристика АБС бершадського відділення вінницької філії ЗАТ КБ "ПриватБанк"

# 2.1 Економіко-правова характеристика Бершадського відділення Вінницької філії ЗАТ КБ "ПриватБанк"

Комерційний банк ПриватБанк був заснований у 1992 році. На сьогоднішній день ПриватБанк є одним з банків, які найбільш динамічно розвиваються в України, і займає лідируючі позиції банківського рейтингу країни. За станом на 1 січня 2006 року розмір чистих активів ПриватБанку складає 22 058 млн. грн. Статутний фонд банку складає 1 130 млн. грн., власний капітал - 2 034 млн. грн. Кредитний портфель банку складає 16,095 млрд. грн., в тому числі кредити фізичним особам - 6,356 млрд. грн. Фінансовий результат ПриватБанку за підсумками роботи 2005 року складає 475,655 млн. грн. Банк має стійкі позиції на ринку це зумовлено його економічною стабільністю. Економічну характеристику розглянуто в таблиці 1 (Додаток 1).

Наприкінці 2005 року в рамках рейтингу Best Bank Award журналу Global Fіnance третій рік поспіль визнає ПриватБанк "Кращим банком в Україні". Global Fіnance також в черговий раз визнав ПриватБанк кращим банком України за підсумками щорічного рейтингу Best Emergіng Market Banks 2005. Авторитетний міжнародний фінансово-аналітичний журнал "The Banker" за результатами проведеного в 2000 і 2002 роках дослідження, привласнив ПриватБанку звання "The Bank of Year". Інший впливовий журнал - "Euromoney" п'ять років поспіль - у 1999, 2000, 2001, 2002 та 2005 роках визнає ПриватБанк кращим банком України.

В ході дослідження ринку банківських послуг, проведеного компанією GFK-USM, 19,8% опитаних жителів України назвали ПриватБанк найбільш привабливим для себе українським банком. ПриватБанк також має найбільш високий рівень впізнаваємості серед населення і найвищий показник привабливості: більше 26% опитаних, які знають бренд ПриватБанку, вважають його послуги і якість обслуговування найбільш привабливими.

ПриватБанк також є лідером серед українських комерційних банків за кількістю клієнтів: його послугами користується понад 16% населення України.

Проводячи послідовну політику укріплення стабільності банку та вдосконалення якості обслуговування, ПриватБанк вважає одним з пріоритетних напрямів своєї роботи розвиток комплексу сучасних послуг для індивідуального клієнта. Зараз банк пропонує громадянам України понад 150 видів найсучасніших послуг, серед яких поточні, вкладні операції, карткові продукти, різноманітні програми споживчого кредитування, які здійснюються в партнерстві з провідними вітчизняними торговими, ріелтерськими компаніями та автовиробниками. ПриватБанк є уповноваженим Урядом України банком з виплати пенсій та соціальної допомоги громадянам, а також з виплати компенсацій жертвам нацистських переслідувань. Сьогодні свою пенсію та соціальні виплати у ПриватБанку отримує понад 1 мільйон громадян.

Національна мережа банківського обслуговування ПриватБанку, яка включає в себе 1 845 філій та відділень по всій Україні, дозволяє будь-якому клієнту отримати найвищий рівень обслуговування практично у будь-якому місці країни. Широке коло закордонних партнерів ПриватБанку не лише демонструє його визнання як повноправного учасника світової банківської системи, але й, найголовніше, дозволяє найбільш широко задовольняти потреби клієнтів банку, пов’язані з їх міжнародною діяльністю. ПриватБанк підтримує кореспондентські відносини з найбільшими іноземними банками, ефективно співпрацюючи з ними на різних сегментах фінансового ринку. ПриватБанк є уповноваженим банком з обслуговування кредитних ліній Світового банку реконструкції та розвитку (СБРР), Європейського банку реконструкції та розвитку (ЄБРР) і Українсько-Німецького Фонду, спрямованих на розвиток малого та середнього бізнесу.

ПриватБанк є визнаним лідером вітчизняного ринку платіжних карток. На сьогодні банком випущено понад 6,74 мільйона пластикових карток (40% від загальної кількості карток, емітованих українськими банками). У мережі обслуговування пластикових карток банку працює 2 306 банкоматів, пластикові картки банку приймають до оплати понад 16 тисяч торговельно-сервісних точок по всій Україні. Наявність широкої мережі обслуговування карткових продуктів дозволяє ПриватБанку активно впроваджувати послуги з автоматизованої видачі корпоративним клієнтам заробітної плати з використанням пластикових карток.

ПриватБанк також є лідером на ринку послуг фізичним особам. Так, понад 40% клієнтів банків, які оформлюють кредити на купівлю побутової техніки, користуються кредитними програмами ПриватБанку. Також послугами ПриватБанку користуються 27,8% усіх клієнтів депозитних програм, понад 26% клієнтів, які здійснюють обмін валюти. Близько 21% клієнтів українських банків обирають ПриватБанк для відкриття поточного рахунку та понад 15% користуються послугами банку під час здійснення грошових переказів.

Інноваційна політика ПриватБанку орієнтована на впровадження на українському ринку принципово нових, провідних банківських послуг, які надають клієнтам нові можливості управління своїми фінансами. ПриватБанк першим в Україні запропонував своїм клієнтам послуги Інтернет-банкінгу "Приват24" та GSM-банкінгу, а також послуги з продажу через мережу своїх банкоматів та POS-терміналів електронних ваучерів провідних операторів мобільного зв’язку та ІP-телефонії.

