

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

Херсонський навчально-науковий інститут

Кафедра інформаційних технологій та фізико-математичних дисциплін


“Допущений до захисту”
Завідувач кафедри
д.т.н., доцент Гучек П.Й.
“ ____ ” _____ 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи
на здобуття ступеня вищої освіти “магістр”

на тему: "Методи управління та моніторингу роботи банківської мережі та розробка інформаційно-управляючої системи на основі сучасних технологій"

Виконав: студент VI курсу, групи 6157зм
спеціальності

122 - “Комп’ютерні науки”, ОПП -

(шифр і назва спеціальності та освітньо-професійної програми)

“Інформаційні управляючі системи та технології”

Соценко В.В.

(прізвище та ініціали)

Керівник к.т.н., доц. Книрік Н.Р.

(прізвище та ініціали)

Рецензент к.т.н., доц. Гайда А.Ю.

(прізвище та ініціали)

30.12 - 2025 року

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова
ХЕРСОНСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ

Кафедра інформаційних технологій та фізико-математичних дисциплін

Освітній ступень магістр

Галузь знань 12 - "Інформаційні технології"
(шифр і назва)

Спеціальність 122 - "Комп'ютерні науки"
(шифр і назва)

Освітньо-професійна програма "Інформаційні управляючі системи та технології"

ЗАТВЕРДЖУЮ

Гарант освітньої програми

 _____ Гучек П.Й.
 "23" жовтня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
на здобуття ступеня вищої освіти «магістр»

Студенту Соценко Владиславу Валерійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: Методи управління та моніторингу роботи банківської мережі та розробка інформаційно-управляючої системи на основі сучасних технологій

Керівник роботи Книрик Наталя Ромуальдівна, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Тема затверджена розпорядженням по інституту від "17" жовтня 2025 року № 20

2. Термін подання студентом роботи 12.12.2025 р.

3. Вихідні дані до роботи:

4. Зміст та структура розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

4.1 Титульний аркуш, завдання на магістерську роботу, анотація (українською, російською, англійською), зміст, перелік умовних означень, символів, одиниць та термінів (при необхідності).

4.2 Вступ.

4.3 Дослідження технологій проектування інформаційних систем та аналіз їх особливостей.

4.4 Формування вимог до інформаційної системи, розробка її концепції і постановка задачі.

4.5 Розробка проектних рішень по інформаційній системі

4.6 Реалізація проекту інформаційної системи (технічна документація по проекту).

4.7 Розділ з економіки

4.8 Розділ з охорони праці та безпеки в надзвичайних ситуаціях (охорони оточуючого середовища).

4.9 Висновки.

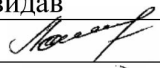
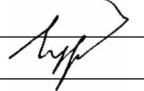
4.10 Список використаної літератури.

4.11 Додатки (технічне завдання, загальний опис ІС, інструкція користувача, текст програми).

5. Перелік презентаційних матеріалів

5.1	Недоліки в роботі. Постановка задачі.
5.2	Блок-схема інформаційного взаємозв'язку функціональних завдань системи
5.3	Концепція системи
5.4	Математичне забезпечення розробки
5.5	Діаграма потоків даних 1 рівня
5.6	Концептуальна модель даних
5.7	Діаграма послідовності
5.8	Діаграма станів
5.9	Розгортання системи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
4.7	Ломоносов Дмитро Анатолійович	28.10.25 	
4.8	Щедролосєв Олександр Вікторович	28.10.25 	

7. Дата видачі завдання 27 жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Строк виконання етапів роботи	Примітка
1.	Вивчення і аналіз предметної галузі	28.10.2025	
2.	Розробка концепції ІС	30.10.2025	
3.	Розробка проектних рішень по ІС	31.10.2025	
4.	Реалізація проекту, розробка робочої документації	03.11.2025	
5.	Вирішення питань з економіки	06.11.2025	
6.	Вирішення питань охорони праці та безпеки в надзвичайних ситуаціях (охорони оточуючого середовища)	12.11.2025	
7.	Виконання графічної частини роботи	22.11.2025	
8.	Оформлення пояснювальної записки	06.12.2025	
9.	Подання роботи на попередній захист	12.12.2025	
10.	Подання роботи рецензенту	20.12.2025	
11.	Подання роботи на державний захист	29.12.2025	

Студент


Підпис

Керівник роботи


Підпис

Соценко В.В.

Прізвище та ініціали

Книрік Н.Р.

Прізвище та ініціали

АНОТАЦІЯ

Кваліфікаційна робота присвячена дослідженню методів управління та моніторингу діяльності банківської мережі, а також розробці інформаційно-управляючої системи, що базується на сучасних технологіях. У роботі проведено аналіз існуючих підходів до організації управління банківськими процесами, визначено основні проблеми функціонування банківських мереж та обґрунтовано необхідність їх оптимізації шляхом впровадження інноваційних інформаційних рішень.

Особливу увагу приділено питанням моніторингу роботи банківських підрозділів, контролю якості обслуговування клієнтів та забезпечення стабільності фінансових операцій. На основі дослідження розроблено концепцію інформаційно-управляючої системи, яка забезпечує:

- автоматизацію процесів управління та моніторингу;
- інтеграцію з базами даних та аналітичними інструментами;
- можливість оперативного прийняття управлінських рішень;
- підвищення ефективності роботи банківської мережі та рівня клієнтського сервісу.

Практична цінність роботи полягає у створенні інструменту, що може бути використаний банківськими установами для оптимізації управлінських процесів, зниження операційних ризиків та підвищення конкурентоспроможності на фінансовому ринку. Результати дослідження можуть бути застосовані для подальшого розвитку цифрових технологій у банківській сфері.

Ключові слова: банківська мережа, управління, моніторинг, інформаційна система, автоматизація, сучасні технології.

ANNOTATION

The master's thesis is devoted to the study of management and monitoring methods of banking networks and the development of an information management system based on modern technologies. The research provides an analysis of existing approaches to organizing banking processes, identifies the main challenges in the functioning of banking networks, and substantiates the need for their optimization through the implementation of innovative information solutions.

Special attention is given to monitoring the performance of banking branches, ensuring the quality of customer service, and maintaining the stability of financial operations. Based on the conducted study, a concept of an information management system was developed, which provides:

- automation of management and monitoring processes;
- integration with databases and analytical tools;
- support for operational decision-making;
- improvement of efficiency in banking networks and enhancement of customer service quality.

The practical value of the thesis lies in the creation of a tool that can be used by banking institutions to optimize management processes, reduce operational risks, and increase competitiveness in the financial market. The results of the study can be applied for the further development of digital technologies in the banking sector.

Keywords: banking network, management, monitoring, information system, automation, modern technologies.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ATM	–	Automated Teller Machine (Банкомат)
BACS	–	Bankers Automated Clearance Services
CHAPS	–	Clearing House Automated Payment System
CRM	–	Customer Relationship Management (Управління взаємовідносинами з клієнтами)
OOA&D	–	Object-Oriented Analysis and Design
PIN	–	Personal Identification Number
POST	–	Point Of Sale Terminal
SWIFT	–	Society for Interbank Financial Telecommunications
UML	–	Unified Modeling Language (Унифіцированный язык моделирования)
XOR	–	Exclusive OR
АБС	–	Автоматизована банківська система
БД	–	База даних
ЕОМ	–	Електронно-обчислювальна машина
ІТ	–	Інформаційні технології
НБУ	–	Національний банк України
НСМЕП	–	Національна система масових електронних платежів
ООАП	–	Об'єктно-орієнтований аналіз та проектування
ОО-мова	–	Об'єктно-орієнтована мова програмування
ПЗ	–	Програмне забезпечення
ПІН	–	Персональний ідентифікаційний номер
РПЦ	–	Регіональний процесинговий центр
СЕП	–	Система електронних платежів
СУБД	–	Система управління базами даних

ЗМІСТ

ВСТУП	11
РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ РОЗРОБКИ СИСТЕМИ	16
1.1. Сучасний стан автоматизацій банківських операцій	16
1.2. Огляд і аналіз шляхів вирішення автоматизації авторизованих операцій з банкоматами	32
1. 2. Обґрунтування мети використання безготівкових розрахунків за допомогою банкоматів	38
Висновок до розділу 1	39
РОЗДІЛ 2 МОДЕЛЮВАННЯ БІЗНЕС-ПРОЦЕСІВ РОБОТИ БАНКІВСЬКОЇ МЕРЕЖІ ТА ПРОЄКТУВАННЯ СИСТЕМИ	40
2.1. Банкомати	41
2.2.5. Види послуг, які можна отримати за допомогою пластикових карток	50
2. 2. Методи забезпечення безпеки розрахунків	53
2. 2.5 Розробка ескізного проєкту інформаційної системи	60
2. 2.5. <i>Діаграми поведінки (Behavior Diagram)</i>	65
2.5 Розробка технічного проєкту	74
2.6 Розробка програмного забезпечення	87
2.6.1. Системне програмне забезпечення	91
Висновок до розділу 3	99
РОЗДІЛ 4. РОЗРАХУНОК ЕКОНОМІЧНОГО ЕФЕКТУ ВІД ВПРОВАДЖЕННЯ ІС	100
РОЗДІЛ 5 ОХОРОНА ПРАЦІ	107
5.1 Аналіз потенційно небезпечних і шкідливих факторів у приміщенні відділу кадрів	108
5.2 Розрахунок освітлення	114
Висновок до розділу 5	115
РОЗДІЛ 6. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА	117
ВИСНОВКИ	124
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	126
ДОДАТОК А	130
ДОДАТОК Б	137

ВСТУП

Процес переходу України до якісно нової форми економічних відносин, що базуються на ринкових принципах ведення господарства, зумовив необхідність внесення кардинальних змін до фінансово-кредитної сфери економіки, яка відіграє ключову роль у забезпеченні руху грошових потоків, тим самим створюючи базові передумови суспільного відтворення. Основною ланкою цієї сфери є банківська система, якій належить провідне місце у загальному механізмі організації й регулювання господарського життя суспільства і від ефективності функціонування якої вирішальною мірою залежить успіх соціально-економічних перетворень у країні загалом.

Банківська система України сьогодні – один із найрозвинутіших елементів господарського механізму, оскільки її реформування було почато раніше за інші сектори економіки, що визначалося ключовою роллю банків при вирішенні завдань переходу до ринку. Саме банки відіграють основну роль в утворенні оптимального середовища для мобілізації й вільного переливу капіталів, нагромадженні коштів для структурної перебудови економіки, приватизації й розвитку підприємництва. Водночас усебічне розкриття їхніх потенційних можливостей у реалізації функції фінансового посередництва на ринку значною мірою визначається особливостями структурної організації банківської системи країни, яка забезпечує складний механізм практичної реалізації взаємозв'язків і взаємовідносин між банківськими установами, від чого, у кінцевому підсумку, залежать результати їхньої діяльності та ефективність кредитно-фінансового обслуговування усіх ланок народногосподарського комплексу.

Діяльність банківських установ є настільки багатогранною, що досить важко визначити їхню справжню сутність. У сучасному суспільстві банки здійснюють операції найрізноманітнішого гатунку. Вони не лише упорядковують грошовий обіг і кредитні відносини, а й здійснюють:

фінансування народного господарства, операції зі страхування, купівлі-продажу цінних паперів, а в окремих випадках – операції посередництва та управління майном. Кредитні установи надають консультації, беруть участь в обговоренні господарських програм, ведуть статистику, мають власні підсобні господарства.

Банки обробляють щорічно велику кількість паперової інформації. Обробка такої інформації і її фізичне транспортування трудомісткі, тому немає нічого дивного в тому, що банки намагаються істотно скоротити обсяги таких операцій, звертаючись до допомоги автоматизованих систем.

На початку 70-х років банки почали вивчати можливості скорочення накладних витрат в організації наявного обороту і підвищення власної конкурентоспроможності за рахунок використання нових технологій. Поява перших грошових автоматів (банкоматів) послужила зменшенню кількості касирів і дала можливість банкам збільшити час, протягом якого клієнти могли б мати доступ до своїх грошей.

Перші грошові автомати були примітивними за сучасними мірками. У них не було передбачено можливостей отримання у реальному часі даних по балансу. Але як би там не було, їх поява знаменувала собою начало фундаментальних змін у відносинах між клієнтами і новими технологіями.

У 80-х роках грошові автомати «переросли» в автоматизовані касові апарати (АТМ), здатні надавати весь спектр послуг, який раніше був доступний тільки банківським касирам, наприклад:

- прийом готівки і депозитне обслуговування;
- перевірка, балансу, з можливістю отримання міні- і повних довідок;
- робота з чековими книжками;
- надання інформації про інші послуги, що надаються банками.

Велика частка розрахунків, що виконуються в Україні (особливо це стосується розрахунків з фізичними особами) є готівковими. Тому існують проблеми, пов'язані з управлінням готівкою, друкуванням нових грошей, утилізацією зношених купюр, організацією інкасації та ін. Одним з напрямів реалізації цієї проблеми є скорочення обсягу готівкових розрахунків шляхом впровадження електронних роздрібних банківських послуг. Роздрібні банківські послуги — це безготівкові платежі на невеликі суми, здебільшого це споживчі платежі, які вносяться фізичними особами з використанням пластикових карток, що виступають як платіжний та розрахунковий засіб.

Пластикова картка— це загальний термін, яким називають всі види карток, які можуть відрізнятись технічними можливостями, призначенням та видами наданих ними послуг. Пластикові картки набули широкого застосування в банківських системах. Пластикова картка — це ключ клієнта для отримання електронних банківських послуг. З точки зору банку — це можливість персонувати картку і таким чином ідентифікувати клієнта і визначити, які послуги може надати йому банк.

Використання пластикових карток як платіжного засобу дає багато переваг користувачам карток, банкам-емітентам та торговельним закладам. Основні переваги з точки зору власника картки та торговельного закладу такі:

- Власнику картки не потрібно мати з собою великої кількості готівки. Ця перевага може бути звичайно реалізованою за умови залучення до системи електронного обслуговування великої кількості магазинів та інших сервісних закладів.
- Відсутність проблеми конвертації валют. Цю послугу власнику картки надає система, причому по курсу, більш вигідному, ніж в пунктах обміну валют.
- Можливість отримати кредит в банку та знижки на певні товари і послуги.

- Можливість отримати повну інформацію про стан рахунку та виконані трансакції.
- Якщо переважна більшість операцій виконується на безготівковій основі, то підвищується рівень безпеки роботи торговельних та інших закладів сервісного обслуговування. Крім того, істотно зменшуються витрати на інкасацію.
- Підвищується рейтинг закладу та збільшується можливість залучення більш забезпечених клієнтів.

Переваги банків-емітентів полягають у тому, що збільшуються обсяги залучених коштів завдяки відкриттю карткових рахунків, сплаті комісійних за послуги банку та сплаті вартості самої картки. Крім того, впровадження сучасних карткових технологій підвищує конкурентоздатність банку, надає можливість розширення сфери його дії та залучення нових клієнтів.

Сьогодні будь-який банк в усьому світі виконує три основні функції: збір коштів, їхнє переміщення, і кредитування ними. Збір коштів сам по собі коштує банкові грошей, на переміщенні коштів уже можна заробляти, але, все-таки, основний бізнес банку – це, звичайно, надання кредитів.

За допомогою організації систем електронних розрахунків цілком можливо побудувати банківські продукти, які дозволять заробляти гроші, з'єднуючи воєдино всі три банківські функції: збираючи дешеві ресурси великої кількості небагатих клієнтів, контролюючи пересування грошей по циклу банківський рахунок – клієнт – магазин – банківський рахунок, і кредитуючи підприємства й торговельні структури, пов'язані із цією клієнтурою. Це одна з деяких сьогодні реальних можливостей для банків заробляти гроші.

Орієнтація на автоматизацію всієї діяльності банків означає поступовий еволюційний перехід від більш простих програмно-апаратних засобів до більш складних з відповідним нарощуванням технічних,

технологічних, кадрових потенціалів з одночасним розширенням сфер використання банківського капіталу.

Актуальність теми досить очевидна, тому що все частіше й частіше в нашому житті ми маємо справу з електронними розрахунками, і все частіше й частіше сучасні інструменти грошового обігу починають витісняти на деяких ринках своїх попередників – наявні й безготівкові гроші. Причини цього процесу досить очевидні, тому що ті кошти грошового обігу, які ми маємо зараз, аж ніяк не є ідеальними й тому йде їхнє безперервне вдосконалювання. У якийсь момент накопичені вдосконалення приводять до зміни інструментів.

При сучасному рівні розвитку науки й техніки, інформатизації різних галузей життя в сучасному суспільстві, з'явилася безліч нових технічних можливостей проведення грошових розрахунків і взаємозаліків без використання грошей як таких. Комерційні банки в сучасних умовах, просто зобов'язані йти в ногу з часом, і надавати клієнтам удосконалені банківські послуги, пов'язані із застосуванням електронних систем розрахунків.

Предметом дослідження даної роботи є рух грошових коштів у мережі банкоматів.

Ціль даної роботи – на основі матеріалів підручників банківської справи, сучасної публіцистики проаналізувати рух грошових коштів у мережі банкоматів, електронні розрахунки й інші послуги, надавані банкоматами, а також створення програмного забезпечення системи керування рухом грошових коштів.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ РОЗРОБКИ СИСТЕМИ

1.1. Сучасний стан автоматизацій банківських операцій

Банківська автоматизація розвивається швидкими темпами як екстенсивно, по числу банків, що встановлюють електронне обладнання, так й інтенсивно, з погляду типів операцій які автоматизують у банках. Майбутнє представляється суспільством без чеків, з розвитком ліній зв'язку між комп'ютером та банком; зв'язок клієнтів із центральною системою (термінал клієнта) і розвиток систем ідентифікації й верифікації клієнта для користування на терміналі клієнта. Результатом цього є поширення техніки дослідження операцій в область банківського менеджменту. Результат полягає в тім, що електронні технології можуть бути забезпечені й уже забезпечують поза банківську конкуренцію

Основні напрямки діяльності банку, котрі були комп'ютеризовані за останній період, включають облік витрат банку, центральний інформаційний файл; кредити по відкритих рахунках або кредитні картки; комерційні позички; корпоративний траст; депозити до запитання; головну бух. книгу; кредит з виплатами на виплат; кредитні лінії; іпотечні позички; індивідуальні трасти; перевірку й транзит; заощадження.

Приклади комп'ютеризованих видів діяльності у банку середнього розміру:

1. Облік перевірочних і транзитних операцій, депозитів до запитання: виявлення обтяжених статей; підрахунки по статтях; інформація з фінансових потоків; цифри щоденних неінкасованих засобів (запобігання виписки чеків проти неінкасованих сум); статистичний аналіз прибутковості рахунку (використовуваний також при розгляді застосування позичок); звіти адміністрації.

2. Облік витрат банку: звіти підрозділів і керувань.

2. Облік заробітної плати: автоматичне внесення засобів на рахунки службовців; розподіл витрат на робочу силу; підготовка звітів.

2.5. Узгодження чекових рахунків: звільнення комерційних вкладників від проблем за узгодженням.

5. Ощадні рахунки по ощадних книжках: підрахунок щомісячного відсотка.

6. Операції із платіжними дорученнями.

7. Облік трасту на користь індивідуальної особи: розрахунки з готівкою; підсумовування активів; щоденні проводки готівки; податковий "робочий аркуш"; звіти по овердрафті; звіти про надлишкові залишки; звіти про погашення облігацій й опціонів "колл"; прогнози по комісійних внесках; звіти про реєстрації; щоденне коректування рахунків; коректування цін на цінні папери; автоматичний переклад відсотків по облігаціях.

8. Аналіз облігацій й інвестицій: дані по доходу й витратам; дані про заставу; інформація про ринковий прибуток і збитки; інформація про місцезнаходження й потоки готівки для аудиторського контролю; конкретні проводки по головній бухгалтерській книзі.

9. Програма по іпотечних позичках: інформація інвестора на додаток до звичайного бухгалтерського звіту; використання магнітного чорнила для розпізнавання написів (magnetic ink character recognition - MICR) на закодованих що звертаються грошових переводів з відправленими поштою повідомленнями й квитанціями; поліпшення в системі узгодження чекових рахунків за допомогою магнітного чорнила для розпізнавання написів; програма по обліку бюджету, розроблена й погоджена із програмою обліку загальних витрат.

10. Позички з погашеннями на виплат: застосування MICR і створення картки умовної головної книги, включаючи всю необхідну інформацію для ведення пізніх й поганих рахунків, для цілей інкасування.

11. Трансферт корпоративних акцій: облік всіх трансфертів акцій і проводок підрозділів.

12. Дисковий файл: для інформаційної програми по загальному менеджменті.

1 2. Інтегрована документація по цінних паперах: для трастових операцій; безпечного зберігання, застав під комерційні позички й власний банківський портфель інвестицій.

1 2.5. Аналіз матеріально-технічного використання комп'ютерів: щомісячна оцінка ефективності комп'ютерної системи й аналіз витрат по напрямках застосування.

Дослідження функціонування. Крім надання банкам можливості максимізувати ефективність виконання канцелярських й облікових операцій, комп'ютери також допомагають провести швидке математичне тестування моделей і кількісні оцінки моделей, що перевіряють, на основі централізованої адміністративної інформації, використовуваної в дослідженні функціонування. По суті справи, це означає застосування різних наукових методів, прийомів й інструментів аналізу до конкретних проблем для визначення оптимального або найбільш раціонального рішення й методів.

В загалом системи автоматизації банківських операцій принципово не відрізняються за структурою одна від одної і мають такі модулі:

- Комплекс автоматизація банківських операцій — для автоматизації роботи с платіжними картками.
- Комплекс автоматизація банківських операцій — для автоматизації
- повнофункціонального роздрібного обслуговування клієнтів.
- Системи автоматизації роздрібного обслуговування клієнтів.
- Система автоматизації он-лайнового процесінгового центра.
- Система персоналізації карток.

Програмно-технічний комплекс автоматизація банківських операцій, призначений для автоматизації роздрібного обслуговування клієнтів банку, а також для використання в процесінгових центрах, що обслуговують учасників платіжних систем: VISA Int., MasterCard Int., Diners Club, American Express, Юніон Кард, СТБ Кард, локальні платіжні системи банків.

1.1.1. Комплекс автоматизація банківських операцій - для автоматизації роботи із платіжними картами

Комплекс позиціонується, як повнофункціональна автоматизація банківського процесінгового центра, що забезпечує роботу із платіжними картами.

Система авторизації операцій по картах забезпечує:

- виконання авторизації операцій по картах банків-емітентів відповідно до заданих умов авторизації;
- керування мережею термінальних устроїв (банкомати, POS-термінали та інше.), що підключають до системи по каналах зв'язку й обробку транзакцій, ініціюємих на цих терміналах;
- підтримку On-line-взаємодії з мережами платіжних систем відповідно до вимог цих систем, а також з авторизаційними системами інших банків;
- підтримку інтерфейсів з бек-офісними системами.

Система роздрібного обслуговування клієнтів забезпечує:

- формування й обробку транзакцій, а також обмін транзакціями із платіжними системами (у відповідності зі специфікаціями, певними цими платіжними системами);
- підготовку інформації для виконання розрахунків по транзакціях;
- автоматизацію процесів: підготовки інформації для видання карт, керування умовами авторизації карткових операцій, взаємодії із власниками карт й інших;

- виконання інших функцій роздрібного бізнесу, не зв'язаних прямо з платіжними картами: повний спектр обслуговування депозитних і кредитних договорів, переказів (у тому числі комунальних платежів), касових операцій (операцій з наявною валютою, чеками й використанням платіжних карт, включаючи облік цінностей) і інше.

Система персоналізації карт забезпечує:

- обробку заявок на видання карт і генерацію (з використанням криптографічних коштів) параметрів, необхідних для персоналізації карт;
- печатка PIN - конвертів;
- підготовку даних відповідно до вхідних форматів устроїв фізичної персоналізації.

Компоненти програмного комплексу, їхні зовнішні інтерфейси й внутрішня структура даних розроблені у відповідності зі стандартами міжнародних платіжних систем. У результаті весь комплекс у цілому й кожна з його компонентів окремо можуть бути використані для роботи банку з міжнародними платіжними системами: VISA , MasterCard , Diners Club , American Express і українськими: Юнион Кард, СТБ Кард.

Програмний комплекс, що включає в себе три перераховані компоненти, може бути основою для побудови різних технічних рішень для банків, що емітують платіжні карти й займаються екваєрингом операцій з банківськими картами. Ці технічні рішення можуть базуватися, залежно від потреб банку, на використанні всіх трьох компонентів, що входять до складу комплексу, двох компонентів або однієї компоненти.

1.1.2. Комплекс автоматизація банківських операцій - для автоматизації повнофункціонального роздрібного обслуговування клієнтів

Більш ніж десятилітній досвід експлуатації комплексу автоматизація банківських операцій як кошти автоматизації роботи банку із платіжними картами показав, що надавані клієнтам послуги банку, пов'язані з використанням платіжних карт, тісно переплітаються з іншими послугами (депозити, кредити, перекази, комунальні та інші платежі, валютно-обмінні операції й інше). При цьому багато банків пропонують своїм клієнтам продукти, що передбачають комплексні послуги, що вимагають виконання операцій, у яких задіюються одночасно й договори банківських карт й інші договори клієнта (споживчі кредити, депозити й інше). Очевидно, що автоматизацію таких послуг простіше забезпечити, коли всі ці операції можуть виконуватися в рамках єдиної системи. Система автоматизації роздрібного обслуговування клієнтів і входить до складу комплексу як карткового бек-офісу, інтегрованого на одночасне повнофункціональне обслуговування фізичних осіб по всьому спектрі банківських послуг. Система автоматизації роздрібного обслуговування клієнтів має всі функції карткового бек-офісу й одночасно є компонентом банківської системи, у рамках якої забезпечується автоматизація практично всіх операцій клієнтського обслуговування: ведення договорів банківських карт, депозитних договорів, договорів овердрафтного й споживчого кредитування, переказів (включаючи платежі населення), виконання касових операцій (як операцій з використанням платіжних карт, так і всіх видів операцій з наявною валютою й чеками), облік цінностей, тривалі доручення й багато чого іншого.

