**\_\_\_\_\_Тернопільський національний технічний університет імені Івана Пулюя\_\_\_\_\_\_**

(повне найменування вищого навчального закладу)

Кафедра \_\_\_\_\_\_\_\_\_**кібербезпеки**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДЛЯ ВИКОНАННЯ ЛАБОРАТОРНИХ РОБІТ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

\_\_**5.9 «Інформаційні банківські технології»**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(шифр і назва навчальної дисципліни)

напрям підготовки \_\_**6.170101 «Безпека інформаційних і комунікаційних систем»**

(шифр і назва напряму підготовки)

спеціальність **7.17010101 «Безпека інформаційних і комунікаційних систем»**\_\_\_\_\_\_\_\_

(шифр і назва спеціальності)

(назва спеціалізації)

факультет \_\_\_\_**комп’ютерно-інформаційних систем і програмної інженерії**\_\_\_\_\_\_\_\_\_

(назва інституту, факультету, відділення)

Тернопіль – 201\_\_ рік

Методичні рекомендації для виконання лабораторних робіт з дисципліни

**«Інформаційні банківські технології»**\_\_для студентів

(назва навчальної дисципліни)

за напрямом підготовки 6.170101 «Безпека інформаційних і комунікаційних систем», спеціальністю 7.17010101, 8.17010101 «Безпека інформаційних і комунікаційних систем».

"\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_ 201\_\_ року - 80 с.

Розробники:доц. Кареліна О. В.

Методичні рекомендації для виконання лабораторних робіт затверджені на засіданні кафедри кібербезпеки ТНТУ ім. І. Пулюя

Протокол від. "\_\_"\_\_\_\_\_\_\_\_\_\_ 201\_\_ року № \_\_\_

Завідувач кафедри кібербезпеки

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_Козак Р. О.\_\_\_)

(підпис) (прізвище та ініціали)

"\_\_"\_\_\_\_\_\_\_\_\_\_ 201\_\_ року

Схвалено Методичною радою факультету комп’ютерно-інформаційних систем і програмної інженерії

Протокол від "\_\_"\_\_\_\_\_\_\_\_\_\_ 201\_\_ року № \_\_\_

"\_\_"\_\_\_\_\_\_\_\_\_\_ 201\_\_ року Голова \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_Осухівська Г.М. \_\_)

(підпис) (прізвище та ініціали)

© Кареліна О. В., 201\_\_ р.

© ТНТУ, 201\_\_ р.

# Лабораторна робота №1

# Вивчення та аналіз захищеності «Національної ПЛАТІЖНОЇ системи «пРОСТІР».

## 1.1. Мета роботи.

Ознайомитися з принципами роботи проекту «Національна платіжна система «Простір», основними його елементами, порядком взаємодії між ними, розглянути принципи організації захисту інформації в проекті.

## 1.2. Методичні вказівки з організації самостійної роботи студентів.

При підготовці до лабораторної роботи необхідно:

- засвоїти лекційний матеріал, який стосується системи «Простір»;

- вивчити і засвоїти основні поняття і визначення підрозділу 1.4;

- засвоїти основні поняття і терміни, що використовуються в проекті «Простір» (див. додаток А);

- підготувати відповіді на питання, наведені в методичних вказівках.

## 1.3. Опис лабораторної установки.

Використовується комп’ютер із процесором не нижче ніж Intel 486. У якості програмного забезпечення для виконання роботи використовуються браузер та пакет MS Office.

## 1.4. Теоретичні відомості.

Починаючи з 1997 р. Національним банком України розробляється проект (НСМЕП), що повинен забезпечити перехід більшої частини наявних грошових розрахунків на безготівкові. Проект припускає введення пластикової картки як основного інструмента розрахунків для фізичних і юридичних осіб. У 2016 р. НБУ провів ребрендинг. Наступником НСМЕП стала Національна платіжна система «Простір».

### 1.4.1. Короткий опис проекту.

Проект пропонує пластикові картки як основний інструмент для розрахунку при оплаті товарів і послуг масового споживання. Планується також використання таких типів карток як електронний гаманець і електронний чек.

Електронний гаманець призначений для здійснення платежів дрібними сумами. Є обмеження на максимальну суму залишку на картці і максимальну суму платежу. Електронний гаманець може бути двох видів – анонімний і персоналізований.

Придбання анонімного електронного гаманця не припускає відкриття рахунка в банку. Завантаження і дозавантаження здійснюються тільки готівкою.

Для персоналізованого гаманця відкривається спеціальний рахунок, з якого можна здійснювати завантаження  картки або виконувати прямий платіж (з рахунка на рахунок). Можливість прямого платежу обмовляється окремо.

Електронний чек – платіжний інструмент для дій з більшими сумами, ніж електронний гаманець, хоча для нього також передбачені ліміти. Придбання електронного чека зобов'язує клієнта відкрити в банку спеціальний картрахунок, на який клієнт вносить необхідну йому суму. Така ж сума заноситься в пам'ять картки, і далі всі операції здійснюються з рахунком клієнта. Завантаження може здійснюватися як наявними, так і з рахунка завантаження (як персоналізований електронний гаманець).

Основне призначення пластикових карток – здійснення безготівкових платежів у сфері товарів народного споживання і послуг. Для цього в торгових точках, які беруть участь у проекті, повинні бути встановлені платіжні термінали.

Одним із режимів роботи проекту обраний режим off-line. У цьому режимі обробка платіжних транзакцій здійснюється автономно, без встановлення зв'язку з банком - емітентом картки. Транзакції накопичуються протягом деякого часу в пам'яті термінала, а потім усі відразу передаються для подальшої обробки в систему. Передача може здійснюватися або по on-line каналу, або за допомогою спеціальних трансферних карток.

Передбачений і режим on-line. Деякі критичні операції (завантаження картки, розблокування й ін.) виконуються тільки в режимі on-line. При цьому встановлюється прямий зв'язок між терміналом і банком-емітентом. Або операція виконується безпосередньо в банку-емітенті. Такий режим забезпечує більш високу надійність, але при цьому має більш високу вартість.

Наступною ланкою в проекті є еквайри. Їхня основна задача – надавати комерсантам усі необхідні послуги, зокрема, здійснювати регулярне розвантаження терміналів, забезпечувати зворотний зв'язок (із системи в термінал передається деяка інформація), обчислювати результуючі платежі й ін. Зазвичай еквайром є банк, хоча ним може стати й інша організація.

Банк-емітент – організація, що здійснює випуск карток. Він здійснює замовлення карток у виробника, виконує персоналізацію (прив'язку картки до рахунка і до клієнта), укладає договори з клієнтами. Саме емітент відкриває картрахунки для клієнтів. Для всіх електронних гаманців, випущених даним банком, відкривається єдиний рахунок (пул), що містить усі кошти, внесені власниками електронних гаманців на картки.

Кожна картка має прив'язку до свого банку-емітента і до свого власника. При персоналізації і персоніфікації в картку записується код ЄДРПОУ емітента й ідентифікаційний код платника податків клієнта. Ця інформація використовується при формуванні транзакції в off-line режимі.

Основними елементами управління є процесингові центри. У кожній області відкривається регіональний процесинговий центр, що бере на обслуговування усі банки регіону (емітенти і еквайри). Його функції:

1.  Збір транзакцій від еквайрів.

2.  Сортування і розсилання їх емітентам.

3.  Передача керуючої інформації в систему та із системи.

4. Передача міжрегіональних транзакцій у головний процесинговий центр.

5.  Розрахунок нетто-позицій банків свого регіону.

Основним елементом управління всією системою в цілому є головний процесинговий центр. Для банків свого регіону (м. Київ) він виконує функції регіонального процесингового центру та функції по управлінню системою.

Заключні розрахунки між учасниками системи здійснюються наприкінці банківського дня за кліринговою схемою з використанням системи міжбанківських електронних платежів (СЕП). **КЛІРИНГ** (clearing) – механізм, що включає збирання, сортування, реконсиляцію та проведення взаємозаліку зустрічних вимог учасників платіжної системи, а також обчислення за кожним із них сумарного сальдо за визначений період часу між загальними обсягами вимог та зобов’язань (Про платіжні системи та переказ коштів в Україні //   
Закон України від 05.04.2001 № 2346-ІІІ).

Кліринг виконується головним процесинговим центром за участю інших елементів системи. Остаточні розрахунки за підсумками клірингу здійснює розрахунковий банк. Розрахунковий банк також виступає гарантом функціонування всієї системи в цілому. Розрахунковим банком є НБУ.

Системою передбачене обмеження деяких дій з метою підвищити надійність функціонування. Для цього існує набір лімітів (максимальна сума платежу, максимальна сума завантаження й ін.). Деякими лімітами керує розрахунковий банк, деякими – банки-емітенти або система (процесингові центри).

Основний платіжний документ у системі «Простір» – платіжна транзакція. Платіжна транзакція дозволяє за інформацією, що міститься в ній, установити власника картки, емітента картки, суму платежу й ін. необхідні параметри.

Відношення між учасниками системи «Простір» визначаються нормативно-правовою базою, яка розроблена спеціально для цього проекту. Кожен учасник при вступі в систему укладає договір, у якому обговорені права та обов'язки сторін. Для сумісності з міжнародними платіжними системами при розробці системи «Простір» використовувалися міжнародні стандарти.

### 1.4.2. Система захисту інформації.

Використання як інструменту смарт-картки відкриває більш широкі можливості для реалізації механізмів захисту. Частина криптографічних перетворень у такому разі може здійснюватися карткою незалежно.

У системі використовуються такі криптографічні методи:

1.  DES для формування кодів автентифікації на всіх рівнях нижче процесингових центрів (банки, термінали, картки).

2.  3-DES для шифрування інформації  на цих же рівнях.

3.  RSA на рівні розрахункового банку і між серверами баз даних і авторизації усередині банків.

Для функціонування симетричних алгоритмів шифрування необхідним компонентом є ключова система. У системі «Простір» вона багаторівнева і складається з трьох незалежних частин – транспортні ключі, системні ключі і банківські ключі.

Транспортні ключі використовуються тільки при емісії картки. У процесі емісії картка проходить через кілька елементів системи, де здійснюється ініціалізація, системна і банківська персоналізація і персоніфікація. Для захисту від несанкціонованого використання картки між цими процесами на час передачі картка блокується. Для блокування і розблокування використовуються транспортні ключі. При блокуванні в картку записується транспортний ключ, відомий тільки приймальній та передавальній стороні. Розблокувати картку можна тільки при наявності цього ключа.

Системні ключі призначені для ідентифікації системою картки при основних операціях (платіж, завантаження). У системі існує шість версій ключів, при цьому одночасно використовується тільки одна з них. Перехід на чергову версію відбувається або планово, або достроково (при підозрі на компрометацію).

Банківські ключі призначені для ідентифікації картки у банку-емітенті або транзакції при режимі off-line.

Системні і банківські ключі незалежні і не пов'язані один з одним. Єдиним елементом системи, що володіє як системними, так і банківськими ключами, є картка. В інших елементах системи ці ключі розділені.

Багаторівневість ключової системи полягає в наступному. На рівні головного процесингового центра формуються майстер-ключі, на основі яких розраховуються похідні ключі для всіх рівнів нижче. У системі виділяються наступні рівні: головний процесинговий центр (ГПЦ), регіональний процесинговий центр (РПЦ) і банки, термінали, пластикові картки. Кожен ієрархічно вищий рівень розраховує ключі для нижчих. Для цього використовується однобічна функція, що робить неможливим відновлення ключа вищого рівня. При цьому дуже імовірно, що похідний ключ залежить від індивідуальних параметрів елементу, для якого він розраховується. У такий спосіб значно розширюється множина ключів і підвищується стійкість.

При такій організації ключової схеми обмін інформації здійснюється за наступною схемою:

1. Ієрархічно вищий рівень має вихідний ключ, нижчий рівень – похідний;

2. При передачі інформації “зверху вниз” верхній рівень розраховує відповідний похідний ключ, на якому і здійснює передачу (підпис) інформації.

3. Передача “знизу нагору” здійснюється на похідному ключі, для розшифровки (перевірки ЦП) верхній рівень також розраховує відповідний похідний ключ.

4. При необхідності перед початком обміну сторони надсилають індивідуальну інформацією, від якої може залежати ключ.

Cистема захисту інформації у «Простір» реалізована на програмно-апаратному рівні. Елементами апаратури, що відповідають за безпеку, є:

1. Модуль безпеки термінала (МБТ). Являє собою спеціалізовану пластикову картку, що повинна бути постійно встановлена в терміналі (без цієї картки термінал не функціонує). Номера термінала і МБТ завжди збігаються (при першому включенні термінала в МБТ записується номер термінала) і різні для всіх терміналів у системі. МБТ містить:

- усі системні ключі;

- індивідуальний номер;

- загальну суму здійснених платежів електронними гаманцями по кожному емітенту з моменту введення термінала в експлуатацію. Значення даної комірки пам'яті може тільки зростати;

- інші параметри.

2. Швидкісний модуль безпеки (Hi-speed Secure Module). Представляє спеціалізовану плату для збереження ключів і виконання криптографічних перетворень (шифрування, дешифрування, формування і перевірка МАС-коду, генерація ключів). Установлюється на серверах системи «Простір» (у банках).

Крім цього, у системі присутні спеціальні картки доступу. Вони виконані на тих же носіях, що й інші і містять інформацію, що дозволяє здійснити авторизацію особи–власника картки. Для виконання більшості “керуючих” операцій у системі повинна виконуватися разова або постійна авторизація співробітника системи. При разовій авторизації картка співробітника вставляється в пристрій зчитування, до початку операції, при постійній – повинна знаходитися в ньому на протязі всієї операції. Інформація про співробітника системи, яка отримана з картки доступу, використовується при здійсненні транзакції. Картки доступу замовляються кожною організацією–учасником системи «Простір».

У системі ведеться архів проведення всіх операцій, в якому присутні отримані при авторизації дані. Тобто всі операції в системі авторизовані і в разі потреби можна з'ясувати дані про осіб що їх виконали.

Для своєчасного вилучення з обігу карток (у випадку втрати, крадіжки або виходу із системи емітента) передбачена система стоп-лістів. Перед кожною операцією з карткою здійснюється перевірка на наявність її в стоп-лістах. У разі виявлення картки в стоп-лісті вона блокується.

Для підвищення надійності функціонування всієї системи в цілому передбачена система лімітів – ряду обмежень для картки, термінала, банку. Якщо при проведенні платіжної операції порушується хоча б один із установлених лімітів, операція не виконується.

## 1.5. Порядок проведення роботи.

1. Ознайомитися з теоретичним матеріалом.

2. Переглянути презентацію про систему «Простір».

3. Пройти тестування у системі дистанційного навчання.

## 1.6. Зміст звіту.

1. Назва і мета роботи.

2. Короткі відомості з теорії.

3. Можливі загрози в системі «Простір».

5. Аналіз сильних і слабких сторін системи захисту.

6. Висновки по виконаній роботі.

## 1.7. Контрольні запитання.

1. Призначення Національної платіжної системи «Простір».

2. Основні функції банків-емітентів і банків-еквайрів.

3. Принципи функціонування системи стоп-лістів.

5. Основні недоліки системи захисту у НСМЕП.

6. Дайте характеристику носіїв конфіденційної інформації, що використовуються в системі.

7. Яким чином забезпечується конфіденційність даних картки?

8. Поясніть послідовність взаємодії власника картки та продавця товарів чи послуг та назвіть учасників цієї взаємодії.

9. Поясніть протокол взаємодії платіжного автомату та сервера банку.

10. Дайте характеристику системи ключів безпеки у «Простір».

11. Як повинен діяти клієнт у випадку загублення картки і чому?

## ДОДАТОК А

## Основні терміни проекту «Простір»

**Банк-еквайр** - банк - член системи «Простір», що проводить первинну обробку транзакцій та займається підключенням і обслуговуванням торгових підприємств, які приймають до сплати платіжні картки.

**Банк-емітент -** банк, що випускає в обіг (емітує) платіжні картки.

**Банківська платіжна картка (БПК) -** пластикова картка, засіб ідентифікації клієнта-власника картки, за допомогою якого клієнту надається можливість виконувати різні операції (платіж, одержання коштів і ін).

**Банкомат** - електронний пристрій, що може без участі оператора виконувати основні касові операції (видача коштів, переведення грошей з рахунка на рахунок і ін.) за допомогою БПК.

**Внутрішньобанківські транзакції** - транзакції, у яких відправником і одержувачем транзакції є один банк.

**Дебетова картка -** вид платіжної картки для оплати товарів і послуг в межах суми, яка є на рахунку.

**Завантаження (дозавантаження) картки -** внесення інформації на платіжну картку про наявність коштів.

**Картковий рахунок (картрахунок) -** банківський рахунок, управління яким може здійснюватися за допомогою БПК. На картковий рахунок зараховуються кошти, призначені для подальшого використання за допомогою БПК.