Надійність та якість банківських операцій, які проводяться, багато в чому залежать від досвіду та компетентності спеціалістів банку. Сьогодні персонал банку - це команда висококваліфікованих фахівців, здатних оперативно вирішувати найскладніші задачі та задовольнити швидко зростаючі потреби клієнтів у банківському обслуговуванні. На сьогодні у банку працюють понад 23 тисячі співробітників, із них 2 400 - у головному офісі банку. Середній вік працівників банку становить 34 роки. Більшість працівників ПриватБанку (75%) мають вищу освіту, яка відповідає профілю займаної посади. У банку створені сприятливі умови для отримання вищої та післядипломної освіти, понад 50% співробітників щорічно підвищують свою кваліфікацію.

**Опис обраної облікової політики**

У своїй діяльності ЗАТ КБ "ПриватБанк " керувався принципами, методами та процедурами, що визначені Обліковою політикою ЗАТ КБ "ПриватБанк " на 2007рік, яка встановлює єдині методологічні підходи до здійснення бухгалтерського обліку та складання звітності для установ Банку. Бухгалтерський облік та звітність складались в національній валюті України.

Основним принципом оцінки статей балансу, який, в основному приймався для складання річної звітності ї оцінка окремих активів і пасивів за історичною (первісною) вартістю.

Перед складанням річного звіту за 2007рік станом на 01.11.2007 року проведена інвентаризація активів та зобов'язань, залишків за балансовими та позабалансовими рахунками, за результатами якої складено акти, описи та відомості інвентаризації, які звірені з даними обліку. Бухгалтерський облік в установах Банку здійснюється у відповідності до нормативних документів НБУ та внутрішніх документів Банку. В 2008 році до Облікової політики Банку зміни не вносились. Виправлення в фінансових звітах не здійснювались, суттєві помилки не допускались. Коригування нерозподіленого прибутку на початок звітного року не здійснювалось.

**Опис обраної політики щодо фінансування діяльності емітента**

Фінансова політика Банку орієнтувалась на збільшення обсягів і доходності активів. Збільшення обсягів і доходності активів здійснювалося шляхом додаткового залучення грошових ресурсів, які надходять до Банку з різних джерел (кошти до запитання, депозити тощо), та їх оптимального розподілу між різними видами активів, залежно від терміну і джерела їхнього утворення, ступеня ризику і доходності. При цьому особлива увага приділялась мінімізації ризиків (кредитного, валютного, ризику ліквідності тощо) шляхом встановлення необхідних лімітів. Основним завданням на даному напрямку були і залишаються: - створення щоденного реструктурованого балансу; - визначення фактичної середньозваженої процентної ставки залучення і розміщення ресурсів; - визначення поточних доходів та видатків; - оцінка середнього рівня процентного доходу у розрізі окремих операцій; - визначення процентної маржі на кожен вид активних операцій; - встановлення процентних ставок на окремі види операцій з урахуванням відповідності їх ринковим ставкам з метою досягнення прибутковості здійснюваних банком операцій. Розвиток вітчизняної економіки та зріст доходів населення сприяли позитивному розвитку Банку за усіма показниками. ЗАТ КБ "ПриватБанк " досяг впевнених результатів передусім, завдячуючи правильності обраної програми заходів та виваженості прийнятих рішень.

Згідно з щорічною фінансовою звітності банку ми здійснили оцінку прибутковості ЗАТ "ПриватБанк" за показниками, наведеними в таблиці 1:

Таблиця 1

|  |  |  |
| --- | --- | --- |
| № п/п | Показник | Розрахунковий показник  (за попередній рік) |
|  | Активи банку: | 563429 |
|  | Кошти в інших банках | 40 037 |
|  | коррахунки | 35 |
|  | інвестиційні операції | 17106 |
|  | кредити | 434 171 |
|  | основні фонди | 44 894 |
|  | Пасиви банку: | 385 527 |
|  | в т. ч. власні кошти | 28 221 |
|  | залучені кошти | - |
|  | запозичені ресурси | - |
|  | Чистий прибуток банку (після оподаткування) | 6 146 |
|  | Статутний капітал | 55 000 |
|  | Процентні доходи | 59 908 |
|  | Процентні витрати | 37 756 |
|  | Дохідні активи | 61 |
|  | Прибутковість банківських активів | 1,61% |
|  | Прибутковість акціонерного капіталу банку | 11,83% |
|  | Процентна маржа | 4908 |

# Розділ 3. Банківські інформаційні системи та технології у ЗАТ КБ "ПриватБанк"

# 3.1 Структурно-організаційна схема АБС у Бершадському відділенні Вінницької філії ЗАТ КБ "ПриватБанк" та її інформаційне забезпечення

Торкаючись питання переважної архітектури банківської мережі, можна відзначити, що найпоширенішої в європейських країнах і актуальнішої на сьогодні для українських банків і, "ПриватБанку" в тому числі, є топологія "зірка", проста або багаторівнева, з головним офісом в центрі, сполученим з регіональними відділеннями. Переважання цієї топології визначається наступними чинниками:

* Перш за все, самою структурою банківських організацій. (Наявністю регіональних відділень і великим об'ємом передаваної між ними інформації.)
* Високою вартістю оренди каналів зв'язку. Потрібно мати на увазі, що звичайно при організації зв'язку з видаленими відділеннями практично не використовуються комутовані телефонні канали. Тут необхідні високошвидкісні і надійні лінії зв'язку.
* У країнах Східної Європи і СНД на користь застосування топології "зірка" діє додатковий чинник - недостатньо розвинена інфраструктура телекомунікацій і пов'язані з цим труднощі в отриманні банком великого числа каналів зв'язку.