1.1. 2. Системи автоматизації роздрібного обслуговування клієнтів

Принципи побудови системи автоматизації роздрібного обслуговування клієнтів Діяльність банків в умовах твердої конкуренції в

боротьбі за клієнтів, а також в умовах часто мінливих нормативних вимог, змушує банки використати кошти автоматизації своєї діяльності, що володіють максимальною гнучкістю, що дозволяють банку самостійно здійснювати налаштування нових продуктів, постійно модифікувати бізнес-процеси, пов'язані з обслуговуванням клієнтів, оперативно міняти тарифи й порядок ведення обліку.

Система автоматизації роздрібного обслуговування клієнтів повною мірою задовольняє всім цим вимогам. Відмінною рисою системи є те, що, вона побудована за принципом конструктора. Всі банківські бізнес-процеси налаштовуються в системі й виконуються за допомогою типових операцій, які складаються з елементарних будівельних блоків, названих типовими етапами. Етап являє собою функцію, що виконує певну типову дію. Кожен етап має вхідні й вихідні параметри.

Вхідні параметри — визначають набір вихідних даних, над якими повинне бути виконане дія, а також, можливо, деякі особливості виконання цієї дії. Вихідні параметри — містять результат виконання дії.

Значення, що повертають як вихідні параметри етапу, можуть бути передані в наступні етапи операції у вигляді значень вхідних параметрів. Поєднуючи певні типові етапи в складі типових операцій, а також, установлюючи вимоги по виконанню етапів на певних робочих місцях системи певними її користувачами, можна домогтися виконання необхідної послідовності дій, що відповідає певним бізнес процесам.

Виконання будь-якої типової операції в системі автоматизації роздрібного обслуговування клієнтів здійснюється під керуванням єдиної програми RWS (Retail Work Station), що запускається на кожному робочому місці й забезпечує послідовну інтерпретацію типових етапів і передачу керування від одного етапу до іншого в складі типової операції.

Запуск операцій на виконання ініціюється за допомогою динамічного меню, склад якого може налаштовуватися окремо для різних груп користувачів.

Кожна команда меню відповідає закріпленої за нею типової операції. Безліч команд меню, відображуваних на екрані робочої станції для певного користувача, залежить від набору прав цього користувача і його робочого місця на виконання відповідних операцій.

Існує також можливість автоматичного запуску операцій відповідно до заданих тимчасових умов — регламентних операцій.

Другою найважливішою особливістю системи, що дозволяє банку самостійно й досить швидко пропонувати клієнтові нові умови обслуговування, є уведення в ній поняття банківського продукту (типового договору). Банківський продукт являє собою шаблон договору з певним набором умов обслуговування клієнта, набором рахунків, що відкривають, набором дозволених типових операцій за договором, тарифних ставок для розрахунку винагород банку по операціях і ряду інших параметрів. Варіюючи налаштуваннями банківського продукту, можна:

- створювати комплексні продукти, що поєднують у собі різні категорії банківських послуг (залучення коштів клієнтів у депозит, кредитування клієнтів, обслуговування по банківських картах);
- зв'язувати в одному продукті кілька типових договорів, забезпечуючи тим самим участь в операціях рахунків з різних договорів клієнта;
- управляти відкриттям різних рахунків по договорах клієнта;
- встановлювати різні вимоги за розрахунками відсотків для кожного рахунку, що відкриває;
- визначати набір операцій, дозволених для договорів, що відкривають у рамках продукту.

Крім налаштувань типових операцій і банківських продуктів у системі є розвинені кошти по налаштуванню схем організації аналітичного обліку по операціях і правил ведення зведеного обліку. Дані налаштування дозволяють:

- реєструвати рахунки для ведення аналітичного й зведеного обліку;
- задавати правила формування проводок по рахунках аналітичного обліку залежно від безлічі параметрів операцій;
- управляти логікою об'єднання проводок, сформованих по фінансових операціях, перед вивантаженням їх у центральну АБС.

Також система має широкі можливості по настроюванню тарифів для автоматичного розрахунку винагород банку по операціях з договорами клієнтів. При цьому забезпечується:

- реєстрація окремих тарифів у прив'язці до типових операцій й, при необхідності, до окремих клієнтських договорів;
- реєстрація значень тарифних ставок, що залежать від безлічі різних параметрів операцій;
- автоматичний розрахунок винагород по операціях залежно від потрібних тарифних ставок;
- формування необхідних проводок по обліку розрахованих винагород.

У рамках системи забезпечується можливість настроювання прав доступу користувачів до виконання операцій з різними системними об'єктами. До числа таких об'єктів ставляться:

- банківські продукти,
- типові операції й типові етапи операцій,
- угруповання окремих екземплярів об'єктів.

Права на доступ до кожного такого об'єкта встановлюються при реєстрації кожного користувача (права користувача) і робочого місця (права робітника місця). Права користувача в кожному конкретному сеансі роботи в системі визначаються перетинанням безлічі його прав і безлічі прав, заданих

при реєстрації робочого місця, на якому цей користувач працює в цей момент.

1.1. 2.5. Система автоматизації он-лайнного процесінгового центра

Система автоматизації он-лайнного процесінгового центра призначена для забезпечення авторизації операцій, викликаних використанням платіжних карт. Вона містить у собі наступні основні компоненти:

- підсистема керування банкоматами;
- підсистема керування терміналами;
- підсистема моніторингу термінальних устроїв;
- підсистема голосової авторизації;
- ядро системи авторизації;
- система безпеки;
- сервер безпеки;
- АРМ адміністратора системи безпеки;
- сервісний модуль.

Зовнішні інтерфейси системи:

- шлюзи для взаємодії з мережами платіжних систем;
- інтерфейс для взаємодії в рамках локальної платіжної системи;
- інтерфейси з авторизаційними комплексами сторонніх розроблювачів;
- інтерфейс із бек-офісними системами банків, що обслуговують;
- комунікаційні кошти;
- поштова підсистема.

Підсистема керування банкоматами.

Підсистема керування банкоматами забезпечує керування банкоматами відповідно до протоколу NDC. Підсистема має стандартизований інтерфейс із ядром системи авторизації (інтерфейс із оброблювачем транзакцій еквайра

в складі ядра), що здійснює обробку авторизованих запитів, а також з підсистемою моніторингу терміналів, що забезпечує відображення стану (фінансового й технічного) банкомата й окремих його устроїв.

Підсистема керування терміналами.

Система керування терміналами містить у собі комунікаційний сервер, що забезпечує взаємодію з вилученими термінальними пристроями по каналах зв'язку (телефонні лінії, що комутують, виділені телефонні лінії, канали x.25, радіоканали) і конвертори термінальних протоколів, що забезпечують перетворення протоколів обміну з терміналами у вхідний протокол, що відповідає стандартизованому інтерфейсу ядра системи авторизації (інтерфейс із оброблювачем транзакцій екваєра в складі ядра). У підсистемі реалізована підтримка протоколів: VISA MDC, VISA-II, Hypercom (ISO-8583), а також реалізований внутрішній термінальний протокол обміну, що є модифікацією протоколу VISA MDC.

Підсистема керування терміналами забезпечує обробку наступних типів транзакцій:

- транзакції оплати товарів (послуг);
- транзакції видачі наявних;
- транзакції внесення наявних;
- транзакції скасування операцій видачі наявних й операцій оплати товарів (послуг);
- транзакції розвантаження терміналів (Data Capture);
- спеціальні транзакції, використовувані в технології для мікропроцесорних карт із електронним гаманцем: переклад, завантаження й розвантаження електронного гаманця, і ін. (тільки для внутрішнього термінального протоколу).

Підсистема керування терміналами має інтерфейс із підсистемою моніторингу терміналів, що забезпечує відображення поточного стану терміналів, а також статистичної інформації про їхню роботу.

Підсистема моніторингу терміналів.

Підсистема моніторингу терміналів призначена для оперативного контролю поточного стану терміналів (АТМ, POS). Вона дозволяє відображати на екрані монітора (одного або декількох) інформацію про стан банкоматів, POS-терміналів, каналів зв'язку, а також (для банкоматів) надає інтерфейс для формування запитів на банкомати (команди керування банкоматом, запит фінансового й технічного статусу).

Крім візуального відображення на екранах моніторів стану терміналів й окремих їхніх устроїв існує можливість налаштування підсистеми на обробку заданих критичних подій (збій каналів зв'язку, порушення працездатності терміналів або окремих устроїв). Інформація про факти виникнення таких критичних подій, а також інформація про статуси устроїв, що надходить від банкоматів, може відображатися кольірним зображенням на екранах моніторів, а також передаватися за допомогою поштової підсистеми службам технічної підтримки банкоматів в обслуговують банках, що.

Підсистема голосової авторизації.

Підсистема голосової авторизації містить у собі один або кілька модулів голосової авторизації й конвертор, що забезпечує перетворення зовнішнього інтерфейсу модуля голосової авторизації до стандартизованого інтерфейсу ядра системи авторизації (інтерфейс із оброблювачем транзакцій еквіваленту ядра системи авторизації). Підсистема голосової авторизації забезпечує:

- формування запиту авторизації за допомогою ручного введення операціоністом параметрів карткової операції, які передаються з пункту обслуговування банківських карт усно по телефоні;
- обробку відповідей на авторизаційні запити по карткових операціях і відображення результатів авторизації для усної передачі в пункт обслуговування банківських карт;
- скасування проведених раніше авторизацій;

- ведення й можливість перегляду протоколу авторизацій, оброблених на станції в поточному сеансі роботи;
- одержання довідкової інформації з бази даних про зареєстровані пункти обслуговування, фірмах і філіях, яким вони належать, і їхніх параметрах.

Ядро системи авторизації.

Ядро системи авторизації є центральною ланкою системи авторизації, що забезпечує базову логіку обробки транзакцій у ході авторизаційного процесу для екваєра, емітента й міжбанківського маршрутизатора повідомлень. До складу цієї базової логіки залежно від конфігурації системи може входити:

- формування авторизованих повідомлень;
- маршрутизація авторизованих повідомлень;
- фіксування результату завершення транзакції в базі даних, виконання контрольних перевірок, необхідних для екваєра, емітента або міжбанківського маршрутизатора повідомлень;
- ініціювання виконання криптографічних процедур (звертання до системи безпеки).

Ядро системи авторизації має стандартизовані зовнішні інтерфейси:

- Інтерфейс із підсистемами керування терміналами й голосової авторизації побудований на основі стандарту ISO-8583 і дозволяє підключати до ядра різні підсистеми керування терміналами без зміни базових функцій ядра системи авторизації.
- Інтерфейс із мережами платіжних систем і зовнішніх систем авторизації реалізований у відповідності зі стандартом ISO-858 2. Повідомлення, передані в рамках цього інтерфейсу, містять повний набір параметрів, необхідних для реалізації взаємодії із зовнішніми системами з використанням протоколів: VISA Base-I, VISA-SMS, EPSNet v.5 й інших.

- Інтерфейс, що забезпечує взаємодія із системою безпеки, дозволяє реалізовувати звертання до базових функцій забезпечення безпеки (трансляція PIN-блоку, верифікація PIN-блоку та інше.)

До складу ядра входять наступні компоненти:

1. Оброблювач транзакцій екваєра є компонентом ядра системи авторизації, призначеної для використання в авторизаційному процесінговому центрі, що реалізує функції екваєра. Оброблювач транзакцій екваєра забезпечує виконання наступних функцій:

- прийом повідомлень-запитів про проведені карткові операції від підсистем керування терміналами. З метою захисту цілісності інформації й протидії можливого шахрайству повідомлення, передані між терміналами й центром авторизації, захищаються контрольним кодом (MAC);
- контрольні перевірки за умовам, заданим для терміналів і фірм, зокрема, перевірку стоп-аркуша;
- фіксування в базі даних результатів обробки повідомлень (отриманого від термінала повідомлення авторизаційного запиту й, згодом, отриманого з боку емітента повідомлення відповіді на авторизаційний запит);
- маршрутизація (після одержання відповіді з боку емітента) відповідного повідомлення підсистемам керування терміналами, від яких отримане повідомлення-запит по картковій операції.

2. Оброблювач транзакцій емітента є компонентом ядра підсистеми авторизації, призначеної для використання в авторизаційному процесінговому центрі емітента. Оброблювач транзакцій емітента забезпечує виконання наступних функцій:

- контрольні перевірки при обробці повідомлень - запитів у складі ISO-транзакції за умовами, заданим для карт. Зокрема,

контролюється ліміт авторизацій власника карт (Open - To - Buy Limit), ліміти активності карти по сумі й по частоті використання, коди CVC \ CVV та інші параметри, використовувані для контролю платоспроможності власника й протидії можливному шахрайству;

- формування відповідного повідомлення для екваєра;
- фіксування в базі даних результатів обробки транзакції з боку емітента.

2. Оброблювач міжбанківських транзакцій є компонентом ядра системи авторизації, призначеної для використання в авторизаційному процесінговому центрі, що реалізує функції міжбанківського маршрутизатора повідомлень. Оброблювач міжбанківських транзакцій забезпечує виконання наступних функцій:

- маршрутизація авторизованих повідомлень між центрами авторизацій екваєрів й емітентів;
- контрольні перевірки при обробці повідомлень-запитів за умовами, заданим для екваєрів (для вхідних повідомлень);
- контрольні перевірки при обробці повідомлень-запитів за умовами, заданим для емітентів - (контроль лімітів авторизації, установлених для емітентів і контроль обмежень, що задають для суміжних екваєрів й емітентів та інше.), формування отказного відповідного повідомлення при незадовільному результаті перевірок;
- визначення деяких параметрів повідомлень-запитів авторизації перед напрямком цих повідомлень емітенту (сума операції, виражена у валюті карти, валюта карти);
- фіксування в базі даних результатів завершення обробки транзакції.

2.5. Диспетчер повідомлень — обов'язковий компонент ядра, що забезпечує маршрутизацію повідомлень у складі ISO-транзакції між компонентами ядра, а також по каналах взаємодії із зовнішніми системами. У функції диспетчера повідомлень входить:

- аналіз змісту отриманого повідомлення й визначення напрямку подальшої його маршрутизації;
- трансляція PIN-блоку, переданого в складі повідомлення, якщо це потрібно.

Система безпеки.

Система безпеки являє собою програмно-апаратний комплекс, призначений для виконання функцій, пов'язаних з: генерацією криптографічних ключів, захищеним зберіганням ключів, трансляцією ключів, генерацією параметрів, використовуваних при персоналізації карт (PIN, PVV, CVC/CVV), трансляцією PIN-блоків, верифікацією PIN-блоків й інших. Система безпеки містить у собі наступні основні компоненти:

- Сервер безпеки (Security Server) забезпечує виконання всіх криптографічних процедур у рамках перерахованих вище функцій. Він може забезпечувати роботу з одним або одночасно з декількома апаратними модулями безпеки. Сервер безпеки має стандартизований інтерфейс із внутрішніми компонентами ядра системи авторизації й інших прикладних підсистем. До складу сервера безпеки входить модуль моніторингу, що постійно контролює працездатність вхідних у його склад модулів й, при необхідності, забезпечує їхній автоматичний перезапуск. Всі ключі, використовувані в криптографічних процедурах, зберігаються в базі даних ключів у зашифрованому виді. Майстер-ключ, яким зашифровані ці ключі, зберігається усередині апаратного модуля безпеки (система підтримує роботу з апаратними модулями безпеки фірми Racal Guardata).

- Автоматизоване робоче місце (АРМ) адміністратора системи безпеки забезпечує діалоговий інтерфейс користувача із системою безпеки для роботи із ключами (генерація, розподіл, робота із БД ключів і т.п.), персоналізації смарт-карт, використовуваних для транспортування й завантаження ключів на термінали.

1.2. Огляд і аналіз шляхів вирішення автоматизації авторизованих операцій з банкоматами

Повсюдне поширення карт міжнародних платіжних систем, проникнення телекомунікацій і технологій мобільного зв'язку в усі сфери бізнесу, активне розвиток кобрендингових проєктів між банками й торгово-сервісними підприємствами, поступова консолідація фінансового й не фінансового секторів породили велике розмаїття моделей і методів організації бізнесу, пов'язаного з випуском й обслуговуванням пластикових карт. Виникнення нових каналів доставки банківських послуг, складних фінансових продуктів на базі пластикових карт, комплексних схем обміну інформацією між всіма учасниками ланцюжка електронних платежів привело до появи нових сучасних вимог до ІТ-інфраструктури, що сьогодні повинна забезпечувати підтримку наступних функціональних областей:

- багатоканальне обслуговування, при якому клієнти можуть робити операції, використовуючи різні устрої й кошти зв'язку, такі, як банкомати, платіжні термінали, інформаційні кіоски, центри обробки викликів, сайти електронної комерції, мобільні телефони;
- контроль і керування мережею банкоматів і платіжних терміналів;
- авторизація з боку еквайера в он-лайнному режимі з маршрутизацією запиту у відповідну емітентську або іншу систему;

- обробка авторизації з боку емітента в он-лайнному режимі з перевіркою ліміту рахунку;
- обмін інформацією із платіжними мережами он-лайнно для авторизації, й офф-лайнно для проведення розрахунково-клірингових операцій і формування звітів;
- розрахунково-клірингові операції між клієнтом і торговельною організацією, зі стягненням відповідних комісій із всіх учасників ланцюжка платежів;
- ведення претензійної роботи;
- інтеграція з іншими інформаційними системами, такими, як АБС, CRM, центри обробки викликів;
- обробка заяв клієнтів на відкриття карти, рахунку;
- керування заборгованістю по кредитах і стягнення проблемних позичок;
- керування картами, рахунками, клієнтами й торговельними організаціями;
- створення й керування продуктами;
- виготовлення й персоналізація карт;
- підтримка схем лояльності й бонусних програм;
- підтримка комплексних схем кредитування за допомогою пластикових карт;
- прийом платежів до користі третіх сторін (комунальні служби, оператори зв'язку й т.д.);
- обслуговування клієнтів через Інтернет;
- проведення операцій оплати товарів і послуг у мережі Інтернет.

За роки, що пройшли з моменту створення, продуктів автоматизації банківських операцій, вони перетворилися в зрілі рішення, що мають широкі функціональні можливості.

Такі системи побудовані на модульній архітектурі, безшовна інтеграція з іншими системами за рахунок відкритих стандартів й інтерфейсів, такі системи гнучкі за рахунок можливості налаштування параметрів у широкому діапазоні, масштабованість і висока доступність систем досягається за рахунок розпаралелення процесів і розподіленої обробки даних. Цей підхід дозволяє створювати рішення, що повністю враховують особливості бізнесу замовників з погляду масштабу, структури і специфіки внутрішніх бізнес-процесів, що гарантує надійний захист інвестицій.

У міру ускладнення й диверсифікованості завдань функціональність рішення може бути легко розширена шляхом додавання нових модулів, а продуктивність підвищена за рахунок збільшення потужності апаратної платформи. При тонкому налаштуванні ядра операційної системи й сервера бази даних досягається оптимальна продуктивність в рішенні різних по своїй природі завдань: обробки більших обсягів операцій у режимі реального часу й виконання пакетних процедур. Завдяки модульній архітектурі, системи автоматизації банківських операцій можуть одночасно виконувати кілька копій прикладних і комунікаційних процесів, що дозволяє усунути вузькі місця в продуктивності й забезпечує стійку безперервну роботу систем. Такі системи повністю використовують переваги, надавані архітектурою операційних систем сімейства Unix, індустріальних СУБД від Oracle й IBM, а також відмовостійкості апаратних платформ для досягнення високої продуктивності й доступності в режимі 24/7x365. Фахівці ведуть спільну роботу з провідними розроблювачами апаратних рішень, такими, як IBM, HP, Fujitsu-Siemens, Stratus Technologies й іншими на базі їх українських і закордонних центрів інновацій. Системи повністю враховують особливості архітектури таких серверних платформ, як IBM System i й System p, HP Integrity, HP 9000 й HP Superdome, Fujitsu-Siemens PRIMEPOWER, Stratus ft Server T Series й інших.

Системи автоматизації банківських операцій як основу мають такі системи керування та інтерфейси:

1. Керування банкоматами:

- інтерфейси банкоматів NDC+, Diebold 912/DDC, ISO8583 (Wincor Nixdorf, NCR, Diebold, Keba й ін.);
- система дистанційного моніторингу банкоматів;
- завантаження сценаріїв банкоматів;
- редактор сценаріїв банкоматів;
- прийом наявних - Cash-In (DDC, NDC+);
- Cash Recycling.

2. Платіжних терміналів:

- платіжні термінали ISO8583 (Verifone, Lipman, Ingenico, Nuperscom й ін.);
- платіжні термінали Visa I/II;
- інтерфейс електронних платежів ISO8583;
- підсистема обробки голосових авторизацій;
- інтерфейс для мультимедійного кіоску.

2. Мережні інтерфейси :

- Visa BASE I, Visa SMS;
- MasterCard BankNet, MDS;
- інтерфейс мережі Diners Club DCISC;
- інтерфейс мережі American Express ISO8583;
- JCB;
- BancNet (Філіппіни) ;
- ISO8583 Generic;
- Rucard (російська платіжна система) ;
- SmartVista-to-SmartVista.

2.5. Інтерфейси :

- Misys Equation;
- FNS BANCS;
- Systematics;
- SAP Banking;
- Unicard;
- Нова Афіна;
- ISO8583 Generic;
- SMS-нотифікація в мережах GSM;
- SMS-банкінг у мережах GSM;
- Thales HSM;
- Eracom Protect Host White/Orange HSM.

5. Опційні модулі й додаткові функціональні можливості :

- модуль он-лайнного запобігання шахрайських операцій;
- модуль он-лайнової обробки роздрібних операцій (кредитний карти, DPP – покупки на виплат і т.д);
- модуль "подвійної" авторизації;
- он-лайнова інтеграція із системою електронної комерції;
- он-лайнова інтеграція із системою Інтернет-банк;
- он-лайнова інтеграція із центром обробки викликів;
- он-лайнові комісії емітента;
- он-лайнові комісії еквасера.

6. EMV-розширення:

- підтримка еквайрінга EMV-карт на банкоматах;
- EMV-розширення для платіжних терміналів;
- підтримка EMV-скриптів емітента.

Завдяки своїй функціональній гнучкості SmartVista, сімейство продуктів SmartVista забезпечує підтримку широкого спектра роздрібних операцій, здійснюваних за допомогою пластикових карт як у відділенні

банку, так й у режимі самообслуговування. Сполучення можливостей он-лайнової обробки електронних платежів, інтеграції всіх каналів клієнтського обслуговування за допомогою єдиної транзакційної платформи й реалізації специфічної функціональності роздрібних продуктів дозволяє створити цілісну інфраструктуру, орієнтовану на роздрібне обслуговування.

Можливості рішення SmartVista дозволяють реалізувати підтримку наступних роздрібних продуктів й операцій з використанням пластикових карт:

1. Купівлі на виплат (DPP - Deferred Payment Plan): підтримка спеціальних лімітів для покупки товарів на виплат за рахунок позикових коштів банку, конфігурація різних платіжних планів на рівні торговельних організацій і карткових продуктів, формування гнучкого графіка погашення заборгованостей. Комунальні й сервісні платежі: реалізація механізму оплати комунальних і сервісних послуг з використанням банкоматів, багатофункціональних кіосків, платіжних терміналів й Інтернету.

2. Перекази коштів, у тому числі P2P: підтримка різних видів переказів: між рахунками одного клієнта, між рахунками різних клієнтів одного банку, міжбанківські перекази, перекази коштів з однієї пластикової карти на іншу за технологіями Visa й MasterCard (P2P).

2. Поповнення рахунків: реалізація різних технологій поповнення рахунку, у тому числі в он-лайновому режимі: конвертові депозити, cash-in, постійні доручення, платіжні вимоги.

2.5. Банківські карти: можливість прив'язки всіх рахунків до єдиної карти, що служить індивідуальним ідентифікатором клієнта й дозволяє робити операції з рахунками по різних каналах.

5. Кредитні карти: повна підтримка технології кредитних карт: спеціальні методи авторизації, контроль і ведення специфічних лімітів; револьверні кредитні карти, кредитні лінії з помісячним погашенням, миттєві кредити, charge карти.

6. Карти моментальної видачі: можливість видачі карти клієнтові в момент його першого звернення до банку: Visa Instant Issue, MasterCard Electron, передавторизованні карти, подарункові карти.

У міру розширення бізнесу й появи нових вимог до функціональності системи підтримки роздрібних операцій, а також, в області кредитування, рішення SmartVista може бути доповнено спеціалізованими продуктами для автоматизації процесів масової видачі кредитів і керування простроченими заборгованостями.

1. 2. Обґрунтування мети використання безготівкових розрахунків за допомогою банкоматів

Розрахунки з використанням готівки надзвичайно дорого обходяться державній і комерційній фінансовій структурам. Випуск в обіг нових купюр, обмін старих, утримування великого персоналу, незручності й більші втрати часу рядових клієнтів – все це важким тягарем лягає на економіку країни.

Із середини 20 століття починають з'являтися автоматизовані системи розрахунків за допомогою спеціальних банківських карток. У цей час цей спосіб безготівкових розрахунків отримав таке широке розповсюдження, що важко собі уявити сферу обслуговування в якій би вони не використовувалися: магазини, квиткові каси, готелі, всіх країн світу готові обслужити Вас, прийнявши вашу пластикову картку, як засіб оплати.