**Комерсант (торговець) -**  тут юридична особа, що здійснює свою діяльність у сфері продажу товарів і послуг, у т.ч. за допомогою БПК.

**Міжбанківські транзакції** – транзакції у який відправник і одержувач - різні банки.

**Міжрегіональні транзакції** - міжбанківські транзакцїі, у яких відправник і одержувач зв'язані з різними регіональними системами процесингу.

**Нетто-позиція** – сума, яку банк повинний одержати або відправити в систему за підсумками дня.

**Он-лайн (on-line) -** тип зв'язку між учасниками системи, при якому зв'язок підтримується в режимі реального часу.

**ПІН -** персональний ідентифікаційний номер, секретний код, відомий тільки власнику картки і необхідний для виконання операцій з карткою.

**Платіжна картка -** документ на носії електронної інформації у виді пластикової картки, що випускається кредитно-фінансовими установами. Документ дає можливість його пред'явнику одержати товари і послуги, у тому числі готівку через банкомати або банківські установи, і підтверджує особам, що надають товари і послуги, що оплата їхньої вартості буде здійснена з рахунків банку-емітента картки.

**Платіжна система -** сукупність нормативних, договірних, фінансових і інформаційно-технічних засобів і рішень учасників (банків, організацій, компаній), що регламентують свої взаємини про порядок використання БПК. Усі БПК, що належать до однієї платіжної системи, повинні мати ознаки, що дозволяють їх ідентифікувати з платіжною системою.

**Платіжний термінал -** електронний пристрій, за допомогою якого здійснюється авторизація платіжної картки й основні операції оплати вартості товарів і послуг.

**Процесинговий центр -** спеціалізований інформаційно-обчислювальний центр, що виконує збір, обробку, збереження і передачу кредитно-фінансовим установам інформації про необхідність переведення з рахунків власників БПК коштів за товари і послуги на рахунки осіб, що їх надають, а також виконує інші операції по обслуговуванню учасників системи електронних платежів, у якій використовуються пластикові картки .

**Розрахунковий банк -** банківська установа, у якій інші банки-учасники відкривають спеціальні рахунки для здійснення розрахунків за допомогою пластикових карток.

**Стоп-ліст генеральний** - стоп-ліст карток клієнтів, що формується процесинговим центром на підставі заявок від клієнтів про втрату (крадіжку) картки. Даний стоп-ліст забезпечує захист залишків на карткових рахунках клієнтів.

**Стоп-ліст термінальний** - стоп-ліст, що є підмножиною генерального стоп-ліста і призначений для завантаження в термінал.

**Транзакція** - електронний документ, що містить дані про переміщення засобів за допомогою БПК. Формується в ході взаємодії клієнта з терміналом або банкоматом. Включає інформацію про окрему операцію, що виконалася за допомогою БПК (завантаження, одержання готівки, платіж і ін.).

**Транзакція в режимs off-line (off-line транзакцiя)** - електронний документ, який визначає списання електронних грошей з картки (або картрахунку) на рахунок продавця товару або послуги. Передається в систему після завершення відповідної операції з карткою.

**Транзакция в режимі on-line (on-line транзакцiя)** - електронний документ, що визначає списання електронних грошей з картки (або картрахунку) на рахунок продавця товару або послуги або на рахунок картки з розрахункового рахунка клієнта. Передається в систему під час виконання відповідної операції з карткою.

**Учасник системи -** юридична (банк, комерсант) або фізична особа, що уклала певні договірні відносини з членами платіжної системи.

**Електронний гаманець -** вид платіжної картки для оплати товарів і послуг у розмірі, що не перевищує заздалегідь внесеної в банк суми шляхом безпосереднього списання коштів зі спеціального рахунка банку-емітента, спільного для всіх електронних гаманців даного емітента. У пам'яті картки знаходиться залишок (сальдо) від внесеної суми, який змінюється при кожній операції. Гаманець може бути анонімним або персоналізованим.

**Електронний чек -** вид платіжної картки для оплати товарів і послуг шляхом прямого списання коштів з карткового рахунка власника картки в розмірі, що не перевищує залишку на рахунку. При цьому в пам'яті картки також ведеться залишок, що дебетується (або кредитується) при кожній операції.

## ЛАБОРАТОРНА РОБОТА №2

**АНАЛІЗ ІНВЕСТИЦІЙ.**

## 2.1. Мета роботи.

# Зрозуміти суть дисконтування грошових потоків, усвідомити поняття «теперішня вартість» та «майбутня вартість». Навчитись порівнювати грошові потоки, які виникають у різні часові інтервали, з урахуванням факторів знецінення.

## 2.2. Методичні вказівки з організації самостійної роботи студентів.

При підготовці до лабораторної роботи необхідно:

- вивчити і засвоїти основні поняття і визначення підрозділу 1.4;

- зрозуміти теорію дисконтування грошових потоків;

- ознайомитись із функціями Microsoft Excel для аналізу інвестицій.

## 2.3. Опис лабораторної установки.

Використовується комп’ютер із процесором не нижче ніж Intel 486. У якості програмного забезпечення для виконання роботи використовуються браузер та пакет MS Office.

## 2.4. Теоретичні відомості, приклади їх використання на практиці та задачі для самостійного розв’язування.

# Розрахунок теперішньої вартості

Для оцінки руху фінансових потоків у часі застосовують формули фінансової математики, до яких належить і розрахунок теперішньої вартості чи метод дисконтування грошових потоків. Дисконтування є оберненою операцією до розрахунку складних відсотків.

Введемо позначення:

FV – майбутня вартість,

PV – теперішня вартість,

r – ставка дисконтування,

n – кількість періодів.

Тоді формула для розрахунку дисконтування грошового потоку має вигляд:

Наприклад, якщо через рік планується отримати 1000 грн. при ставці 15% річних, то вкласти потрібно 869, 57 грн.

Для аналізу інвестицій використовуються такі функції Microsoft Excel: БС, КПЕР, ПЛТ, ПС, СТАВКА. Аргументи цих функцій наведено у табл. 1.

Таблиця 1. Аргументи функцій для аналізу інвестицій.

|  |  |  |
| --- | --- | --- |
| Аргумент | Назва | Опис |
| ПС | Теперішня вартість | Сума, яка на даний момент рівноцінна ряду майбутніх виплат |
| БС | Майбутня вартість | Сума, яка буде досягнена після останньої виплати |
| ПЛТ | Виплата | Сума, яка виплачується у кожний період і не змінюється протягом усього часу виплати |
| КПЕР | Загальна кількість періодів виплати | Розраховується як добуток кількості років інвестиції на кількість виплат за рік. Наприклад, кредит виданий на 5 років з виплатою двічі на рік. Кількість періодів: 5⋅2=10. |
| СТАВКА | Відсоткова ставка за період | Розраховується як відсоткова ставка за рік, поділена на кількість виплат за рік. Наприклад, кредит виданий під 10% річних із щоквартальними виплатами. Відсоткова ставка за період: 10:4=2,5% |
| ТИП | Вид ануїтету | Набуває значень 0 або 1. 0 означає, що виплата здійснюється вкінці періоду, 1 – на початку. |

Фінансові функції пов’язані з інтервалами виплат. Ануїтет – це ряд постійних виплат протягом періоду. Наприклад, кредит на купівлю автомобіля є ануїтетом. У функціях, пов’язаних з ануїтетами, гроші, які виплачуються, подають від’ємними числами, а отримані гроші – додатними. Наприклад, депозит у банк на суму 1000 грн. подається аргументом -1000 для вкладника і аргументом 1000 для банку.

Функція **ПС** є одним із поширених способів оцінки привабливості тривалих вкладень, вона обчислює теперішню вартість ряду рівних за величиною періодичних виплат або однієї виплати.

Синтаксис функції **ПС (СТАВКА, КПЕР, ПЛТ, БС, ТИП)**

Для обчислення теперішньої вартості ряду виплат використовується аргумент ПЛТ. Для обчислення теперішньої вартості однієї виплати використовується аргумент БС. Для вкладу з першим внеском та періодичними виплатами використовуються обидва ці аргументи.

**Приклад 1. Визначення теперішньої вартості ряду періодичних виплат.**

Існує два варіанти вкладання грошей з метою отримати 5000 грн. протягом 2,5 років:

* укласти угоду, яка щопівроку повертає 1000 грн. протягом 2,5 років; для цього потрібно вкласти 4000 грн.;
* вкласти деяку суму в банк під 8% річних з виплатами (нам) щопівроку 1000 грн.

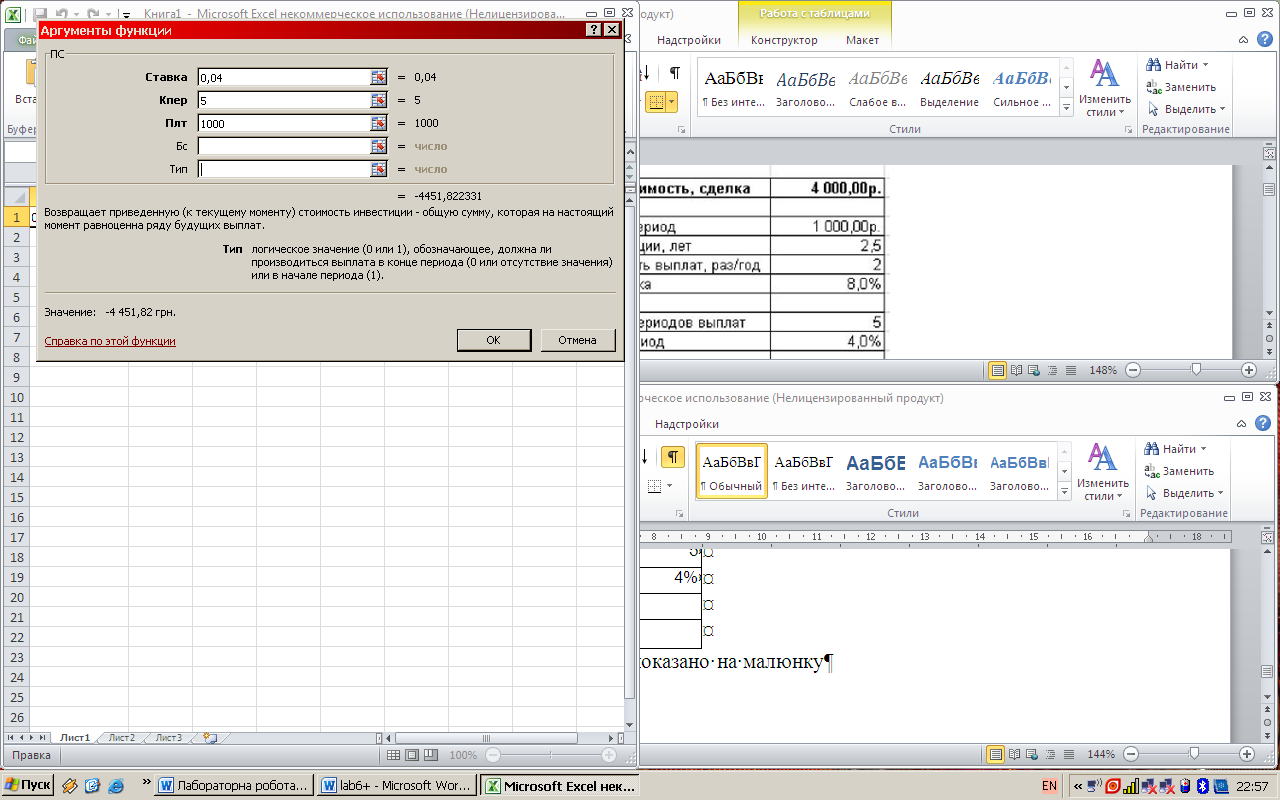
Визначте, який із варіантів вкладання грошей є більш вигідним.

**Розв’язання.**

1. Внесіть дані задачі на лист Microsoft Excel.

|  |  |
| --- | --- |
| **Поточна вартість, угода** | **4 000 грн.** |
|  |  |
| Виплата за період | 1 000 грн. |
| Термін інвестиції, років | 2,5 |
| Періодичність виплат, раз/рік | 2 |
| Річна ставка | 8% |
|  |  |
| Кількість періодів виплат | 5 |
| Ставка за період | 4% |
|  |  |
| **Поточна вартість, банк** |  |

1. Встановіть аргументи функції ПС, як показано на малюнку



Результатом функції є число -4451. Отже, у банк потрібно вкласти 4451 грн., а угода коштує 4000 грн., тому вигідніше укласти угоду.

**Задача 2. Визначення теперішньої вартості одномоментної виплати**

Визначити, який варіант вкладення грошей є більш вигідним, щоб отримати 5000 грн. за 2,5 роки:

* укласти угоду за 4000 грн.;
* вкласти певну суму на рахунок у банку під 8% річних з нарахуванням відсотків кожних півроку.

Для розв’язання задачі використайте функцію ПС з аргументом БС.

**Задачі для самостійного розв’язування**

1. Фірмі знадобиться 50000 грн. через 3 роки. Яку суму потрібно покласти на депозит, якщо річна ставка становить 12%?
2. Визначте поточну вартість щомісячних платежів по 1000 грн. протягом 5 років, якщо процентна ставка 12% річних.
3. Визначити, який варіант є більш вигідним для оплати за будинок: заплатити відразу 99000 грн. чи платити по кредиту 940 грн. щомісячно протягом 15 років із платою за кредит 8% річних.

# Розрахунок чистої теперішньої вартості.

Функція ЧПС обчислює величину чистої теперішньої вартості інвестиції, використовуючи ставку дисконтування та послідовність майбутніх виплат (від’ємні значення) та надходжень (додатні значення).

Синтаксис: ЧПС (Ставка, Значення1, [Значення2], …), де

Ставка – ставка дисконтування за період (обов’язковий аргумент);

Значення1, Значення2, … Аргумент Значення1 обов’язковий, інші – необов’язкові Допускається від 1 до 254 аргументів, які подають виплати та надходження. Аргументи Значення1, Значення2 повинні бути рівномірно розподілені у часі, виплати повинні здійснюватись вкінці кожного періоду. Для функції ЧПС важливий порядок платежів, тому їх не можна міняти місцями.

Інвестиція, значення якої обчислює функція ЧПС, починається за один період до дати внеску Значення1 і завершується з останнім внеском у списку. Якщо перший внесок припадає на початок першого періоду, його значення потрібно додати до результату функції ЧПС, але не включати до списку аргументів.

Якщо n – кількість грошових потоків у списку значень, формула для функції ЧПС має вигляд:

Відмінності між функціями ПС і ЧПС:

* функція ПС допускає, щоб платежі відбувались як на початку, так і вкінці періоду, тоді як у функції ЧПС платежі відбуваються вкінці періоду;
* у функції ЧПС внески можуть змінюватись, тоді як у функції ПС внески є постійними протягом усього періоду інвестиції.

**Приклад 1.**

Інвестиції у проект до кінця першого року його реалізації становлять 10000 грн. У наступні три роки очікуються річні доходи по проекту 30000 грн., 42000 грн., 68000 грн. Витрати на залучення капіталу – 10% річних. Розрахуйте чисту поточну вартість проекту.

Розв’язання.

Оскільки інвестиція 10000 грн. відбувається вкінці першого періоду, її потрібно внести до списку аргументів функції ЧПС.

ЧПС (10%; -10000; 30000; 42000; 68000) = 93702 грн.

**Задачі для самостійного розв’язування.**

1. Затрати по проекту у початковий момент його реалізації становлять 37000 грн. (*зверніть увагу, що ця витрата належить до теперішнього моменту, тому дисконтувати її не потрібно*), а доходи за перших 5 років: 18000, 19000, 20000, 23000, 24000. На шостий рік очікується збиток 5000 грн. Ціна капіталу 8% річних. Розрахуйте чисту поточну вартість проекту.
2. Визначте ефективність інвестиції розміром 200000 грн, якщо очікувані щомісячні доходи за перші 5 місяців становлять 20000 грн, 40000 грн., 50000 грн., 80000 грн., 100000 грн. Витрати на залучення капіталу становлять 13,5% річних.

**Лабораторна робота №3**

**ДОСЛІДЖЕННЯ ЦЕНТРА УПРАВЛІННЯ І СЕРТИФІКАЦІЇ КЛЮЧІВ БАНКУ**

**3.1. Мета роботи.**

Одержання практичних умінь і вивчення основних принципів роботи центра управління ключами (ЦУК) – важливого елемента сучасної банківської системи захисту інформації.