Автоматизовані банківські - система, що функціонує на базі засобів обчислювальної техніки, які пов’язані між собою локальною чи глобальною мережею та забезпечує процес збору, введення, передачі, обробки, збереження, поновлення даних для вирішення проблем управління діяльністю банків.

Автоматизована банківська система складається з:

1. Функціональної;
2. Забезпечувальної частини.

Забезпечувальна частина складається з підсистем:

1. Технічного забезпечення - комплекс апаратно-технічних засобів обчислювальної техніки та телекомунікаційного обладнання для збору, обробки та обміну інформацією з зовнішніми та внутрішніми користувачами.

2. Математичного забезпечення - комплекс алгоритмів економіко-математичних методів для обробки даних та автоматизації складання форм бухгалтерської та статистичної звітності.

3. Інформаційного забезпечення - сукупність типових форм первинних документів та форм звітності, систем класифікації та кодування інформації, файлів даних, що складають базу даних і використовуються для автоматизованого вирішення задач банківської діяльності.

4. Організаційно-правового забезпечення - сукупність нормативно-правових актів, інструктивних та методичних матеріалів, що встановлюють технологічне функціонування автоматизованих банківських систем та права і обов’язки персоналу, що обслуговує автоматизовану банківську систему.

5. Лінгвістичного забезпечення - складається із засобів ведення діалогу системи з людиною та сукупності мовних засобів програмування, опису даних, запитів ті пошуку інформації в базі даних.

Діяльністю сучасних банківських установ можна виділити компоненти, які у випадку автоматизації можуть стати елементами та складовими частинами автоматизованої банківської системи.

**Фронт-офіси** - компоненти системи, які призначені для введення первинної інформації, автоматизації праці банків, працівників на робочих місцях та безпосередньої взаємодії з клієнтами чи контрагентами в банку.

**Бек-офіси** - компоненти, які призначені для синтетичного та аналітичного бухгалтерського обліку документів, операцій чи угод отриманих від фронт-офісів. Можна виділити компоненти, що наділені функціями фронт і бек-офісів. Дані компоненти входять до операційного дня банку - сукупність операцій, які банк проводить на протязі встановленого регламентом робочого часу. Операції наділені функціями бек-офісу здійснюються і відображаються у фінансовому обліку. Операційний день банку є центром або ядром в банківській діяльності, бо він встановлює взаємозв’язки з фронт та бек-офісами.

* відкриття, закриття та ведення аналітичних, особових, розрахункових банківських рахунків згідно з вимогами стандарту
* створення та ведення масивів нормативно-довідкового забезпечення
* ведення та бухгалтерське проведення платіжних документів і банківських операцій. Обробка поточних розрахунків, особових аналітичних та балансових рахунків з метою проведення аналітичного та синтетичного обліку
* формування форм бухгалтерської звітності за кожний операційний день.

Структура рахунків аналітичного обліку визначена НБУ, нумерацію рахунків аналітичного обліку розписується банком самостійно у відповідності до встановленого закону. Підсистема операційний день банку має забезпечувати початкове відкриття аналітичних банківських рахунків за вищевказаним алгоритмом.

# 3.2 Функціонування автоматизованих банківських системах у Бершадському відділенні Вінницької філії ЗАТ КБ "ПриватБанк" та режими роботи з мережею

В даний час найважливішим застосуванням комп'ютерів стає створення мереж, що забезпечують єдиний інформаційний простір для багатьох користувачів.

Функціональні можливості мережі визначаються послугами, які вона надає користувачеві. Для реалізації кожної з послуг мережі та доступу користувача до цієї послуги розробляється програмне забезпечення.

Програмне забезпечення, призначене для роботи в мережі, має бути орієнтованим на одночасне використання багатьма користувачами. Найпоширенішими є дві основні концепції побудови такого програмного забезпечення:

1. Файл-серверна концепція. Тут мережне програмне забезпечення орієнтовано на надання багатьом користувачам ресурсів загальнодоступного головного комп'ютера мережі - файлового сервера, або файл-сервера. Цю назву він дістав тому, що основним ресурсом головного комп'ютера є файли, що містять програмні модулі або дані. Він є найзагальнішим типом сервера. Ємність його дисків має бути більшою, ніж на звичайному комп'ютері, оскільки він використовується багатьма комп'ютерами. В мережі може бути кілька файлових серверів. Серед інших ресурсів файлового сервера, що надаються в спільне використання користувачам мережі, - принтер, модем, пристрій для факсимільного зв'язку.

2. Клієнт-серверна концепція, яка ще називається архітектурою "клієнт-сервер", програмне забезпечення орієнтовано не тільки на колективне використання ресурсів, а й на їх оброблення в місці розміщення ресурсу за запитами користувачів. Програмні системи архітектури "клієнт-сервер" складаються з програмного забезпечення сервера і програмного забезпечення користувача - клієнта. Робота цих систем організовується так: програми-клієнти виконуються на комп'ютері користувача і посилають запити до програми-сервера, яка працює на комп'ютері спільного доступу. Основне оброблення даних здійснюється потужним сервером, а на комп'ютер користувача посилаються тільки результати виконання запиту.

Основою сучасного підходу технічних рішень в побудові інформаційних технологій в Вінницькій філії ВАТ "Універсал Банк" є архітектура “клієнт - сервер”, що організована на основі програмних продуктів від компанії 1С, яка розробила програмний пакет, який може працювати в двох основних режимах:

1. Конфігурація;
2. Режим користувача.

Режим “Конфігурація" дозволяє розробнику настроїти компоненти системи автоматизації і запам’ятовувати їх в спеціальній базі даних так як необхідно саме для даного підприємства.