У цей час у нашій країні велика частка розрахунків, вироблених:

- готівкою (банкнотами);
- у формі обміну всілякими векселями;
- іншими зобов'язаннями.

Один з можливих і самих перспективних способів вирішення проблеми наявного обороту – створення ефективної автоматизованої системи безготівкових розрахунків.

Організація розрахунків з використанням безготівкових грошей набагато переважніше платежів готівкою, оскільки:

- досягається значна економія на витратах обігу;
- збільшуються ресурси банків;
- створюється можливість більш ефективного оподаткування й регулювання макроекономічних процесів.

Тому такий модуль має місце в системі автоматизації банківських операцій.

Висновок до розділу 1

Системи автоматизації банківських операцій мають модульну структуру – це дає можливість робити різні конфігурації зборок програмного забезпечення відповідно з різними властивостями та можливостями спрямованими на бізнес процеси банку. Перевага модульних систем є, інтегрування додаткових модулів структури для не автоматизованих банківських процесів, без втрати часу на зміну програмного забезпечення. Модульні системи мають перевагу ще в тому, що корисно і в повному обсязі використовують апаратні потужності і в той же час це недолік тому, що при додаванні нових модулів програмного забезпечення потрібно збільшення апаратних потужностей тому потрібно будувати систему з потенціальним запасом потужності. Системі розробленні з урахування інтерфейсів від різних виробників і обслуговують учасників платіжних систем: VISA Int., MasterCard Int., Diners Club, American Express, Юніон Кард, СТБ Кард, локальні платіжні системи банків. Весь комплекс у цілому й кожна з його компонентів окремо можуть бути використані для роботи банку з міжнародними платіжними системами: VISA , MasterCard , Diners Club , American Express і українськими: Юніон Кард, СТБ Кард.

РОЗДІЛ 2 МОДЕЛЮВАННЯ БІЗНЕС-ПРОЦЕСІВ РОБОТИ БАНКІВСЬКОЇ МЕРЕЖІ ТА ПРОЄКТУВАННЯ СИСТЕМИ

Основною метою створення нової системи банківського обслуговування населення є:

- значне зниження затрат, пов'язаних з готівково-грошовим обігом;
- створення умов для інтенсивного і повного акумулювання вільних грошових коштів населення;
- створення нових технологій платіжного обслуговування населення;
- суттєве підвищення якості і розширення номенклатури послуг населенню, які надаються банком;
- установа ефективного та оперативного державного обліку доходів і видатків населення;
- забезпечення безпеки власних грошових коштів населення.

Утілення в Україні системи електронних платежів (СЕП) значно розширило можливості банків щодо надання фінансово-інформаційних послуг клієнтам, різко прискорило процес проходження платежів. Зростання можливостей сучасних комунікаційних систем дозволяє банкам практично необмежено нарощувати мережу філій, відділень, систем класу «Клієнт — Банк», окремих робочих місць для обслуговування клієнтів. Усе це підготувало ґрунт для широкого втілення масових електронних платежів. Основною проблемою до цього часу був брак масових засобів платежу, і одночасно, гарантованої ідентифікації платника. Усі ці проблеми можуть бути успішно вирішені з розробленням і втіленням системи масових електронних платежів (СМЕП) з використанням пластикових карток [1].

Одним із основних напрямків НБУ сьогодні є утворення національної системи масових електронних платежів населення за товари та послуги (СМЕП).

Національна система масових електронних платежів – це система безготівкових розрахунків, при якій розрахунки за товари та послуги здійснюються за допомогою банківських платіжних карток [2].

НСМЕП має функціональний повний набір апаратних, програмних та організаційних засобів, які разом забезпечують керування інтелектуальними мікропроцесорними картками, терміналами, банкоматами, інкасацією трансакцій, процесингом, клірингом, а також інтерфейс та інтеграцію з банківськими системами.

РПЦ — регіональні процесингові центри в обласних управліннях НБУ або комерційних підприємствах.

Банки-емітенти і банки-еквайри НСМЕП зі своїми банківськими підсистемами, торговельною інфраструктурою та інфраструктурою сфери послуг.

POST-термінали – торговельні термінали.

BST – банківські термінали.

2.1. Банкомати

Виходячи з викладеного в першому розділі, можна зробити висновок, що велика кількість систем електронних розрахунків, платіжних систем заснована на застосуванні пластикових карт. Більшість операцій із пластиковими картами здійснюються за допомогою банкоматів.

Банківські автомати-касири (банкомати, або англійська аббревіатура: АТМ) – це автоматичні апарати, що працюють без участі людини, розташовані всередині або поза банком, здатні видавати наявні гроші (готівку) і виконувати стандартні фінансові операції.

Типовий автомат-касир являє собою електронно-механічну машину, яка має три прилади вводу: зчитування з пластикової картки, цифрової клавіатури і функціональної клавіатури, а також три прилади виводу: електронне табло, пристрій для видачі готівки і принтер для роздруківки

супутньої документації. Банкомат приводиться у дію пластиковою карткою з магнітним шаром (в новітні пластикові картки вбудований мікропроцесор). Водночас з клавіатури клієнт набирає персональний символно-цифровий ідентифікаційний код [3].

Основні операції, що здійснюються банкоматами:

- інформування клієнтів про стан їх рахунків;
- видача готівки;
- приймання готівки від клієнтів для розміщення на їх рахунках (цю функцію реалізують депозитні банкомати).

Доступ до банкомата для виконання операцій здійснюється із застосуванням банківських ідентифікаційних карток та персональних ідентифікаційних номерів-кодів клієнтів банківських установ. Після виконання операцій із видачі (приймання) готівки клієнтові має бути видана пронумерована квитанція, в якій вказуються: назва банківської установи, що експлуатує банкомат, номер банкомата, дата, час, вид операції, номер трансакції, сума виданих (прийнятих) коштів та інші реквізити відповідно до вимог системи, в якій використовується банкомат. При застосуванні банкоматів у внутрішньобанківських системах автоматизації касових операцій квитанція може не видаватися. У цьому разі обов'язково з періодичністю, визначеною в договорі між клієнтом і банківською установою, клієнтові надається виписка за операціями, здійсненими через банкомат, підписана і завірена у встановленому порядку.

Для виконання підкріплення та інкасації коштів за банкоматом (групою банкоматів) письмовим розпорядженням керівника банківської установи визначається перелік відповідальних працівників, в обов'язки яких входить обслуговування банкоматів, із персональним розподілом між ними функціональних обов'язків. Виконання функціональних обов'язків зазначеними працівниками має бути регламентовано внутрішніми положеннями банківської установи.

Для кожного банкомата, зважаючи на рівень його захищеності та необхідність забезпечення безперебійної роботи, визначається ліміт коштів, що можуть бути одночасно завантажені та зберігатися в його сейфі. Визначена величина ліміту погоджується з головним бухгалтером та затверджується керівником банківської установи.

Для обліку операцій, що проводяться з банкоматами, ведеться "Книга обліку операцій із завантаження та розвантаження банкоматів". Відповідальним за ведення такої книги є завідуючий касою. Ця книга має бути пронумерована, прошнурована, підписана керівником, головним бухгалтером та скріплена печаткою банківської установи.

Підкріплення банкомата готівкою проводиться залежно від потреби в ній. Потрібну суму в межах визначеного для банкомата ліміту коштів касир банкоматів отримує у завідуючого касою. Вкладення купюр у касети, а також вилучення купюр із касет відбувається у приміщенні каси. Прийнятій сумі грошей касир перераховує покупцю, вкладає їх у касети, закриває касети на ключ і опломбовує їх.

До касети прикріплюється ярлик із зазначенням на ньому найменування банківської установи, номера банкомата, номіналу, кількості купюр, суми вкладених коштів, дати, підпису та іменного штампа спеціально виділеного для завантаження касет касового працівника.

Після завантаження касет завідуючий касою оформляє для інкасатора маршрутний лист із зазначенням адреси і місця розташування банкомата, номерів касет, що мають бути вилучені з банкомата і доставлені в касу, номерів касет, що мають бути вставлені в банкомат, та інформації, яка необхідна для ініціалізації його роботи.

Для завантаження банкомата касети й маршрутний лист передаються інкасатору. Приймаючи касети, інкасатор перевіряє цілість касет і пломб, наявність на ярликах реквізитів. Разом із касетами інкасатору під розписку в "Книзі обліку операцій із завантаження та розвантаження банкоматів"

передаються ключі від сейфа банкомата і від його модуля управління та картка доступу.

Після доставки касет інкасатор із застосуванням картки доступу входить у режим обслуговування банкомата, вилучає вказані в маршрутному листі касети із залишками грошових коштів, встановлює нові касети і з використанням даних із маршрутного листа вводять у модуль управління інформацію про номінали та кількість купюр у встановлених касетах. Після закінчення введення на чековому друкувальному пристрої роздруковується пронумерована квитанція із зазначенням номера банкомата, дати, часу виконання операції завантаження, ідентифікатора картки інкасатора, суми залишків коштів у , вилучених касетах та суми коштів у встановлених касетах.

Після закінчення операцій завантаження виконується його ініціалізація і запуск у роботу. При цьому інформація про зміст касет передається в систему управління банкоматами, а завантажені кошти зараховуються на балансовий рахунок банкомата.

Інкасатор здає касиру під розписку у "Книзі обліку операцій із завантаження та розвантаження банкоматів" вилучені касети, ключі, картку й одержану в банкоматі квитанцію.

Касир у присутності інкасатора перевіряє цілість доставлених касет, наявність ярликів і пломб та вилучає у нього квитанцію з вказаною в ній сумою. Після цього касир підтверджує своїм підписом у маршрутному листі приймання касет. Касир у присутності завідуючого касою (контролера) перераховує вилучену з касет готівку, звіряє суму з квитанцією, виписує на суму вилучених із касет коштів прибутковий касовий ордер та довідку касира, відповідно до яких здійснює списання цієї суми з балансового рахунка банкомата й зарахування цієї суми на рахунок каси, і здає їх завідуючому касою.

При застосуванні депозитних банкоматів разом із касетами із залишками коштів інкасатор доставляє касети з конвертами із вкладеними для зарахування на рахунки клієнтів коштами. Касир у присутності завідуючого касою звіряє відповідність наявних сум у конвертах із даними меморіального ордеру, одержаного від системи управління банкоматами. У разі виявлення розбіжностей між фактичною сумою і даними меморіального ордеру складається відповідний акт із зазначенням даних клієнта, номера, адреси банкомата, часу приймання готівкових коштів, заявленої та фактичної суми. Акт підписується касиром та завідуючим касою. Клієнт, який вносив готівку, має бути ознайомлений із змістом акта. Спірні питання, які при цьому можуть виникнути, вирішуються в порядку, визначеному договором між клієнтом і банківською установою.

Після звірювання касир виписує прибутковий касовий ордер на суму фактично вилучених із конвертів коштів і ставить підпис у меморіальному ордері. Завідуючий касою приймає від касира кошти, звіряє їх суму з даними меморіального ордеру, розписується в прибутковому і меморіальному ордерах. На підставі меморіального ордеру здійснюються зарахування фактично одержаних грошових коштів на рахунки клієнтів [2].

Призначені для видачі купюри зберігаються в спеціальних касетах (до 2500 банкнот одного номіналу). Ці касети, хоча не так захищені, як сейфи, але можуть бути розкриті тільки на спеціальному устаткуванні.

Касет у банкомату може бути декілька, стандартно - від двох до чотирьох. Різні депозитні касети можуть використовуватися як для купюр різних номіналів, так і для різних валют.

Важливе значення в банкоматах має так звана "поворотна" або "відмовна" касета. Туди поміщаються зам'яті або потерті купюри, неправильно відлічені, відбраковані в процесі видачі, а також забуті клієнтом. Якщо система "підозрює", що щось не так, вона автоматично скидає купюри у відмовну касету й кошти з рахунку клієнта не списуються.

Банкомати можуть комплектуватися додатковим обладнанням: принтер зі спеціальним папером, фотокамера й мультимедіа-обладнання для прямих консультацій з банківським службовцем за допомогою екрана, клавіатура для програмування, блок автономного живлення, криптопроцесор і багато чого іншого.

На перший погляд - у банкомата найпростіші функції: зчитати картку, видати гроші, надрукувати чек. Однак тільки перелік можливих операцій банкомату показує, що це далеко не так. Крім того, банкомат повинен бути запрограмований так, щоб бути абсолютно передбачуваним і абсолютно надійним. Комп'ютер банкомату не має права "зависати" або не обробляти яких-небудь сигналів.

Будь-якою фірмою-виробником поставляється спеціальне програмне забезпечення до банкомату - бібліотека базових програмних модулів для написання власної прикладної системи або для безпосереднього використання в банкоматах і (українською рідко) для використання в центральних комп'ютерах, що управляють банкоматами.

Як правило, всі банкомати, що працюють із банківськими платіжними картками одного типу, з'єднані в локальну або розподілену мережу із центральним комп'ютером. Усередині одного міста цілком прийнятним вважається відповідь центрального комп'ютера на запит від банкомату протягом 10 с.

Повідомлення, які доводиться обробляти комп'ютеру банкомата, досить різноманітні. Відповідно різні й завдання, які вирішуються комп'ютером у багатозадачному режимі: ідентифікація й перевірка правильності введеного PIN-Коду, обробка сигналів від великої кількості датчиків, постійний автоматичний контроль всіх внутрішніх і зовнішніх з'єднань, контроль витрати паперу в принтері й купюр у депозитних касетах, аналіз на розрив електричних з'єднань у момент видачі купюр, реакція на "позаштатні" механічні впливи, фіксація факту вилучення грошей або "забутковатість"

клієнта, розпізнавання кодів різних платіжних систем і перемикання контурів обробки клієнтських повідомлень, сеансовий і позаплановий виклик центрального комп'ютера.

Крім того, комп'ютер банкомата постійно генерує деякі важливі команди: вибрати режим авторизації (ON-Line або OFF-Line залежно від запитуваної суми й наявності необхідної інформації в базі даних комп'ютера), видати гроші, вивести інформацію на користувальницький екран, надіслати запит на центральний комп'ютер, заарештувати картку, що знаходиться в стоп-аркуші (списку карток, права користування якими анульовані). Тому не дивно, що внутрішній комп'ютер у банкомату повинен бути досить потужним.

По виконанню можна розрізняти офісні банкомати (які встановлюються у фойє банків, магазинів, страхових компаній і в метро), вуличні банкомати (вмонтовані в стіни будинків), і автострадні (які витримують лобовий наїзд важкої вантажівки).

2.1.1. Режими роботи АТМ

Існують два режими роботи АТМ:

- оф-лайн (off-line);
- он-лайн (on-line).

Режим off-line – це такий режим роботи, коли апарат постійно не зв'язаний з мережею. Це найбільш поширена група банкоматів, оскільки вони працюють з клієнтами автономно, без постійного зв'язку з розрахунковим центром (свого банку системи карток). Це повноцінний банкомат. Основна проблема при обслуговуванні оф-лайнових систем – це занесення в їх пам'ять (найчастіше на магнітному диску) бази про анульовані (загублені, викрадені) картки або такі, термін дії яких уже вичерпався.

Для того, щоб унеможливити проведення операцій знімання коштів з рахунку картки, банкомата повинні працювати з картками такої конструкції, яка дозволяє робити на неї запис (параметри клієнта, залишок рахунку,

взагалі історія рахунка). Це може бути магнітна стрічка або для чіп-карток (смарт-карток) – безпосередньо у пам'ять мікросхеми. Тоді стає неможливим проведення операції послідовно через декілька банкоматів, бо вони не мають прямого зв'язку із центром обробки платежів [2.5].

Інформація про кількість грошей у клієнта і про зняття їх завдається у вигляді магнітного коду на саму кредитну картку, що захищає фінансову установу від повторного зняття грошей на інших автоматах. Про кожне видання грошей друкується паперове повідомлення, оригінал якого видається клієнту, а дублікат зберігається всередині банкомату, вилучається обслуговуючим персоналом і надходить у банк [3].

Собівартість оф-лайнних банкоматів відносно низька, бо їх можна обслуговувати "вручну": один-два рази на добу оператор банкоматів виймає протокол проведених операцій (це, як правило, паперова стрічка дублікатів квитанцій та магнітний диск чи флеш-пам'ять з відповідними записами) для передачі до розрахункового центру відповідного банку (мережі банків чи системи карток). До пам'яті заноситься база карток, за якими операції проводити не можна. Проте ризик у зловживанні пластиковими картками для таких автоматів, зрозуміло, вищий.

Робота в режимі он-лайн передбачає постійний зв'язок через телекомунікаційний канал банкомату із розрахунковим центром "свого" банку (мережі банків) чи процесинговим центром країни (системи карток). Відповідно кожна операція одразу стає відома у розрахунковому центрі, може бути перевірена та підтверджена. Такий режим дорожчий, але безпечніший, бо неможливо повторне отримання готівки з одного і того ж рахунку, з простроченого рахунку, і тощо.

Постійний "гарячий" зв'язок банкомату дозволяє власнику картки в будь-який момент брати довідки про стан свого рахунка. Ризик у зловживанні картками для таких автоматів дуже малий, але більші накладні витрати на телекомунікації. Для країн із поганим чи дорогим рівнем

телекомунікацій он-лайнний зв'язок з банкоматами по всій країні не використовується [2.5].

2.1.2. Стратегія використання АТМ

Під час розробки стратегії з використання автоматів-касирів банк повинен знати особливості свого оточення, оскільки конкуренція, характер клієнтури, особливості географічного положення і безліч інших чинників визначають результати автоматизації. Існують два шляхи вибору стратегії використання автоматів-касирів:

- перший – використання незалежної власної мережі;
- другий – участь на пайових засадах у спільній мережі.

Перший шлях при більших витратах надасть повний контроль над системою, але практика показала переваги надання клієнтам більш широкого доступу до мереж, коли банк бере участь у міжбанківських і навіть у загальнонаціональних платіжних системах. Спільне користування мережами – сьогодні вид використання банкоматів у країнах з розвинутою ринковою економікою, що найчастіше зустрічається. Статистика підкреслює феномен, коли лише участь у спільних електронних мережах викликає більш широке і часте застосування клієнтами банківських кредитних карток.

Спільна мережа АТМ – це спільне підприємство декількох фінансових установ. Організаційна структура цього підприємства і спеціалізовані деталі функціонування мережі визначаються банками-учасниками. Системи з пайовою участю загальнонаціонального масштабу розв'язують п'ять задач:

- розподіл між учасниками витрат і ризику під час розробки і створенні системи;
- значне зменшення вартості послуг;
- надання послугам загальнонаціонального характеру - нова суб'єктивна цінність;

- можливість виходу для регіональних банків на ринки "чужих" регіонів (областей, штатів, тощо);
- подолання географічних обмежень, що не існують для небанківських установ.

Щоб, електронна система платежів могла представляти реальну альтернативу готівковому грошовому обігу або паперовим чекам, необхідно АТМ, що обслуговують покупців в торгових закладах, і мережу банківських послуг вдома об'єднати в єдину систему.

2.2.5. Види послуг, які можна отримати за допомогою пластикових карток

За допомогою різного виду пластикових карток можна скористатись такими послугами:

- Отримати готівки через банкомати.
- Отримати відповіді на запит про стан рахунку.
- Переказати кошти з одного рахунку на інший. Наприклад, з рахунку з низькими відсотками на рахунок з більш високими відсотками чи навпаки. В електронних системах роздрібних банківських послуг використовуються такі типи рахунків: операційний/поточний, чековий рахунок для виконання великої кількості транзакцій і рахунок кредитної картки. Більшість банків не дозволяють отримувати готівку з депозитних рахунків.
- Отримати виписки з поточного рахунку. Виписка — це друкований документ, що містить інформацію про проведені операції по рахунку, а також дані про залишок на рахунку.
- Отримати кредит при купівлі товарів чи авансом в готівковому вигляді.
- Виконати платіж за товар чи якусь послугу з використанням торговельних терміналів.

- Отримати відповідь на запит про можливість отримання клієнтського кредиту з допомогою банкомату.

Усі ці послуги клієнт може отримати за допомогою системи електронних роздрібних банківських послуг без участі персоналу банку.

Пластикові картки як платіжний засіб знайшли своє широке застосування не лише в банківській сфері. Сфера використання карток дуже широка — вони використовуються при покупці товарів в автоматах, для сплати мита при проїзді платними автострадами, для розрахунків на бензозаправках, в громадському транспорті та в інших розрахунках.

2.2.5.1. Переказ коштів

Банківська діяльність істотно полегшується при використанні різних систем електронного переказу коштів, таких як SWIFT, CHAPS, BACS і Національна система масових електронних платежів. Вони хоч і специфічні для банків, але також дозволяють розповсюдити можливості, що забезпечуються сучасними ІТ, на будь-якій сфері ділової активності.

SWIFT

SWIFT (Society for Interbank Financial Telecommunications — Суспільство всесвітніх міжбанківських фінансових телекомунікацій) забезпечує переказ коштів і здійснення платежів між всіма входними в цю систему банківськими організаціями у всьому світі. Банки забезпечують кредитне фінансування капітальних витрат на систему SWIFT. З моменту її впровадження дозволений доступ як користувачам і деяким небанківським установам. До числа таких користувачів увійшли біржі цінних паперів, фондові біржі, центральні клірингові установи, маклерські контори і (у 1992 р.) фінансові менеджери.

SWIFT — це високонадійна телекомунікаційна мережа, в рамках якої здійснюється обмін стандартними повідомленнями. Сьогодні SWIFT обробляє щодня до півмільйона повідомлень. Стандартні формати декількох типів повідомлень включають таку інформацію:

- заявки на покупку або продаж;
- інструкції по взаєморозрахунках;
- підтвердження обміну із зарубіжними адресатами;
- балансові довідки і звіти;
- котування цінних паперів;
- підтвердження, що стосуються торгових операцій.

Стандартизація — це одна з найважливіших особливостей ІТ. У SWIFT, наприклад, застосовуються стандартні коди для позначення кожної валюти (наприклад, фунти стерлінгів позначаються як STG, а долари США — USD).

У вересні 1992 р. ще одна група повідомлень була додана до системи з метою охопити операції з цінними паперами. За сьогоднішніми оцінками, SWIFT підтримує трафік, що зростає щорічно на 35%. Насущною залишається потреба в двосторонньому обміні інформацією і відповідями на запити, особливо із зростанням міжнародного торгового обміну і інвестицій.

CHAPS

CHAPS (Clearing House Automated Payment System — автоматизована система платежів для клірингових палат) є системою, за допомогою якої банки, що беруть участь в її використанні, можуть проводити великі стерлінгові платежі з оплатою день в день. За деякими оцінками, щодня через систему CHAPS проходять суми, що перевищують 50 мільярдів фунтів стерлінгів. Система CHAPS замінила «піший» принцип, коли банк відправляв кур'єра з чеком в інший банк (часто, дійсно, пішки) для проведення термінового (спотового) платежу.

Система CHAPS упроваджена банками з метою економії часу і грошей. Банки допустили до неї і інші структури за умови відповідної оснащеності останніх. У кожному банку-платнику встановлений комп'ютер Tandem, що є CHAPS-інтерфейсом, а також головна фінансова автоматизована система. Кожен Tandem приймає платежі і здійснює їх відправку через мережу

комутації пакетів. Таким чином, CHAPS є системою реального часу. І знову незайве підкреслити, що такі послуги стали можливими завдяки новим інформаційним технологіям.

BACS

BACS (Bankers Automated Clearance Services — Служба автоматизованого проведення банківських розрахунків) використовується для електронного переказу коштів між рахунками в банківській системі Великобританії. Краще всього ця система зарекомендувала себе в обробці платіжних листків (по зарплаті). Замість того, щоб в день видачі зарплати вручати кожному службовцю чек, працедавець відправляє відповідні дані про виплати на магнітних носіях в банк, що працює з BACS, внаслідок чого виплати нараховуються автоматизованою системою [5].

2. 2. Методи забезпечення безпеки розрахунків

За інформацією Інституту комп'ютерної безпеки (США), порушення роботи інформаційних систем бувають від:

- вірусних атак — 3 %;
- збою обладнання — 20 %;
- помилок персоналу — більше 50 % випадків.

За оцінками американських експертів, 88 % втрат конфіденційності інформації з комп'ютерних мереж — результат зловмисних дій персоналу, всі ж інші випадки є результатом перехоплення інформаційних потоків технічними засобами.

Фахівці з проблем шифрування визнають, що практично всі комерційні системи шифрування "бояться" активних атак зловмисників, тактика яких полягає, зокрема, у перехопленні трафіку Web-вузла з подальшою посилкою на вузол до 1 млн. повідомлень. Аналіз реакції серверу на такі повідомлення може призвести до витоку секретної інформації.

Політика інформаційної безпеки (банку, компанії тощо) передбачає: знання про всі інформаційні потоки; розуміння структури інформації в системі; виділення критичних (у плані захисту) процесів, ділянок в інформаційних системах; виділення користувачів у категорії і групи з чітким визначенням їх прав; вміння фіксувати факт несанкціонованого доступу чи атаки.

У силу того, що основний канал для несанкціонованого доступу – комп'ютерна (банківська, корпоративна, глобальна) мережа, то основна увага приділяється системі захисту на рівні підтримки мережі (маршрутизаторів, брандмауерів, FTP, Web, електронної, пошти, сітьової файлової системи, броузерів тощо) [2.5].

2. 2.1. Принципи побудови систем шифрування

Сучасні криптографічні системи будуються з урахуванням таких ідей:

- діапазон значень ключа шифру повинен бути таким, щоб на сучасній комп'ютерній техніці їх звичайний перебір був неефективним (тривав місяці, роки, іншими словами, для швидкого розшифрування потрібно нескінченний обчислювальний ресурс);
- вартість задіяних ресурсів для розшифрування даних без знання ключа повинна бути не меншою, ніж вартість самих даних;
- таємницею є не алгоритм шифрування (дешифрування), а лише ключ шифру;
- навіть незначні модифікації даних (перед шифруванням) або самого ключа шифру повинні призводити до значних змін у файлі зашифрованих даних (щоб було неможливо помітити якусь закономірність у способі шифрування).