## 3.2. Методичні вказівки з організації самостійної роботи студентів.

При підготовці до лабораторної роботи необхідно:

- засвоїти лекційний матеріал, який стосується ключів для захисту банківської інформації;

- вивчити і засвоїти основні поняття і визначення підрозділу 1.4;

- підготувати відповіді на питання, наведені в методичних вказівках.

## 3.3. Опис лабораторної установки.

Використовується комп’ютер із процесором не нижче ніж Intel 486. У якості програмного забезпечення для виконання роботи використовується «Центр управління ключами».

## 3.4. Теоретичні відомості.

Необхідні показники конфіденційності, справжності, цілісності, причетності, а також захищеності від несанкціонованого доступу (НСД) у будь-якій системі захисту забезпечується тільки в тому випадку, якщо особисті ключі залишаються в таємниці і недоступні криптоаналитику. При цих умовах для розкриття системи криптоаналитик повинний здійснити атаку на криптосистему (факторизация модуля, рішення дискретного логарифма в системах класу Ель - Гамаля й ін.). Якщо особистий ключ скомпрометований, то злом системи захисту здійснюється миттєво. Для цього досить увести правильно паролі і ключі. У широкому змісті під компрометацією ключів і паролів розуміється факт протиправного розголошення ключів і паролів стороннім особам. У спеціальному наказі по кожному підприємству визначаються особи, що допущені до роботи з ключами. Особистий ключ - виключна власність користувача, яка не може бути переданий нікому, включаючи прямих начальників.

Для рішення задач генерації, розподілу і т.д. ключів створюється спеціальна служба керування ключовими структурами. Крім того в системі повинний бути створений центр управління ключами (ЦУК). При цьому під керуванням ключовими структурами розуміється сукупність процедур, алгоритмів у змісті прийняття рішень, спрямованих на генерацію, сертифікацію, розподіл, передачу, прийом, запис, збереження, використання, знищення ключових даних, а також відновлення їх у випадку компрометації (пряма зміна скомпрометованих ключів). Можна сформулювати наступні вимоги до ключових систем:

   ключова система повинна бути стійкою до компрометації ключів у будь-якого числа кореспондентів мережі, тобто компрометації не повинні впливати на безпечну роботу учасників платіжної системи з нескомпрометованими ключами;

* ключова система повинна дозволяти швидке відновлення при будь-якому числі компрометацій;
* ключова система повинна передбачати як можна менше число ключів, що підлягають охороні організаційними заходами користувачів;
* носії ключової інформації повинні забезпечувати високий ступінь захисту їх від копіювання;
* генерація ключів електронного цифрового підпису (ЕЦП) повинна виконуватися власниками підпису, реєстрація, облік і розсилання відкритих компонентів ключів ЕЦП повинна вироблятися централізовано адміністраторами безпеки на регіональному і міжрегіональному рівнях із забезпеченням неможливості їхньої фальсифікації і підміни.

Системи керування ключами повинні бути в максимальному ступені автоматизовані і припускати мінімальну участь кінцевих користувачів у процесах керування ключами (підтримка баз відкритих ключів, зміна ключів при позаштатних ситуаціях і т.п.).

**Генерація ключів.**

Як симетричні, так і несиметричні ключі повинні генеруватися за допомогою випадкових процесів. Для забезпечення надійності застосовуються комбіновані схеми, у яких використовуються як випадкові, так і псевдовипадкові процеси з необхідними властивостями. Ключі і ключові параметри повинні задовольняти вимогам :

          - випадковості їхньої появи;

          - рівноймовірності;

          - незалежності ключів і символів між собою;

          - неоднорідності.

Як конкретні алгоритми можуть використовуватися симетричні алгоритми шифрування (ДСТУ 28.147-89, DES) і несиметричний алгоритм RSA.

Вимоги до ключів відрізняються в залежності від криптосистеми. Для ДСТУ 28.147-89 необхідно забезпечити генерацію секретного ключа (СК) довжиною 256 біт і довгострокового ключа (ДК) довжиною 512 біт.

У RSA-системах ключові параметри Pj,Qj повинні вибиратися випадково. Генерують початкові наближення NPj і NQj, починаючи з яких формується просте число. Випадково генерується Ek і перевіряється на взаємну простоту з функцією Эйлера від Nj , тобто (Ek,  (Nj)) =1. Далі з порівняння Ek \* Dk  1( mod (Nj)) знаходиться другий ключ Dk.

Для генерації ключів створюються спеціальні комплекси. Задача генерації може покладатися як на спеціальний центр, так і безпосередньо на користувача. Рекомендується ключі генерувати особисто. Для забезпечення високого рівня захисту необхідно застосовувати централізовані і децентралізовані принципи генерації ключа, сутність яких полягає в застосуванні багаторівневої ключової системи.

Поширення ключів повинне здійснюватися за допомогою використання спроможних протоколів. Спроможним називається протокол керування ключами, що забезпечує їхню гарантовану конфіденційність, дійсність, цілісність і вірогідність на всіх етапах життєвого циклу ключа.

Спроможні протоколи можуть бути реалізовані з використанням як симетричних, так і несиметричних систем. Але у кожному протоколі повинно застосовуватися кілька рівнів ключів. Система повинна бути двох- чи трьох-рівневою.

          1 рівень. Головні ключі.

          2 рівень. Робочі ключі.

          3 рівень. Сеансові ключі.

Головні ключі генеруються центром управління (ЦУК). Вони, як правило є спрямованими, тобто призначені для роботи центра з одним окремим кореспондентом і призначені винятково для шифрування робочих ключів.

Робочий ключ повинен генеруватися кореспондентом за принципом “сам собі” і не виходити з меж особистого володіння. Використовується для шифрування і підпису повідомлень, даних, програм і т.д. У ряді випадків робочі ключі використовуються тільки для шифрування сеансовых ключів.

Сеансові ключі виробляються користувачем на кожен сеанс, використовуються для шифрування повідомлень, даних, програм.

**Приклад спроможних протоколів у симетричній системі.**

Нехай попередньо абонентам доставлений ключ КАВ. Протокол вироблення сеансових ключів виконується із забезпеченням цілісності, справжності і конфіденційності.

          1) ВА: В, СЧ i , “Прошу зв'язок”                    ( 1 )

           СЧ i  - випадкове число.

          2) А по ідентифікатору В визначає і вибирає головний ключ КАВ і формує відповідь.

          АВ : А, ЕКав ( f(СЧ i ),CЧ j , А, Кс  )

           f ( СЧ i ) - функція ( можливо необоротна ) від СЧ i.

Важливо в процесі обміну бути упевненим, що процес цілісний і ніхто в нього не включився. Для цього на кроці 1 кореспондент В виробляє випадкове число і посилає його А в запиті. А перетворить його за законом f , тільки їм обом відомим шляхом і повертає назад. В, одержавши СЧ i  , установлює, що процес цілісний.

          3) ВА : В, ЕКс ( f(СЧ j ), B )

Якщо протокол неспроможний, то, незважаючи на те, що застосовується стійка криптосистема, у цілому система може бути легко зламана за рахунок протоколу.

**Приклад протоколу з відкритими ключами.**

Нехай у системі застосовується алгоритм із відкритим ключем RSA. Для А і В вироблені ключі Еа й Ев. До Еа й Ев  ставиться вимога, щоб на етапі розсилання були забезпечені їхня цілісність і дійсність.

1) ВА : В, Еа ( Счi , В )                                       ( 2 )

В виробляє випадкове число СЧi  і направленно шифрує його разом зі своїм ідентифікатором (дешифрувати його може тільки А своїм особистим ключем Da )

2) А дешифрує повідомлення, порівнює В шифроване з В відкритим, щоб довідатися, чи була модифікація. Потім виробляє СЧ j, перетворить його (f(СЧ j )) і направлено шифрує.

АВ : А, ЕВ (f(СЧ i ),CЧ j , А, Кс)

3) В с допомогою DB дешифрує повідомлення. На основі аналізу СЧ i  засвідчується в дійсності повідомлення, виділяє сеансовий ключ зв'язку Кс

          ВА : В, ЕКс ( f(СЧ j ), В )                                        ( 3 )

А, використовуючи раніше посланий Кс , дешифрує повідомлення, по СЧ i встановлює цілісність і , порівнюючи В, визначає дійсність адресата.

Власне кажучи А переконується в цілісності, дійсності і конфіденційності ключа. В надалі використовує Кс для шифрування інформації.

**Стислі практичні відомості**:

1 ПРИЗНАЧЕННЯ ПРОГРАМНОГО КОМПЛЕКСУ

Програмний комплекс «Щит» призначений для визначення списку відділень і віддалених робочих місць, генерації сертифікаційних дискет, сертифікації відкритих ключів та виконання інших функцій центра управління ключами (ЦУК), який є важливим елементом сучасних систем захисту інформації.

ІНСТАЛЯЦІЯ ПРОГРАМИ

## Склад інсталяційного пакета

Перед запуском програми перевірте вміст каталогу інсталяційного пакета центра керування ключами. У каталозі повинні бути підкаталоги і файли:

InstCntr.exe               ‑ головна програма інсталяції ЦУК;

Shld32.dll                 ‑ бібліотека, що динамічно завантажується;

Cryppass.lst               ‑ допоміжний файл;

Install.ini                   ‑ файл ініціалізації;

Pass.lst                      ‑ файл із паролем інсталяції ЦУК і його відділень;

Каталог Inst512        ‑ каталог, що містить компоненти необхідні для інсталяції ЦУК. Каталог повинен містити наступні файли:

bank.exe                    ‑ файл, необхідний для інсталяції ЦУК;

Keygen.exe               ‑ файл, необхідний для інсталяції ЦУК;

Install.bin                  ‑ файл, необхідний для інсталяції ЦУК;

Label.bin                   ‑ файл, необхідний для інсталяції ЦУК;

## Інсталяція ЦУК

При інсталяції центра можна вибрати один з двох режимів.

Режим 1. Інсталяція без прив'язки. У цьому випадку інстальовану програму можна буде переносити на інший комп'ютер при збереженні каталогу, куди встановлена програма.

Режим 2. Інсталяція з прив'язкою. Перенос на інший комп'ютер без переінсталяції не допускається.

Для завдання режиму прив'язки відкрийте файл Install.ini з інсталяційного пакета й установіть параметр LINK =0 при інсталяції без прив'язки і LINK =1 при інсталяції з прив'язкою.

Для інсталяції центра управління ключами запустіть програму InstCntr.exe з пакета інсталяції. На запит «Введите пароль инсталляции» уведіть пароль для інсталяції центра (перший ключ зі списку паролів інсталяції у файлі pass.lst).

Заповніть поля:

   Глобальное имя

   Локальное имя

   Ответственное лицо

   Пароль входа в программу ЦУК и его подтверждение

Виберіть версію програми (512), яку необхідно инсталювати і натисніть на кнопку «Вперед» .

Укажіть місце установки компонентів програми:

   Каталоги для установки програми («Место установки»);

   Каталог відкритих робочих ключів;

   Каталог відкритих ключів сертифікації;

   Вхідний каталог для ключів, що надсилаються на сертифікацію («Входной каталог»);

   Вихідний каталог для сертифікованих ключів («Выходной каталог»);

   Каталог для неопрацьованих файлів («Каталог ошибок»);

   Каталог журналу №1

   Каталог журналу №2

Натисніть на кнопку «Вперед».

Виберіть номер дисковода, на якому розташовується ключ сертификаци,  і шлях до робочого ключа на дискеті.

|  |
| --- |
| **Увага**!!! Використання твердого диска для збереження конфіденційних ключів сертифікації не допускається! |

Укажіть термін дії ключа сертифікації і термін дії робочих ключів. Терміни дій визначаються спеціальною інструкцією. Натисніть на кнопку «Готово» і дочекайтеся закінчення інсталяції (Повідомлення «Инсталляция завершена успешно»).

Робота з ЦУК

## Запуск програми

Перед запуском програми перевірте вміст каталогу, де встановлений центр (нижче робочий каталог). У робочому каталозі  повинні бути підкаталоги:

In                              каталог для одержуваних файлів

Out                            каталог для файлів, що відсилаються

Log                           каталог для файлу протоколу

Workbase                  каталог для відкритих ключів

Inst0                          каталог для інсталятора центра більш низького рівня

Bad                           каталог для запису файлів, оброблених з помилкою

Public                        каталог для відкритих ключів сертифікації.

Імена каталогів можуть відрізнятися, якщо при інсталяції задані відмінні від прийнятих за замовчуванням імена.

У робочому каталозі повинні бути файли:

bank.exe                    -основна програма;

bank.lg1                    -файл протоколу;

config.cfg                  -файл конфігурації;

cryppass.lst               -допоміжний файл.

label.bin                    -допоміжний файл;

Shld32.dll

|  |
| --- |
| **Увага**!!! Коректування файлів робочого каталогу не допускається! У противному випадку буде потрібно переінсталяція центра! |

1.      Підготуйте 2+i чистих дискет, де i - кількість відділень клієнтів

2.      Запустіть програму bank.exe.

3.      При запиті програми введіть  пароль, установлений при інсталяції.

4.      Введіть задані програмою символи, якщо цього вимагає програма.

5.      При запиті програми потрібно вставити дискету і потім підписати її назву:  
 перша - сертифікаційна дискета;

 друга - конфіденційна (робоча) дискета арбітра.

Перед створенням другої дискети програма запросить встановити пароль доступу до робочого ключа арбітра.

6.      Перевірте вміст дискет.

Сертифікаційна дискета повинна містити файл Psertif.key.

Конфіденційна дискета повинна містити каталог для конфіденційних ключів, заданий при інсталяції (за замовчуванням кореневої). У каталозі повинний бути файл  Private.key.

## Список відділень і робочих місць

### Створення списку відділень і робочих місць відділення.

1.      Запустити програму bank.exe, якщо вона не була запущена раніше.

2.      Натиснути кнопку «**Добавить»** і по запиту програми ввести пароль для відділення зі списку паролів інсталяції Pass.lst (паролі задаються розроблювачем).

3.       Ввести необхідну інформацію за запитам програми.

4.       Виділити рядок з відділенням, створеним у пунктах 1-3.

5.       Натиснути кнопку «**Рабочие места».**

6.      У діалоговому вікні вибрати команду «**Добавить»**.

По запиту програми ввести необхідну інформацію для чергового робочого місця. Допускається створення робочих місць двох типів:

     с правом підпису і шифрування;

     тільки з правом підпису.

7.       Виконати пункти 5,6 для всіх робочих місць.

8.      Закрити діалогове вікно для створення робочих місць.

9.      Пункти 2 - 9 виконати для усіх відділень, для яких у даному сеансі планується генерація ключів.

### Створення робочих місць для ЦУК

Допускається створення робочих місць двох типів:

 із правом підпису і шифрування;

 тільки з правом підпису.

1.      Запустити програму bank.exe, якщо вона не була запущена раніше.

2.      Вибрати в списку відділень рядок, у якому знаходиться глобальне ім'я ЦУК.

3.      Натиснути кнопку «**Рабочие места»** (чи двічі клацнути мишею на рядку списку, чи натиснути «Enter» знаходячись у списку, чи вибрати пункт меню «**Клиенты\Рабочие места**»).

4.      Натиснути кнопку «**Добавить»** (чи натиснути клавішу «Insert»).

5.      Задати необхідну інформацію про робоче місце, що додається.

6.      Виконати пункти 4 - 5 для всіх робочих місць.

7.      Після додавання всіх робочих місць натиснути кнопку «**Закрыть»**.

8.      У випадку помилки при створенні робочих місць, робоче місце можна видалити командою **«Удалить»** у діалоговому вікні даного відділення.

### Створення і зміна робочої дискети для робочих місць центрального відділення

1.      Підготувати чисті дискети для кожного робочого місця центрального відділення.

2.      Виділити рядок з інформацією про центральне відділення;

3.      Натиснути кнопку«**Рабочие места».**

4.      Вибрати рядок з інформацією про робоче місце відділення;

5.      Натиснути кнопку **«Сгенерировать»** для генерації робочої дискети

6.      По запиту вказати дату введення ключа в дію і термін дії ключа.

7.      По запиту програми введіть пароль доступу.

8.      Після генерації ключа підпишіть дискету  «Робочий ключ. ФИО. Термін дії ключа\_\_\_\_\_ »

Виконати пункти 4 - 8 для всіх робочих місць, для яких потрібно згенерувати ключі.

### Створення генераторів ключів для відділень.

Для кожного відділення повинна бути створена дискета з генератором ключів. Для створення дискети необхідно виконати наступні дії.

1.  Приготувати чисті дискети: одну для кожного відділення .