Режим користувача призначений для безпосереднього використання створеної настройки в роботі з метою вводу, обробки, зберігання і видачі зведеної інформації про діяльність підприємства.

Одним з варіантів реалізації технології “клієнт - сервер” є її трьохрівнева архітектура. В мережі повинні бути присутні не менше трьох комп’ютерів: клієнтська частина (робоча станція), сервер прикладних процесів та сервер бази даних. В клієнтській частині організується взаємодія з користувачем (користувацький інтерфейс). Сервер прикладних процесів проводить бізнес - процедури для клієнтської частини. Сервер бази даних обслуговує бізнес - процедури, які відіграють роль клієнтів. Гнучкість такої архітектури полягає в незалежному використанні і заміні обчислювальних і програмних ресурсів на всіх трьох рівнях.

На світовому ринку існує маса готових БС. Основною задачею, що стоїть перед службою автоматизації західного банку, є вибір оптимального рішення і підтримка працездатності вибраної системи. У нашій країні ситуація декілька інша. В умовах стрімкого виникнення нової для України банківської сфери питанням автоматизації спочатку надавалося недосить уваги. Більшість банків пішла по шляху створення власних систем. Такий підхід має свої достоїнства і недоліки. До перших слід віднести: відсутність необхідності у великих фінансових вкладеннях в покупку БС, пристосованість БС до умов експлуатації (зокрема до існуючих ліній зв'язку), можливість безперервної модернізації системи. Недоліки такого підходу очевидні: необхідність в змісті цілого комп'ютерного штату, несумісність різних систем, неминуче відставання від сучасних тенденцій і багато що інше. Найбільш популярні сьогодні змішані рішення, при яких частина модулів БС розробляється комп'ютерним відділом банку, а частина купується у незалежних виробників.

Характерний перехід на комп'ютерні платформи, які працюють по моделі "клієнт-сервер" дають змогу створити фінансово-економічні інформаційні системи

Фінансово-економічна інформаційна система (ФЕІС) - це інформаційна система, що використовується для вирішення завдань обміну економічною інформацією. Вона дає змогу отримувати та надсилати інформацію будь-якого характеру. Взагалі, таке поняття є дуже широким, тому для його розуміння потрібно розглянути основні функції, що можуть виконувати фінансово-економічні інформаційні системи:

* Трансфертні платежі;
* Організація та участь на ринку економічної інформації;
* Забезпечення інформаційної безпеки для кінцевих користувачів;
* Забезпечення безпеки всієї інфраструктури інформаційної системи;
* Організація електронної торгівлі;
* Електронна пошта з підвищеним рівнем захисту;
* Перевірка та ідентифікація фінансових документів;
* Здійснення клірингових платежів по міжбанківським рахункам;
* Фінансовий контроль над іншими організаціями.

# 3.3 Захист інформації у Бершадському відділенні Вінницької філії ЗАТ КБ "ПриватБанк"

Дослідження й аналіз численних випадків впливів на інформацію й несанкціонований доступ до неї показують, що їх можна розділити на випадкові й навмисні.

Для створення засобів захисту інформації необхідно визначити природу погроз, форми й шляхи їхнього можливого прояву й здійснення в автоматизованій системі. Для рішення поставленого завдання все різноманіття погроз і шляхів їхнього впливу приведемо до найпростіших видів і форм, які були б адекватні їхній безлічі в автоматизованій системі.

Дослідження досвіду проектування, виготовлення, випробувань і експлуатації автоматизованих систем говорять про те, що інформація в процесі уведення, зберігання, обробки, уведення й передачі піддається різним випадковим впливам.

Причинами таких впливів можуть бути:

* Відмови й збої апаратури
* Перешкоди на лінії зв'язку від впливів зовнішнього середовища
* Помилки людини як ланки системи
* Системні й системотехнічні помилки розроблювачів
* Структурні, алгоритмічні й програмні помилки
* Аварійні ситуації
* Інші впливи.

Частота відмов і збоїв апаратури збільшується при виборі й проектуванні системи, слабкої відносно надійності функціонування апаратури. Перешкоди на лінії зв'язку залежать від правильності вибору місця розміщення технічних засобів АСУ відносно один одного й стосовно апаратури сусідніх систем.

До помилок людини як ланки системи варто відносити помилки людини як джерела інформації, людини-оператора, неправильні дії обслуговуючого персоналу й помилки людини як ланки, що приймає рішення.

Помилки людини можуть підрозділятися на логічні (неправильно ухвалені рішення), сенсорні (неправильне сприйняття оператором інформації) і оперативні, або моторні (неправильна реалізація рішення). Інтенсивність помилок людини може коливатися в широких межах: від 1-2% до 15-40% і вище загального числа операцій при рішеннях завдання.

До погроз випадкового характеру варто віднести аварійні ситуації, які можуть виникнути на об'єкті розміщення автоматизованої системи. До аварійних ситуацій ставляться:

* Відмова від функціонування САУ в цілому, наприклад вихід з ладу електроживлення
* Стихійні лиха: пожежа, повінь, землетрус, урагани, удари блискавки й т.д.

Імовірність цих подій зв'язана насамперед із правильним вибором місця розміщення АСУ, включаючи географічне положення.

Навмисні погрози пов'язані з діями людини, причинами яких можуть бути певне невдоволення своєю життєвою ситуацією, сугубо матеріальний інтерес або простої розвага із самоствердженням своїх здатностей, як у хакерів, і т.д.