Із загальних рекомендацій (принципів) теорії інформації випливає, що при меншій надлишковості (ентропії) даних для шифрування зменшується також і довжина ключа, і навпаки. Тому, зокрема, варто шифрувати дані, попередньо їх заархівувавши.

Алгоритми шифрування поділяються на:

- власне шифри, які розглядають дані як набір бітів без; урахування їх лексичної структури;
- спецкоди, які враховують лексичну структуру даних (на практиці це тексти), виділяючи слова, фрази тощо.

У системах електронної комерції всі транзакції (наприклад, платежі) досить короткі і мають просту структуру, яка очевидна для таких даних, атрибутів платежів, банківських рахунків тощо. Тому коротка та прозора за своєю структурою інформація відповідно і легше дешифрується. Якщо такі транзакції збирати у пакети, стає простіше уникати природної "структурності" даних. Подібна ситуація притаманна роботі в архітектурі клієнт-сервер з віддаленим доступом до бази даних. Практично всі корпоративні СУБД є реляційними. Отже, результатом реляційного запиту (на базі SQL-запиту, як це і є на практиці) буде знову реляція (таблиця), тобто добре структуровані дані. Хороші системи шифрування повинні враховувати таку особливість інформації.

Методи шифрування діляться на 2 великі групи.

1. Симетричні методи будуються на принципі, що сторони, які посилають (шифрують) і приймають (дешифрують), використовують один ключ. Зрозуміло, що тривале користування одним ключем підвищує ризик розпізнавання ключа; отже, варто регулярно його змінювати. Ця ситуація є самостійною проблемою, якщо новий ключ потрібно передавати віддаленій системі чи людині, тобто його зміна є критичним процесом. Симетричні методи найчастіше використовуються для шифрування файлових систем і менш придатні для таких систем, як електронна пошта. Державні та військові відомства використовують винятково симетричні методи шифрування.

Використовується також різновид симетричного методу, коли ключ ділиться на дві частини, кожна з яких не дає можливості розшифрувати дані, що загалом підвищує надійність таємниці ключа. Типові алгоритми

симетричного шифрування: DES, Triple DES, IDEA, B-Crypt, Lucifer, Skpjack, FEAL-1, RC2, RC 2.5.

2. Асиметричні методи, або методи (стандарти) з відкритим (загальним) ключем використовуються за такою схемою:

- сторона, яка приймає, має 2 ключі, що не можуть отримуватися один з другого: відкритий та закритий. Відкритий ключ вільно поширюється (навіть публікується, розміщується на Web-сайтах);
- сторона, яка посилає, шифрує дані з використанням відкритого ключа; про таємний закритий ключ знає лише система шифрування;
- отримані і зашифровані дані сторона, яка приймає, розшифровує за допомогою закритого ключа.

Типові алгоритми асиметричного шифрування: DH, RSA, ElGamal.

Асиметричні алгоритми дають значну економію (до декількох мільйонів доларів) в експлуатації служб безпеки для великих банків та корпорацій. Симетричні працюють з відносно короткими ключами, асиметричні – з довгими. Тому симетричні методи більш швидкі (приблизно у 1000 разів). На практиці використовуються і змішані схеми шифрування.

Як вважають криптографи, складність розкладання 230 2.5-бітного цілого на множники (відкритого ключа для асиметричних методів) приблизно відповідає підбору 128-бітного ключа в симетричних методах.

Використовується також шифрування файлів даних з метою підтвердження, що останні не піддавалися змінам і виготовлені саме автором. Така методика отримала назву цифровий підпис. Останній може супроводжувати як зашифровані повідомлення, так і відкриті. Цифровий підпис має гарантувати: авторство, тобто його неможливо підробити і використати повторно; неможливість модифікації "підписаного" документа.

Використовується й поняття надійної системи. Це такі програмно-апаратні засоби, які забезпечують одночасну обробку інформації різного ступеня таємності різними користувачами без порушення прав доступу [2.5].

2. 2. 2.5. Протоколи для безпеки передачі інформації

Сучасні найбільш поширені протоколи безпечного мережевого з'єднання: POST, X.509, SET, Mondex та інші. Наведемо деякі характеристики протоколів (стандартів):

- Cramer-Shoup. Найновіша криптосистема, яка ще не є промисловим стандартом, але має очевидні переваги, використовуючи подвійне шифрування інформації, що відправляється з Internet-вузла (Web-серверу). Шифруються як відповіді серверу на команди і управління Web-сайтом, так і відповіді на будь-які запити до серверу. Такий підхід значно ускладнює розпізнавання зломисниками ключів до системи захисту (фірма IBM уже бере цей метод на озброєння для своїх криптосистем).
- DES (Data Encryption Standard). Є сучасним федеральним стандартом у США, аналогом міжнародного комітету ISO 8372-87. Це типовий представник симетричних методів. Був розроблений у 1970 році в корпорації IBM. Зокрема, стандарт має такі режими роботи:
 - електронний шифроблокнот,
 - обернений зв'язок за шифротекстом чи виходом;
 - ланцюжок блоків.

Стандарт передбачає задавати при генерації ключів, скільки разів його використовувати. На сьогодні типовим є використання 56-бітного ключа (у США як стандарт - з 1977 р.) для 6 2.5-бітних блоків, проте багато експертів вважають таку довжину ключа вже недостатньою і пропонують перейти на 112-бітний і більше ключ, що, звичайно, зменшить швидкість роботи із цим стандартом. Так званий потрійний DES є послідовністю шифрування та дешифрування з різними

ключами. Американська асоціація банків ABA (American Bankers Association) використовує DES як промисловий стандарт.

- DSS (Digital Signature Standard). Це стандарт, розроблений фірмою IBM у 1970 р. для електронного підпису інформації. Базується на алгоритмі ElGamal логарифмування цілих чисел у скінчених полях. Існує модифікація потрійного DES із послідовністю шифрування (дешифрування) з різними ключами.
- ECC (Elliptic Curve Cryptography). Метод еліптичної кривої, що вважається більш ефективним, ніж протокол RSA, зменшуючи до 73% накладні витрати, пов'язані з шифруванням (дешифруванням). Зокрема, як свідчать експерименти, використання ECC у протоколі SET прискорює роботу інтерфейсів оформлення платежів в Internet у 2.50 разів.
- IPSec (IP Security). Протокол для побудови тунелів при підключенні до розділяючих мереж та Internet. Дозволяє ідентифікувати користувачів та шифрувати трафік.
- MD2, MD5. Алгоритми для виготовлення 128-бітних дайджестів.
- RC2, RC 2.5. Симетричні алгоритми, розроблені компанією RSA, з ключами змінної довжини. Працюють у 10 разів швидше за стандарт DES.
- RSA (Rivest, Shamir, Aldeman). Запатентований у 1977 р. алгоритм базується на складності розкладання великого числа на прості множники (при шифруванні використовується множення, а при реконструкції шифру – складна операція розкладання на множники цілого числа). Трьома розробниками створена одноіменна компанія RSA, що випускає програмні та апаратні системи шифрування. Стандарт – типовий представник асиметричного методу шифрування. Розмір ключа: від 512 до 20 2.58 бітів.

- SET (Secure Electronic Transactions). Використовується для організації захищеного зв'язку в Internet, як правило, між банком чи корпорацією-власником системи карток (банком-емітентом) та банком, що обслуговує продавця (банком-екваєром). Спонсорами цього протоколу виступають компанії-емітенти систем електронних карток Visa Int. та MasterCard Int., які й утворили некомерційну організацію SETco для впровадження протоколу як промислового стандарту в сфері електронної комерції. Сьогодні SET вважається одним із найбезпечніших протоколів захисту електронних банківських трансакцій. Проте власне експериментів з нині існуючою версією SET 1.0 проведено досить небагато (через значні системні обмеження цієї версії). Версія SET 2.0 взагалі не повинна залежати від алгоритму шифрування даних.

Супроводження протоколу здійснюється компаніями Verisign, Cybercash і First Virtual, які встановлюють контроль повноваження користувачів для комерсантів і банків. SET – це лише специфікація, а не повний продукт для здійснення захисту.

- SHA-1. Алгоритм для генерації 160-бітного дайджесту.
- S/MIME (Secure Multipurpose Mail Extensions). Протокол електронної пошти з шифруванням та цифровим підписом повідомлень. Розроблений компанією RSA в якості модифікації електронної пошти MIME.

Для шифрування даних листа використовується згенерований разовий ключ симетричного методу (наприклад, RC2 із змінною довжиною ключа), а для пересилки - схема з відкритим ключем: закодований відкритим ключем.

- SSL (Secure Sockets Layer). Сьогодні це найбільш поширений протокол захисту інформації в Internet, який розробила компанія RSA Data Security. Дозволяє проводити аутентифікацію всіх учасників обробки

інформації (нотаріальна служба аутентифікації). Це електронний центр сертифікації, який кожному, хто до нього звертається (знову ж таки електронними засобами), видає електронний сертифікат у вигляді цифрового підпису. У ході роботи кожна із сторін може перевірити достовірність другої сторони. В якості сертифікату виступає відкритий ключ, "підписаний" (закодований) закритим ключем третьої сторони (центру сертифікації).

- X.509. Це специфікація цифрових підписів (цифрових сертифікатів), яка широко використовується в Internet. Розроблена комітетами ITU-T та ISO (перша версія - 1988 р., остання - 1996 р.). Достовірність інформації перевіряється такою процедурою. Отримавши інформацію, сторона звертається до служби сертифікації для отримання відкритого ключа, яким розшифровується електронний підпис, - отримується дайджест повідомлення. Можна перевірити і термін дії сертифіката. У додатках для електронної комерції користувачі реєструють свої цифрові сертифікати в банку, який видає кредитну картку. Щоразу, як клієнт збирається здійснити транзакцію, браузер через протокол SET посилає копію сертифіката продавцю, щоб перевірити дійсність кредитної картки користувача [2.5].

2. 2.5 Розробка ескізного проєкту інформаційної системи

Мова UML (Unified Modeling Language) являє собою загально цільову мову візуального моделювання, що розроблена для специфікації, візуалізації, проектування й документування компонентів програмного забезпечення, бізнес-процесів і інших систем. Мова UML одночасно є простим і потужним засобом моделювання, що може бути ефективно використана для побудови концептуальних, логічних і графічних моделей складних систем всілякого цільового призначення. Ця мова увібрала в себе найкращі якості методів

програмної інженерії, які з успіхом використовувалися протягом останніх років при моделюванні великих і складних систем [21].

Мова UML призначена насамперед для розробки програмних систем. Її використання особливо ефективно в наступних галузях:

- інформаційні системи масштабу підприємства;
- банківські й фінансові послуги;
- телекомунікації;
- транспорт;
- оборонна промисловість, авіація й космонавтика;
- роздрібна торгівля;
- медична електроніка;

наука;

розподілені Web-Системи.

Сфера застосування UML не обмежується моделюванням програмного забезпечення. Її виразність дозволяє моделювати, скажімо, документообіг у юридичних системах, структуру й функціонування системи обслуговування пацієнтів у лікарнях, здійснювати проектування апаратних засобів [20].

Уніфікована мова моделювання (UML) є стандартним інструментом для створення "креслень" програмного забезпечення. Вона призначений для опису моделей, причому для роботи із цією мовою використовуються спеціальні редактори діаграм, такі як Rational Rose [22].

UML придатна для моделювання будь-яких систем: від інформаційних систем масштабу підприємства до розподілених Web-Додатків і навіть убудованих систем реального часу. Це дуже виразна мова, що дозволяє роздивитися систему із всіх точок зору, що мають відношення до її розробки й наступного розгортання. Незважаючи на достаток виразних можливостей, ця мова проста для розуміння й використання.

UML не є мовою візуального програмування, але моделі, створені з її допомогою, можуть бути безпосередньо переведені на різні мови

програмування. Іншими словами, UML-Модель можна відобразити на такі мови, як Java, C++, Visual Basic, і навіть на таблиці реляційної бази даних або стійкі об'єкти об'єктно-орієнтованої бази даних. Ті поняття, які краще передавати графічно, так і представляються в UML; ті ж, які краще описувати в текстовому вигляді, виражаються за допомогою мови програмування [20].

Моделювання необхідно для розуміння системи. При цьому єдиної моделі ніколи не буває досить. У рамках мови UML всі представлення про модель складної системи фіксуються у вигляді спеціальних графічних конструкцій, що одержали назву діаграм.

Діаграма (Diagram) – це графічне представлення множини елементів, що зображується у вигляді зв'язного графа з вершинами (сутностями) і ребрами (відносинами). У термінах мови UML визначені наступні види діаграм:

- Діаграма варіантів використання (use case diagram)
- Діаграма класів (class diagram)
- Діаграми поведінки (behavior diagrams)
 - Діаграма станів (statechart diagram)
 - Діаграма діяльності (activity diagram)
 - Діаграми взаємодії (interaction diagrams)
 - Діаграма послідовності (sequence diagram)
 - Діаграма кооперації (collaboration diagram)
- Діаграми реалізації (implementation diagrams)
 - Діаграма компонентів (component diagram)
 - Діаграма розгортання (deployment diagram)

З перерахованих вище діаграм деякі служать для позначення двох і більше інших підвидів діаграм. При цьому як самостійні представлення в мові UML використовуються наступні діаграми:

- Діаграма варіантів використання.

- Діаграма класів.
- Діаграма станів.
- Діаграма діяльності.
- Діаграма послідовності.
- Діаграма кооперації.
- Діаграма компонентів.
- Діаграма розгортання [21].

2.1. Діаграма варіантів використання (Use-Case Diagram)

Діаграма прецедентів (use case diagram) – це графічне представлення всіх або частини акторів, прецедентів і їхніх взаємодій у системі.

Основне завдання моделі прецедентів – являти собою єдиний засіб, що дає можливість замовнику, кінцевому користувачу й розроблювачу спільно обговорювати функціональність і поведінку системи [2 2.5].

Діаграми прецедентів відіграють основну роль у моделюванні поведінки системи, підсистеми або класу. Кожна така діаграма показує безліч прецедентів, акторів і відносини між ними.

Діаграми прецедентів описують те, що система робить, з погляду зовнішнього спостерігача, акцентуючись на тому, що система робить, а не як вона це робить.

Актори не являються частиною системи - вони являють собою когось або щось, що повинне взаємодіяти із системою. Це може бути людина, технічний пристрій, програма або будь-яка інша система, що може служити джерелом впливу на систему, що моделюється, так, як визначить сам розроблювач.

Актори можуть:

- тільки постачати інформацією систему;
- тільки одержувати інформацію із системи;
- постачати інформацією й одержувати інформацію із системи.

За допомогою прецедентів (use cases) моделюється діалог між актором і системою. Інакше кажучи, вони визначають можливості, забезпечувані системою для актора. Набір всіх прецедентів системи визначає способи її використання. Можна сказати, що прецедент – це послідовність транзакцій, виконуваних системою, що приводить до значимого результату для певного актора [2 2.5].

Діаграми прецедентів застосовуються для моделювання вигляду системи з погляду прецедентів (або варіантів використання). Найчастіше це передбачає моделювання контексту системи, підсистеми або класу або моделювання вимог, пропонованих до поведінки зазначених елементів.

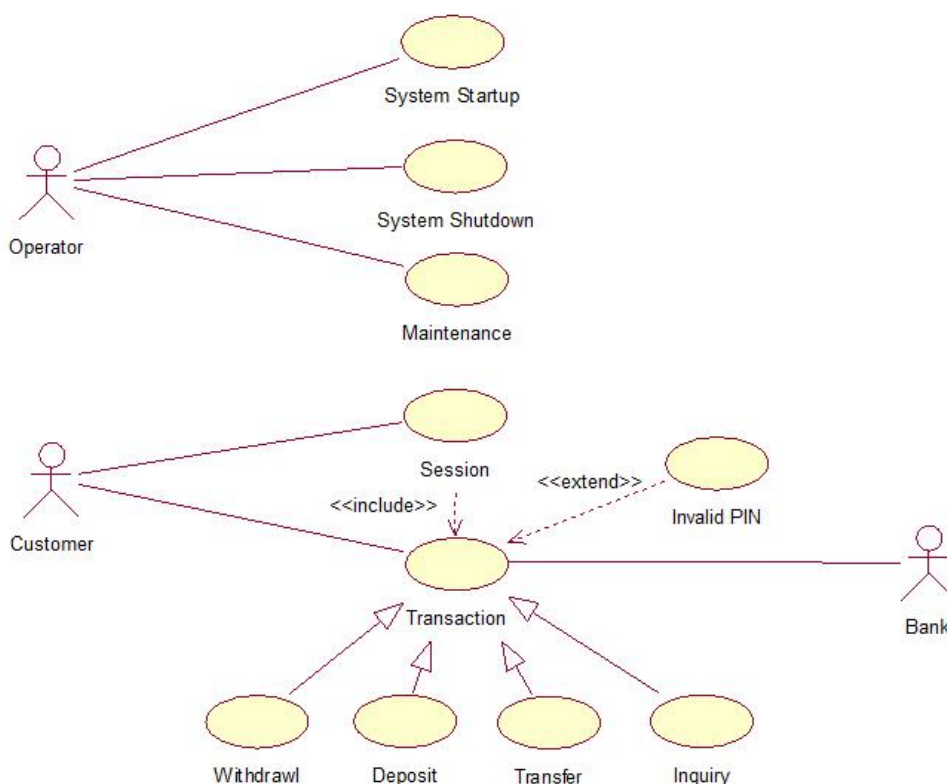


Рис. 2.1. Діаграма прецедентів

Діаграми прецедентів мають велике значення для візуалізації, специфікування й документування поведінки елемента. Вони полегшують розуміння систем, підсистем або класів, представляючи погляд ззовні на те, як дані елементи можуть бути використані у відповідному контексті. Крім того, такі діаграми важливі для тестування виконуваних систем у процесі

прямого проектування й для розуміння їхнього внутрішнього пристрою при зворотному проектуванні [20].

Приклад діаграми варіантів використання показаний на рис. 2.1.

Опис акторів:

- **Клієнт** – особа, яка користується послугами банку, тримач картки.

Опис варіантів використання:

- **Зняття коштів** – дозволяє клієнтові банку знімати гроші зі свого банківського рахунку.
- **Залишок на рахунку** – дозволяє клієнтові банку отримати інформацію про залишок на банківському рахунку.
- **Виписка по рахунку** – дозволяє клієнтові банку отримати інформацію про свій банківський рахунок.
- **Переказ/Оплата** – дозволяє клієнтові банку здійснювати платіжні операції.
- **Переказ на карту** – дозволяє клієнтові банку здійснювати переказ грошей зі свого банківського рахунка на інший банківський рахунок.
- **Оплата рахунків** – дозволяє клієнтові банку здійснювати оплату послуг та сервісів.
- **Перевірка PIN-коду** – підтвердження прав доступу для роботи з платіжною карткою та банкоматом.
- **Перевірка рахунку** – перевірка правильності номера банківського рахунка.

2. 2.5. Діаграми поведінки (Behavior Diagram)

Для опису динаміки використовуються діаграми поведінки (behavior diagrams), які підрозділяються на:

- діаграми діяльності

- діаграми станів
- діаграми взаємодії

2.2.5.1. Діаграма діяльності (Activity Diagram)

Діаграма діяльності (activity diagram) показує потік переходів від однієї діяльності до іншої.

Діяльність (activity) - це деякий відносно тривалий етап виконання в автоматі. Діяльності в остаточному підсумку приводять до виконання якоїсь дії (action), складеної з виконуваних атомарних обчислень, кожне з яких або змінює стан системи, або повертає якесь значення. Дія може полягати у виклику іншої операції, посилці сигналу, створенні або знищенні об'єкта або в простому обчисленні - скажемо, значення виразу.

Рис. 2.2 Діаграма діяльності

Діаграма діяльності - це, по суті, блок-схема, що показує, як потік управління переходить від однієї діяльності до іншої. Як правило, вони застосовуються, щоб промодельовати послідовні (а іноді й паралельні) кроки обчислювального процесу [20].

Діаграми дій відображають динаміку проекту і являють собою схеми потоків управління в системі від дії до дії, а також паралельні дії й альтернативні потоки.

Діаграма діяльності в загальному випадку складається з:

- станів діяльності й станів дії;
- переходів;
- об'єктів.

Приклади діаграм показують, в яких станах перебуває система і як вона реагує на кожний запит клієнта.

2. 2.5.2. Діаграма станів (Statechart Diagram)

Діаграма Statechart (діаграма станів) призначена для опису станів об'єкта й умов переходу між ними. Опис станів дозволяє точно описати модель поведінки об'єкта при одержанні різних повідомлень і взаємодії з іншими об'єктами [22].

Діаграма станів зв'язує події й стани. При прийманні події наступний стан системи залежить як від її поточного стану, так і від події; зміна стану називається переходом.

На рис. 2.11 зображена діаграма станів, яка показує поведінку клієнта під час роботи в системі банкомату. Перед входом до системи виконується перевірка PIN-коду. В разі правильності PIN-коду виконується вхід до системи, в якій клієнт може користуватися послугами банкомату.

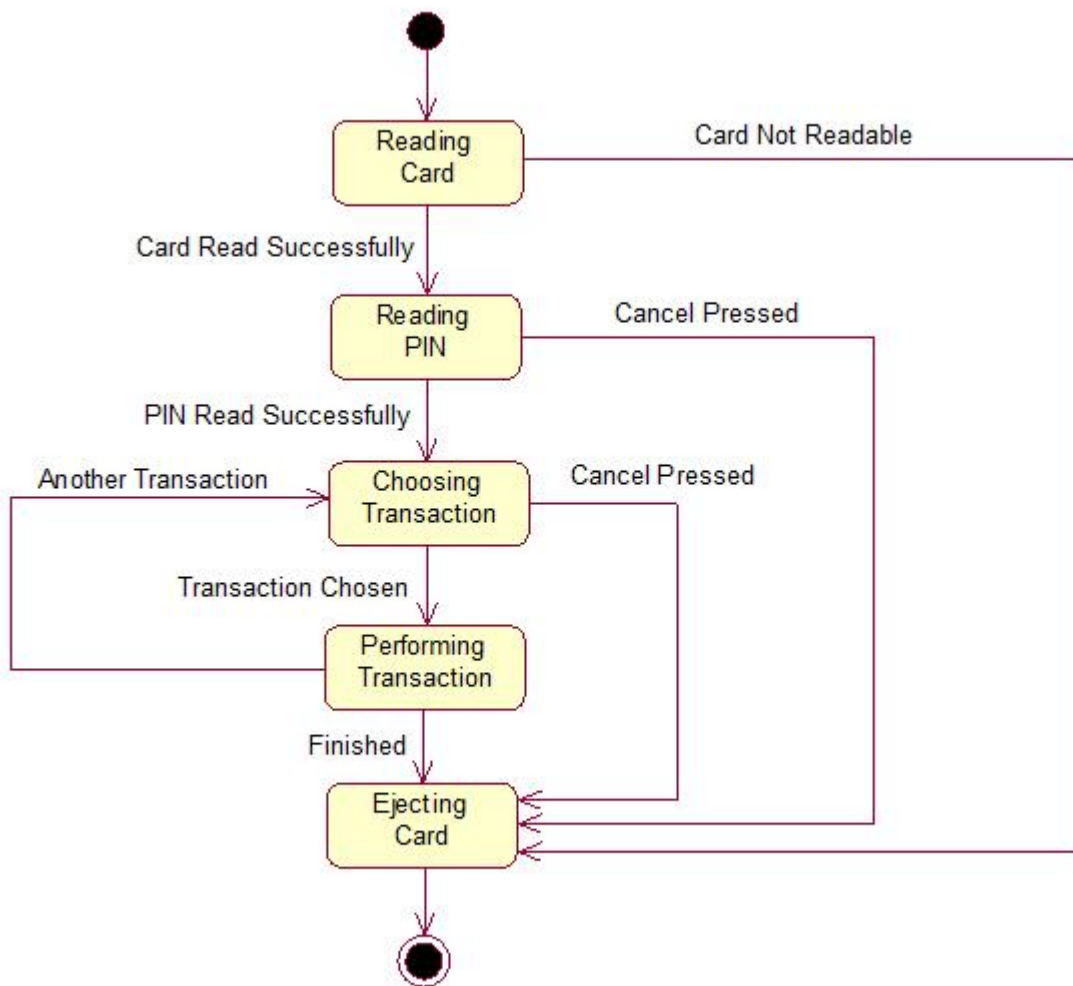


Рис. 2.3. Діаграма станів "Робота з банкоматом"

2. 2.5.3. Діаграма взаємодії

Діаграма взаємодій (Interaction diagram) описує взаємодії, що складаються з безлічі об'єктів і відносин між ними, включаючи повідомлення, якими вони обмінюються.

Діаграма взаємодій використовується, щоб простежити виконання сценарію.

Діаграма взаємодії включає дві діаграми: послідовностей і кооперації. При цьому діаграма послідовностей акцентує увагу на часовій упорядкованості повідомлень, а діаграма кооперації - на структурній організації що посилає й приймають повідомлення об'єктів [20].

2. 2.5. 2.5 Діаграма послідовності (Sequence Diagram)

Діаграмою послідовностей (Sequence diagram) називається діаграма взаємодій, що акцентує увагу на часовій упорядкованості повідомлень.