2.  Виділити рядок з інформацією про відділення, для якого створюється дискета.

3. Натиснути кнопку «**Создать дискету**»(чи задати команду через меню «**Отделение\Создать дискету**»).

4.  По запиту програми ввести необхідні дані.

5.  Підписати на дискеті її назву: «Генератор ключів для відділення \_\_\_\_».

6.  Повторити пункти 2-5 для усіх відділень.

Дискета після створення повинна містити:

каталог KEYGEN з файлами

keygen.exe,

label.bin

і файли:

SERTIF.kbi

Psertif.key

Sertif.key

PUBLIC.kbi

Public.key

STATION.CNF

clt.dat

cryppass.lst

### Видалення робочого місця відділення.

1.  Виділити рядок з назвою відділення, з якого потрібно видалити робоче місце;

2.  Натисніть кнопку«**Рабочие места».**

3.  Виділите рядок з інформацією про робоче місце, що видаляється.

4.  Виберіть команду **«Удалить».** Після підтвердження запиту робоче місце буде видалено.

### Видалення відділення.

Перед видаленням відділення повинні бути вилучені всі його робочі місця.

1.  Виділити рядок з інформацією про відділення, що видаляється;

2.  Вибрати режим **«Удалить».** Після підтвердження запиту видаляється виділене відділення.

|  |
| --- |
| **Увага!!!** Не допускається видалення центрального відділення! |

### Пересилання сертифікатів

Пересилання сертифікатів, як правило, виконується при необхідності повторного пересилання сертифікатів у яке-небудь відділення;

Для пересилання сертифікатів необхідно:

1.  Виділити рядок з інформацією про відділення.

2.  Натиснути кнопку **«Отправить ключи».**

При успішному виконанні операції у вихідному каталозі (OUT) з'являються файли сертифікатів <глобальне\_ім'я\_відділення>.KB1 (для діючих ключів) і <глобальне\_ім'я\_відділення>.KB2 (для нових ключів).

### Роздруківка ключів

Роздруківку можна виконати тільки тоді, коли в даного відділення є діючі робочі ключі.

Роздруківка ключів може бути виконана на принтер або у файл. Якщо планується використовувати принтер, його необхідно підготувати.

1.  Вибрати відділення в списку і натиснути кнопку **«Печать».**

2.  Переглянути текст для друку.

3.  Натиснути на клавішу **«Печать»** для друку на принтер, чи поставити галочку біля **«Печать в файл»** і натиснути клавішу **«Печать»** для збереженні документа у файлі.

4.  Вказати ім'я файлу для запису ключа.

## 4.3 Планова зміна ключів відділень

Планова зміна ключів виконується при установці системи та при закінченні терміну дії робочих ключів. При плановій зміні ключів у вхідному каталозі (IN) повинні знаходитися файли <глобальне\_ім'я\_відділення>.KSG із ключами відділень, прислані від генератора ключів.

Для планової зміни ключів необхідно ввійти в пункт меню «**Смена ключей|Плановая смена ключей клиентов»** і вказати дату введення ключа в дію, зазначена дата повинна бути не менше поточної. Якщо дата дорівнює поточній, то ключі вводяться в дію негайно.

Виконати запити програми.

При успішному виконанні операції у вихідному каталозі (OUT) з'являються файли сертифікатів <глобальне\_ім'я\_відділення>.KB1 (для діючих ключів) і <глобальне\_ім'я\_відділення >.KB2 (для нових ключів). У каталозі можуть бути додаткові файли.

## Аварійна зміна ключів відділень

Аварійна зміна ключів виконується при компрометації робочого ключа користувача або при виході з ладу дискети з робочим ключем. При аварійній зміні ключів у вхідному каталозі (IN) повинні знаходитися файли <глобальне\_ім'я>.KSG із ключем (ключами) даного користувача.

Для аварійної зміни ключів необхідно ввійти в пункт меню «**Смена ключей| Аварийная смена ключей клиентов»**.

При успішному виконанні операції у вихідному каталозі (OUT) з'являються файли сертифікатів <глобальне\_ім'я\_відділення>.KB1 (для діючих ключів) і <глобальне\_ім'я\_відділення>.KB2 (для нових ключів).

## Зміна ключа сертифікації

Зміна ключа сертифікації ЦУК виконується:

   при виникненні підозри на компрометацію сертифікаційного ключа;

   при закінченні терміну дії сертифікаційного ключа;

   за вказівкою служби безпеки регіонального керування.

Для зміни ключа сертифікації необхідно виконати наступні дії.

1.  Підготувати порожню відформатовану дискету.

2.  Ввійти в пункт меню «**Смена ключей|Смена ключа сертификации».**

3.  Підтвердити необхідність зміни ключа сертифікації, при виникненні запиту ввести символи, що задаються програмою.

4.  Після успішного завершення зміни ключа сертифікації підписати на сформованій дискеті: «Сертифікаційна дискета».

Після зміни сертифікаційного ключа ЦУК необхідно:

1.  Створити генератори ключів для усіх відділень.

|  |
| --- |
| **Увага!!!** Зміна відкритих ключів сертифікації в базі даних генератора ключів відбудеться автоматично після чергового прийому сертифікованих робочих ключів робочих станцій цього відділення |

## Зміна робочого ключа арбітра

Зміна робочого ключа арбітра виконується:

   при виникненні підозр на компрометацію ключа;

   за рішенням служби безпеки регіонального керування.

Для зміни ключа необхідно виконати такі дії.

1.  Підготувати порожню відформатовану дискету.

2.  Ввійти в  пункт меню «**Смена ключей|Смена рабочего ключа арбитра».**

3.  Підтвердити необхідність зміни ключа арбітра, при виникненні запиту ввести символи, що задаються програмою.

4.  Після успішного завершення зміни ключа підписати сформовану дискету, як «Конфіденційна дискета арбітра».

При успішному виконанні операції у вихідному каталозі (OUT) з'являються файли сертифікатів <глобальне\_ім'я\_відділення>.KB1 для усіх відділень.

## Сервісні операції

### Зміна пароля входу в програму

1.  Ввійти в пункт меню «Сервис/ Смена пароля входа»

2.  Виконати запити програми

### Створення копії дискет.

#### Копія робочої дискети .

1.  Ввійти в пункт меню «Сервис|Копия рабочей дискеты»;

2.  Підготувати чисту дискету;

3.  Задати пароль і прізвище відповідальної особи;

4.  Відповісти на запити програми.

#### Копія сертифікаційної  дискети.

1.  Ввійти в пункт меню «Сервис|Копия сертификационной дискеты»;

2.  Підготувати чисту дискету;

3.  Відповісти на запити програми.

# 

# 5 Інсталяція робочого місця відділення

Перед запуском програми перевірити вміст інсталяційного пакету. У пакеті  повинні бути файли:

InstWork.exe – головна програма

INSTALL.ini – файл конфігурації

Shld32.dll – бібліотека, що динамічно завантажується

Для інсталяції робочого місця:

1. Запустити програму InstWork.exe

2. У вікні ввести пароль, інсталяції, виданий у ЦУК разом з інсталяційним пакетом.

3. Вибрати  дисковод, уставити дискету з робочим ключем, натиснути клавішу «Вперед».

4. Указати:

 відповідальну особу;

 папку інсталяції файлів робочого місця;

 місце розташування робочих ключів відділення (Цю інформацію одержати в адміністратора безпеки відділення).

5. Натисніть на кнопку «Вперед» і дочекайтеся закінчення інсталяції (повідомлення «Инсталляция завершена успешно»).

Інсталяція генератора ключей

Перед запуском програми перевірити вміст інсталяційного пакету. У пакеті  повинні бути файли:

InstClient.exe    ‑ головна програма інсталяції генератора ключей (ГК);

Shld32.dll         ‑ бібліотека, що динамічно завантажується;

Install.ini           ‑ файл конфігурації;

Keygen.lnk       ‑ ярлик для запуску програми ГК.

Для інсталяції генератора ключей:

1.  Запустити програму інсталяції InstClient.exe.

2.  За вимогою програми ввести пароль відділення, зазначений з інформацією про відділення в ЦУК; задайте номер дисковода з дискетою генератора ключів. Натисніть на кнопку «Вперед».

3.  Указати глобальне ім'я відділення, ім'я відповідальної особи, задати пароль входу в програму генератора ключів. Натиснути на кнопку «Вперед».

4.  Указати директорії розташування програми ГК і його компонентів. Указати номер дисковода для робочих дискет робочих місць. Натиснути на кнопку «Готово».

5.  Дочекатися закінчення інсталяції.

Робота з генератором ключів

Запуск програми

Перед запуском програми необхідно перевірити вміст каталогу, де встановлений ГК. У каталозі  повинні бути підкаталоги:

In                              ‑ каталог для файлів, що відсилаються

Out                            ‑ каталог для одержуваних файлів

Log                           ‑ каталог для копії файлу протоколу

Workbase                  ‑ каталог для відкритих ключів

Bad                           ‑ каталог для запису файлів, опрацьованих з помилкою

Імена каталогів можуть відрізнятися, якщо при інсталяції задані відмінні від прийнятих за замовчуванням назви каталогів

У робочому каталозі повинні бути файли:

clt.dat                        ‑ список користувачів

config.cfg                  ‑ файл конфігурації;

cryppass.lst               ‑ допоміжний файл.

keygen.lg1                ‑ файл протоколу

keygen.lnk                ‑ ярлик запуску ГК;

label.bin                    ‑ допоміжний файл;

Shld32.dll                 ‑ допоміжний файл.

|  |
| --- |
| **Увага**!!! Коректування файлів робочого каталогу не допускається! У протилежному випадку буде потрібно переінсталяція генератора! |
| **Увага**!!! Програма запускається файлом KEYGEN.LNK з головної директорії ГК. Перед запуском програми необхідно сконфігурувати ярлик keygen.lnk у такий спосіб. Указати файл, що запускається, A:\Keygen\keygen.exe чи B: \Keygen\keygen.exe у залежності від дисковода, що використовується для ГК, і робочий каталог - місце установки програми на жорсткому диску. |

1. Вставити дискету з назвою «генератор ключів відділення ... ». Запустити командний файл KEYGEN.LNK.

2. По запиту програми ввести пароль, установлений при інсталяції ГК.

7.2 Генерація ключів

Перед запуском програми підготуйте чисті відформатовані дискети для запису ключових даних відповідно до кількості робочих місць, для яких необхідно створити ключі.

Для генерації робочих ключів необхідно:

1. Для кожного користувача, якому необхідно згенерувати ключі, виконати такі дії:

1.1.  Вибрати робоче місце в списку і натиснути кнопку «Сгенерировать»**.**

1.2.  Вставити дискету генератора ключів по запиту програми.

1.3.  По запиту програми ввести необхідні символи.

1.4.  Задати пароль доступу до робочого ключа.

1.5.  Вставити чисту дискету для запису робочого ключа.

1.6.  Повторити пункти 1.1 - 1.5 для генерації ключів для всіх робочих місць.

2. Для підготовки до відправлення згенерованих ключів вибрати команду з меню **«Команды|Пересылка откр. ключей».** В процесі закриття програми виконується підготовка файлу робочих ключів до відправлення в ЦУК автоматично.

3. При успішній генерації у вихідному каталозі (OUT) повинен з'явитися файл з ім'ям <глобальне\_ім'я>.KSG.

4. Після створення дискет конфіденційних ключів для необхідного числа робочих місць переконатися, що на дискетах присутні файли Station.cnf, Private.key, cryppass.lst. Підписати дискети: «конфіденційний ключ робочого місця ...».

Реєстрація ключів

Отримані з ЦУК сертифікати (файли <глобальне\_ім'я\_відділення.KB1> і (чи) <глобальне\_ім'я\_відділення>.KB2.) записуються у вхідний підкаталог IN і автоматично при першому після одержання ключів запуску програми keygen.exe записуються в базу ключів (реєструються). Якщо при реєстрації відбувся збій, то повторну реєстрацію можна виконати по натисканню на кнопку **«Зарегистрировать»**.

Для реєстрації робочих ключів необхідно:

1.  Для кожного робочого місця, якому необхідно зареєструвати ключі, виконати такі дії:

1.1.  Вибрати робоче місце в списку і натиснути кнопку **«Зарегистрировать».**

1.2.  Указати пароль доступу до робочого ключа.

1.3.  По запиту програми вставити робочу дискету.

2.  Натиснути кнопку «**Закрыть».**

Роздруківка відкритого ключа

Виконується після сертифікації ключа. Відкритий ключ може бути виведений на принтер чи у файл.

1.  Вибрати користувача в списку і натиснути кнопку «**Печатать».**

2.  Підготувати принтер до друку;

3.  Відредагувати текст на екрані, вибрати принтер;

4.  Якщо необхідно вивести інформацію у файл, відзначити галочкою пункт **«Печать в файл»**. Натиснути на кнопку **«Печать»**

Зміна пароля входу в програму

Зміна пароля необхідна при його можливій компрометації чи по закінченню строку дії, який визначено спеціальною інструкцією.

1.  Вставити дискету з генератором ключів;

2.  Вибрати пункт меню **«Смена пароля»**;

3.  Ввести старий і новий паролі.

**Хід роботи:**

1. Ознайомитися з теоретичними матеріалами.

2. Інсталювати ЦУК.

3. Створити відділення.

4. Створити робочі місця (по-одному) для ЦУК і для кожного відділення.

5. Створити робочі дискети для робочих місць центрального та інших відділень.

6. Інсталювати робочі місця відділень.

7. Інсталювати генератори ключів для робчих місць відділень.

8. Згенерувати ключі для робчих місць відділень.

9. Одержати на них сертифікати в ЦУК.

10. Зареєструвати у відділеннях отримані сертифікати.

**Контрольні питання:**

1. Призначення ЦУК і його роль у рішенні задачі забезпечення безпеки банківської інформації.

2. Основні функції ЦУК.

3. Загальні вимоги до ключів і ключових параметрів.

4. Принципи функціонування багаторівневих ключових систем.

5. Що таке спроможний протокол?

6. Пояснити схему спроможного протоколу в симетричній системі.

7. Пояснити схему спроможного протоколу в системі з відкритими ключами.

## ЛАБОРАТОРНА РОБОТА №4

**ПЛАН ПОГАШЕННЯ КРЕДИТУ**

## 4.1. Мета роботи.

З’ясувати види виплат при отриманні та сплаті кредиту. Навчитись визначати більш вигідні умови кредитування, розробляти план погашення кредиту та обчислювати загальну суму переплат по кредиту.

## 4.2. Методичні вказівки з організації самостійної роботи студентів.

При підготовці до лабораторної роботи необхідно:

- засвоїти лекційний матеріал, який стосується банківського кредитування;

- вивчити і засвоїти основні поняття і визначення підрозділу 1.4;

- засвоїти основні поняття і терміни, що використовуються в проекті «Простір» (див.

- підготувати відповіді на питання, наведені в методичних вказівках.

## 4.3. Опис лабораторної установки.

Використовується комп’ютер із процесором не нижче ніж Intel 486. У якості програмного забезпечення для виконання роботи використовуються браузер та пакет MS Office.

## 4.4. Задачі.

**Задача 1. Вибір умов кредитування**

Позичальнику потрібно взяти кредит розміром $ 200 000, терміном на 5 років, погашати який (основний борг і відсотки) він буде рівномірними платежами вкінці кожного року. Запит на фінансування направлений у 3 банки. Порівняйте умови (вони вказані у табл. 1) та визначте найвигідніший варіант.

*Таблиця 1. Умови кредитування.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Розмір кредиту** | **Видача (%)\*** | **Плата за оформлення** | **Ставка (%)** | **Термін (років)** |
| **Банк 1** | $200 000 | 95,0% | $300 | 12,0% | 5 |
| **Банк 2** | $200 000 | 96,0% | $250 | 13,5% | 5 |
| **Банк 3** | $200 000 | 96,5% | $350 | 14,2% | 5 |

\* Надання кредиту не означає, що видадуть усю суму повністю. Певну частину (дізажіо) потрібно залишити у банку як плату за виконання операції та підвищений ризик, на який іде банк.

Розв’язання

1.      Внесіть дані про умови кредитування на лист Excel.

2.      Обчисліть дізажіо:

3.      Обчисліть суму, яку видадуть у банку:

4.      За допомогою функції ПЛТ визначте розмір річної виплати по кредиту, яка охоплює як погашення основного боргу, так і виплату відсотків.

5.      Визначте відношення річної виплати до отриманої суми. Це допоможе оцінити вигідність умов кредитування.

6.      Проаналізуйте, у якому банку умови кредитування є вигіднішими.