Для обчислювальних систем характерні наступні штатні канали доступу до інформації:

* Термінали користувачів
* Термінал адміністратора системи
* Термінал оператора функціонального контролю
* Засоби відображення інформації
* Засоби завантаження програмного забезпечення
* Засоби документування інформації
* Носії інформації
* Зовнішні канали зв'язку.

Маючи на увазі, що при відсутності захисту порушник може скористатися як штатними, так і іншими фізичними каналами доступу, назвемо можливі канали несанкціонованого доступу (ВКНСД) в обчислювальній системі, через які можливо одержати доступ до апаратури, ПО й здійснити розкрадання, руйнування, модифікацію інформації й ознайомлення з нею:

* Всі перераховані штатні засоби при їхньому використанні законними користувачами не по призначенню й за межами своїх повноважень
* Всі перераховані штатні засоби при їхньому використанні сторонніми особами
* Технологічні пульти керування
* Внутрішній монтаж апаратури
* Лінії зв'язку між апаратними засобами даної обчислювальної системи
* Побічне електромагнітне випромінювання апаратури системи
* Побічні наведення по мережі електроживлення й заземлення апаратури
* Побічні наведення на допоміжних і сторонніх комунікаціях
* Відходи обробки інформації у вигляді паперових і магнітних носіїв.

Очевидно, що при відсутності законного користувача, контролю й розмежування доступу до термінала кваліфікований порушник легко скористається його функціональними можливостями для несанкціонованого доступу до інформації шляхом уведення відповідних запитів і команд. При наявності вільного доступу в приміщення можна візуально спостерігати інформацію на засобах відображення й документування, а на останні викрасти паперовий носій, зняти зайву копію, а також викрасти інші носії з інформацією: лістинги, магнітні стрічки, диски й т.д.

Особливу небезпеку являє собою безконтрольне завантаження програмного забезпечення в ЕОМ, у якій можуть бути змінені дані, алгоритми або уведений програма “троянський кінь”, що виконує додаткові незаконні дії: запис інформації на сторонній носій, передачу в канали зв'язку іншого абонента обчислювальної мережі, внесення в систему комп'ютерного вірусу й т.д.

Небезпечної є ситуація, коли порушником є користувач системи, що по своїх функціональних обов'язках має законний доступ до однієї частини інформації, а звертається до іншої за межами своїх повноважень.

З боку законного користувача існує багато способів порушити роботу обчислювальної системи, зловживати нею, витягати, модифікувати або знищувати інформацію. Вільний доступ дозволить йому звертатися до чужих файлів і банок даних і змінювати їх випадково або навмисно.

При технічному обслуговуванні (профілактиці й ремонті) апаратури можуть бути виявлені залишки інформації на магнітній стрічці, поверхнях дисків і інших носіїв інформації. Звичайне стирання інформації не завжди ефективно. Її залишки можуть бути легко прочитані. При транспортуванні носія по неохоронюваній території існує небезпека його перехоплення й наступного ознайомлення сторонніх осіб із секретною інформацією.

Не має змісту створення системи контролю й розмежування доступу до інформації на програмному рівні, якщо не контролюється доступ до пульта керування ЕОМ, внутрішньому монтажу апаратури, кабельним з'єднанням.

Спрацьовування логічних елементів обумовлено високочастотною зміною рівнів напруг і струмів, що приводить до виникнення в ефірі, ланцюгах харчування й заземлення, а також у паралельно розташованих ланцюгах і індуктивностях сторонньої апаратури, електромагнітних полів і наведень, що несуть в амплітуді, фазі й частоті своїх коливань ознаки оброблюваної інформації. Зі зменшенням відстані між приймачем порушника й апаратних засобів імовірність прийому сигналів такого роду збільшується.

За останнім часом у різних країнах проведена велика кількість дослідницьких робіт з метою виявлення потенційних каналів несанкціонованого доступу до інформації в обчислювальних мережах. При цьому розглядаються не тільки можливості порушника, що получили законний доступ до мережного встаткування, але й впливу, обумовлені помилками програмного забезпечення або властивостями використовуваних мережних протоколів. Незважаючи на те, що вивчення каналів НСД триває дотепер, уже на початку 80-их років були сформульовані п'ять основних категорій погроз безпеки даних в обчислювальних мережах:

1. Розкриття змісту переданих повідомлень
2. Аналіз трафіку, що дозволяє визначити приналежність відправника й одержувача даних до однієї із груп користувачів мережі, зв'язаних загальним завданням
3. Зміна потоку повідомлень, що може привести до порушення режиму роботи якого-небудь об'єкта, керованого з вилученої ЕОМ
4. Неправомірна відмова в наданні послуг
5. Несанкціоноване встановлення з'єднання.

Погрози 1 і 2 можна віднести до витоку інформації, погрози 3 і 5 - до її модифікації, а погрозу 4 - до порушення процесу обміну інформацією.

В “ПриватБанку” використовують п'ять основних засобів захисту інформації:

* Технічні,
* Програмні,
* Криптографічні,
* Організаційні,
* Законодавчі.

Розглянемо ці засоби докладніше й оцінимо їхньої можливості в плані подальшого їхнього використання при проектуванні конкретних засобів захисту інформації у ЛВС.

Технічні засоби захисту - це механічні, електромеханічні, оптичні, радіо, радіолокаційні, електронні й інші пристрої й системи, здатні виконувати самостійно або в комплексі з іншими засобами функції захисту даних.

Технічні засоби захисту діляться на фізичні й апаратні. До фізичних засобів ставляться замки, ґрати, охоронні сигналізація, устаткування КПП і ін.; до апаратних - замки, блокування й системи сигналізації про розкриття, які застосовуються на засобах обчислювальної техніки й передачі даних.