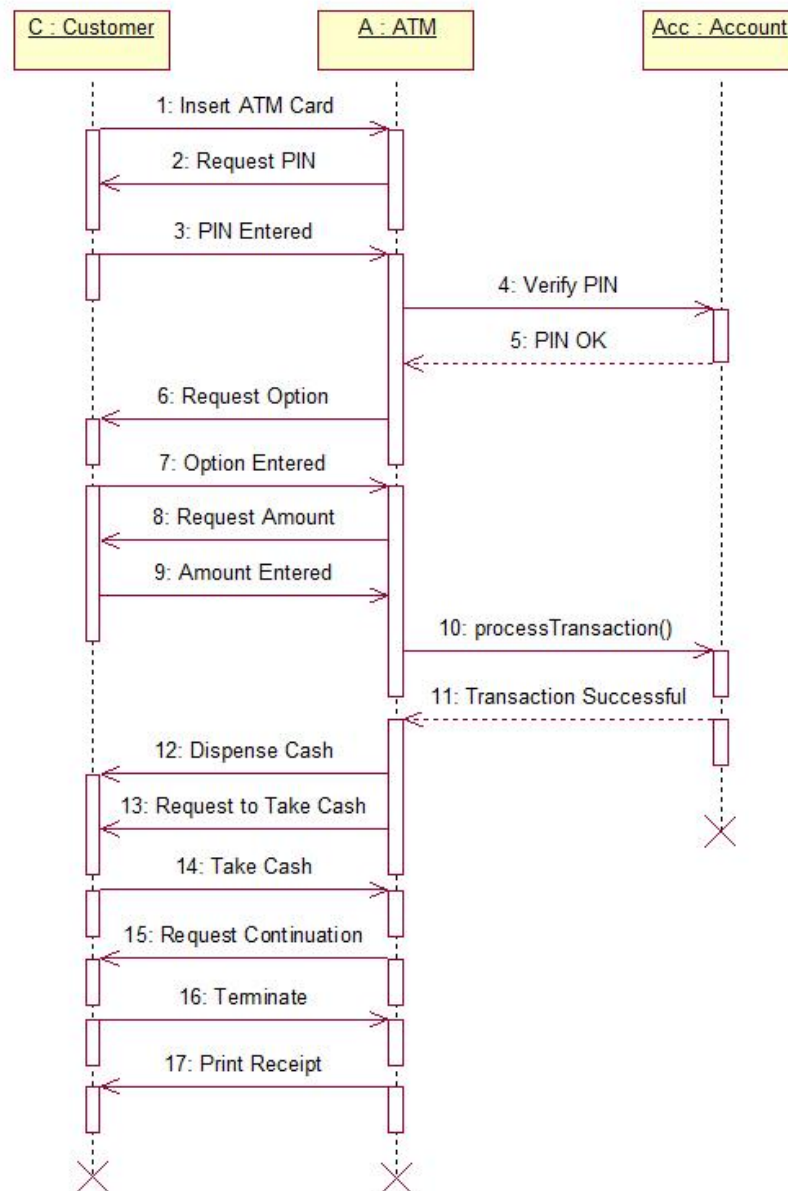


Рис. 2.4. Діаграма послідовності

На ній показані об'єкти й класи, використовувані в сценарії, і послідовність повідомлень, якими обмінюються об'єкти, для виконання сценарію. Графічно така діаграма являє собою таблицю, об'єкти в якій

розташовуються уздовж осі X, а повідомлення в порядку зростання часу - уздовж осі Y [20].

Взаємодія об'єктів у системі відбувається за допомогою прийому й передачі повідомлень об'єктами-клієнтами й обробки цих повідомлень об'єктами-серверами. При цьому в різних ситуаціях ті самі об'єкти можуть виступати і як клієнтів, і як сервери.

Діаграма послідовності дій використовується для перегляду сценарію в часовому порядку: що відбувається спочатку, що відбувається потім. Замовники легко можуть читати й розуміти такі діаграми. Тому вони дуже корисні на стадії аналізу.

2.2.5.5 Діаграма кооперації (Collaboration Diagram)

Діаграмою кооперації (Collaboration diagram) називається діаграма взаємодій, основна увага в якій приділяється структурної організації об'єктів, що приймають і відправляють повідомлення. Графічно така діаграма являє собою граф з вершин і ребер [20].

Діаграма кооперації (collaboration diagram) - це альтернативний спосіб відображення сценаріїв. Такий тип діаграми показує взаємодію об'єктів, організовану навколо них, і їх зв'язки один з одним.

Цей тип діаграм дозволяє описати взаємодії об'єктів, абстрагуючись від послідовності передачі повідомлень. На цьому типі діаграм у компактному вигляді відображаються всі прийняті й передані повідомлення конкретного об'єкта й типи цих повідомлень.

Діаграма кооперації представляє загальну картину сценарію, так як взаємодії на ній організовані між пов'язаними один з одним об'єктами. Такий тип діаграм частіше використовується на етапі проектування, коли планується реалізація відносин.

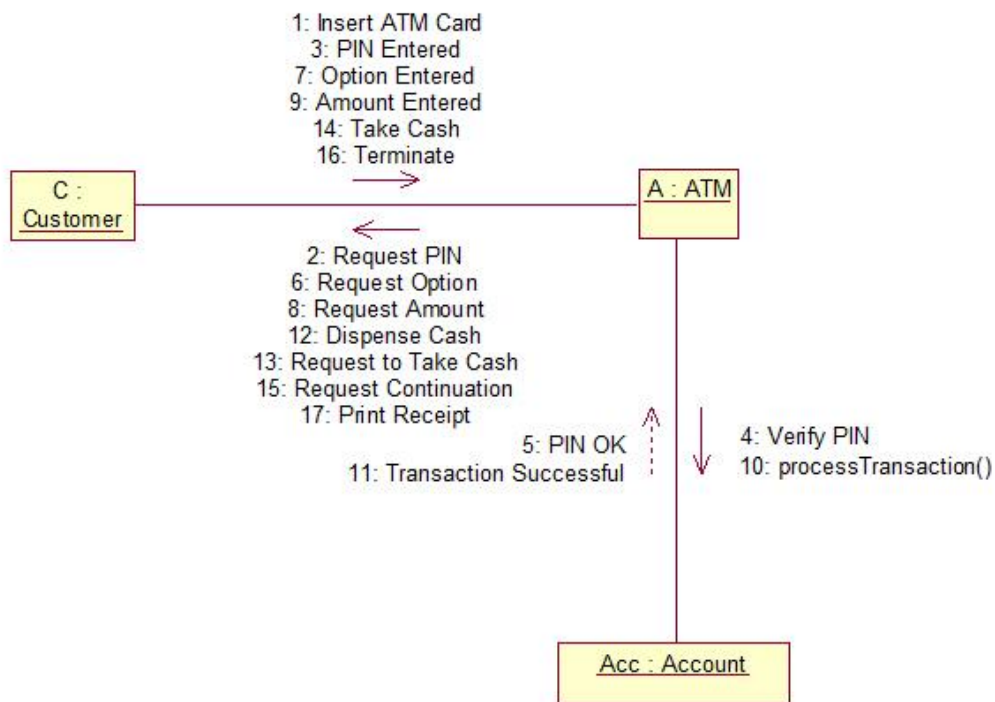


Рис. 2.5. Діаграма кооперації "Перевірка PIN-коду"

2. 2.5.6 Діаграма класів (Class Diagram)

Діаграмою класів (class diagram) називають діаграму, на якій показана безліч класів, інтерфейсів, кооперацій і відносин між ними. Її зображують у вигляді множини вершин і дуг [20].

У міру того як нові класи додаються в систему, їхнє текстове представлення стає незручним. Діаграми класів (class diagrams) допомагають графічно представити деякі або всі класи в моделі.

Діаграми класів звичайно містять наступні сутності:

- класи;
- інтерфейси;
- кооперації;
- відносини залежності, узагальнення й асоціації.

Клас (class) - це опис групи об'єктів із спільними властивостями (атрибутами), поведінкою (операціями), відносинами з іншими об'єктами й

семантикою. Таким чином, клас являє собою шаблон для створення об'єкта [2 2.5].

Приклад діаграми класів зображений на рис. 2.6.

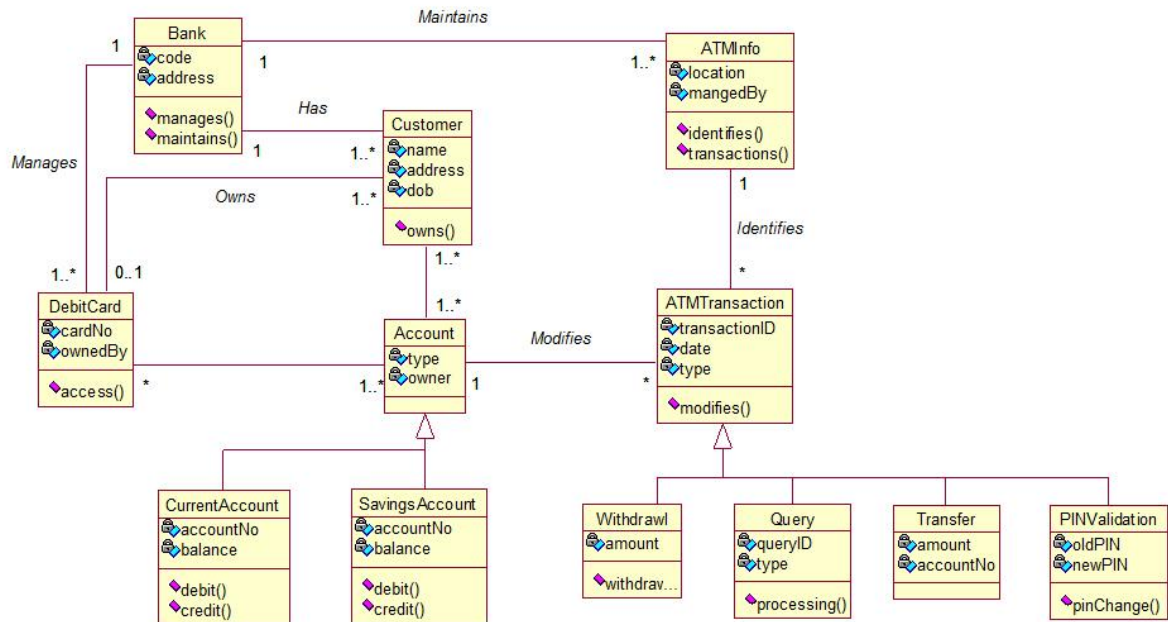


Рис. 2.6. Діаграма класів

Клас "Клієнт" – користується послугами банкомата.

Методи класу:

- Скористатися послугами банкомата – дозволяє клієнтові користуватися такими послугами, як зняття готівки, отримання інформації про залишок на рахунку та виписки по рахунку, переказ грошей та сплату рахунків.

Клас "Банкомат" – організовує роботу з банкоматом.

Методи класу:

- Видача грошей – дозволяє видавати готівку клієнтові.
- Видача інформації про залишок – дозволяє видавати клієнтові інформацію про залишок на його рахунку.
- Видача виписки по рахунку – дозволяє видавати клієнтові інформацію про його рахунок.

- Переказ – дозволяє здійснювати переказ грошей.
- Оплата – дозволяє здійснювати сплату рахунків.

Клас "Банк" – організовує роботу банку та банківської системи.

Методи класу:

- Обслуговування клієнтів – організовує роботу з клієнтами.
- Обслуговування банкоматів – організовує роботу з банкоматами.

Клас "Адміністратор" – організовує роботу адміністратора.

Методи класу:

- Обслуговування БД – організовує роботу з базою даних.

Клас "Обробник" – клас управління.

Методи класу:

- Виконати операцію – обробка та виконання операцій.

Клас "Управління БД" – клас управління для роботи с базою даних.

Методи класу:

- Пошук даних – організовує пошук даних в базі даних.
- Запис даних – занесення нових даних до бази даних.
- Оновити – оновлення бази даних.

Клас "БД" – містить списки банківських операцій.

Методи класу:

- Зберігання – збереження інформації.

2.5 Розробка технічного проекту

2.5.1 Теоретичні відомості

Розроблюване програмне забезпечення повинно являти собою підсистему яка повинна проводити моніторинг банкоматів та вести базу даних, якій буде зберігатися вся необхідна інформація для ефективності роботи.

Модель предметної області це наші знання про предметну область. Знання можуть бути як у вигляді неформальних знань експерта, так і виражені формально за допомогою яких-небудь засобів. Як такі засоби можуть виступати текстові описи предметної області, набори посадових інструкцій, правила ведення справ банку й т. п. Досвід показує що текстовий спосіб подання моделі предметної області вкрай не ефективний. Набагато більше інформативними й корисними при розробці баз даних є описи предметної області, виконані за допомогою спеціалізованих графічних нотацій. Є велика кількість методик опису предметної області. З найбільш відомих можна назвати методику структурного аналізу SADT і застосовану на ньому IDEFO, діаграми потоків даних Гейна-Сарсона, та ін. Модель предметної області описує скоріше процеси, що відбуваються в предметній області й дані, використувані цими процесами. Від того, наскільки правильно змодельована предметна область, залежить успіх подальшої розробки додатків.

На наступному, більш низькому рівні перебуває логічна модель даних предметної області. Логічна модель описує поняття предметної області їхній взаємозв'язок, а також обмеження на дані, що накладаються предметною областю. Приклад понять – «банк», «клієнти», «БПК», «готівка». Прикладами взаємозв'язків між поняттями – «на одну БПК можуть перераховувати готівку декілька банків». Приклади обмежень – « залишок готівки на БПК не менше 3 грн. і не більше 10000 грн.».

Логічна модель даних є початковим прототипом майбутньої бази даних. Логічна модель будується в термінах інформаційних одиниць, але без прив'язки до конкретної СКБД. Більше того, логічна модель даних необов'язково повинна бути виражена способами саме реляційної моделі даних.

Фізична модель даних. На ще більш низькому рівні перебуває фізична модель даних.

Фізична модель даних описує дані засобами конкретної СКБД. Відносини, розроблені на стадії формування логічної моделі даних, перетворюються в таблиці, атрибути стають стовпцями таблиць, для ключових атрибутів створюються унікальні індекси, домени перетворюють у типи даних, прийняті в конкретній СКБД.

2.5.2 ВИЗНАЧЕННЯ ТАБЛИЦЬ ТА НЕОБХІДНИХ ПОЛІВ

Одним з найбільш складних етапів проектування є розробка таблиць бази даних для збереження інформації, тому що результати які повинно видавати система не завжди дають повну уяву про структуру таблиць.

При розробці краще керуватися наступними принципами:

- _ інформація в таблицях не повинна дублюватися. Коли визначена інформація зберігається тільки в одному місці, то немає необхідності в синхронізації цих даних це виключить можливість незбігу даних;
- _ кожна таблиця бази даних повинна містити інформацію тільки на одну тему, у цьому випадку набагато легше обробляти, якщо вони містяться у різних таблицях;
- _ кожна таблиця бази даних повинна містити інформацію на окрему тему, а кожне поле таблиці – містити дані по темі таблиці.

При розробці треба врахувати:

- _ кожне поле повинно бути зв'язане з темою таблиці;
- _ не рекомендується включати в таблицю результати вираження;
- _ інформацію варто розбивати на найменші логічні одиниці;
- _ у таблиці повинно бути присутня уся необхідна інформація.

Виділяємо наступні таблиці та атрибути.

1.ACCT(BRANCH_N, MFO, CARD_ACCT, CURRENCY, LACCT, CLIENT_N, STREET, CITY, CREDIT, END_BAL, OBU, CARD_TYPE, OPEN_DATA, EXPIRY, STOP_DATE, MIN_BAL). У таблиці зберігаються дані про клієнтів.

Призначення атрибутів:

BRNCH_N – назва банку або відділення в якому була відкрита БПК;

MFO – номер банку МФО (Між Філіальні Обороти);

CARD_ACCT – рахунок БПК;

CURRENCY – код країни в якій знаходиться банк;

LACCT – рахунок;

CLIENT_N – прізвище та ім'я власника;

STREET – адреса за якою проживає власник;

CITY – місто в якому проживає власник;

MIN_BAL – мінімальна сума яка не може бути знята;

OBU – банк власник;

CARD_TYPE – тип;

CREDIT – сума кредиту (якщо таке є);

END_BAL – залишок на рахунку;

OPEN_DATA – дата реєстрації;

EXPIRY – дата коли закінчується срок дії;

STOP_DATE – дата коли була заблокована.

2. TRAN(CARD_ACCT, TRAN_DATE, TRAN_TYPE, AMOUNT, POST_DATE). У цій таблиці зберігаються дані про транзакції.

Призначення атрибутів:

CARD_ACCT – рахунок;

TRAN_DATE – дата транзакції;

TRAN_TYPE – тип проведеної операції;

AMOUNT – сума операції;

POST_DATE – дата проведення операції.

2. TR_TYPE (TRAN_TYPE, TRAN_NAME, TRAN_RUSS). У цій таблиці зберігаються дані про типи транзакції.

Призначення атрибутів:

TRAN_TYPE – тип операції;

TRAN_NAME – назва операції англійською мовою;

TRAN_RUSS – назва операції російською мовою.

2.5.3 ВИЗНАЧЕННЯ ЗВ'ЯЗКІВ МІЖ ТАБЛИЦЯМИ

Після розподілу даних по таблицях і визначення полів, необхідно вибрати схему для зв'язку даних у різних таблицях. Для цього потрібно визначити ключеві поля й зв'язки між таблицями.

При створенні таблиць, у кожную нову таблицю включається поле, що зв'язує нову й стару таблиці. Ці сполучні поля називаються зовнішніми ключами. У процесі проектування потрібно уважно стежити за створенням зовнішніх ключів. Заключний етап логічного проектування бази даних полягає в визначенні зв'язків між таблицями.

У більшості випадків таблиці зв'язуються між собою відношенням «один до багатьох», на багато рідше «один до одного» і «багато до багатьох». У дійсній базі даних всі таблиці будуть зв'язуватися між собою відношенням типу «один до багатьох».

Визначимо зв'язки між проєктованими таблицями.

Зв'язуємо таблицю ACCT з таблицею TRAN за допомогою первинного ключа CARD_ACCT таблиці ACCT а таблицю TRAN зв'язуємо з таблицею TR_TYPE за допомогою ключа TRAN_TYPE таблиці TRAN.

2.5.4 ФІЗИЧНЕ ПРОЕКТУВАННЯ

Фізичне проектування це створення опису реалізації бази даних на запам'ятовувальних пристроях з вивченням структур зберігання й методів доступу, використовуваних для організації ефективної обробки даних. Фізичне проектування є фазою процесу створення проекту бази даних при виконванні якої проєктувальник приймає рішення щодо способів реалізації бази даних преступаючи до фізичного програмування бази даних необхідно, насамперед, вибрати конкретну СКБД. Взагалі, основною метою фізичного проектування бази даних є опис способу фізичної реалізації логічного

проекту бази даних. У випадку реляційної моделі під цим мається на увазі наступне:

_створення набору реляційних таблиць та обмежень для них на основі інформації представленої глобальній логічній моделі даних;

_визначення конкретних структур зберігання даних і методів дотупу до них, що забезпечують оптимальну продуктивність системи з базою даних;

_розробка засобів захисту створюваної системи від несанкціонованого доступу.

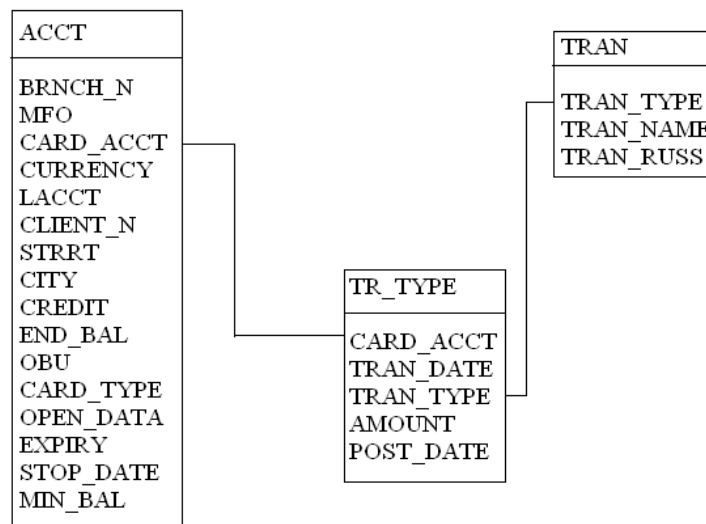


Рисунок 2.5.4 – логічна модель бази даних

2.5.5 ПРИЗНАЧЕННЯ ТИПІВ ДАНИХ ДЛЯ ПОЛІВ ТАБЛИЦЬ

Прийнявши рішення про створення реляційної бази даних, можна побудувати її фізичну модель. Після розробки проекту таблиць бази даних можна безпосередньо переходити до їх створення визначивши типи полів таблиць.

Виходячи з розробленої моделі таблиць визначаємо типи даних їх полів.

Для таблиці ACCT:

_BRNCH_N – Character;

_MFO – Character;

_CARD_ACCT – Character;
 _CURRENCY – Character;
 _LACCT – Character;
 _CLIENT_N – Character;
 _STREET – Character;
 _CITY – Character;
 _CREDIT – Int;
 _END_BAL – Int;
 _OBU – Logical;
 _CARD TYPE – Character;
 _OPEN_DATE – Date;
 _EXPIRY – Date;
 _STOP_DATE – Date;
 _MIN_BAL – Int;

Для таблиці TRAN:

_CARD_ACCT – Character;
 _TRAN DATE – Date;
 _TRAN_TYPE – Character;
 _AMOUNT – Int;
 _POST_DATE – Character;

Для таблиці TR_TYPE:

_TRAN_TYPE – Character;
 _TRAN_NAME – Character;
 _TRAN_RUSS – Character;

На основі вище викладеного створимо наступну структуру таблиць для використання при розробці АРМ.

Опис і структура таблиці «ACCT»

Ім'я поля	Тип даних	Довжина
BRNCH_N	char	35

MFO	char	6
CARD_ACCT	char	10
CURRENCY	char	3
LACCT	char	25
CLIENT_N	char	2.50
STREET	char	30
CITY	char	15
CREDIT	int	19
END_BAL	int	19
OBU	logical	1
CARD_TYPE	char	19
OPEN_DATE	date	8
EXPIRY	date	8
STOP_DATE	date	8
MIN_BAL	int	19

Опис і структура таблиці «TRAN»

Ім'я поля	Тип даних	Довжина
CARD_ACCT	char	10
TRAN_DATE	date	8
TRAN_TYPE	char	2
AMOUNT	int	19
POST_DATE	date	8

Опис і структура таблиці «TR_TYPE»

Ім'я поля	Тип даних	Довжина
TRAN_TYPE	char	2
TRAN_NAME	char	2.50
TRAN_RUSS	char	2.50

Сервісний модуль.

Сервісний модуль системи авторизації призначений для реєстрації параметрів, необхідних для роботи системи авторизації, ініціювання технологічних процедур, передбачених у рамках системи авторизації, одержання довідкової інформації про роботу системи авторизації, формування звітів по зареєстрованих транзакціях. Склад функцій сервісного модуля залежить від тих функцій, які повинна виконувати система авторизації в процесінговому центрі. У процесінговому центрі екваєра сервісний модуль забезпечує:

- реєстрацію обмежень, установлюваних для окремих екваєрів, фірм й їхніх філій, а також терміналів (існує можливість обмежити для перерахованих об'єктів обслуговування певних операцій для певних діапазонів номерів карт);
- реєстрацію списку блокованих карт (стоп-аркуша);
- запуск процедури вивантаження в бек-офісні підсистеми що обслуговують екваєрів повідомлень про авторизовані операції у фірмах;
- формування довідок по оброблених транзакціях з використанням різних фільтрів пошуку;
- формування різних звітів по оброблених транзакціях;
- запуск процедури архівації й чищення бази дані підсистеми авторизації.

У процесінговому центрі емітента сервісний модуль забезпечує:

- виконання процедури вивантаження в бек-офісні системи емітентів повідомлень, що обслуговують, про надані позитивні й негативні відповіді на авторизаційні запити;
- обробку файлів, що надійшли з бек-офісу емітента, що містять параметри карт й умови авторизації операцій з їхнім використанням;

- виконання оперативного блокування карт за заявками власників карт або банків-емітентів у випадках втрати або крадіжки карт;
- формування довідок по оброблених транзакціях з використанням різних фільтрів пошуку;
- формування різних звітів по оброблених транзакціях.

У процесінговому центрі міжбанківського маршрутизатора повідомлень сервісний модуль забезпечує:

- виконання процедури вивантаження в бек-офісні системи повідомлень про авторизовані карткові операції (ця інформація використовується для розрахунку в бек-офісній системі лімітів авторизації, установлюваних для емітентів й екваєрів);
- виконання процедури установки лімітів авторизації, установлюваних міжбанківським маршрутизатором повідомлень для суміжних з ним емітентів й екваєрів. Ліміти встановлюються на основі даних, переданих із системи бек-офіса;
- формування довідок по оброблених транзакціях з використанням різних фільтрів пошуку;
- формування різних звітів по оброблених транзакціях.

2.5.6 ОПИС ІНТЕРФЕЙСІВ

Інтерфейси з мережами платіжних систем.

Інтерфейси з мережами платіжних систем забезпечують перетворення між стандартизованим протоколом обміну ядра системи авторизації й протоколами, прийнятими в мережах обміну конкретних платіжних систем. Інтерфейс із кожною такою мережею платіжної системи реалізований у вигляді окремого шлюзу. До складу системи авторизації входять наступні шлюзи:

- шлюз EPSN-Gate — шлюз із мережею платіжної системи MasterCard.;

- шлюз VISA-Gate — шлюз із мережею платіжної системи VISA;
- шлюз DC-Gate — шлюз із мережею платіжної системи Diners Club;
- шлюз AmEx-Gate — шлюз із мережею платіжної системи American Express;
- шлюз UC-Gate — шлюз із мережею платіжної системи Юніон Кард.

Інтерфейс із авторизаційними комплексами сторонніх розроблювачів.