**Задача 2. План погашення кредиту.**

Розробіть план погашення кредиту у банку 1

**Розв’язання**

1.      Спочатку визначте, яка сума з річної виплати у перший рік становитиме погашення відсотків по кредиту.

2.      Визначте, яка частина річної виплати у перший рік піде на погашення основного боргу.

3.      Визначте залишок основного боргу на кінець першого року.

4.      Визначте, яка сума у другий рік становитиме погашення відсотків (у формулі застосуйте абсолютну адресацію, оскільки закономірність буде скопійована на діапазон для наступних років).

5.      Визначте, яка сума у другий рік становитиме виплату основного боргу (застосуйте абсолютну адресацію).

6.      Визначте залишок основного боргу на кінець другого року.

7.      Скопіюйте формули для другого року вниз по таблиці.

**Завдання для самостійного розв’язування**

Розробіть плани погашення кредиту для Банку 2 і Банку 3.

**Лабораторна робота 5**

**Вивчення особливостей різних видів дистанційного банківського обслуговування**

**5.1 Мета роботи**

Вивчити особливості функціонування та порядок взаємодії учасників при різних видах дистанційного банківського обслуговування. Визначити загрози що можуть бути реалізовані для схем дистанційного банківського обслуговування (ДБО) та запропонувати заходи щодо вдосконалення цих схем.

**5.2 Методичні вказівки з організації самостійної роботи студентів**

При підготовці до лабораторної роботи необхідно:

- вивчити і засвоїти лекційні матеріали по ДБО;

- вивчити і засвоїти основні поняття і визначення підрозділу 5.3;

- підготувати відповіді на контрольні запитання, які наведені в підрозділі 5.7 методичних вказівок.

**5.3 Теоретичні відомості**

У цьому підрозділі викладено погляд на історію розвитку дістанційного банківського обслуговування.

Дистанційне банківське обслуговування (ДБО) з'явилося на початку 80-х рр. XX ст., і з кожним роком завойовує усе більше значення як фінансових інститутів, так і для їхніх клієнтів. У сучасній економічній науці різні технології ДБО фізичних і юридичних осіб поєднуються загальним поняттям - віддалений банкінг (remote banking, direct banking). Сьогодні послуги ДБО надаються різними суб'єктами фінансового ринку різним суб'єктам цього ринку з використанням різних каналів доступу до цих послуг. Крім того, дистанційні банківські послуги розрізняються по ступені універсальності наданих операцій.

Таким чином, першим різновидом класифікації віддаленого банкінга є *поділ з погляду суб'єкта, якому надається даний вид послуг:*віддалений банківський сервіс для корпоративних клієнтів (corporate remote banking) і віддалений банківський сервіс для фізичних осіб (retail remote banking).

Віддалений банківський сервіс для корпоративних клієнтів може надаватися як по обмеженому колу операцій (переказ коштів в автоматичній кліринговій системі, відстеження поточних платежів і інші), так і по широкому, який часто нічим не поступається традиційному корпоративному обслуговуванню (надання інформації про стан рахунка, про умови одержання позички, пряме обслуговування депозиту, дебетування і кредитування рахунків, платежі постачальникам і в податкові органи й інші). Незважаючи на те, що корпоративний сектор для багатьох банків є стратегічно дуже важливим сегментом ринку, у сфері дистанційного банківського обслуговування, в силу об'єктивних причин (менший обсяг первісних інвестицій, менш тверді вимоги до інтеграції, більш проста програмна реалізація), більше поширення одержав віддалений банківський сервіс для фізичних осіб.

ДБО фізичних осіб відомо за назвою домашній банкінг (home banking), хоча, часто в термін домашній банкінг включають і сферу дистанційного банківського обслуговування юридичних осіб. Домашній банкінг являє собою технологію віддаленого банківського обслуговування, що дозволяє клієнту одержувати банківські послуги, не відвідуючи банківський офіс.

*З погляду каналів доступу до банківських послуг, можна виділити шість форм сучасного віддаленого банкінга:*телефонний банкінг (phone-banking); ПС-банкінг (PC-banking); відео-банкінг (video-banking); Інтернет-банкінг (Internet-banking); мобільний банкінг (mobile-banking); цифровий телевізійний банкінг (DTV-banking). Ці форми дистанційного банківського обслуговування розрізняються за часом впровадження в банківській практиці.

Першою формою дистанційного банківського обслуговування був телефонний банкінг (1983 р.). Цей вид дистанційного банківського обслуговування в силу поширеності і доступності телефонних терміналів дотепер залишається однієї із самих популярних різновидів віддаленого банкінга. Перевагами телефонного банкінга є: доступність і простота використання. Його недоліками є: обмежений набір наданих банківських операцій і відсутність візуального інформаційного моніторингу.

Наступною формою дистанційного банківського обслуговування є ПС-банкінг (використовується з 80-х рр.). При даній формі домашнього банкінга клієнту надається спеціальне програмне забезпечення для роботи зі своїм рахунком. Програмне забезпечення може бути інтегроване в одну з популярних програм для керування особистими фінансами, такими як Quicken чи Microsoft Money. До переваг даної форми дистанційного банкінга відносяться: широкий спектр банківські операції, можливість візуального спостереження прийнятих рішень. До недоліків ПС-банкінга можна віднести: необхідність виділеної лінії зв'язку для підключення до мережі банку, а також необхідність використання спеціального програмному забезпечення.

На початку 90-х рр. з'явилася ще одна форма дистанційного банківського обслуговування — відео-банкінг. Для відео-банкінга використовуються пристрої, які називаються мультимедійні кіоски (multimedia kiosks) чи спеціально призначені для цих цілей банкомати (automated teller machines). Це апарати із сенсорним екраном, що дозволяють клієнту одержати доступ до різної інформації, а також у режимі онлайн спілкуватися з банківськими службовцями і проводити з їх допомогою практично будь-які операції. Ці пристрої встановлюються, як правило, у супермаркетах, аеропортах, університетах і інших місцях. Істотною перевагою даної форми дистанційного банкінга є можливість проведення широкого спектра банківських операцій у режимі онлайн. Суттєвим недоліком відео-банкінга є те, що його послугами можна скористатися тільки в спеціально відведених місцях.

Наступною формою домашнього банкінга став інтернет-банкінг, що з'явився в середині 90-х рр. Поява Інтернет-банкінга з'явилося дійсним проривом у дистанційному банківському обслуговуванні. На відміну від телефонного банкінга, при якому телефон з самого початку був погано пристосований для здійснення банківських операцій, на відміну від ПС-банкінга, при якому було потрібно встановлення спеціального програмного забезпечення й обов'язкове модемне приєднання до мережі банку, на відміну від відео-банкінга, при якому було потрібно залишати свій будинок для здійснення банківських операцій, Інтернет-банкінг був ідеально пристосований для дистанційного банківського обслуговування в силу своєї доступності, універсальності і гнучкості мережного середовища (для проведення операцій за допомогою Інтернет-банкінга досить мати тільки персональний комп'ютер з підключенням до Інтернет).

Значне зниження вартості персональних комп'ютерів і телекомунікаційного устаткування, а також доступу до Інтернет протягом другої половини 90-х рр. обумовили підвищений інтерес до Інтернет-банкінгу як з боку самих банків, так і з боку банківських клієнтів. Єдиним недоліком Інтернет-банкінга є утрата фізичного контакту з банківськими службовцями, що для багатьох клієнтів є серйозною психологічною проблемою.

У 1997-98 р. з'явилася новітня форма дистанційного банківського обслуговування - мобільний банкінг. В даний момент існує два основні різновиди мобільного банкінга: на базі протоколу Wireless Access Protocol - WAP-банкінг і з використанням протоколу Short Message Service - SMS-банкінг. У випадку WAP-банкінга стільниковий телефон грає приблизно таку ж роль, як комп'ютер при Інтернет-банкінгу. Зміст сторінок передається в мікробраузер стільникового телефону і відображається на дисплеї. Введення даних та їх передача в банк виконується, як і при Інтернет-банкінгу, за допомогою відповідної форми. SMS-банкінг заснований на використанні механізму коротких повідомлень - спеціального каналу передачі даних. За допомогою таких коротких повідомлень на стільниковий телефон передається інформація банку, наприклад, список рахунків або виписка по рахунку, а в банк передаються дані, які введені клієнтом. Очевидною перевагою WAP-банкінга є його зручність для користувача - можливість навігації по сайту банка, візуальний контроль і достатньо зручне введення інформації. Очевидною перевагою SMS-банкінг є його простота і доступність.

Безумовними лідерами мобільного банкінга сьогодні є скандинавські фінансово-кредитні організації Фінляндії та Швеції. Наприклад, фінсько-шведська банківська група MeritaNordbanken сьогодні обслуговує кожного шостого клієнта по WAP-каналах1. Крім того, активно мобільний-банкінг розвивається в Німеччині і Великобританії. Сполучення мобільності з обчислювальними здібностями й екраном дисплея робить інтелектуальні мобільні пристрої прекрасною платформою для надання банківських послуг.

На сьогоднішній день Інтернет-банкінг і мобільний-банкінг є найбільш сучасними і затребуваними технологіями дистанційного банківського обслуговування фізичних осіб. Однак в останні два роки позначився ще один напрямок розвитку домашнього банкінга - цифровий телевізійний банкінг. В даний момент системи цифрового телевізійного банкінга знаходяться в стадії іспитів. У майбутньому, ці системи дозволять здійснювати банківські операції з використанням звичайних телевізійних приймачів, що здатно значно розширити клієнтську базу. Технологія цифрового телевізійного банкінга буде поєднувати в собі практично всі переваги інших систем домашнього банкінга за винятком високої мобільності, якою володіють системи мобільного-банкінга.

Наступним різновидом класифікації віддаленого банкінга є *поділ з погляду об'єкта, що надає дану послугу:*традиційний банк (traditional bank) чи віртуальний банк (virtual bank). Частина банків розвиває системи домашнього банкінга у виді додаткового сервісу, насамперед, тому, що клієнту це зручно. При такому підході банк не одержує значної економії, зате виграє в конкурентів. Клієнтам пропонується максимально широкий вибір послуг, вони можуть робити операції як через звичайні філії, так і через телекомунікаційні канали доступу. Інтерактивність сполучається з можливістю «людського» спілкування з працівниками банку в офісі і по телефону. Такий підхід можна назвати сервіс-орієнтовним, а банки, що дотримують цієї концепції, - «многоканальними» банками. Як правило, по такому шляху йдуть великі роздрібні банки (Wells Fargo, Deutsche Bank, MeritaNordbanken і ін.), що бажають знаходитися в руслі передових тенденцій розвитку і розраховують у перспективі домогтися раціоналізації своєї роздрібної мережі.

Інші фінансові інститути в главу кута ставлять мінімізацію витрат і з цією метою організують окремий віртуальний банк, що працює тільки через Інтернет і інші канали електронного доступу. Одержувану економію такі банки розділяють зі своїми клієнтами. Як правило, віртуальні банки надають клієнтам більш високі ставки по внесках, чим звичайні банки. Крім того, деякі з віртуальних банків повертають клієнтам частину комісій за зняття грошей у банкоматах, як би компенсуючи відсутність власної інфраструктури. На сьогоднішній момент у світі нараховується близько 30 віртуальних банків, найбільш відомими з який є: NetBank, CompuBank, BankDirect.

Нарешті, ще одним різновидом класифікації віддаленого банкінга є *поділ з погляду універсальності послуг, що наадються.*Можна виділити простий сервіс, просунутий сервіс і універсальний дистанційний банківський сервіс. Послуги простого дистанційного сервісу, як правило, обмежуються одержанням інформації про залишок на рахунку. Просунутий дистанційний сервіс, як правило, дозволяє проводити безготівкові внутрібанківські платежі, переводити кошти по своїх рахунках, відслідковувати всі банківські операції по своїх рахунках за будь-який проміжок часу. Універсальний дистанційний сервіс містить у собі повний набір банківських послуг, що надаються фізичним особам у традиційних офісах банку (внутрібанківські і міжбанківські платежі, операції по купівлі-продажу безготівкової валюти і ЦБ, одержання кредиту в режимі віддаленого доступу), за винятком операцій з готівкою.

Банк, що надає своїм клієнтам універсальний набір послуг домашнього банкінга, тим самим стає телекомунікаційно-фінансовим центром, у якому по різних каналах стікаються розпорядження клієнтів. Клієнти такого «телекомунікаційного» банку можуть використовувати для проведення операцій будь-який з каналів доступу у залежності від ситуації. Наприклад, можна використовувати комп'ютер на робочому місці при керуванні рахунками з роботи, мобільний телефон - по дорозі, «мультимедійний кіоск» - у аеропорті чи супермаркеті і звичайний телефон або інтерактивний телевізор - вдома.

Не виключено, що найближчим часом на світовому ринку з'явиться кілька сотень банків, що пропонують весь спектр послуг домашнього банкінга, оскільки розвиток сучасних форм дистанційного банківського обслуговування означає для банків одержання конкурентних переваг на фінансовому ринку. Сучасні форми дистанційного банківського обслуговування здатні замінити багатьом банкам філіальні мережі, оскільки володіють значною кількістю достоїнств у порівнянні з традиційними формами банківського обслуговування:

1) *Підвищення конкурентноздатності.*Інтерактивне середовище відкриває можливість створення принципово нових банківських продуктів, а також швидкого масштабування й інтегрування банківських послуг з іншими фінансовими послугами, що використовують віддалений доступ до грошових рахунків.

2) *Зниження собівартості послуг.*Використання дистанційного банкінга дозволяє скоротити як безпосередню собівартість банківських операцій, так і знизити операційні витрати за рахунок зниження накладних витрат на керування філіями.

3) *Підвищення якості послуг.*Використання дистанційного банкінга дозволяє також усунути фактор тимчасового обмеження доступу до банківських операцій і виключити «географічну складову» при роботі з клієнтами.

**5.4 Опис лабораторної установки**

Як лабораторна установка використовується комп’ютер із процесором не гірше ніж Intel 486. У якості програмного забезпечення для виконання роботи використовується демонстраційна програма start.exe.

Start.exe – це програма, яка демонструє основні властивості та особливості, а також приклади роботи найбільш популярних на сьогодні видів дистанційного банківського обслуговування: телефонний банкінг (phone-banking); ПС-банкінг (PC-banking) та Інтернет-банкінг (Internet-banking).

**5.5 Порядок виконання роботи і методичні вказівки з її виконання**

1. Ознайомитися з теоретичним матеріалом

2. Запустити програму start.exe.

3. Завантажити опис підсистеми «Банк-Клиент». Для цієї підсистеми розглянути: призначення, вимоги до клієнтів, завдання, які підсистема вирішує, склад підсистеми та призначення основних елементів, продивитися приклад роботи.

4. Завантажити опис підсистеми «Интернет-Клиент». Для цієї підсистеми також розглянути: призначення, вимоги до клієнтів, завдання, які підсистема вирішує, склад підсистеми, продивитися приклад роботи.

5. Завантажити опис підсистеми «Компьютерная телефония». Для цієї підсистеми також розглянути: призначення, вимоги до клієнтів, завдання, які підсистема вирішує, склад підсистеми та призначення основних елементів, продивитися приклад роботи.

## 5.6. Зміст звіту

1. Назва і мета роботи.

2. Короткі відомості з теорії.

3. Структура однієї з розглянутих систем дистанційного банківського обслуговування.

4. Можливі загрози в цієї системі.

5. Аналіз сильних і слабких сторін системи захисту.

6. Висновки по роботі.

## 5.7. Контрольні запитання та завдання

1. Призначення систем ДБО.

2. Класифікації систем ДБО.

3. Переваги та недоліки різних видів ДБО.

4. Принципи функціонування системи лімітів і розв'язувані задачі.

5. Підсистема «Банк-Клиент». Призначення, вимоги до клієнтів, завдання, які підсистема вирішує, склад підсистеми.

6. Захист інформації у підсистемі «Банк-Клиент». Можливі погрози у системі, шляхи їх перекриття, пропозиції щодо вдосконалення механізмів захисту інформації.

7. Підсистема «Интернет-Клиент». Призначення, вимоги до клієнтів, завдання, які підсистема вирішує, склад підсистеми та призначення основних елементів.

8. Захист інформації у підсистемі «Интернет-Клиент». Можливі загрози у системі, шляхи їх перекриття, пропозиції щодо вдосконалення механізмів захисту інформації.

9. Підсистема «Компьютерная телефония». Призначення, вимоги до клієнтів, завдання, які підсистема вирішує, склад підсистеми та призначення основних елементів.

10. Захист інформації у підсистемі «Компьютерная телефония». Можливі загрози у системі, шляхи їх перекриття, пропозиції щодо вдосконалення механізмів захисту інформації.