Програмні засоби захисту - це спеціальні програми, що включаються до складу програмного забезпечення системи, для забезпечення самостійно або в комплексі з іншими засобами, функцій захисту даних.

По функціональному призначенню програмні засоби можна розділити на наступні групи:

1. Програмні засоби ідентифікації й аутентифікації користувачів.

Ідентифікація - це присвоєння якому-небудь об'єкту або суб'єктові унікального образа, ім'я або числа. Установлення дійсності (аутентифікація) полягає в перевірці, є об'єкт, що перевіряється чи (суб'єкт) тим, за кого себе видає.

Кінцева мета ідентифікації й установлення дійсності об'єкта в обчислювальній системі - допуск його до інформації обмеженого користування у випадку позитивного результату перевірки або відмова в допуску в противному випадку.

Одним з розповсюджених методів аутентифікації є присвоєння особі унікального ім'я або числа - пароля й зберігання його значення в обчислювальній системі. При вході в систему користувач уводить свій код пароля, обчислювальна система порівнює його значення зі значенням, що зберігається у своїй пам'яті, і при збігу кодів відкриває доступ до дозволеного функціонального завдання, а при розбіжності - відмовляє в ньому.

Найбільш високий рівень безпеки входу в систему досягається поділом коду пароля на дві частини, одну, що запам'ятовується користувачем і вводи\_ вручну, і другу, розташовувану на спеціальному носії - картці, установлюваної користувачем на спеціальний пристрій, що зчитує, пов'язане з терміналом.

1. Засоби ідентифікації й установлення дійсності технічних засобів.

Додатковий рівень захисту стосовно паролів користувачів.

В ЕОМ зберігається список паролів і інша інформація про користувачів, яким дозволено користуватися певними терміналами, а також таблиця ресурсів, доступних з певного термінала конкретному користувачеві.

1. Засоби забезпечення захисту файлів.

Вся інформація в системі, збережена у вигляді файлів ділиться на деяку кількість категорій по різних ознаках, вибір яких залежить від функцій, виконуваних системою. Найбільше часто можна зустріти поділ інформації:

* по ступені важливості
* по ступені таємності
* по виконуваних функціях користувачів
* по найменуванню документів
* по видах документів
* по видах даних
* по найменуванню томів, файлів, масивів, записів
* по імені користувача
* по функціях обробки інформації: читанню, запису, виконанню
* по областях оперативної й довгострокової пам'яті
* за часом і т.д.

Доступу посадових осіб до файлів здійснюється відповідно до їхніх функціональних обов'язків і повноважень.

1. Засобу захисту операційної системи й програм користувачів.

Захист операційної системи - найбільш пріоритетне завдання. Здійснюється забороною доступу в області пам'яті, у яких розміщається операційна система.

Для захисту користувальницьких програм застосовується обмеження доступу до займаних цими програмами пам'яті.

1. Допоміжні засоби.

До допоміжних засобів програмного захисту інформації ставляться:

* Програмні засоби контролю правильності роботи користувачів,
* Програмні знищувачі залишків інформації
* Програми контролю роботи механізму захисту
* Програми реєстрації звертань до системи й виконання дій з ресурсами
* Програми формування й печатки грифа таємності
* Програмні засоби захисту від комп'ютерних вірусів і ін.

Криптографічні засоби захисту - це методи спеціального шифрування даних, у результаті якого їхній зміст стає недоступним без застосування деякої спеціальної інформації й зворотного перетворення.

Суть криптографічного захисту полягає в перетворенні складових частин інформації (слів, букв, складів, цифр) за допомогою спеціальних алгоритмів, або апаратних рішень і кодів ключів, тобто приведенні її до неявного виду. Для ознайомлення із закритою інформацією застосовується зворотний процес: декодування (дешифрування). Використання криптографії є одним з розповсюджених методів, що значно підвищують безпека передачі даних у мережах ЕОМ, даних, що зберігаються у вилучених пристроях пам'яті, і при обміні інформацією між вилученими об'єктами.

Організаційні засоби захисту - спеціальні організаційно-технічні й організаційно-правові заходи, акти й правила, здійснювані в процесі створення й експлуатації системи для організації й забезпечення захисту інформації.

Організаційні заходи здійснюють подвійну функцію:

* Повне або часткове перекриття каналів витоку інформації,
* Об'єднання всіх використовуваних засобів захисту в цілісний механізм.

Приклади по захисту інформації повинні охоплювати етапи проектування, виготовлення, випробувань, підготовки до експлуатації й експлуатації системи.

Законодавчі засоби захисту - це законодавчі акти, які регламентують правила використання й обробки інформації, і встановлюють відповідальність і санкції за порушення цих правил.

Законодавчі заходи щодо захисту інформації від НСД полягають у виконанні існуючих у країні або введенні нових законів, постанов, положень і інструкцій, що регулюють юридичну відповідальність посадових осіб - користувачів і обслуговуючого персоналу за витік, втрату або модифікацію довіреної йому інформації, що підлягає захисту, у тому числі за спробу навмисного несанкціонованого доступу до апаратури й інформації. У такий спосіб ціль законодавчих мір - попередження й стримування потенційних порушників.

На основі прийнятої концепції засобу захисту інформації діляться на засоби захисту від навмисного НСД (СЗИ ПНСД) і від випадкового НСД (СЗИ СНСД). Засоби керування захистом інформації (СУЗИ) від НСД є об'єднуючими, що дають можливість за допомогою цілеспрямованих і взаємозалежних функцій у сполученні з найбільш повним охопленням можливих каналів НСД об'єкта окремими засобами захисту створити закінчену й строгу систему захисту в комплексі засобів автоматизації.