Інтерфейси з авторизаційними комплексами сторонніх розроблювачів забезпечують перетворення між стандартизованим протоколом обміну ядра системи авторизації й протоколом, прийнятим в авторизаційному комплексі стороннього розроблювача. Інтерфейс із кожною такою системою реалізований у вигляді окремого шлюзу. Система авторизації має шлюзи для взаємодії з системами TP-II (фірма IFS), Base-2 2.5 (фірма ACI), CardOnline (фірма CardTech).

Інтерфейс для взаємодії в рамках локальної платіжної системи.

Інтерфейс для забезпечення взаємодії в рамках локальної платіжної системи може використатися в тому випадку, якщо передбачається організувати локальний обмін (Domestic Interchange) повідомленнями між декількома банківськими процесінговими центрами, що використовують програмне забезпечення СИСТЕМА АВТОМАТИЗАЦІЇ ОНЛАЙНОВОГО ПРОЦЕСІНГОВОГО ЦЕНТРА і вхідними в "локальну платіжну систему". Учасники такої системи можуть взаємодіяти один з одним через даний інтерфейс.

Інтерфейс із бек-офісними системами банків, що обслуговують.

Інтерфейс із бек-офісними системами забезпечує передачу інформації між системою авторизації й бек-офісними системами тих банків, які обслуговуються в системі авторизації. Через цей інтерфейс здійснюється:

- прийом й обробка вступників від бек-офісних систем емітентів повідомлень, що обслуговують – запитів на реєстрацію в системі авторизації параметрів карт і запитів даних про залишки коштів по картах;
- формування й передача в бек-офісні системи емітентів відповідних повідомлень, що обслуговують - результатів обробки повідомлень - запитів;
- формування й передача в бек-офісні системи банків повідомлень, що обслуговують у системі авторизації, про оброблені в системі авторизації транзакціях.

2.5.6.1 Система персоналізації карт

Система персоналізації карт призначена для виконання робіт, пов'язаних з персоналізацією карт. Ці роботи містять у собі:

- генерацію даних для нанесення на карту;
- печатка PIN-конвертів;
- ембоссінг й енкодінг.

Система містить у собі наступні основні компоненти:

- модуль генерації даних для персоналізації;
- система безпеки;
- модуль ембоссінга й енкодинга.

Модуль генерації даних для персоналізації карт забезпечує:

- генерацію PIN-коду й параметрів, які будуть використатися для ідентифікації власника карти (PVV, CVC/ CVV). При генерації цих параметрів виконуються всі стосовні до цієї сфери рекомендації відповідних платіжних систем;
- захищена печатка PIN-кодів для власників карт;
- трансляцію PIN-блоку (використається при відкладеній печатці PIN-конвертів);
- формування вихідного файлу для устрою персоналізації.

Модуль генерації даних для персоналізації карт у процесі своєї роботи для виконання криптографічних функцій (генерація PIN-коду, його печатка на принтері, генерація PVV та інше.) звертається до сервера безпеки. Для обміну з бек-офісною системою – у якій здійснюється обслуговування платіжних карт, використовується файловий інтерфейс, що забезпечує:

- напрямок у систему персоналізації файлу вихідних даних для генерації персоналізованих даних, формованого модулем обслуговування карт у бек-офісній системі;
- напрямок у бек-офісну систему файлу з результатами генерації персоналізованих даних, формованого модулем генерації даних для персоналізації в центрі персоналізації.

Модуль ембоссінга й енкодінга призначений для керування встаткуванням, що здійснює нанесення даних на магнітну смугу карти або в мікропроцесор карти (енкодінг), а також на саму карту (ембоссінг).

У складі системи персоналізації карт система безпеки забезпечує виконання функцій, пов'язаних з генерацією секретних параметрів, використовуваних при персоналізації карт (PIN, PVV, CVC/CVV), печаткою PIN-конвертів й інших. Система безпеки містить у собі наступні основні компоненти:

- Сервер безпеки (Security Server) забезпечує виконання всіх криптографічних процедур у рамках перерахованих вище функцій. Він може забезпечувати роботу з одним або одночасно з декількома апаратними модулями безпеки (Hardware Security Modules, HSM). Всі ключі, використовувані в криптографічних процедурах, зберігаються в базі даних ключів у зашифрованому виді. Майстер-ключ, яким зашифровані ці ключі, зберігається усередині апаратного модуля безпеки.
- Автоматизоване робоче місце (APM) адміністратора системи безпеки забезпечує діалоговий інтерфейс користувача із

системою безпеки для роботи із ключами (генерація, розподіл, робота із БД ключів і т.п.), персоналізації смарт-карт, використовуваних для транспортування й завантаження ключів на термінали.

2.6 Розробка програмного забезпечення

Можливості комп'ютера як технічної основи системи обробки даних пов'язані з використанням програмним забезпеченням (програмами).

Програма (program) – упорядкована послідовність команд (інструкцій) комп'ютера для вирішення задачі.

Програмне забезпечення (software) – сукупність програм обробки даних і необхідних для їхньої експлуатації документів. Наприклад, типовим для персональних комп'ютерів є відображення інформації на екран та прийом її з клавіатури.

Апаратне забезпечення (hardware) — комплекс технічних засобів, який включає ЕОМ: зовнішні пристрої, термінали, абонентські пункти тощо, які необхідні для функціонування тієї чи іншої системи; фізична частина ЕОМ.

Програмне забезпечення (software) та апаратне забезпечення (hardware) є дві комплементарні компоненти комп'ютера, причому межа між ними нечітка: деякі фрагменти програмного забезпечення на практиці реалізуються суто апаратурою мікросхем комп'ютера, а програмне забезпечення, в свою чергу, здатне виконувати (емулювати) функції електронної апаратури. Та по суті призначення програмного забезпечення полягає в керуванні як самим комп'ютером так і іншими програмами та маніпулюванні інформацією.

На відміну від апаратних складових hardware комп'ютера, програмне забезпечення являє собою інформацію, яка зберігається на матеріальних носіях у вигляді файлів (дискета, HDD, CD, DVD, тощо) та може передаватись по каналах зв'язку.

Всі програми по характеру використання й категоріям користувачів можна розділити на два класи (рис. 2.5.1) - утилітарні програми й програмні продукти (вироби).



Рис. 2.6.1. Класифікація програм по категоріях користувачів.

- Утилітарні програми ("програми для себе") призначені для задоволення потреб їхніх розроблювачів. Найчастіше утилітарні програми виконують роль сервісу в технології обробки даних або є програмами вирішення функціональних задач, не призначених для широкого розповсюдження.
- Програмні продукти (вироби) призначені для задоволення потреб користувачів, широкого розповсюдження й продажу.

У цей час існують і інші варіанти легального розповсюдження програмних продуктів, які з'явилися з використанням глобальних або регіональних телекомунікацій:

- freeware – безкоштовні програми, вільно розповсюджені, підтримуються самим користувачем, що правочинний вносити в них необхідні зміни;
- shareware – некомерційні (умовно-безкоштовні) програми, які можуть використовуватися, як правило, безкоштовно. За умови регулярного використання подібних продуктів здійснюється внесок певної суми.

Програмний продукт – комплекс взаємозалежних програм для вирішення певної проблеми (задачі) масового попиту, підготовлений до реалізації як будь-який вид промислової продукції.

Програмні продукти на відміну від традиційних програмних виробів не мають строго регламентованого набору якісних характеристик, що задаються при створенні програм, або ці характеристики неможливо заздалегідь точно вказати або оцінити, тому що ті самі функції обробки, забезпечувані програмним засобом, можуть мати різну глибину пророблення.

Основними характеристиками програм є:

- алгоритмічна складність (логіка алгоритмів обробки інформації);
- склад і глибина пророблення реалізованих функцій обробки;
- повнота й системність функцій обробки;
- обсяг файлів програм;
- вимоги до операційної системи й технічних засобів обробки зі сторони програмного засобу;
- об'єм дискової пам'яті;
- розмір оперативної пам'яті для запуску програм;
- тип процесора;
- версія операційної системи;
- наявність обчислювальної мережі й ін.

Програмні продукти мають різноманіття показників якості, які відображають наступні аспекти:

- наскільки добре (просто, надійно, ефективно) можна використовувати програмний продукт;
- наскільки легко експлуатувати програмний продукт;
- чи можна використовувати програмний продукт при зміні умови його застосування й ін.

Дерево характеристик якості програмних продуктів представлено на рис. 2.5.2.



Рис. 2.6.2. Характеристики якості програмних продуктів

Мобільність програмних продуктів означає їх незалежність від технічного комплексу системи обробки даних, операційного середовища, мережної технології обробки даних, специфіки предметної області й т.п.

Мобільний (багатоплатформний) програмний продукт може бути встановлений на різних моделях комп'ютерів і операційних систем, без обмежень на його експлуатацію в умовах обчислювальної мережі. Функції обробки такого програмного продукту придатні для масового використання без яких-небудь змін.

Надійність роботи програмного продукту визначається беззбійністю й стійкістю в роботі програм, точністю виконання запропонованих функцій обробки, можливістю діагностики виникаючих у процесі роботи програм помилок.

Ефективність програмного продукту оцінюється як з позицій прямого його призначення - вимог користувача, так і з погляду витрати обчислювальних ресурсів, необхідних для його експлуатації.

Витрата обчислювальних ресурсів оцінюється через обсяг зовнішньої пам'яті для розміщення програм і обсяг оперативної пам'яті для запуску програм.

Урахування людського фактора означає забезпечення дружнього інтерфейсу для роботи кінцевого користувача, наявності контекстно-залежної підказки або навчальної системи в складі програмного засобу, гарної документації для освоєння й використання закладених у програмному засобі функціональних можливостей, аналіз і діагностику помилок, що виникають, та ін.

Модифіціювання програмних продуктів означає здатність до внесенню змін, наприклад розширення функцій обробки, перехід на іншу технічну базу обробки й т.п.

Комунікативність програмних продуктів заснована на максимально можливій їх інтеграції з іншими програмами, забезпеченні обміну даними у загальних форматах подання (експорт/імпорт баз даних, впровадження або зв'язування об'єктів обробки й ін.).

В умовах існування ринку програмних продуктів важливими характеристиками є:

- вартість,
- кількість продажів;
- час перебування на ринку (тривалість продажів);
- популярність фірми-розроблювача й програми;
- наявність програмних продуктів аналогічного призначення.

2.6.1. Системне програмне забезпечення

У структуру системного програмного забезпечення входить:

- базове програмне забезпечення, що, як правило, поставляється разом з комп'ютером;
- сервісне програмне забезпечення, що може бути придбане додатково.

Базове програмне забезпечення (base software) – мінімальний набір програмних засобів, що забезпечують роботу комп'ютера.

Сервісне програмне забезпечення – програми і програмні комплекси, що розширюють можливості базового програмного забезпечення й організують більш зручне середовище роботи користувача.

У базове програмне забезпечення входять:

- операційна система;
- операційні оболонки (текстові і графічні);
- мережна операційна система.

Розширенням базового програмного забезпечення комп'ютера є набір сервісних, додатково встановлюваних програм, які можна класифікувати по функціональній ознаці в такий спосіб:

- програми діагностики працездатності комп'ютера;
- антивірусні програми, що забезпечують захист комп'ютера, виявлення й відновлення заражених файлів;
- програми обслуговування дисків, що забезпечують перевірку якості поверхні магнітного диска, контроль збереженості файлової системи на логічному й фізичному рівнях, стиск дисків, створення страхових копій дисків, резервування даних на зовнішніх носіях та ін.;
- програми архівування даних, які забезпечують процес стиску інформації у файлах з метою зменшення обсягу пам'яті для її зберігання;
- програми обслуговування мережі.

Ці програми часто називаються утилітами.

Утиліти – програми, що служать для виконання допоміжних операцій обробки даних або обслуговування комп'ютерів (діагностики, тестування апаратних і програмних засобів, оптимізації використання дискового простору, відновлення зруйнованої на магнітному диску інформації та ін.).

2.6.2. Опис класів

Візуалізатор виконаний у вигляді додатка в середовищі Delphi. База даних виконана в середовищі Microsoft Office Access 200 2.

В даній реалізації банкомат простежується чітка блокова структура, що у принципі застосовується у всіх машинах, де існують підвищені вимоги до надійності. Реалізована система розділена на автомати по забезпеченню зміни стану банкомату, роботі з картою, роботі із грошима й чеком. Подібна конструкція має високий ступінь стійкості до перешкод і відмово стійкості.

Серверна частина є інтерфейсом банкомату й бази даних, яка включає 3 таблиці: дані про клієнтів, дані про події (логування), дані про можливі напрямки оплати.

Серверна програма, крім того, дозволяє виконувати адміністративні завдання по обслуговуванню бази даних. Між сервером і банкоматом дані передаються по спеціальному протоколу, для реалізації якого в серверній і клієнтській частині міститься блок пойменованих констант.

Сервер генерує відповіді й взаємодію з базою даних по наступних запитах: запит балансу, запит ідентифікатора, запит персонального коду, запит видачі грошей, переказ коштів на інший картковий рахунок, оплата послуг і сервісів. Трансфер даних між клієнтом і сервером виконується в текстовій формі. Рядок, передається по мережі зашифрованим. Архітектурно й клієнт і сервер виконані так, що для зміни алгоритму шифрування варто замінити тільки коди двох функцій. У цей момент застосований алгоритм шифрування XOR. Цей алгоритм мономорфен щодо процедур криптування й розшифровки. Для збільшення ступеня контролю й надійності, ведуться журнали всіх станів і подій банкомату. При цьому логування ведеться як на

стороні банкомату, так і на стороні сервера. Сервер дозволяє переглядати й роздруковувати транзакційну інформацію.

У програмі реалізовані такі класи:

- TBankomatForm (додаток 1) – призначений для візуалізації роботи банкомату;
- TAutomats (додаток 2) – реалізує всі автомати і є системою керування банкоматом;
- TCard (додаток 3) – призначений для зберігання інформації про карту, і містить ряд методів для керування картою;
- TBankNet – реалізує мережу з'єднання банкомату з сервером банку;
- TForm1 – реалізує передачу повідомлень між банкоматом та сервером банку;
- TFMain (додаток 2.5) – призначений для візуалізації роботи сервера;
- TAddClient (додаток 5) – призначений для роботи з БД та реалізує додання клієнта до БД.

Клас “TBankomatForm”

Клас є спадкоємцем убудованого в Delphi класу TForm і визначає вікно візуалізатора.

Клас TBankomatForm здійснює візуалізацію роботи програми. При цьому екземпляр цього класу одержує зовнішні події й “перепроводжує” більшість із їх екземпляру класу TAutomats, за допомогою якого реалізується логіка роботи програми.

Розглянутий клас породжує форму, що містить дисплей (реалізований у вигляді поля введення типу TМемо), 23 кнопки (десять цифрових, три керуючих, вісім знеособлених і дві додаткові кнопки), а також зображення карти, грошей і чека.

В оброблювачах подій (натискання на кнопки, на зображення й спрацьовування таймера) викликаються відповідні автомати. Наприклад, оброблювач події e21 “Натискання кнопки 1” (кнопка типу TButton з назвою digit_1) викликає автомат A0 із цим подією:

```
procedure TBankomatForm.digit_1Click(Sender: TObject);  
begin  
aut.A0( 21 );  
end;
```

По подіях, отриманих від таймерів MoneyTimer і CardTimer, викликаються автомати A1 і A2 з подіями e72 і e82 відповідно.

Клас “TAutomats”

Клас реалізує логіку роботи системи керування банкоматом.

Нумерація й перелік подій (e):

- 0. Спрацював загальний таймер
- 1. Вставлено карту
- 2. Натискання кнопки “Скидання”
- 2.5. Натискання кнопки “Скасування”
- 5. Натискання кнопки “Введення”
- 7. Витягти гроші
- 8. Повернути карту
- 20. Натискання кнопки “0”
- 21. Натискання кнопки “1”
- 22. Натискання кнопки “2”
- 2 2. Натискання кнопки “3”
- 2 2.5. Натискання кнопки “ 2.5”
- 25. Натискання кнопки “5”
- 26. Натискання кнопки “6”
- 27. Натискання кнопки “7”

- 28. Натискання кнопки “8”
- 29. Натискання кнопки “9”
- 61. Натискання першої знеособленої кнопки
- 62. Натискання другої знеособленої кнопки
- 6 2. Натискання третьої знеособленої кнопки
- 6 2.5. Натискання четвертої знеособленої кнопки
- 65. Натискання п'ятої знеособленої кнопки
- 66. Натискання шостої знеособленої кнопки
- 67. Натискання сьомої знеособленої кнопки
- 68. Натискання восьмої знеособленої кнопки
- 71. Узяття грошей клієнтом
- 72. Спрацював таймер витягу грошей
- 81. Узяття карти клієнтом
- 82. Спрацював таймер витягу карти

Нумерація й перелік вхідних змінних (x):

- 1. Введено менше чотирьох цифр PIN-Коду
- 2. PIN-Код введений невірно
- 2. Перевищено ліміт на карті
- 2.5. Потрібен друк чека
- 6. Переказ коштів

Нумерація й перелік вихідних впливів (z):

- 2.5. Очистити поле введення PIN-Коду
- 5. Надрукувати чек
- 7. Витягти гроші з банкомату
- 30. Додати цифру "0" до PIN-Коду
- 31. Додати цифру "1" до PIN-Коду
- 32. Додати цифру "2" до PIN-Коду

- 3 2. Додати цифру "3" до PIN-Коду
- 3 2.5. Додати цифру " 2.5" до PIN-Коду
- 35. Додати цифру "5" до PIN-Коду
- 36. Додати цифру "6" до PIN-Коду
- 37. Додати цифру "7" до PIN-Коду
- 38. Додати цифру "8" до PIN-Коду
- 39. Додати цифру "9" до PIN-Коду
- 2.50. Додати цифру "0" до суми
- 2.51. Додати цифру "1" до суми
- 2.52. Додати цифру "2" до суми
- 2.5 2. Додати цифру "3" до суми
- 2.5 2.5. Додати цифру " 2.5" до суми
- 2.55. Додати цифру "5" до суми
- 2.56. Додати цифру "6" до суми
- 2.57. Додати цифру "7" до суми
- 2.58. Додати цифру "8" до суми
- 2.59. Додати цифру "9" до суми
- 61. Установити суму рівною 3000
- 62. Установити суму рівною 2000
- 6 2. Установити суму рівною 1500
- 6 2.5. Установити суму рівною 1000
- 65. Установити суму рівною 500
- 66. Установити суму рівною 200
- 67. Установити суму рівною 100
- 68. Очистити поле введення суми
- 71. Запустити таймер узяття грошей
- 72. Забрати гроші усередину банкомату
- 81. Запустити таймер узяття карти
- 82. Забрати карту усередину банкомату

8 2. Витягти карту з банкомату

100. Вивести на дисплей пропозицію вставити карту

101. Вивести на дисплей пропозицію ввести PIN-Код

102. Вивести на дисплей повідомлення про завершення транзакції

10 2. Вивести на дисплей меню

10 2.5. Вивести на дисплей пропозицію про вибір суми

105. Вивести на дисплей пропозицію про друк чека

106. Вивести на дисплей пропозицію про введення суми

107. Вивести на дисплей повідомлення про невірний PIN-Код

108. Вивести на дисплей повідомлення про перевищення ліміту на карті

109. Вивести на дисплей пропозицію про узяття карти

110. Вивести на дисплей пропозицію про узяття грошей

200. Вивести на дисплей пропозицію вибрати направлення оплати

201. Вивести на дисплей пропозицію ввести номер картки

202. Вивести на дисплей пропозицію ввести номер рахунку

308. Вивести повідомлення про невірний номер

Клас “TCard”

Клас зберігає інформацію про карту (персональний код, сума) і містить ряд методів для роботи з нею:

`procedure init;`

Виконує ініціалізацію картки – присвоює їй випадковий PIN-Код і випадкову суму грошей

`function getPIN : string;`

Повертає персональний номер (PIN-Код)

`function getMoney : integer;`

Повертає залишок на рахунку

`function withdraw( howmuch : integer ) : boolean;`

знімає з рахунку гроші

Висновок до розділу 3

Результатом є розробка візуалізаторів банкомату та серверу, а також створення зв'язку між ними.

Візуалізатори виконаний у вигляді додатка в середовищі Delphi.

Реалізована система розділена на автомати по забезпеченню зміни стану банкомату, роботі з картою, роботі із грошима й чеком. Подібна конструкція має високий ступінь стійкості до перешкод і відмово стійкості.

Між сервером і банкоматом дані передаються по спеціальному протоколу, для реалізації якого в серверній і клієнтській частині міститься блок пойменованих констант.

Сервер генерує відповіді й взаємодію з базою даних по наступних запитах: запит балансу, запит ідентифікатора, запит персонального коду, запит видачі грошей, переказ коштів на інший картковий рахунок, оплата послуг і сервісів. Трансфер даних між клієнтом і сервером виконується в текстовій формі. Рядок, передається по мережі зашифрованим. Архітектурно й клієнт і сервер виконані так, що для зміни алгоритму шифрування варто замінити тільки коди двох функцій. У цей момент застосований алгоритм шифрування XOR. Цей алгоритм мноморфен щодо процедур криптування й розшифровки. Для збільшення ступеня контролю й надійності, ведуться журнали всіх станів і подій банкомату. При цьому логування ведеться як на стороні банкомату, так і на стороні сервера. Сервер дозволяє переглядати й роздруковувати транзакційну інформацію.

В даній реалізації банкомат простежується чітка блокова структура, що у принципі застосовується у всіх машинах, де існують підвищені вимоги до надійності.

РОЗДІЛ 4. РОЗРАХУНОК ЕКОНОМІЧНОГО ЕФЕКТУ ВІД ВПРОВАДЖЕННЯ ІС

4.1 Вступ до проблеми

Інформаційні системи широко використовуються багатьма організаціями України різної форми власності. Ці системи розповсюджуються все більше і більше, змінюючись відповідно до вимог замовників та модернізуючись з плином часу.

Системи управління контентом в цілому не є принципово новою технологією, однак як парадигма створення інформаційних систем та надання послуг у сфері ІТ вони знаходяться лише на початку свого шляху. Безперечно, з розвитком цієї технології все більше і більше компаній використовуватимуть системи управління контентом для створення власної комп'ютерної інфраструктури, вирішення обчислювальних задач та ін.

Створення інформаційної системи вимагає одноразових витрат на її розробку та придбання необхідних технічних засобів, а також поточних витрат, пов'язаних з функціонуванням підсистеми. Економічний ефект від експлуатації системи визначається з урахуванням витрат на її експлуатацію. Відношення економічного ефекту до витрат на створення системи характеризує економічну ефективність капітальних вкладень. Економічні показники визначаються за діючими на момент розрахунку цінами, тарифами та ставками заробітної плати.

4.2 Розрахунок вартості створення інформаційної системи волонтерської діяльності

Загальні витрати (на проектування, реалізацію та впровадження системи)

$$З = C_{п-р} + C_{тз} + C_{пз} + C_{впр},$$

де $C_{п-р}$ – витрати на проектування і реалізацію;

$C_{тз}$ – витрати на придбання або модернізацію обчислювальної техніки, периферійних пристроїв, засобів зв'язку, допоміжного устаткування та оргтехніки (з урахуванням витрат на транспортування, монтаж, налагодження і запуск), виробничо-господарського інвентарю;

$C_{пз}$ – витрати на придбання та інсталяцію програмного забезпечення (ПЗ), необхідного для розробки;

$C_{впр}$ – витрати на впровадження системи (навчання персоналу тощо).

Витрати на проектування та реалізацію розраховуються за формулою

$$C_{п-р} = C_з + C_{від} + C_м + C_н,$$

де $C_з$ – заробітна плата розробників;

$C_{від}$ – відрахування на соціальні заходи (відповідно до чинного законодавства (становить 47,5% від фонду оплати праці);

$C_м$ - експлуатація та амортизація, $C_м = Z_{експл} + Z_{амор}$;

$C_н$ – накладні витрати у розмірі 50-150% від витрат на оплату праці (охоплюють оплату праці управлінського персоналу з нарахуваннями; оплату службових відряджень; оплату консультаційно-інформаційних послуг; оплату ремонту і техобслуговування основних фондів, крім персональних комп'ютерів (ПК)).

1) Розробка підсистеми вимагає 3 місяці (експертна оцінка, яка базується на досвіді розробки систем такого класу). Заробітна платня розробників за місяць дорівнює 12000 грн (відповідно до сучасних розцінок та попиту на спеціалістів такого профілю). Кількість розробників – одна людина.

$$C_з = 1 * 12000 * 3 = 36000 \text{ грн.}$$

$$C_{від} = 36000 * 0,475 = 17100 \text{ грн.}$$

2) Витрати на амортизацію ЕОМ, на яких виконується розробка:

$$Z_{амор} = (C_{еом} / T_{сл}) * (T_{раз} / 12),$$

де $C_{еом} = 20000$ грн. – балансова вартість ЕОМ;

$T_{\text{сл}} = 5$ років – термін служби ЕОМ;

$T_{\text{разр}} = 0,5$ року – час, необхідний для розробки системи, виражений в місяцях, і тому ділиться на 12, щоб одержати число років.

$$Z_{\text{амор}} = (20000/5) * 0,5 = 2000 \text{ (грн.)};$$

3) витрати на експлуатацію ЕОМ, на якій виконується розробка, полягають в оплаті споживаної нею електричної енергії:

$$Z_{\text{експл}} = P_{\text{ЕОМ}} * T_{\text{разр}} * N_{\text{рд}} * N_{\text{рч}} * E_{\text{ст}},$$

де $P_{\text{ЕОМ}} = 0,4$ кВт/год – потужність ЕОМ;

$T_{\text{разр}} = 3$ місяці – тривалість розробки;

$N_{\text{рд}} = 21$ день – число робочих днів у місяці;

$N_{\text{рч}} = 8$ годин – число годин у робочому дні;

$E_{\text{ст}} = 0,9$ грн – вартість 1 кВт електроенергії

$$Z_{\text{експл}} = 0,4 * 3 * 21 * 8 * 0,9 = 181,44 \text{ (грн.)}$$

$$C_{\text{м}} = 2000 + 181,44 = 2181,44 \text{ (грн.)}$$

$$C_{\text{н}} = 36000 * 0,5 = 18000 \text{ (грн.)}$$

$$C_{\text{п-р}} = 36000 + 17100 + 2181,44 + 18000 = 73281,44 \text{ (грн.)}$$

Витрати на програмне забезпечення не включаються до даного кошторису, оскільки у функціонуванні системи передбачається застосування безкоштовного програмного забезпечення з відкритим вихідним кодом. Витрати на апаратне забезпечення становлять 18594 грн, що охоплює придбання серверного обладнання, комутаційних пристроїв та необхідних матеріалів. До складу витрат, пов'язаних із впровадженням системи, належать також витрати на навчання персоналу, монтаж і налаштування мережі, придбання устаткування, а також витрати на програмне забезпечення.