**ЛАБОРАТОРНА РОБОТА №6**

**ДОХІДНІСТЬ ЦІННИХ ПАПЕРІВ**

## 6.1. Мета роботи.

Ознайомитися із видами цінних паперів та джерелами доходу він них. Навчитись обчислювати дохідність цінних паперів засобами функцій Microsoft Excel.

## 6.2. Методичні вказівки з організації самостійної роботи студентів.

При підготовці до лабораторної роботи необхідно:

- засвоїти лекційний матеріал, який стосується автоматизації роботи банку із цінними паперами;

- вивчити і засвоїти основні поняття і визначення підрозділу 6.4;

- пройти тестування на дистанційному навчанні.

## 6.3. Опис лабораторної установки.

Використовується комп’ютер із процесором не нижче ніж Intel 486. У якості програмного забезпечення для виконання роботи використовуються браузер та пакет MS Office.

## 6.4. Теоретичні відомості та їх практичне використання.

Задача, що розглядається у лабораторній роботі, пояснює, як розмістити вільні кошти, щоб вони давали максимальний дохід. Приклад показує, як із допомогою Excel приймати рішення про здійснення операцій з цінними паперами. Для розрахунків використовуються два види цінних паперів – твердовідсоткові і дисконтні.

Цінний папір – це:

- грошовий документ, що засвідчує майнове право чи відношення позики власника документа до особи, що випустила такий документ;

- джерело формування статутного капіталу акціонерних товариств та фінансування витрат держави, територіально-адміністративних органів управління, муніципалітетів.

Акція – це емісійний цінний папір, який випускає акціонерне товариство при його створенні або при перетворенні державного підприємства в акціонерне товариство, а також при залученні акціонерним товариством вільних грошових засобів шляхом додаткової емісії акцій.

Облігація – це борговий емісійний папір, що засвідчує внесення інвестором певних грошових засобів та підтверджує зобов’язання емітента відшкодувати інвестору вартість цього цінного паперу у визначений час – повернути внесені засоби зі сплатою зафіксованого в облігації відсотку від її номінальної вартості.

Параметри прибутковості облігації:

- номінальна вартість,

- ставка купона,

- дата погашення.

Номінальна вартість являє собою суму, яку отримає інвестор, коли облігація буде погашена.

Ставка купона – це ті суми грошей, які держатель облігації буде регулярно отримувати. Ставка купона виражається у процентах від номінальної вартості. В облігації також вказано, коли виплачується купонний дохід – щомісячно, щоквартально, раз у півроку чи раз на рік.

Дата погашення – це день, коли емітент повинен повернути позичальнику основну суму боргу. Після того, як позичальник виплатить основну суму боргу, він не зобов’язаний проводити відсоткові виплати.

Інколи компанія вирішує відкликати свої боргові зобов’язання, що означає, що вона повертає своїм позичальникам їх гроші до дати погашення облігації. На всіх облігаціях вказується, чи є можливість дострокового відкликання, та як швидко це може відбутись.

Є менш значимі характеристики цінних паперів:

Періодичність виплати купонів. Найчастіше купон виплачується щоквартально. Календар купонних виплат визначає, в які дні будуть виплачені купони, що залишились.

Накопичений купонний дохід (НКД). Коли облігація продається до настання дати купонного платежу, покупець повинен надати продавцю компенсацію пропорційно до того часу, який пройшов з останнього купонного платежу. Розмір НКД змінюються від 0 (купон був виплачений щойно) до розміру купона (купон повинен бути виплачений сьогодні).

Оферта – це можливість для інвестора погасити свої облігації до настання терміну погашення, якщо він вважатиме це необхідним. Емітент самостійно встановлює в оферті ціну викупу облігацій, яка дасть інвестору певний рівень дохідності, якщо інвестор виявить бажання погасити свої облігації достроково і акцептує оферту. Оферта знижує кредитний ризик інвестора (ризик неповернення коштів емітентом) та процентний ризик (ризик несприятливої для інвестора зміни процентних ставок на ринку). Ціна викупу може дорівнювати номінальній вартості або бути більшою чи меншою.

Обсяг випуску – загальна номінальна вартість всього випуску облігацій.

Дивіденди – це прибуток, який розподіляє акціонерне товариство між своїми акціонерами згідно підсумків роботи за рік, півріччя чи квартал. У більшості випадків отримання дивідендів по акціях не є метою їх придбання. Частіше акції купляють заради значного збільшення їх ринкової вартості з часом. Ринкова вартість визначається ефективністю, інноваційністю роботи компанії. Деякі, навіть високоприбуткові компанії, можуть тривалий період не виплачувати дивіденди коли розумно реінвестувати прибуток у розвиток бізнесу. Це може бути вигідно й акціонерам, оскільки призводить до зростання курсової вартості акцій компанії.

Будь-який інвестиційний актив, включно із цінними паперами – це потік платежів, які в майбутньому має право отримати власник даного активу. Складовими потоку платежів є регулярні виплати (проценти, дивіденди) та суми, які будуть отримані при погашенні цінного паперу чи продажу його на ринку. Повною характеристикою грошового потоку є сукупність даних про терміни майбутніх надходжень, їх величину та імовірність надходження. Із врахуванням даних факторів цінні папери поділяють на два класи:

- цінні папери з невизначеними майбутніми надходженнями;

- твердовідсоткові цінні папери.

Найтиповіші цінні папери з невизначеними майбутніми надходженнями – це акції. Твердовідсоткові цінні папери – це термінові облігації з фіксованими купонними виплатами.

Дохідність цінних паперів є одним з основних об’єктів інвестиційного аналізу. Поняття дохідності в інвестиційному аналізі аналогічне поняттям рентабельності, ефективності в інших галузях економічних досліджень.

R= (W¹-Wº)/Wº;

R – дохідність, W¹ - капітал інвестора на кінець періоду, Wº - капітал інвестора на початок періоду.

1.      Оскільки потрібно визначити дохідність на поточну дату, на листі Excel задайте формулу =СЕГОДНЯ(), яка виведе поточну дату на екран.

2.      Створіть таблицю із даними про твердовідсоткові ЦП.

3.      Для визначення доходу задайте формулу ДОХОД.

4.      Створіть таблицю з даними про дисконтні ЦП:

5.      Для визначення доходу задайте формулу:

6.      Обґрунтуйте рекомендації щодо формування портфелю цінних паперів.

**ЛАБОРАТОРНА РОБОТА №7**

**ВИВЧЕННЯ ТА АНАЛІЗ ЗАХИЩЕНОСТІ ПРОТОКОЛУ SET**

**7.1 Мета роботи**

Вивчити порядок взаємодії учасників платежів по протоколу SET, дослідити механізми захисту від основних загроз у системах платежів з використанням платіжних карток.

**7.2 Методичні вказівки з організації самостійної роботи студентів**

При підготовці до лабораторної роботи необхідно:

-  вивчити і засвоїти лекційні матеріали по протоколу SET;

- вивчити і засвоїти основні поняття і визначення підрозділу 7.3;

- детально ознайомитися з криптографічними алгоритмами DES та RSA що використовуються в протоколі SET;

-   підготувати відповіді на контрольні запитання, наведені в методичних вказівках;

- пройти тест у системі дистанційного навчання.

**7.3 Теоретичні відомості**

7.3.1 Загальні відомості про SET

Протокол SET (Secure Electronic Transaction — протокол захищених електронних транзакцій) являє собою відкриті специфікації, розроблені з метою захисту транзакцій, здійснюваних у Internet за допомогою пластикових платіжних карток. Поточна версія протоколу, протокол SETvl, з'явилася в лютому 1996 року через виниклу необхідность створення стандарту захисту для кредитних карток MasterCard і Visa. У розробці оригінальних специфікацій брали участь багато відомих компаній, включаючи IBM, Microsoft, Netscape, RSA, Terisa і VeriSign. Починаючи з 1996 року покладена в основу протоколу концепція пройшла ретельну перевірку практикою, і до 1998 року на ринку з'явилися перші продукти реалізації протоколу SET.

SET є не платіжною системою, а набором протоколів захисту і форматів даних, що дозволяють деяким захищеним чином використовувати існуючу інфраструктуру платіжних систем пластикових карток у відкритих мережах типу мережі Internet. По суті, SET забезпечує три види сервісу:

• Створення захищеного комунікаційного каналу, що зв'язує всі сторони, що беруть участь у транзакції.

• Забезпечення довіри за допомогою цифрових сертифікатів X509v3.

• Забезпечення таємності через те, що інформація виявляється доступною тільки учасникам транзакції і тільки тоді і там, де вона необхідна.

Повна специфікація SET описується в трьох книгах, опублікованих у травні 1997 року.

• Книга 1. Опис можливостей застосування (Business Description), 80 стор.

• Книга 2. Керівництво програміста (Рrоgrаmmеr's Guide), 629 стор.

• Книга 3. Формальне визначення протоколу (Formal Protocol Definition), 262 стор.

Усе разом це складає 971 сторінку специфікацій. Для порівняння помітимо, що специфікації SSL займають 63 сторінки, а специфікації TLS — 71 сторінку. Відповідно, у даному розділі будуть наведені лише загальні дані про специфікації SET.

Опис протоколу SET найкраще почати з огляду вимог до SET, головних можливостей SET, а також ролі учасників транзакцій, що виконуються по протоколу SET.

У книзі 1 специфікацій SET перераховані такі вимоги, що повинні виконуватися при опрацюванні платежів по кредитних картах в Internet і інших подібних мережах.

• Конфіденційність платежу й інформації про замовлення. Необхідно гарантувати власникам пластикових карт, що дана інформація надійно захищена і виявиться доступною тільки тому, кому вона призначена. Конфіденційність до того ж зменшує ризик обману кожного з учасників при здійсненні транзакції. Для забезпечення конфіденційності застосовується шифрування.

• Гарантія цілісності всіх переданих даних означає, що в ході передачі інформація, що міститься в повідомленні SET, не зазнає жодних змін. Для забезпечення цілісності призначений механізм цифрового підпису.

• Автентифікація пред'явника кредитної картки як законного власника відповідного рахунка. Механізм, що зв'язує пред'явника кредитної картки з відповідним номером рахунка, повинен зменшувати імовірність шахрайства і знижувати загальну вартість обробки платежів. Для перевірки того, що пред'явник кредитної картки є законним власником відповідного дійсного рахунка, застосовуються такі засоби, як цифровий підпис і сертифікати.

• Автентифікація продавця як особи, що має право приймати транзакції по кредитних картках, за допомогою з'ясування його зв'язку з відповідною фінансовою організацією. Ця вимога доповнює попереднє. Власники платіжних карт повинні мати можливість ідентифікувати продавців, яким вони можуть направляти захищені транзакції. Для цього також використовуються цифрові підписи і сертифікати.

• Гарантоване використання кращих конструктивних рішень і методів захисту для забезпечення найвищого ступеня захисту всіх легальних учасників електронних комерційних транзакцій. Специфікації SET будуються на застосуванні криптографічних алгоритмів і протоколів, що мають високий рівень захищеності і добре перевірені.

• Незалежність протоколу від механізмів захисту транспортування даних за відсутності будь-яких обмежень на використання таких механізмів. SET може забезпечувати захист, спираючись безпосередньо і винятково на стек протоколів TCP/IP. Але при цьому SET ніяк не впливає на роботу інших механізмів захисту, таких як IPSec чи SSL/TLS, і не залежить від них.

•Сприяння і підтримка сумісності між прикладними програмними і мережними продуктами різних постачальників. Протоколи і формати SET не залежать від апаратних платформ, операційних систем і програмного забезпечення, призначеного для роботи в Web.

7.3.2 Головні можливості SET

Щоб відповідати названим вище вимогам, у протоколі SET peaлізовані такі можливості.

• Конфіденційність інформації. Інформація про рахунок власника карти і платежі захищається під час пересилання по мережі.  Цікава і важлива особливість SET полягає в тому, що продавець при цьому не може з'ясувати номер кредитної картки її власника – ця інформація виявляється доступною тільки банку, який видав кредитну картку. Для забезпечення конфіденційності використовується шифрування за традиційною схемою за допомогою симетричного алгоритму DES а також за допомогою несиметричного алгоритму RSA.

• Цілісність даних. Інформація про платіж, що надсилається власником карти продавцю, містить інформацію про замовлення, особисті дані й інструкції для здійснення платежу. SET гарантує, що зміст відповідних повідомлень не буде змінено під час їх передачі. Цілісність даних досягається за допомогою цифрових підписів RSA, що використовують хеш-коди SHA-1.

• Автентифікація рахунка власника карти. SET дає продавцю можливість перевірити, чи є пред'явник кредитної картки законним користувачем відповідного дійсного рахунка. Для цієї мети в SET передбачене використання цифрових сертифікатів X.509v3 з підписами RSA.

• Автентифікація продавця. SET дозволяє власнику карти перевірити, чи має продавець відношення до відповідної фінансової організації і право приймати платежі по кредитних картках. Для цієї мети в SET передбачене використання цифрових сертифікатів X.509v3 з підписами RSA.

Зверніть увагу на те, що на відміну від IPSec і SSL/TLS протокол SET для рішення кожної конкретної задачі пропонує тільки по одному алгоритму. Це пояснюється тим, що SET є протоколом, що відповідає цілком конкретному набору вимог, тоді як IPSec і SSL/TLS відносяться до універсальних протоколів, призначених для вирішення широкого спектра задач.

7.3.3 Учасники транзакцій SET

Учасниками транзакцій, здійснюваних за допомогою SET, є такі сторони (рис. 7.2.1).

• Власник платіжної карти. У середовищі електронних платежів індивідуальні і корпоративні споживачі взаємодіють із продавцями зі своїх персональних комп'ютерів через Internet. Власником карти в даному випадку є будь-який зареєстрований власник пластикової платіжної карти (MasterCard, Visa і т.п.), виданої йому деяким уповноваженим емітентом.

• Продавець. Продавець є особою, у якої власник карти може придбати товари чи послуги. Звичайно такі товари чи послуги пропонуються на продаж на Web-вузлі чи по електронній пошті. Продавець, що має право приймати платежі по платіжних картах, повинен мати відповідні відносини з операційним центром.

• Емітент платіжної картки. Емітент – це фінансова організація (наприклад банк), що видала платіжну карту відповідній особі (власнику карти). Як правило, відкрити рахунок можна поштою чи, з'явившись в офіс емітента, особисто. Усю відповідальність по оплаті заборгованості власника карти по даній карті несе емітент.

• Операційний центр (acquirer). Фінансова організація, що веде розрахунки з продавцем, виконує авторизацію платіжних карт і здійснює відповідні платежі. Продавці звичайно готові приймати  кредитні карти різних видів, але не хочуть мати справа з великим числом різних банківських асоціацій чи безліччю окремих емітентів платіжних карт. Операційний центр проводить для продавця перевірку того, що рахунок кредитної карти є дійсним, і пропонована покупка по вартості не виходить за рамки допустимого кредитного ліміту. Операційний центр також виконує електронний переказ грошових сум на рахунок продавця. Згодом операційний центр одержує за це визначену компенсацію від емітента карти через банківську платіжну мережу.

• Шлюз платіжної мережі (payment gateway). Сукупність засобів, контрольованих операційним центром чи уповноваженою ним третьою стороною і використовуваних для обробки платіжних повідомлень продавця. Шлюз платіжної мережі зв'язує SET і існуючі банківські платіжні мережі, виконуючи функції авторизації і передачі платежів. Продавець обмінюється повідомленнями SET зі шлюзом платіжної мережі через Internet, а шлюз платіжної мережі зв'язаний безпосередньо чи по внутрішній мережі із системою обробки фінансових документів відповідного операційного центра.

• Центр сертифікації (Certification Authority — СА). Об'єкт, якому довіряється видавати сертифікати X.509v3 відкритих ключів власників карт, продавців і шлюзів платіжної мережі. Успішна робота SET багато в чому залежить від наявності добре організованої інфраструктури сертифікації, доступної для використання у відповідних цілях. Як вже було візначено, може використовуваться ієрархія центрів сертифікації, так що учасники системи електронних платежів можуть бути сертифіковані не тільки головним центром сертифікації безпосередньо.

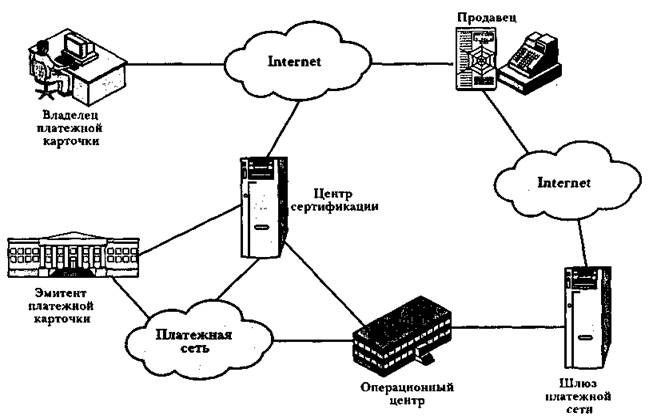


Рис. 7.1 – Учасники та компоненти захищеної системи електронної комерції

Тепер опишемо коротко послідовність подій, що відбуваються під час транзакції, а потім зупинимося докладніше на деяких криптографічних деталях даного процесу.