СЗИ ПНСД включає 1-й контур захисту - систему контролю доступу на територію об'єкта (СКДТО), 2-й контур захисту - систему контролю й розмежування доступу в приміщення (СКРПД) і основний контур захисту (ОКЗ). СКДТО, що містить систему охоронної сигналізація (СОС) і контрольно-пропускні пункти (КПП), служить для обмеження доступу осіб на територію об'єкта, а також спільно зі спеціальними апаратними рішеннями становить засіб захисту від побічних електромагнітних випромінювань і наведень.

Засобу висновку апаратура з робочого контуру (СВАРК) забезпечують блокування НСД до інформації при ремонті й профілактиці апаратури. У числі засобів основного контуру застосовуються також засоби захисту ресурсів (СЗР) і організаційні міри. СЗР націлені на недопущення блокування користувачем-порушником роботи інших користувачів, а також для контролю й обмеження доступу користувачів до ресурсів.

Засобу захисту інформації на носіях (СЗИН) включають засобу шифрування даних (СШД), засобу знищення залишків інформації на носіях (СУОИ), засобу аутентифікації інформації на носіях (САИН), засобу верифікації програмного забезпечення (СВПО) і організаційно-технічні заходи. Система контролю розкриття апаратури включає датчики розкриття, установлені на контрольованій апаратурі, ланцюзі збору сигналів (ЦСС) і пристрій контролю розкриття апаратури (УКВА).

СОРДИ містить термінал служби безпеки інформації (ТСБИ), функціональні завдання програмного забезпечення (ФЗ ПО), що реалізують на програмному рівні ідентифікацію й аутентифікацію користувачів, а також розмежування їхніх повноважень по доступі до інформації. З метою захисту кодів паролів від НСД для них також повинні бути передбачені засоби захисту (СЗКП).

Засобу захисту від випадкового НСД включають засобу підвищення вірогідності інформації (СПДИ) і засобу захисту інформації від аварійних ситуацій (СЗИ АС). СПДИ містять систему функціонального контролю (СФК), пристрій захисту від помилок у каналах зв'язку (УЗО КС), засобу контролю цілісності програмного забезпечення (СКЦ ПО) і спеціальні технічні рішення (СТР). Вони включають засоби захисту від переадресації пам'яті (СЗПП), ізоляції функціональних завдань (СИФЗ) і інші технічні рішення.

Засоби керування захистом інформації містять автоматизоване робоче місце служби безпеки (АРМ СБ) інформації, ФЗ ПО, спеціально розроблені для виконання керування захистом на програмному рівні, включаючи ведення журналу обліку й реєстрації доступу (ЖУРД) і організаційні заходи. АРМ СБ включає термінал безпеки, УКВА, апаратуру запису кодів у фізичні ключі-паролі (АЗКП), необхідна кількість ключів-паролів і апаратуру реєстрації й документування інформації (АРДИ). Щоб забезпечити необхідний рівень безпеки інформації у ЛВС підрозділи, система безпеки повинна мати наступні засоби:

* Засоби ідентифікації й перевірки повноважень
* Засоби забезпечення захисту файлів
* Засобу захисту ОС і програм користувачів
* Засоби шифрування/дешифрування трафіку мережі
* Засоби знищення залишків інформації в системі
* Засоби реєстрації звертань до системи.

# 3.4 Оцінка ефективності та надійності АБС у Бершадському відділенні Вінницької філії ЗАТ КБ "ПриватБанк"

Для максимально ефективного використання програмного забезпечення банку може бути важливою організація взаємодії між процесами за допомогою засобів ОС. Доступ до файлів процедур операційної системи, які зберігаються, забезпечує архівацію та обробку даних на сервері без завантаження їх у базу даних, що іноді надає переваги у швидкості, дозволяє спростити обмін даними та їх обробку.

Для покращення ефективності і надійності АБС потрібно дотримуватись таких вимог:

1. Система повинна мати модульну структуру, що дозволяє будувати її конфігурацію з базових модулів та підсистем, і складатися з програмних модулів для проведення операцій із цінними паперами та готівкою, обслуговування фізичних осіб, обліку основних засобів і товарно-матеріальних цінностей, управління персоналом та нарахування заробітної плати, фінансового аналізу, управління активами (пасивами), а також виробничими процесами

2. Система повинна бути інтегрованою для забезпечення обміну інформацією між її різними компонентами через загальне інформаційне поле та для зв’язку з іншими системами.

3. Для збереження даних застосовуються сучасні СУБД ОRАСLЕ, SYBASE та ІNFORМІХ, що дозволяють ефективно вирішувати питання, пов’язані з цілісністю, безпекою даних, їх резервуванням та архівацією.

4. Передбачається дворівнева схема побудови:

* центральний апарат;
* обласні управління.

5. Для створення програмних модулів та розв’язання власних задач у межах системи передбачається використання єдиного інструментального засобу.

6. Для зв’язку з іншими системами передбачено два режими:

оff-lіne за узгодженими форматами даних;

оn-lіnе за стандартними протоколами.

7. Для більшості підсистем передбачається можливість роботи в реальному часі.

8. Передбачається використання апаратних та програмних заcобів для надійного забезпечення безпеки даних та захисту від несанкціонованого доступу.

Для підвищення надійності, стійкості до відмов технічних рішень в банківських автоматизованих системах практикується об'єднання серверів в групи (кластери). В такому випадку ресурси і навантаження розподіляються між серверами (вузлами системи) так, що користувач не знає, з яким конкретно сервером він працює в даний момент, а використання технічних засобів в цьому випадку виявляється найефективнішим.