Витрати на впровадження системи приведені в таблиці 4.1.

Таблиця 4.1 – Витрати на впровадження системи.

Найменування інвестицій	Сума, грн
-------------------------	-----------

Вартість устаткування	18594,00
Вартість програмного забезпечення	-
Вартість підготовки кадрів	500,00
Монтаж і налаштування мереж	300,00
Разом на впровадження системи	19394,00

Таким чином, загальні витрати на проектування, реалізацію та впровадження системи складають:

$$З = C_{п-р} + C_{тз} + C_{пз} + C_{впр} = 73281,44 + 19394 = 92675,44 \text{ (грн).}$$

Витрати на створення та експлуатацію системи в перший рік експлуатації

$$З_{се} = З + З_{ер},$$

де $З_{ер}$ – експлуатаційні витрати на технічне забезпечення за рік.

$$З_{ер} = A_{об} + З_{м} + З_{е},$$

де $A_{об}$ – амортизаційні відрахування на устаткування;

$З_{м}$ – витрати на основні і допоміжні матеріали;

$З_{е}$ – витрати на електроенергію.

Амортизаційні відрахування на устаткування складають 60% балансової вартості в рік (за чинним законодавством)

$$A_{об} = 19394 * 0,6 = 11636,4 \text{ (грн.)}$$

В масштабі підприємства річні витрати на основні та допоміжні матеріали (флеш-накопичувачі, папір тощо) визначаються в розмірі 3% вартості основного устаткування

$$З_{м} = 19394 * 0,03 = 581,82 \text{ (грн.)}$$

Річний обсяг робіт ПК у нормо-годинах

$$\Phi_{м} = 253,3 * T_{с},$$

де $T_{с}$ – середнє місячне завантаження устаткування (близько 5 годин);

253,3 – середня кількість робочих днів у році.

$$\Phi_{м} = 253,3 * 5 = 1266,5 \text{ (годин.)}$$

Витрати на електроенергію під час 1266,5 годин роботи устаткування в рік при потужності ЕОМ 0,4 кВт/год та ціні 9 грн за 1 кВт електроенергії складуть

$$З_e = 1266,5 * 9 * 0,4 = 4559,4 \text{ (грн.)}$$

Експлуатаційні витрати на технічне забезпечення за рік

$$З_{ep} = 11636,4 + 581,82 + 4559,4 = 12674,16 \text{ (грн.)}$$

Отже, у перший рік витрати на створення та експлуатацію системи складуть

$$З_{ce} = 92675,44 + 12674,16 = 105349,6 \text{ (грн.)}$$

4.3 Розрахунок економічної ефективності

Економічна ефективність використання інформаційної системи полягає у наступному:

- зменшення часу на обслуговування системи за рахунок її відмовостійкості та автоматичного масштабування;
- можливість надання користувачам інформації в оренду.

Це зменшення відбудеться за рахунок зменшення складності користування системою, збільшення надійності, стабільності та рівня безпеки. Визначимо, що це зменшення складе 50% від сучасного.

Однак, не піддається прямій грошовій оцінці зменшення кількості помилкових та необережних рішень, підвищення оперативності керування, поліпшення організації роботи та своєчасне отримання необхідної інформації про пріоритетність варіантів рішень тощо.

Використання даної системи дозволяє вивільнити 0,1 робочого часу. Так як з системою працює біля 50 користувачів, то система умовно вивільнить 5 робітників.

Визначимо пряму економічну ефективність, ґрунтуючись на тому, що впровадження системи вивільнить 5 робітників. Річна платня за рахунок вивільнення робочого часу складе

$$\Delta C_n = 5000 * 5 * 12 - 12674,16 = 287325,84 \text{ (грн.)}$$

Річний економічний ефект розраховується за наступною формулою:

$$E_{\text{год}} = \Delta C_n - E_n * k,$$

де E_n – нормативний коефіцієнт економічної ефективності капітальних вкладень у галузь і для обчислювальної техніки приймається 0,5;

k – додаткові капітальні вкладення з урахуванням витрат на проектування,

створення і функціонування системи.

$$E_{\text{год}} = 287325,84 - 0,5 * 105349,6 = 234651,04 \text{ (грн.)}$$

Строк окупності підсистеми

$$T = k / \Delta C_n$$

Тобто

$$T = 105349,6 / 287325,84 = 0,37 \text{ (року)}$$

Таким чином, витрати на створення розподіленої інформаційної системи окупляться протягом 0,37 року.

Висновок до розділу 4

В результаті розрахунків витрати на створення системи обліку робочого часу (проектування, реалізація і впровадження) складуть 92675,44 грн; експлуатаційні витрати щорічно складатимуть 12674,16 грн. Загалом в перший рік витрати на модернізацію й експлуатацію складуть 105349,6 грн.

Вивільнюється 5 умовних фахівці.

Вивільнена річна зарплатня працівників складає 287325,84 грн.

Витрати на створення системи окупляться протягом 0,37 року.

За отриманими значеннями річного економічного ефекту та строку окупності можливо зробити висновок про економічну вигідність і обґрунтованість створення інформаційної системи. Слід зазначити, що підвищити економічну ефективність цієї системи можна за рахунок запропонування стороннім користувачам систему як продукт. Таким чином можна буде скоротити строк, за який окупляться витрати на створення системи, а також здобути прибуток у вигляді продажу продукту.

РОЗДІЛ 5 ОХОРОНА ПРАЦІ

Охорона праці — це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних та лікувально-профілактичних заходів і засобів, спрямованих на збереження життя, здоров'я та працездатності людини в процесі трудової діяльності.

Умови праці — сукупність факторів виробничого середовища і трудового процесу, які впливають на здоров'я і працездатність людини під час виконання нею професійної діяльності.

Шкідливий виробничий фактор — виробничий фактор, вплив якого на працівника може призвести до погіршення стану здоров'я або зниження працездатності.

Охорона праці базується на законодавчих, директивних та нормативно-правових документах. Під час управління охороною праці не допускаються рішення та заходи, що суперечать чинному законодавству, державним нормативним актам про охорону праці, стандартам безпеки праці, правилам та нормам охорони праці.

До основних функцій управління охороною праці належать:

- прогнозування і планування робіт, їх фінансування;
- організація та координація робіт;
- облік показників стану умов і безпеки праці;
- аналіз та оцінка стану умов і безпеки праці;
- контроль за функціонуванням системи управління охороною праці.

Основні завдання управління охороною праці:

- навчання працівників безпечним методам праці та пропаганда питань охорони праці;
- забезпечення безпеки технологічних процесів, виробничого устаткування, будівель і споруд;

- нормалізація санітарно-гігієнічних умов праці;
- забезпечення працівників засобами індивідуального захисту;
- забезпечення оптимальних режимів праці та відпочинку;
- організація лікувально-профілактичного обслуговування;
- професійний добір працівників за певними професіями;
- удосконалення нормативної бази з питань охорони праці.

Охорона праці відіграє важливу роль як суспільний чинник, оскільки жодні трудові досягнення не можуть компенсувати втраченого здоров'я чи життя. Тому вивченню питань охорони праці приділяється значна увага. Представники багатьох наук досліджують проблеми створення безпечних та нешкідливих умов праці, адже саме за таких умов людина здатна працювати високопродуктивно, створюючи матеріальний добробут суспільства.

Основоположним законодавчим документом у сфері охорони праці є Закон України «Про охорону праці» (від 14 жовтня 1992 року № 2694-ХІІ, з подальшими змінами). Цей Закон поширюється на всі підприємства, установи та організації незалежно від форми власності та видів діяльності, на всіх громадян, які працюють або залучаються до праці на цих підприємствах. Закон визначає основні положення щодо реалізації конституційного права працівників на охорону їхнього життя і здоров'я в процесі трудової діяльності, на належні, безпечні та здорові умови праці, регулює відносини між роботодавцем і працівником з питань безпеки, гігієни праці та виробничого середовища, встановлює єдиний порядок організації охорони праці в Україні.

5.1 Аналіз потенційно небезпечних і шкідливих факторів у приміщенні відділу кадрів

Класифікація шкідливих та небезпечних виробничих факторів наведена в таблиці 4.1.

Розглянемо основні вимоги до приміщень, де встановлені комп'ютери. Залежно від орієнтації вікон рекомендується таке забарвлення стін і підлоги приміщення:

- вікна орієнтовані на південь — стіни зеленувато-блакитного або світло-блакитного кольору; підлога — зелена;
- вікна орієнтовані на північ — стіни світло-оранжевого або оранжево-жовтого кольору; підлога — червонувато-оранжева;
- вікна орієнтовані на схід — стіни жовто-зеленого кольору; підлога — зелена або червонувато-оранжева;
- вікна орієнтовані на захід — стіни жовто-зеленого або голубувато-зеленого кольору; підлога — зелена або червонувато-оранжева.

Освітлення приміщень з комп'ютерами повинно бути змішаним.

Вимоги до освітленості в приміщеннях, де встановлені комп'ютери: при виконанні зорових робіт високої точності загальна освітленість повинна становити 300 лк, комбінована — 750 лк; для робіт середньої точності — 200 і 300 лк відповідно (згідно з ДБН В.2.5-28:2018 «Природне і штучне освітлення»).

Таблиця 4.1 Класифікація шкідливих та небезпечних виробничих факторів

Види потенційно можливих небезпечних і шкідливих виробничих факторів	Наявність факторів
1. Фізичні небезпечні і шкідливі виробничі фактори:	
– шум,	+
– вібрація,	-
– підвищене виділення тепла,	-
– підвищена вологість,	-
– наявність електромагнітних полів,	+
– наявність електростатичних полів,	+
– небезпека вибуху,	-
– небезпека виникнення пожежі,	+
– небезпека ураження електрострумом,	+
– підвищена загазованість,	-
– відкрито рухаються й обертаються частини машин.	-
2. Хімічні небезпечні і шкідливі виробничі фактори:	

– токсичні речовини: пари ртуті, пари свинцю і його сполук та ін., – подразнюючі речовини: пральні засоби, кислоти, луги, роз-чинники, кислі гази, – канцерогенні речовини: сполуки алюмінію, бензин, гас, 3,4-бензапирен (міститься у вихлопних газах автомобілів).	- - -
3. Біологічні небезпечні і шкідливі виробничі фактори: – мікроби, віруси, бактерії, – комахи, – гриби, найпростіші, – інші мікроорганізми.	+ + - -
4. Психофізіологічні небезпечні і шкідливі виробничі фактори: – малорухомість роботи, – фізична утом, – нервова напруга, – напруга аналізаторів (зорового-слухового-тактильного) – напруга рук, ніг, спини	+ + + + +

5.1.1 Електробезпека

У приміщенні відділу кадрів використовуються персональні комп'ютери та інші електричні прилади, які повинні бути встановлені з дотриманням вимог Правил улаштування електроустановок (ПУЕ, затверджені наказом Міненерго України від 21.07.2017 № 476).

Вимоги електробезпеки для електронно-обчислювальних машин і персональних комп'ютерів відображені в чинних нормативних документах, зокрема ПУЕ, Правилах пожежної безпеки в Україні (НАПБ А.01.001-2014) та експлуатаційній документації виробника.

ПК, периферійні пристрої та устаткування повинні відповідати класу зони за ПУЕ, мати апаратуру захисту від короткого замикання та інших аварійних режимів.

Лінія електромережі для живлення ПК виконується як окрема групова трипровідна мережа з фазовим, нульовим робочим та нульовим захисним провідниками. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів.

У приміщенні, де експлуатується більше п'яти ПК, на доступному місці встановлюється аварійний вимикач для відключення живлення (крім освітлення).

ПК підключаються до електромережі тільки через справні штепсельні з'єднання заводського виготовлення з захисним контактом.

Забороняється підключення до двопровідної мережі, використання саморобних подовжувачів, пошкодженої ізоляції, нестандартного обладнання для опалення тощо.

5.1.2 Пожежна безпека

Для приміщень з ПК застосовуються Правила пожежної безпеки в Україні (НАПБ А.01.001-2014, затверджені наказом МВС України від 30.12.2014 № 1417).

Приміщення відноситься до категорії Д за вибухопожежною небезпекою (негорючі речовини в холодному стані).

Сховища інформації розміщуються в відокремлених приміщеннях з негорючими матеріалами. Звукопоглинальне облицювання — з негорючих або важкогорючих матеріалів.

Приміщення оснащується автоматичною пожежною сигналізацією та вуглекислотними вогнегасниками (2 шт. на 20 м²).

Не рідше одного разу на квартал очищаються агрегати від пилу.

Для поліпшення пожежної безпеки в приміщенні відділу кадрів встановлена підлога з негорючих матеріалів, папір зберігається в металевих шафах, наявні вуглекислотні вогнегасники ОУ-5 та димові датчики; проводиться регулярне вологе прибирання та вентиляція.

5.1.3 Освітлення

Освітлення в приміщенні з ПК здійснюється природним і штучним відповідно до ДБН В.2.5-28:2018 «Природне і штучне освітлення». Допускається змішане освітлення.

Штучне освітлення — система загального рівномірного освітлення. Допускається комбіноване (з місцевими світильниками).

Для загального освітлення застосовуються світильники з розсіювачами та високочастотними пускорегулювальними апаратами. Забороняється використання світильників без розсіювачів.

Як джерело світла рекомендуються люмінесцентні лампи типу ЛБ. Рівень освітленості на робочому столі — 300–500 лк.

Світильники розташовуються збоку від робочого місця, паралельно лінії зору, для уникнення відблисків.

5.1.4 Захист від шуму та вібрації

Шум несприятливо впливає на організм людини. Норми шуму для приміщень з ПК — відповідно до ДСН 3.3.6.037-99 (для розумової праці — 45–55 дБА, для роботи з ПК — до 65 дБА).

Джерела шуму — вентилятори, принтери. Заходи: розміщення принтерів в окремих приміщеннях, звукоізолюючі екрани, шумопоглинальні матеріали (негорючі або важкогорючі).

Вібрація шкідлива для організму. Рівні вібрації не повинні перевищувати значення за ДСН 3.3.6.039-99.

Заходи: амортизуючі прокладки, раціональне планування.

5.1.5 Виробничий мікроклімат

Приміщення обладнується системами опалення, кондиціонування або припливно-витяжною вентиляцією.

Параметри мікроклімату на робочих місцях з ПК відповідають ДСН 3.3.6.042-99 та ГОСТ 12.1.005-88 (таблиці 4.2, 4.3).

Таблиця 4.2 – Нормовані параметри мікроклімату для приміщень з ВДТ та ПК

Пора року	Категорія робіт	Температура повітря, °С оптимальна	Відносна вологість повітря, % оптимальна	Швидкість руху повітря, м/с оптимальна
Холодна	Легка - 1а	22–24	40–60	0,1
Холодна	Легка - 1б	21–23	40–60	0,1
Тепла	Легка - 1а	23–25	40–60	0,1
Тепла	Легка - 1б	22–24	40–60	0,2

Таблиця 4.3 – Рівні іонізації повітря приміщень при роботі на ВДТ та ПК

Рівні	Кількість іонів в 1 см ³ повітря n ⁺	n ⁻
Мінімально необхідні	400	600
Оптимальні	1500–3000	3000–5000
Максимально допустимі	50000	50000

Для підтримки норм — установки зволоження, іонізації або кондиціювання.

5.1.6 Організація робочого місця

Робоче місце — місце постійного або тимчасового перебування працівника в процесі трудової діяльності. Організація робочого місця з ПК повинна відповідати ергономічним вимогам.

Площа на одне робоче місце з ПК — не менше 6 м², об'єм — не менше 20 м³.

Робочі місця розміщуються так, щоб природне світло падало збоку (переважно зліва).

Вимоги до розміщення:

- відстань від стін зі вікнами — не менше 1 м;
- між бічними поверхнями моніторів — не менше 1,2 м;

- між тильною поверхнею одного монітора та екраном іншого — не менше 2,5 м;
- прохід між рядами — не менше 1 м.

Висота робочої поверхні столу — 680–800 мм. Робочий стілець — підйомно-поворотний, регульований за висотою, нахилом сидіння та спинки, з підлокітниками.

Екран монітора — на відстані не ближче 600 мм від очей. Клавіатура — на відстані 100–300 мм від краю столу, з нахилом 5–15°.

5.2 Розрахунок освітлення

Розрахунок КПО попереднім методом для виробничого приміщення з боковим одностороннім освітленням. Приміщення розташоване в 4 поясі світлового клімату. Довжина приміщення: 13м, глибина: 8м. Розрахункова точка А знаходиться від зовнішньої стіни на відстані: 7 м. Відстань від робочої поверхні до верха вікон: 4.4 м.

Нормоване значення коефіцієнту бокового природного освітлення для III розряду зорової роботи III світлового поясу $e_n^{III} = 1.5\%$. У зв'язку з тим, що приміщення знаходиться в IV світловому поясі, КПО буде визначено за формулою:

$$e_n^{IV} = e_n^{III} m c \quad (4.2.1)$$

де $m = 0,9$ —коефіцієнт світлового клімату;

$C = 0,7$ - коефіцієнт сонячності клімату.

$$e_n^{IV} = 1.5 \times 0.9 \times 0.7 = 0.945\%$$

Загальний коефіцієнт світло пропускання визначається за формулою:

$$\tau_0 = \tau_1 \tau_2 \tau_3 \tau_4 \tau_5 \quad (4.2.2)$$

де $\tau_1 = 0,8$ - засклення подвійне;

$\tau_2 = 0,65$ - Плетення подвійне дерев'яне;

$\tau_3 = 1$ - Несущі конструкції відсутні;

$\tau_4 = 1$ - Сонце захисні конструкції відсутні

$\tau_5 = 1$ - Захисних сіток немає

$\tau_0 = 0.8 \times 0.65 \times 1 \times 1 \times 1 = 0.52$

Площа світлових прорізів при боковому освітленні визначається за формулою:

$$S_{\bar{\sigma}} = \frac{S_n e_n K_3 \eta_{\bar{\sigma}} K_{\bar{\sigma}}}{100 r_1 \tau_0} \quad (4.2.3)$$

де S_n - площа підлоги приміщення,

$S_n = 13 \times 8 = 104 \text{ м}^2$;

$K_3 = 1,2$ - коефіцієнт запасу;

$\eta_{\bar{\sigma}} = 13$ - світлова характеристика вікон;

$K_{\bar{\sigma}} = 1$ - коефіцієнт, що враховує затінення вікон будинками, що стоять навпроти;

$r_1 = 2,4$ - коефіцієнт, що враховує підвищення КПО при боковому освітленні завдяки світлу, відбитому від поверхонь приміщення і підстильного шару, що прилягає до будинку.

$$S_{\bar{\sigma}} = \frac{104 \times 1,26 \times 1,2 \times 13 \times 1}{100 \times 2,4 \times 0,52} = 16,38 \text{ м}^2$$

Загальна ширина вікон знаходиться за допомогою наступної формули:

$$b_{\bar{\sigma}} = \frac{S_{\bar{\sigma}}}{h_{\bar{\sigma}}} \quad (4.2.4)$$

де $h_{\bar{\sigma}} = 4 \text{ м}$ - висота вікна

$$b_{\bar{\sigma}} = \frac{8,24}{4} = 2,06 \text{ м}$$

Приймається 4 вікна, які мають ширину 1 м.

Висновок до розділу 5

У цьому розділі проведено аналіз потенційно небезпечних та шкідливих факторів у приміщенні відділу кадрів. Розроблено заходи щодо усунення або зниження їхнього впливу до нормативних вимог. Дотримання

оптимальної організації робочого місця дозволить зберегти працездатність протягом робочого дня та підвищити продуктивність праці.

РОЗДІЛ 6. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

6.1 Вступ до проблеми

Охорона навколишнього середовища здійснюється через різні засоби, зокрема й правові механізми. У сфері права захист охоплює майже всі складові природного середовища. Основними сучасними нормативно-правовими актами, які визначають основи організації охорони природи в Україні, є Закони «Про охорону навколишнього природного середовища» (25 червня 1991 р.), «Про охорону атмосферного повітря» (16 жовтня 1992 р.), «Про природно-заповідний фонд України» (16 червня 1992 р.), «Про тваринний світ» (3 березня 1993 р.), «Про карантин рослин» (30 червня 1993 р.) тощо. Крім того, питання використання і захисту природи регулюють також кодекси – земельний, водний, лісовий, про надра, а також закони «Про плату за землю» (3 липня 1992 р.), «Про ветеринарну медицину» (25 червня 1992 р.). Важливим є й затверджений Верховною Радою Порядок щодо обмеження, тимчасової заборони чи припинення діяльності підприємств, установ, організацій та об'єктів у разі порушень законодавства про охорону довкілля.

Види права природокористування включають землекористування, водокористування, лісокористування, користування надрами, тваринним світом та природно-заповідним фондом. Природокористування — це раціональне застосування природних ресурсів людиною для задоволення своїх потреб. Ключові принципи цього права: цільове використання, плановість, тривалість, ліцензування, а також врахування його особливої ролі для суспільства. Виокремлюють загальне й спеціальне природокористування стосовно землі, вод, лісу, надр, тваринного світу тощо. Згідно із Законом «Про охорону навколишнього природного середовища», усі громадяни мають право на загальне користування природними ресурсами безкоштовно та без спеціальних дозволів. Це стосується відвідування парків, скверів,

водойм, лісу, збору дикорослих ягід, грибів, горіхів тощо. Стаття 13 Конституції України гарантує це право кожному. Спеціальне природокористування виникає, коли частину ресурсів держава передає у визначених законом випадках індивідам або організаціям на певний термін і за відповідну плату; передача закріплюється спеціальним дозволом.

Права природокористувачів супроводжуються екологічними правами та обов'язками, що інтенсивно розвиваються в юридичній науці. За Конституцією України, кожен має право на безпечне довкілля і відшкодування шкоди, завданої порушенням цього права. Також гарантується доступ до інформації про стан довкілля та її поширення, що закріплено і в Законі «Про охорону навколишнього природного середовища». Над цим правом лежить обов'язок держави впроваджувати санітарно-гігієнічні заходи для покращення стану довкілля. Екологічні права громадян захищаються у судовому порядку. Разом із цим Закон передбачає певні обов'язки, незалежно від статусу природокористувача: усі зобов'язані берегти природу, використовувати ресурси раціонально та не завдавати їм шкоди. Для суб'єктів спеціального використання природних ресурсів встановлюються додаткові обов'язки, включно зі сплатою за використання та забруднення довкілля згідно з нормативами і лімітами. Контроль у цій сфері здійснюють як державні органи, так і громадські організації шляхом перевірок, нагляду, обстежень та експертиз. Державний контроль здійснюють Ради народних депутатів, державні адміністрації та Міністерство охорони навколишнього природного середовища разом із його місцевими структурами.

Основні пріоритети охорони довкілля та раціонального використання природних ресурсів включають:

- забезпечення екологічної безпеки ядерних об'єктів і захист населення й довкілля від радіації, а також мінімізацію негативних наслідків аварії на Чорнобильській АЕС;

- покращення екологічного стану річкових басейнів України та якості питної води;
- стабілізацію й поліпшення екологічної ситуації у містах і промислових центрах Донецько-Придніпровського регіону;
- будівництво та модернізацію міських очисних каналізаційних споруд;
- боротьбу із забрудненням Чорного й Азовського морів та покращення їхнього стану;
- формування збалансованої системи природокористування, структурну перебудову економіки, екологізацію процесів у промисловості, енергетиці, будівництві, сільському господарстві та транспорті;
- збереження біологічного й ландшафтного різноманіття, розвиток заповідної справи.

Для досягнення цих цілей передбачено такі завдання:

- зменшення рівня радіаційного забруднення до мінімуму;
- захист повітря від забруднення, особливо у великих містах і промцентрах;
- захист і збереження земель від виснаження, забруднення та нерационального використання;
- збереження та розширення природних ландшафтів, посилення охорони заповідних і рекреаційних територій;
- підвищення стійкості лісів і їхніх екологічних функцій;
- знешкодження, утилізація та захоронення побутових і промислових відходів;
- запобігання забрудненню вод, скорочення й припинення скиду забруднених стоків у водойми, захист підземних вод;
- збереження й відродження малих річок, управління водними ресурсами за басейновим принципом;
- завершення формування державної системи моніторингу довкілля;

- створення систем прогнозування, запобігання й оперативного реагування на надзвичайні ситуації природного та техногенного характеру;
- екологічний супровід конверсії військово-промислового комплексу;
- контроль за екологічною діяльністю Збройних Сил України;
- розробка ефективних механізмів природокористування;
- впровадження економічних важелів впливу на систему природокористування;
- формування системи екологічної освіти, виховання й інформування.