1. Покупець відкриває рахунок. Покупець відкриває рахунок кредитної картки (наприклад, MasterCard чи Visa) у банку, що здійснює електронні платежі і підтримує SET.

2.  Покупець одержує сертифікат. Після встановленої процедури перевірки особи покупець одержує цифрові сертифікати X.509v3,  підписані центром сертифікації. Один з сертифікатів засвідчує відкритий ключ цифрового підпису, другий – відкритий ключ направленого шифрування. Ці сертифікати засвідчують відкриті RSA ключі покупця і їх термін дії. Вони також установлюють відповідність між парою ключів покупця і його кредитною карткою.

3.  Продавець одержує свої сертифікати. Продавець, що має намір приймати оплату по платіжній картці визначеного типу, повинен одержати два сертифікати двох своїх відкритих ключів: один з них буде використовуватися для цифрового підпису, а другий – для направленого шифрування. Продавцю також буде потрібна копія сертифіката відкритого ключа шлюзу платіжної мережі.

4.  Покупець розміщує замовлення. Цей процес може припускати, що покупець спочатку повинен відвідати Web-вузол продавця, щоб вибрати потрібний товар і визначити ціну. Після цього покупець відправляє продавцю список потрібних йому товарів, а продавець у відповідь висилає бланк замовлення з зазначеними в ньому списком обраних товарів, цінами, загальною вартістю замовлення і номером замовлення.

5.  Перевірка продавця. Разом із бланком замовлення продавець висилає копію свого сертифіката, щоб покупець мав можливість переконатися в тім, що він дійсно має справу з справжним продавцем.

6.  Замовлення і платіж відправляються продавцю. Покупець відправляє замовлення і платіжну інформацію продавцю, додаючи до них свій сертифікат. Замовлення підтверджує покупку товарів, зазначених у бланку замовлення. Платіжна інформація містить необхідні дані кредитної картки. Платіжна інформація шифрується таким чином, щоб продавець не зміг її прочитати. Сертифікат покупця дозволяє продавцю виконати верифікацію покупця.

7.  Продавець запитує авторизацію платежу. Продавець відправляє платіжну інформацію шлюзу платіжної мережі з запитом підтвердження того, що доступний покупцю кредит достатній для здійснення даного платежу.

8.  Продавець підтверджує замовлення. Продавець відправляє покупцю підтвердження замовлення.

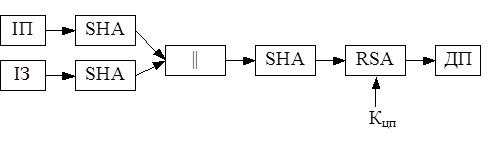
9.  Продавець доставляє товари чи надає послуги. Продавець організує доставку товарів чи виконання послуг покупцю.

10. Продавець запитує одержання платежу. Цей запит відправляється шлюзу платіжної мережі, що опрацьовує всі платіжні доручення.

7.3.4 Дуальний підпис

Перш ніж перейти до розгляду деталей протоколу SET, ми обговоримо одне важливе нововведення SET — *дуальний підпис* (dual signature). Дуальний підпис дозволяє зв'язати два повідомлення, призначені двом різним одержувачам. У даному випадку покупцю потрібно переслати інформацію про замовлення (ІЗ) продавцю і платіжну інформацію (ІП) банку. Продавцю не потрібно знати номер кредитної картки покупця, а банку не потрібні подробиці замовлення. Покупець же, розділяючи ці повідомлення, забезпечує тим самим додатковий захист своїх прав з погляду невтручання в його особисте життя. При цьому потрібно зв'язати ці повідомлення так, щоб їх можна було використовувати при виникненні конфлікту. Зв'язок цих частин потрібен для того, щоб покупець міг довести, що даний платіж призначений для оплати саме цього, а не якогось іншого замовлення.

Щоб зрозуміти необхідність такого зв'язку, припустимо, що покупець відправляє продавцю два підписаних повідомлення IЗ (замовлення) і IП (платіж), а продавець пересилає повідомлення IП у банк. Якщо продавець одержить від покупця якесь інше замовлення, то продавець зможе заявити, що дане повідомлення IП оплачує нове, а не старе повідомлення ІЗ. Зв'язування виключає таку можливість.



|  |  |
| --- | --- |
| ІП — платіжна інформація  ІЗ — інформація про замовлення  SНA — функція хешування  (SHA-1)  ||  — конкатенація | RSA — шифрування (RSA)  KЦП — особистий ключ підпису покупця  ДП – дуальний підпис |

Рис. 7.2 – Створення дуального підпису

На рис. 7.2 показана схема використання дуального підпису для рішення щойно сформульованої проблеми. Спочатку покупець, використовуючи алгоритм SHA-1, обчислює хеш-коди для повідомлень IП і ІЗ. Два отриманих хеш-коди зв'язуються операцією конкатенації, і для результату зв'язування теж обчислюється хеш-код. Нарешті, покупець шифрує підсумковий хеш-код з використанням свого особистого ключа цифрового підпису, у результаті одержуючи дуальний підпис.

Дуальний підпис перевіряють продавець і банк. Розглянемо послідовність перевірки дуального підпису у банку (див. рис. 7.3).

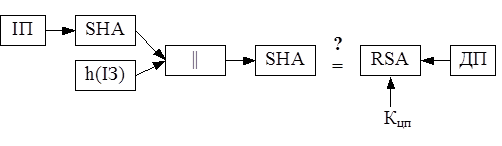


Рис. 7.3

Кожна з перевіряючих сторін повинна мати одне з повідомлень, хеш-код другого повідомлення, відкритий ключ перевірки підпису та сам дуальний підпис. Далі перевіряюча сторона обчислює загальну хеш-функцію (ліва частина рис. 7.3) та з допомогою відкритого ключа перевірки підпису розшифровує ДП (права частина рис. 7.3). Якщо ці два отримані значення збігаються, то перевіряючий робить висновок про справжність дуального підпису.

Підсумок:

1.  Продавець одержує повідомлення IЗ і виконує перевірку підпису покупця.

2.  Банк одержує повідомлення IП і виконує перевірку підпису покупця.

3.  Повідомлення ІЗ і IП виявляються зв'язаними, і покупець може довести їх зв'язок.

Припустимо, що продавець вирішить замінити повідомлення IЗ даної транзакції іншим, у надії мати з цього вигоду. Для цього йому доведеться знайти інше повідомлення ІЗ з точно таким же хеш-кодом. На сьогоднішній день при використанні алгоритму SHA-1 це є практично нерозв'язною задачею. Таким чином, у продавця немає можливості зв'язати з даним повідомленням IП інше повідомлення IЗ.

7.3.5 Обробка платежів

У даному розділі ми розглянемо докладно такі типи транзакцій:

• Запит на покупку (Purchase Request).

• Запит авторизації (Payment Authorization).

• Відповідь на запит авторизації (Authorization Response).

• Запит на платіж (Payment Capture).

7.3.6 Повідомлення “Запит на покупку”

До того як почати формування повідомлення **“запит на покупку”** (Purchase Request), власник платіжної картки повинен завершити перегляд списку доступних товарів, вибрати потрібні й оформити замовлення. Даний попередній етап закінчується відправленням продавцем бланка замовлення покупцю. Усі ці попередні операції не пов'язані з SET.

Обмін даними вимоги на закупівлю складаються з чотирьох повідомлень: Initiate Request (ініціюючий запит), Initiate Response (відповідь на ініціюючий запит), Purchase Request (запит на покупку) і Purchase Response (відповідь на запит на покупку).

Щоб власник платіжної картки мав можливість відправляти повідомлення SET продавцю, необхідно одержати копії сертифіката продавця і сертифіката шлюзу платіжної мережі. Запити на одержання цих сертифікатів містяться в повідомленні Initiate Request (ініціюючий запит), що покупець відправляє продавцю. Це повідомлення містить інформацію про тип кредитної картки, яка використовується покупцем, ідентифікатор, призначений покупцем даній парі повідомлень "запит-відповідь", і порядковий номер даного сеансу зв’язку, покликане гарантувати оригінальність повідомлення.

Продавець генерує відповідь і підписує її своїм особистим ключем цифрового підпису. Відповідь повинна включати порядковий номер даного сеансу зв’язку, порядковий номер повідомлення у цьому сеансу зв’язку, а також ідентифікатор даної транзакции. Крім підписаної відповіді, повідомлення Initiate Response (відповідь на ініціюючий запит) містить сертифікат підпису продавця і сертифікат шлюзу платіжної мережі для обміну ключами.

Власник платіжної картки перевіряє дійсність сертифікатів продавця і шлюзу платіжної мережі шляхом перевірки підписів відповідних центрів сертифікації, а потім створює повідомлення ІЗ і ІП. Обидва ці повідомлення містять ідентифікатор транзакції, сгенерований продавцем. Повідомлення ІЗ може не включати таких даних замовлення, як кількість чи ціна товарів, а містити лише посилання на замовлення, яке створено у процесі обміну повідомленнями між продавцем і покупцем на етапі узгодження ще до першого повідомлення SET. В цьому випадку повідомлення ІЗ може передаватися у відкритому виді. Але частіше повідомлення ІЗ як і ІП перед передачею має бути зашифроване.

Потім власник платіжної картки готує повідомлення Purchase Request (запит на покупку); див. схему на рис. 7.4.

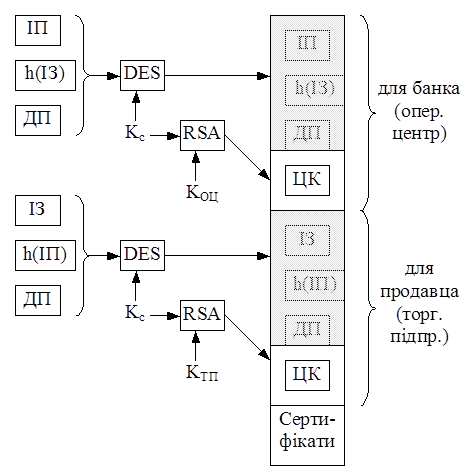


Рис. 7.4 – Повідомлення “запит на покупку”(Purchase Request)

Для цього власник платіжної картки генерує одноразовий ключ Kс для схеми симетричного шифрування з використанням алгоритму DES.

Повідомлення складається з таких блоків інформації.

*1. Інформація про платіж.* Пересилається продавцем шлюзу платіжної мережі і містить такі дані.

• Дані ІП

• Профіль повідомлення ІЗ (h(ІЗ)).

• Дуальний підпис, обчислений для сукупності ІЗ і IП і підписаний з використанням особистого ключа підпису покупця.

Значення h(ІЗ) необхідно для того, щоб шлюз платіжної мережі міг перевірити дуальний підпис, як це було наведено вище. Усі зазначені елементи шифруються за допомогою алгоритма DES та ключа Kс.

Останнім для даного блоку інформації є цифровий конверт. Цифровий конверт формується шляхом шифрування Kс за допомогою відкритого ключа шлюзу платіжної мережі (або операційного центру), призначеного для обміну ключами. Цей елемент називається *цифровим конвертам,* оскільки для того, щоб одержати можливість прочитати елементи, названі вище, цей конверт необхідно відкрити (тобто дешифрувати).

Значення Kс залишається продавцю невідомим. Тому продавець не зможе прочитати повідомлення яке включає ІП.

*2. Інформація про замовлення.* Ця інформація потрібна продавцю і містить такі дані.

• Дані IЗ.

• Профіль повідомлення ІП (h(ІП)).

• Дуальний підпис, обчислений для сукупності ІЗ і IП і підписаний з використанням особистого ключа підпису покупця.

Значення h(ІП) необхідно для того, щоб продавець міг перевірити дуальний підпис, як це було наведено вище. Усі зазначені елементи шифруються за допомогою алгоритма DES та ключа Kс.

Як вже було зазначено, дані IП можуть відправляються у відкритому виді якщо не містять інформації про покупку, а можуть бути зашифровані подібним до інформації про платіж чином (див. рис. 7.4).

*3. Сертифікати власника платіжної картки.* Ця частина повідомлення містить сертифікати відкритого ключа цифрового підпису власника платіжної картки, а також сертифікат відкритого ключа власника картки для ключового обміну. Ці сертифікати необхідні як продавцю, так і шлюзу платіжної мережі.

Після одержання повідомлення “запит на покупку” (Purchase Request) продавець виконує такі дії (рис. 7.4).

1.  Перевіряє сертифікати власника платіжної картки за допомогою підписів центрів сертифікації.

2.  Перевіряє дуальний підпис за допомогою відкритого ключа цифрового підпису власника платіжної картки. Це дозволяє переконатися в тому, що замовлення не було змінено під час пересилання і було підписано власником платіжної картки.

3.  Опрацьовує замовлення і пересилає платіжну інформацію шлюзу платіжної мережі для авторизації платежу (відповідний процес буде описаний нижче).

4.  Відправляє повідомлення Purchase Response (відповідь на вимогу на закупівлю) власнику платіжної картки.

Повідомлення Purchase Response (“відповідь на запит на покупку”) містить блок відповіді, що підтверджує замовлення і посилається на відповідний номер транзакції. Цей блок підписується продавцем за допомогою його особистого ключа цифрового підпису. Після цього блок разом з підписом, а також сертифікат підпису продавця відправляються власнику платіжної картки.

Коли програмне забезпечення, установлене на комп'ютері власника платіжної картки, одержує повідомлення Purchase Response, воно перевіряє спочатку сертифікат продавця, а потім підпис блоку відповіді. Зрештою, у залежності від змісту відповіді, виконується відповідна дія, наприклад, відображається на екрані деяке повідомлення для користувача чи оновлюється інформація про стан замовлення в базі даних.

7.3.7 Повідомлення “Запит авторизації”

Під час опрацювання замовлення, що надійшло від власника платіжної картки, продавець виконує авторизацію транзакції (одержання дозволу на оплату) за допомогою шлюзу платіжної мережі. Таке одержання дозволу на оплату (авторизація платежу) означає санкціонування транзакції емітентом платіжної картки. Авторизація дає продавцю гарантію того, що він одержить плату за проданий товар, і тому продавець може виконати доставку товарів чи послуг покупцю. Обмін даними для одержання дозволу на оплату формується з двох повідомлень: Authorization Request (запит авторизації) і Authorization Response (відповідь на запит авторизації).

Розглянемо повідомлення Authorization Request (запит авторизації) (рис. 7.5).

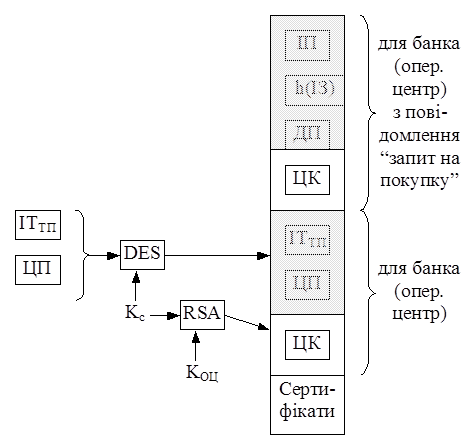


Рис. 7.5 – Повідомлення “запит авторизації”(Authorization Request).

Повідомлення Authorization Request (запит авторизації), що відправляється продавцем шлюзу платіжної мережі, складається з наступних блоків інформації.

1. Інформація про платіж. Ця інформація була отримана від покупця і містить такі дані.

• Дані ІП

• Профіль повідомлення ІЗ (h(ІЗ)).

• Дуальний підпис, обчислений для сукупності ІЗ і IП і підписаний з використанням особистого ключа підпису покупця.

• Цифровий конверт.

2.  Інформація авторизації. Ця інформація генерується продавцем і містить такі дані:

• Блок авторизації, що включає ідентифікатор транзакції (ІТТП), підписаний особистим ключем цифрового підпису продавця і зашифрований одноразовим ключем схеми симетричного шифрування, що генерується продавцем.

• Цифровий конверт, сформований шляхом шифрування одноразового ключа за допомогою відкритого ключа шлюзу платіжної мережі, призначеного для обміну ключами.