# Висновки та пропозиції

Отже, в конкурентних умовах українським банкам не обійтися без ефективної управлінської аналітичної системи, яка дозволяє управляти не тільки банком, але і його філіалами. Сьогодні автоматизацією діяльності банків в Україні займаються вітчизняні розробники банківського програмного забезпечення, самі банки і компанії-інтегратори зарубіжних систем. Кому віддати перевагу, яке "підводне каміння" може виникнути на шляху упровадження, скількох коштує упровадження таких систем - питання, які цікавлять сьогодні керівників багатьох банківських структур України. Інтерес до розвитку комп'ютеризованих банківських систем визначається не бажанням витягти негайну вигоду, а, головним чином, стратегічними інтересами. Як показує практика, інвестиції в такі проекти починають приносити прибуток лише через певний період часу, необхідний для навчання персоналу й адаптації системи до конкретних умов. Вкладаючи кошти в програмне забезпечення, комп'ютерне й телекомунікаційне встаткування й створення бази для переходу до нових обчислювальних платформ, банки, у першу чергу, прагнуть до здешевлення й прискорення своєї рутинної роботи й перемозі в конкурентній боротьбі.

Нові технології допомагають банкам, інвестиційним фірмам і страховим компаніям змінити взаємини із клієнтами й знайти нові засоби для витягу прибутку. Аналітики сходяться в думці, що нові технології найбільше активно впроваджують інвестиційні фірми, потім випливають банки, а сам останніми їх приймають на озброєння страхові компанії.

Банківські комп'ютерні системи та технології на сьогоднішній день є одними з тих галузей, які швидко розвиваються в області прикладного мережевого програмного забезпечення. Як приклади передових технологій, використовуваних у банківській діяльності, можна назвати бази даних на основі моделі "клієнт-сервер" засобу міжмережевої взаємодії для міжбанківських розрахунків; служби розрахунків, цілком орієнтованих на Іnternet, або, так звані, віртуальні банки; банківські експертно-аналітичні системи.

Банк ЗАТ "ПриватБанк" на початку свого розвитку в Україні використовував АБС "Скрудж", але із збільшенням клієнтської бази і глобальним переходом на мережеві технології постала гостра необхідність у програмному забезпеченні, за допомогою якого можна було б простежити рух банківського капіталу, а також мати повну інформацію про клієнтів банку. З січня 2008 р. банк здійснює перехід на нову АБС "Apply", яка має вагомі переваги над вищевказаною. АБС "Apply" має покращений інтерфейс, позбавляє дублювання вхідної інформації про клієнта завдяки впровадженню CІF, дає можливість головному відділенню контролювати роботу філій, тощо.

# Список використаної літератури

1. Вимоги Національного банку України до програмного комплексу ''Операційний день банку" (ОДБ) - Постанова Правління НБУ№106 від 12 травня 1995 року.
2. ДСТУ 2938-94. Системи оброблення інформації. Основні поняття. Терміни та визначення. - К.: Держстандарт України, 1995. - 32 с.
3. ДСТУ 2940-94. Системи оброблення інформації. Керування процесами оброблення даних. Терміни та визначення. - К.: Держстандарт України, 1995. - 28 с.
4. ДСТУ 2941-94. Системи оброблення інформації. Розроблення систем. Терміни та визначення. - К.: Держстандарт України. - 1995. - 20с.
5. Закон України "Про захист інформації в автоматизованих системах" від 05.04.94, № 80/94 ВР.
6. Постанова Кабінету Міністрів України "Про Концепцією технічного захисту інформації в Україні". 1997р.
7. Закон України "Про приєднання України до Договору Всесвітньої організації інтелектуальної власності про авторське право" від 20.09.2001, №2733-111.
8. Закон України "Про банки і банківську діяльність"
9. Закон України "Про Національний банк України".
10. Декрет КМ України "Про систему валютного регулювання і валютного контролю", №1593 від 16.02.93р.
11. Банківські операції: Підручник. - 2-ге вид., випр. і доп. / А.М. Мороз, М.І. Савлук, М.Ф. Пуховкіна та ін.; За ред. д-ра екон. наук, проф. А.М. Мороза. - К.: КНЕУ, 2002. - 476с.
12. Береза А.М. Основи створення інформаційних систем: Навчальний посібник. - К.: КНЕУ, 2004. - 140 с.
13. Васюренко О.В. Банківські операції: Навч. посіб. - 3-тє вид., стер. - К.: Т-во "Знання", КОО, 2002. - 255 с.
14. Галузинський Г.П., Гордієнко І.В. Сучасні технологічні засоби обробки інформації: Навчальний посібник. - К.: КНЕУ, 2001. - 224 с.
15. Єрьоміна Н.В. Банківські інформаційні системи: Навчальний посібник. - К.: КНЕУ, 2000. - 230 с.
16. Операції комерційних банків/Р. Коцовська, B. Ричаківська, Г, Табачук, Я. Грудзевич, М. Вознюк. - 3-тє вид. - К.: Алеута; Львів: ЛБІ НБУ, 2003. - 500 с.
17. Рогач І.Ф., Сендзюк М.А., Антонюк В.А. Інформаційні системи у фінансово-кредитних установах: Навчальний посібник. - К.: КНЕУ, 2001.
18. Титоренко Г.А., Суворова И.Ф., Возгилевич И.Ф. и др. Автоматизированные информационные технологии в банковской деятельности: учебное пособие для вузов. - М.: Финстатинформ, 1997, 268с.
19. Ситник В.Ф., Краєва О.С. Технологія автоматизованої обробки економічної інформації: Навчальний посібник. - К.: КНЕУ, 2001. - 286с.