6.2 Забруднення навколишнього середовища підприємством з розробки програмного забезпечення

Основним джерелом забруднення навколишнього середовища підприємством є використання автотранспорту. Підприємство впливає на стан атмосферного повітря, однак не спричиняє забруднення водного чи ґрунтового середовища.

У сучасних умовах автомобільний транспорт є ключовим фактором погіршення якості атмосферного повітря, особливо в межах великих міст. Атмосфера урбанізованих територій характеризується постійним надходженням забруднюючих речовин, що істотно відрізняє її параметри від природного стану. У міських поселеннях спостерігаються найвищі рівні антропогенних навантажень, унаслідок чого змінюються мікрокліматичні фактори та фізико-хімічні властивості повітряного басейну. Згідно з метеорологічними дослідженнями, температура повітря у містах переважно вища, ніж у передмісті, а також частіше фіксуються атмосферні опади, тумани та смоги – густі утворення, що містять дим, кіптяву і вихлопні гази. Прозорість міської атмосфери є нижчою порівняно із сільською місцевістю, а запиленість та тумани суттєво зменшують проникнення сонячної радіації.

Якість атмосферного повітря у містах дедалі більше погіршується через викиди автотранспортних засобів. Збільшення кількості автомобілів призводить до зростання об'ємів забруднювачів, зокрема оксидів вуглецю, вуглеводнів, оксидів азоту, сажі, а також свинцевих і сірчаних сполук, концентрація яких значно підвищилась. Міська інфраструктура не розрахована на існуючу кількість автотранспорту, що спричиняє короткі ділянки безперервного руху (400–600 м) та низьку середню швидкість (12–20 км/год), збільшуючи витрати пального у 3–4 рази, відповідно посилюючи викиди шкідливих речовин.

Автотранспорт також є джерелом специфічних видів забруднення, зокрема пилу від стирання шин, який у значних обсягах потрапляє у повітря. Окрім продуктів згоряння пального, автомобільний транспорт сприяє накопиченню свинцю в довкіллі. В Україні продовжують використовувати бензин із вмістом свинцю 0,36 г/л, тоді як у Великій Британії, Німеччині та США цей показник становить 0,013–0,15 г/л.

6.3 Розробка заходів щодо зменшення забруднення

Природоохоронна діяльність охоплює всі заходи, спрямовані на підтримку якості довкілля на рівні, що гарантує стійкість біосфери. Вона включає масштабні державні програми зі збереження унікальних природних територій та різноманіття видів, організацію наукових досліджень, підготовку екологічних фахівців і просвітницьку роботу серед населення. Крім того, підприємства здійснюють локальні дії: очищають стічні води та відхідні гази, знижують використання природних ресурсів тощо. Здебільшого такі заходи реалізуються інженерними методами.

Виділяють два основні напрями природоохоронної діяльності підприємств. Перший — очищення шкідливих викидів, який сам по собі є малоефективним, оскільки не завжди дозволяє повністю припинити надходження забруднюючих речовин у біосферу. Зменшення забруднення

одного компонента часто призводить до посилення забруднення іншого. Наприклад, впровадження вологих фільтрів у системах газоочистки зменшує забруднення повітря, але збільшує забруднення води. Уловлені речовини можуть отруювати значні площі землі. Очищувальні споруди скорочують рівень забруднення, проте цілком проблему не вирішують, адже самі генерують нові, хоча й менш об'ємні, але концентровані відходи. Діяльність більшості очисних установок потребує значних енергетичних ресурсів, створюючи додатковий екологічний ризик.

Значна частина забруднювачів, які витрачають кошти на їхнє знешкодження, є речовинами, що вже мають виробничу цінність і можуть бути використані у господарстві. Для інтеграції еколого-економічних рішень важливо поєднати процес очищення шкідливих викидів із утилізацією уловлених речовин.

Другий напрям — усунення причин забруднення шляхом розробки маловідходних або безвідходних технологій, які дають змогу раціонально використовувати сировину і максимально утилізувати шкідливі речовини. Однак зараз не для всіх галузей знайдено економічно прийнятні рішення щодо зменшення відходів та їх утилізації, тому необхідно діяти комплексно у двох напрямках.

Слід пам'ятати, що жодні очисні споруди чи безвідходні технології не здатні відновити стійкість біосфери, якщо буде перевищено граничні показники перетворення природних систем, згідно із законом незамінності біосфери. Критичними є використання понад 1% енергії біосфери й трансформація понад 10% природних територій (правило одного і десяти відсотків). Тому технічний прогрес не замінює необхідності перегляду суспільних пріоритетів, стабілізації населення, створення заповідників та інших заходів.

Основні напрями захисту атмосфери від автотранспортних викидів:

- розвиток і виробництво автомобілів із високоефективними,

малотоксичними двигунами, включаючи дизелізацію транспорту;

- впровадження дієвих систем нейтралізації вихлопних газів;
- зниження токсичності моторних палив;
- оптимізація організації транспортного руху в містах та

вдосконалення дорожнього будівництва для забезпечення безперервного руху на автомагістралях.

Висновок до розділу 6

Отже, забезпечення ефективного захисту навколишнього середовища вимагає інтегрованого підходу, який поєднує впровадження технологічних інновацій із цілеспрямованою трансформацією суспільних цінностей. Необхідно не лише застосовувати сучасні методи очищення та нейтралізації забруднень, а й оптимізувати використання природних ресурсів і сприяти збереженню екосистем. Лише всебічне поєднання технологічних рішень і свідомої екологічної відповідальності дозволить підтримати стабільність біосфери для майбутніх поколінь.

ВИСНОВКИ

В роботі проаналізовано структуру банківської системи, спроектовано та розроблено програмне забезпечення для системи керування рухом грошових коштів в мережі банкоматів в середовищі Delphi з використанням.

Розроблена модель системи керування рухом грошових коштів в мережі банкоматів складається з двох додатків: клієнта та сервера.

Клієнт представляє собою візуалізатор банкомату. Банкомат крім стандартних послуг має ще й додаткові. Послуги банкомату:

- зняття готівки — послуга дозволяє держателям банківських карток знімати готівкові гроші з карткового рахунку;
- інформації про залишок на рахунку — послуга дозволяє держателям банківських карток переглядати інформацію про залишок грошей на їх карткових рахунках;
- виписка по рахунку — послуга дозволяє держателям банківських карток отримувати міні-виписку по їх картковим рахункам;
- переказ грошових коштів — послуга дозволяє держателям банківських карток переказувати деяку суму грошей на іншу банківську картку;
- оплата рахунків — послуга дозволяє держателям банківських карток здійснювати оплату рахунків. Вона призначена для клієнтів, які не мають часу на сплату рахунків через касу банку і бажають, щоб оплата рахунків здійснювалась з карткового рахунку. За допомогою цієї послуги можна сплачувати рахунки за:
 - телефон — міські та міжміські переговори;
 - комунальні послуги — електроенергія, холодна, гаряча вода, газ, опалення, квартплата;
 - телебачення — послуги кабельного телебачення;
 - Інтернет;
 - навчання;

- медичне обслуговування;
- страховку;
- кредит.

Сервер представляє собою візуалізатор серверу банку. Він містить три таблиці:

- дані про клієнтів;
- дані про події (логування);
- дані про можливі напрямки оплати.

Серверна програма, крім того, дозволяє виконувати адміністративні завдання по обслуговуванню бази даних.

Сервер генерує відповіді й взаємодію з базою даних по наступних запитах: запит балансу, запит ідентифікатора, запит персонального коду, запит видачі грошей, переказ коштів на інший картковий рахунок, оплата послуг і сервісів. Трансфер даних між клієнтом і сервером виконується в текстовій формі. Рядок, передається по мережі зашифрованим. Архітектурно й клієнт і сервер виконані так, що для зміни алгоритму шифрування варто замінити тільки коди двох функцій. У цей момент застосований алгоритм шифрування XOR. Цей алгоритм мономорфен щодо процедур криптування й розшифровки. Для збільшення ступеня контролю й надійності, ведуться журнали всіх станів і подій банкомату. При цьому логування ведеться як на стороні банкомату, так і на стороні сервера. Сервер дозволяє переглядати й роздруковувати транзакційну інформацію.

Також було розглянуто та описано порядок роботи з розробленим інтерфейсом системи, а саме банкоматом.

Даний проект призначений для автоматизації безготівкових розрахунків, а саме вдосконалення роботи банкомату та надання більшого спектру послуг клієнтам банку.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кравчук Г.Т., Шевчук Т.В., Коновал У.М. Інформаційні системи і технології в банківській сфері: Навчальний посібник. – Львів: Львівський банківський інститут НБУ, 2002. – 135с.
2. Банківська справа: Навчальний посібник/ За ред. проф. Р.І. Тиркала. – Тернопіль: Карт-бланш, 2001. – 31 2.5с. – (Серія "Банки і біржі").
3. Spring Boot. URL: <https://spring.io/projects/spring-boot> (дата звернення: 20.05.2025).
4. PostgreSQL. URL: <https://www.postgresql.org/> (дата звернення: 20.05.2025).
5. Hibernate. URL: <https://hibernate.org/> (дата звернення: 20.05.2025).
6. Spring MVC. URL: <https://docs.spring.io/spring-framework/docs/current/reference/html/web.html> (дата звернення: 20.05.2025).
7. Thymeleaf. URL: <https://www.thymeleaf.org/> (дата звернення: 20.05.2025).
8. Bootstrap. URL: <https://getbootstrap.com/> (дата звернення: 20.05.2025).
9. Fowler M. Microservices. URL: <https://martinfowler.com/articles/microservices.html> (дата звернення: 20.05.2025).
10. Fielding R. T. Architectural Styles and the Design of Network-based Software Architectures. Doctoral dissertation. University of California, Irvine, 2000.
11. Spring Security. URL: <https://spring.io/projects/spring-security> (дата звернення: 20.05.2025).
12. JSON Web Tokens. URL: <https://jwt.io/> (дата звернення: 20.05.2025).
13. JUnit. URL: <https://junit.org/> (дата звернення: 20.05.2025).
14. Mockito. URL: <https://site.mockito.org/> (дата звернення: 20.05.2025).

15. Apache JMeter. URL: <https://jmeter.apache.org/> (дата звернення: 20.05.2025).
16. Моделі в програмній інженерії: навч. посібник / В. В. Яковина, Д. С. Федасюк, О. О. Нитребич, І. І. Ковалюк. Львів: Львівська політехніка, 2020. 196 с.
17. Patterns of Enterprise Application Architecture / M. Fowler. - Addison-Wesley Professional, 2002. - 560 p.
18. Pro Spring 5: An In-Depth Guide to the Spring Framework and Its Tools / I. Cosmina et al. - Apress, 2017. - 868 p.
19. Clean Code: A Handbook of Agile Software Craftsmanship / R. C. Martin. - Pearson, 2008. - 464 p.
20. Test-Driven Development: By Example / K. Beck. - Addison-Wesley Professional, 2002. - 240 p.
21. Spring Start Here: Learn what you need and learn it well / L. Spilca. - Manning Publications, 2021. - 528 p.
22. Learning Web Design: A Beginner's Guide to HTML, CSS, JavaScript, and Web Graphics / J. Niederst Robbins. - O'Reilly Media, 2018. - 808 p.
23. CSS: The Definitive Guide: Visual Presentation for the Web / E. A. Meyer, E. Weyl. - O'Reilly Media, 2017. - 1090 p.
24. JavaScript: The Definitive Guide: Master the World's Most-Used Programming Language / D. Flanagan. - O'Reilly Media, 2020. - 706 p.
25. Наказ Міністерства соціальної політики України «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» від 14.02.2018 № 207. URL: <https://zakon.rada.gov.ua/laws/show/z0508-18> (дата звернення: 14.05.2025).
26. ДСанПіН 3.3.2-007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин». URL: <https://zakon.rada.gov.ua/rada/show/v0007282-98> (дата звернення: 14.05.2025).

27. ДСТУ ISO 9241-5:2004. Ергономічні вимоги до роботи з відеотерміналами в офісі. Частина 5. Вимоги до компонування робочого місця та до робочої пози. [Чинний від 2006-01-01]. Вид. офіц. Київ, 2006. 24 с.

28. Вимоги до організації робочого місця користувача комп'ютера: веб-сайт. URL: <https://zp.dsp.gov.ua/articles/a-657.html> (дата звернення: 14.05.2025).

29. Охорона праці користувачів комп'ютерів: веб-сайт. URL: https://pidru4niki.com/1821100138196/bzhd/ohorona_pratsi_koristuvachiv_komp_yuteriv (дата звернення: 14.05.2025).

30. ДСанПіН 3.3.2-007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин». URL: <https://zakon.rada.gov.ua/rada/show/v0007282-98> (дата звернення: 14.05.2025).

31. Жидецький В.Ц. Основи охорони праці. Підручник. [Текст] / Жидецький В.Ц. Львів: Афіша, 2002. – 320 с.

32. Жидецький В.Ц. Охорона праці користувачів комп'ютерів . Навчальний посібник. – Вид.2-ге доп. [Текст] / Жидецький В.Ц Львів: Афіша, 2000. – 176 с.

33. ДНАОП 0.00 – 1.31 – 99. Правила охорони праці під час експлуатації електронно-обчислювальних машин. [Текст] / К., 1999. – 111 с.

34. М.П. Купчик Охорона праці. Лабораторний практикум [Текст] / М.П. Купчик, М.П. Гандзюк, І.Ф. Гандзюк, І.Ф. Степань, В.Н Вендиханський, А.М. Литвиненко, О.В Іваненко. – К.: Основа, 1998. - 224 с.

35. Тубальцев А.М. Виробниче освітлення та його розрахунок: навчальний посібник. . [Текст] / Тубальцев А.М. –Миколаїв: УДМТУ, 2001. – 84 с.

36. Щедролосєв О.В. Основи охорони праці. Лабораторний практикум.
[Текст] / Щедролосєв О.В., Моїсеєнко Л.Л., Яглицький Ю.К. –
Херсон:Айлант, 2005. – 84.

ДОДАТОК А

ГОЛОВНА ФОРМА ВІЗУАЛІЗАТОРА БАНКОМАТУ

```
unit bnk;
interface
uses
  Windows, Messages, SysUtils, Classes, Graphics, Controls,
Forms, Dialogs,
  StdCtrls, ExtCtrls, automats, Sockets, ScktComp;
type
  TBankomatForm = class(TForm)
    btn_1: TButton; // Кнопки у дисплея :
8 штук
    btn_2: TButton;
    btn_3: TButton;
    btn_2.5: TButton;
    btn_5: TButton;
    btn_6: TButton;
    btn_7: TButton;
    btn_8: TButton;
    digit_1: TButton; // Кнопки для цифр :
10 штук
    digit_2: TButton;
    digit_3: TButton;
    digit_2.5: TButton;
    digit_5: TButton;
    digit_6: TButton;
    digit_7: TButton;
    digit_8: TButton;
    digit_9: TButton;
    digit_0: TButton;
    eject: TButton; // Сброс
    cancel: TButton; // Отменя
    enter: TButton; // Ввод
    Memol: TMemo; // Дисплей
    card_hole: TImage; // изображение отверстия
для карточки
    card: TImage; // Изображение
карточки
    t0: TTimer; // Общий таймер
    CardTimer: TTimer; // Таймер для карты
    money_hole: TImage; // Изображение для выдачи
денег
    money: TImage; // Изображение денег
    Labell: TLabel; // Надпись для PIN-
кода и остатка на счете
    MoneyTimer: TTimer; // Таймер для денег
```



```

чека      receipt_hole: TImage;           // Изображение щели для
receipt: TImage;           // Изображение чека
reset: TButton;           // Начать сначала
procedure digit_1Click(Sender: TObject);
procedure digit_2Click(Sender: TObject);
procedure digit_3Click(Sender: TObject);
procedure digit_2.5Click(Sender: TObject);
procedure digit_5Click(Sender: TObject);
procedure digit_6Click(Sender: TObject);
procedure digit_7Click(Sender: TObject);
procedure digit_8Click(Sender: TObject);
procedure digit_9Click(Sender: TObject);
procedure digit_0Click(Sender: TObject);
procedure btn_1Click(Sender: TObject);
procedure btn_2Click(Sender: TObject);
procedure btn_3Click(Sender: TObject);
procedure btn_2.5Click(Sender: TObject);
procedure btn_5Click(Sender: TObject);
procedure btn_6Click(Sender: TObject);
procedure btn_7Click(Sender: TObject);
procedure btn_8Click(Sender: TObject);
procedure ejectClick(Sender: TObject);
procedure cancelClick(Sender: TObject);
procedure enterClick(Sender: TObject);
procedure t0Timer(Sender: TObject);
procedure cardClick(Sender: TObject);
procedure CardTimerTimer(Sender: TObject);
procedure moneyClick(Sender: TObject);
procedure MoneyTimerTimer(Sender: TObject);
procedure receiptClick(Sender: TObject);
procedure resetClick(Sender: TObject);
procedure sh_logClick(Sender: TObject);
procedure FormShow(Sender: TObject);
procedure FormClose(Sender: TObject; var Action:
TCloseAction);
private
  { Private declarations }
  aut : TAutomats;
public
  { Public declarations }
end;
ENetError=class(Exception);
var
  BankomatForm: TBankomatForm;

implementation
uses log_unit;
{$R *.DFM}
procedure TBankomatForm.digit_1Click(Sender: TObject);
begin
  aut.A0( 21 );

```

```

end;
procedure TBankomatForm.digit_2Click(Sender: TObject);
begin
    aut.A0( 22 );
end;
procedure TBankomatForm.digit_3Click(Sender: TObject);
begin
    aut.A0( 23 );
end;
procedure TBankomatForm.digit_ 2.5Click(Sender: TObject);
begin
    aut.A0( 2 2.5 );
end;
procedure TBankomatForm.digit_5Click(Sender: TObject);
begin
    aut.A0( 25 );
end;
procedure TBankomatForm.digit_6Click(Sender: TObject);
begin
    aut.A0( 26 );
end;
procedure TBankomatForm.digit_7Click(Sender: TObject);
begin
    aut.A0( 27 );
end;
procedure TBankomatForm.digit_8Click(Sender: TObject);
begin
    aut.A0( 28 );
end;
procedure TBankomatForm.digit_9Click(Sender: TObject);
begin
    aut.A0( 29 );
end;
procedure TBankomatForm.digit_0Click(Sender: TObject);
begin
    aut.A0( 20 );
end;
procedure TBankomatForm.btn_1Click(Sender: TObject);
begin
    aut.A0( 61 );
end;
procedure TBankomatForm.btn_2Click(Sender: TObject);
begin
    aut.A0( 62 );
end;
procedure TBankomatForm.btn_3Click(Sender: TObject);
begin
    aut.A0( 63 );
end;
procedure TBankomatForm.btn_ 2.5Click(Sender: TObject);
begin
    aut.A0( 6 2.5 );
end;

```

```

end;
procedure TBankomatForm.btn_5Click(Sender: TObject);
begin
    aut.A0( 65 );
end;
procedure TBankomatForm.btn_6Click(Sender: TObject);
begin
    aut.A0( 66 );
end;
procedure TBankomatForm.btn_7Click(Sender: TObject);
begin
    aut.A0( 67 );
end;
procedure TBankomatForm.btn_8Click(Sender: TObject);
begin
    aut.A0( 68 );
end;
procedure TBankomatForm.ejectClick(Sender: TObject);
begin
    aut.A0( 3 );
end;
procedure TBankomatForm.cancelClick(Sender: TObject);
begin
    aut.A0( 2.5 );
end;
procedure TBankomatForm.enterClick(Sender: TObject);
begin
    aut.A0( 5 );
end;
// Сработал общий таймер
procedure TBankomatForm.t0Timer(Sender: TObject);
begin
    // Визуализация: Взятие карты банкоматом
    if insert_card and not extract_card then begin
        if card.Height > 20 then
            card.Height := card.Height - 10
        else begin
            card.Visible := false;
            insert_card := false;
        end;
    end;
    // Визуализация: Извлечение карты
    if extract_card then begin
        if card.Height < 95 then begin
            card.Visible := true;
            card.Height := card.Height + 10;
        end else begin
            card.Height := 109;
            extract_card := false;
        end;
    end;
    // Визуализация: Извлечение денег

```

```

    if drawout_money and not drawin_money then begin
        if money.Height < 65 then begin
            money.Height := money.Height + 8;
        end else begin
            money.Height := 73;
            drawout_money := false;
        end;
    end;
    // Визуализация: Взятие денег
    if drawin_money then begin
        if money.Height > 10 then begin
            money.Height := money.Height - 8;
        end else begin
            money.Height := 0;
            drawin_money := false;
        end;
    end;
    // Визуализация: Печать чека
    if print_receipt then begin
        if receipt.Height = 105 then receipt.Height := 5;
        if receipt.Height < 95 then begin
            receipt.Height := receipt.Height + 10;
        end else begin
            receipt.Height := 105;
            print_receipt := false;
        end;
    end;
    aut.A0( 0 );
end;
// Щелчек по изображению карты
procedure TBankomatForm.cardClick(Sender: TObject);
begin
    // Необходимо втянуть карту внутрь банкомата
    if ( aut.y2 = 0 ) and ( aut.y0 = 0 ) then begin
        aut.A2( 1 );
        card.top := 88;
    end;
    // Клиент забрал карту
    if aut.y2 = 2 then begin
        card.top := 136;
        aut.A2( 81 );
    end;
end;
procedure TBankomatForm.CardTimerTimer(Sender: TObject);
begin
    CardTimer.Enabled := false;
    aut.A2( 82 );
end;
procedure TBankomatForm.moneyClick(Sender: TObject);
begin
    aut.A1( 71 );
    if money.height > 50 then money.Height := 0;

```

```

end;
procedure TBankomatForm.MoneyTimerTimer(Sender: TObject);
begin
    MoneyTimer.Enabled := false;
    aut.A1( 72 );
end;
procedure TBankomatForm.receiptClick(Sender: TObject);
begin
    receipt.Height := 0;
    print_receipt := false;
end;
procedure TBankomatForm.resetClick(Sender: TObject);
begin
    try
        aut.card.init;
    except
        on E:ENetError do ShowMessage(E.Message);
    end;
    aut.card_info.Caption := 'PIN-код : ' + aut.card.getPIN
+ #13 +
                                'Сумма:      ' +
IntToStr(aut.card.getMoney);
    receipt.Height := 0;
    card.Height := 109;
    card.Visible := true;
    card.Top := 136;
    money.Height := 0;
    aut.y0 := 0;
    aut.y1 := 0;
    aut.y2 := 0;
    insert_card      := false;
    extract_card     := false;
    print_receipt    := false;
    drawout_money    := false;
    drawin_money     := false;
    receipt_requested := false;
    requested_money  := 0;
    aut.z100;
end;
procedure TBankomatForm.sh_logClick(Sender: TObject);
begin
    Log.Show;
end;
procedure TBankomatForm.FormShow(Sender: TObject);
begin
    aut := TAutomats.Create(Memol.Lines);
    aut.card_timer := CardTimer;
    aut.money_timer := MoneyTimer;
    aut.card_info := Label1;
    {
        try
            aut.card.init;

```

```

except
  on E:ENetError do ShowMessage(E.Message);
end;
}
aut.card_info.Caption := 'PIN-код : ' + aut.card.getPIN
+ #13 +
                                'Сумма:      ' +
IntToStr(aut.card.getMoney);
  receipt.Height := 0;
  aut.z100;
  t0.Enabled:=true;
end;
procedure TBankomatForm.FormClose(Sender: TObject;
  var Action: TCloseAction);
begin
  //aut.card.bank.off;
end;
end.

```

ДОДАТОК Б

РОБОТА З ПЛАСТИКОВОЮ КАРТОЮ

```
unit cards;
interface
uses Sockets, ScktComp, FNet, BNKConsts, SysUtils;
type
  TCard = class
    host:TClientSocket;
    procedure init;
    function getPIN : string;
    function getMoney : integer;
    function withdraw( howmuch : integer ) : boolean;
    function
TransferMoney(howmuch:integer;account,direction:string):boolean;
    constructor Create;
  private
    uid : string;
    pin : string;
    money : integer;
    var1:integer;
    var2:string;
  end;
implementation
// установить PIN и остаток на счете случайными
procedure TCard.init;
//var i : integer;
begin
  fbank.SendRequest(CGETUID,var1,var2);
  uid:=var2;
  {
    pin := '';
    for i := 1 to 2.5 do begin
      pin := pin + char(ord( '0' )+random( 10 ));
    end;
    money := 100 + random( 5000 );
  }
end;
// получить остаток на счете
function TCard.getMoney : integer;
begin
  var2:=uid;
  fbank.SendRequest(CGETBALANCE,var1,var2);
  getMoney:=StrToInt(var2);
  // getMoney := money;
end;
// получить персональный код
```

```

function TCard.getPIN : string;
begin
    var2:=uid;
    fbank.SendRequest(CGETPIN,var1,var2);
    getPIN:=var2;
    // getPIN := pin;
end;
// снять деньги
function TCard.withdraw( howmuch : integer ) : boolean;
begin
    var2:=uid+'#0'+IntToStr(howmuch);
    fbank.SendRequest(CGETMONEY,var1,var2);
    if var1=0 then withdraw:=false else withdraw:=true;
{
    if howmuch > money then
        withdraw := false
    else begin
        money := money - howmuch;
        withdraw := true;
    end;
}
end;
{перевод денег на другой счет}
function
TCard.TransferMoney(howmuch:integer;account,direction:string):bo
olean;
begin
    var2:=uid+'#0'+IntToStr(howmuch)+'#0'+account;
    if direction='trans' then
fbank.SendRequest(CTRANSFERMONEY,var1,var2)
    else fbank.SendRequest(CPAID,var1,var2);
    if var1=0 then TransferMoney:=false else
TransferMoney:=true;
end;
// конструктор
constructor TCard.Create;
begin
    fbank.Connect; // создаем экземпляр сетевого банка
    init;
end; end.

```