3.  Сертифікати. Продавець включає в повідомлення сертифікат цифрового підпису власника платіжної картки (для перевірки дуального підпису), сертифікат ключа свого цифрового підпису (дозволяє перевірити підпис продавця) і сертифікат свого ключа для обміну ключами (необхідний для відповіді шлюзу платіжної мережі).

Одержавши ці дані, шлюз платіжної мережі виконує такі дії:

1.  Перевіряє всі сертифікати.

2.  Дешифрує спочатку цифровий конверт блоку дані авторизації, щоб одержати ключ для схеми симетричного шифрування, а потім дешифрує блок даних авторизації.

3.  Перевіряє підпис продавця для блоку даних авторизації.

4.  Дешифрує спочатку цифровий конверт блоку платіжної інформації, щоб одержати ключ для схеми симетричного шифрування, а потім дешифрує блок платіжної інформації.

5.  Перевіряє дуальний підпис блоку платіжної інформації.

6.  Перевіряє збіг ідентифікатора транзакції, отриманого від продавця, з ідентифікатором, включеним до складу даних IП, що надійшли (через продавця) від власника платіжної картки.

7.  Запитує й одержує дозвіл на оплату в емітента платіжної картки.

7.3.8 Повідомлення “Відповідь на запит авторизації”

Одержавши дозвіл на оплату в емітента платіжної картки, платіжний шлюз повертає продавцю повідомлення Authorization Response (відповідь на запит авторизації) (рис. 7.6).

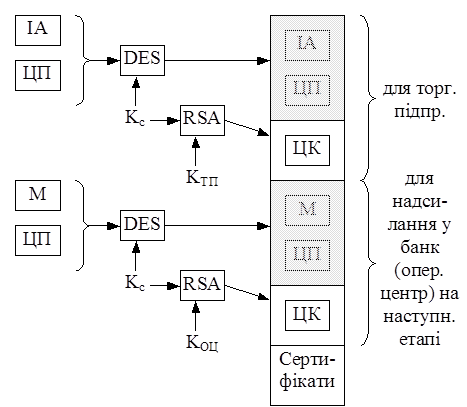


Рис. 7.6 – Повідомлення “відповідь на запит авторизації”(Authorization Response)

Це повідомлення складається з таких блоків інформації.

1.  Інформація авторизації (ІА). Включає блок авторизації, підписаний особистим ключем цифрового підпису шлюзу платіжної мережі і шифрований згенерованим шлюзом платіжної мережі одноразовим ключем для схеми симетричного шифрування. Крім того, включає цифровий конверт, що містить цей одноразовий ключ, шифрований за допомогою відкритого ключа продавця, використовуваного для обміну ключами.

2.  Мандат на одержання платежу (М) (capture token). Ця інформація буде використана для здійснення платежу згодом. Даний блок має ту ж форму, що і попередній, тобто містить підписаний і шифрований мандат з цифровим конвертом. Цей мандат не обробляється продавцем, а повинний бути просто повернутий їм у тім же виді шлюзу платіжної мережі в запиті на оплату.

3.  Сертифікати. Сертифікат цифрового підпису шлюзу платіжної мережі.

Одержавши підтвердження авторизації платежу від шлюзу платіжної мережі, продавець може виконати доставку товарів чи послуг покупцю.

7.3.9 Повідомлення “запит на оплату”

Щоб одержати плату за товари чи послуги, продавець звертається до шлюзу платіжної мережі з ініціативою виконання транзакції одержання платежу, що складається з двох повідомлень: повідомлення запиту на одержання оплати і повідомлення відповіді на запит на одержання оплати.

Структура повідомлення “запит на оплату” (Capture Request) представлена на рис. 7.7.

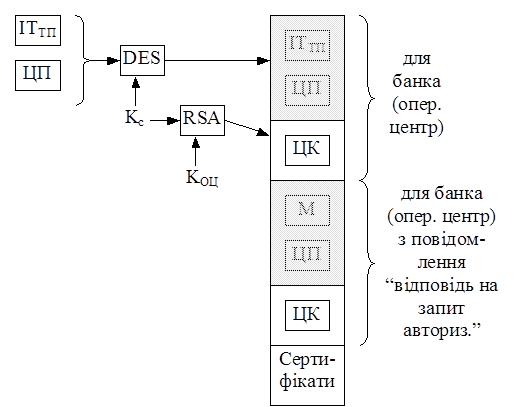


Рис. 7.7 – Повідомлення “запит на оплату”(Capture Request)

Для повідомлення Capture Request(запит на оплату) продавець генерує, підписує і шифрує блок даних запиту на оплату, що включає суму платежу й ідентифікатор транзакції (ІТТП). Дане повідомлення повинне також включати раніше отриманий (у повідомленні Authorization Response) шифрований мандат на одержання платежу для даної транзакции і, крім того, сертифікати ключів продавця для цифрового підпису й обміну ключами.

Одержавши це повідомлення, шлюз платіжної мережі дешифрує і перевіряє блок даних запиту на оплату, а також дешифрує і перевіряє блок мандата на одержання платежу. Потім перевіряється відповідність між даними цих двох блоків. Після цього шлюз платіжної мережі створює розрахунковий запит, що відсилається емітенту платіжної картки по закритій платіжній мережі. У результаті цього запиту кошти перераховуються на рахунок продавця.

Потім шлюз за допомогою повідомлення Capture Response (відповідь на запит на оплату) сповіщає продавця про перерахування коштів. Повідомлення містить підписаний і шифрований шлюзом блок даних відповіді на запит на оплату. Крім того, це повідомлення містить сертифікат цифрового підпису шлюзу платіжної мережі. Програмне забезпечення, установлене на комп'ютері продавця, одержавши дане повідомлення, зберігає його для використання в програмах обліку й узгодження коштів, що надходять від операційного центра.

**7.4 Опис лабораторної установки.**

Як лабораторна установка використовується ЕОМ із процесором не гірше ніж Intel 486. У якості програмного забезпечення для виконання роботи використовуються програми bank.exe, client.exe, merchant.exe.

7.4.1 Програма bank

Програма bank моделює спрощену роботу банка в прототоколі SET. Інтерфейс програми представлено на рис. 7.8.

Для початку роботи банку слід натиснути кнопку “начать обслуживание”.

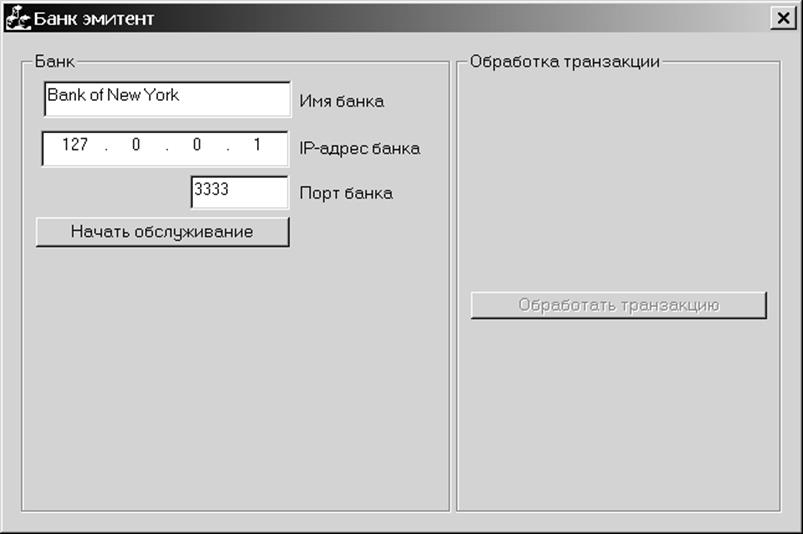


Рис.7.8 – Інтерфейс програми bank

7.4.2 Програма merchant

Програма merchant моделює спрощену роботу родавця або торгового підприємства в прототоколі SET. Інтерфейс програми представлено на рис. 7.9.

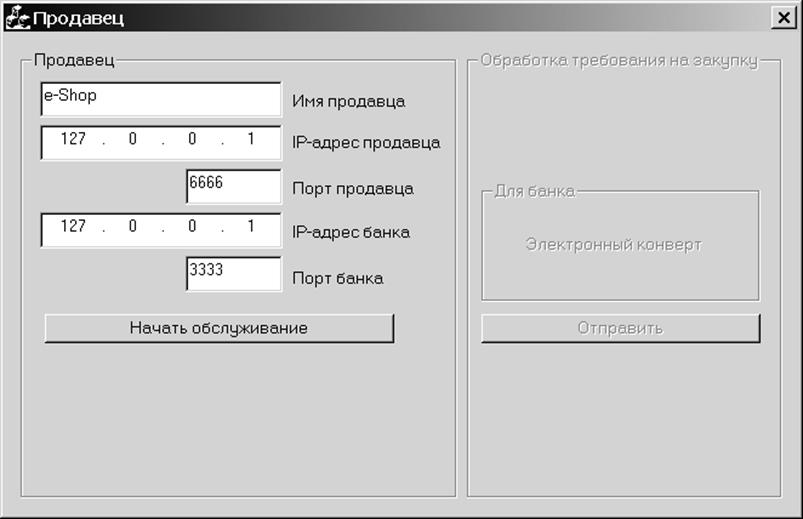


Рис. 7.9 – Інтерфейс програми merchant.

Для початку роботи продавця слід натиснути кнопку “начать обслуживание”. При цьому адреса і порт банка повинні співпадати з тими, що вказані у програмі bank.

7.4.3 Програма client

Програма client моделює спрощену роботу покупця власника платіжної картки в прототоколі SET. Інтерфейс програми представлено на рис. 7.10.

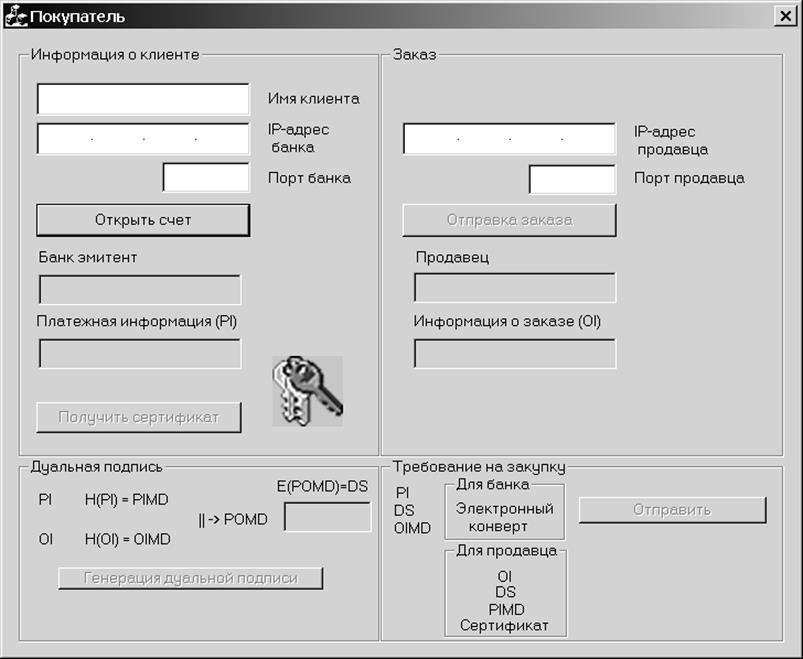


Рис. 7.10 – Інтерфейс програми client.

Для роботи з програмою client необхідно попередньо запустити програми bank та merchant і для обох цих програм почати обслуговування. Далі у програмі client потрібно:

1. Вказати у відповідних полях ім’я покупця і адресу та номер порта, які використовуються у програмі bank. Після цього натиснути кнопку “открыть счет”. При цьому у полі “банк емитент” повинна з’явитися назва банка, у полі “платежная информация” повинне з’явитися цифрове значення та доступною повинна стати кнопка “получить сертификат”.

2. Натиснути кнопку “получить сертификат”.

3. Вказати у відповідних полях адресу та номер порта, які використовуються у програмі merchant. Після цього натиснути кнопку “отправка заказа”. У полі “продавец” повинно з’явитися ім’я продавця, у полі “информация о заказе” повинне з’явитися цифрове значення та доступною повинна стати кнопка “генерация дуальной подписи”.

4. Натиснути кнопку “генерация дуальной подписи”. При цьому повинне з’явитися цифрове значення дуального цифрового підпису та доступною повинна стати кнопка “отправить” на панелі “требование на закупку”.

5. Натиснути кнопку “отправить”. У частині окна “требование на закупку” повинне з’явитися повідомлення “транзакция обрабатывается”.

6. У программі merchant потрібно підтвердити обробку повідомлення “запит на покупку” шляхом натискання кнопки “отправить”.

7. У программі bank потрібно підтвердити обробку транзакції шляхом натискання кнопки “обработать транзакцию”. При цьому у програмах client та merchant повинні відобразитись повідомлення “транзакция обработана”.

**7.5 Порядок виконання роботи і методичні вказівки з її виконання**

1 Промоделювати порядок взаємодії участників платежів SET за допомогою програм bank.exe, client.exe, merchant.exe (див. опис програм у пункті 7.4).

2 Вивчити порядок формування та перевірки дуального підпису.

3 Вивчити структуру та порядок формування основних повідомлень у протоколі SET: «запит на покупку», «запит авторизації», «відповідь на запит авторизації», «запит на оплату».

**7.6 Зміст звіту**

1. Назва і мета роботи.

2. Короткі відомості з теорії.

3. Cтруктурна схема одного з розглянутих повідомлень протокола SET.

4. Можливі погрози безпеки в протоколі SET.

5. Аналіз сильних і слабких сторін системи захисту протокола SET.

6. Висновки по роботі.

**7.7 Контрольні запитання і завдання**

1. Участники платежів по протоколу SET.

2. Основні етапи виконання платежів по протоколу SET.

3. Загальні вимоги до ключів та ключових параметрів.

4. Призначення, порядок формування і перевірки дуального підпису.

5. Структура і порядок формування повідомлення «запит на покупку».

6. Структура і порядок формування повідомлення «запит авторизації».

7. Структура і порядок формування повідомлення «відповідь на запит авторизації».

8. Структура і порядок формування повідомлення «запит на оплату».

**Лабораторна робота №8**

**Розрахунок внутрішньої норми дохідності інвестицій**

## 8.1. Мета роботи.

Зрозуміти суть та метод обчислення показника «внутрішня норма дохідності інвестицій», навчитись використовувати функцію ВСД у Microsoft Excel та визначати доцільність інвестування із врахуванням внутрішньої норми дохідності проекту.

## 8.2. Методичні вказівки з організації самостійної роботи студентів.

При підготовці до лабораторної роботи необхідно:

- вивчити і засвоїти основні поняття і визначення підрозділу 8.4;

- опрацювати приклади задач на визначення внутрішньої норми дохідності.

## 8.3. Опис лабораторної установки.

Використовується комп’ютер із процесором не нижче ніж Intel 486. У якості програмного забезпечення для виконання роботи використовуються браузер та пакет MS Office.

## 8.4. Теоретичні відомості та їх застосування на практиці.

Функція **ВСД** (внутренняя ставка доходности) у Microsoft Excel обчислює норму дисконтування IRR=j, при якій NPV=0.

**NPV** (Net Present Value) чистий приведений дохід – це різниця між приведеною до теперішньої вартості шляхом дисконтування сумою грошового потоку за період експлуатації інвестиційного проекту та сумою інвестованих у його реалізацію коштів.

Чистий приведений дохід розраховують за формулою

,

де ІС – інвестиція, яка протягом n років буде генерувати доходи в розмірі Р1, Р2, …, Р n, j – коефіцієнт дисконтування.

Внутрішня норма дохідності (Internal rate of return - **IRR**) – це дисконтна ставка, за якої майбутня вартість грошового потоку від інвестицій приводиться до теперішньої вартості інвестованих коштів.

Внутрішню ставку дохідності можна охарактеризувати і як дисконтну ставку, за якою чистий приведений дохід у процесі інвестування буде приведено до нуля, тобто IRR=j, при якій NPV=0.

Внутрішню норму дохідності розраховують за такими формулами:

1. IRR=j, яке знаходиться із рівняння , де – притік (відтік) коштів у k-му році, k = 1, 2, …, n; IC=CF0, де ІС – інвестиція, j – коефіцієнт дисконтування, n – тривалість проекту.
2. приблизно величина внутрішньої норми дохідності може бути отримана з формули

,

де – значення коефіцієнта дисконтування, при якому (), – значення коефіцієнта дисконтування, при якому (), . Тобто вибираються два значення коефіцієнта дисконтування таким чином, щоб в інтервалі функція NPV=f(j) змінювала своє значення з «+» на «-» або з «-» на «+».

Синтаксис ВСД у Microsoft Excel: ВСД (значення, передбачення), де

Значення – це масив чисел або адрес, для яких потрібно визначити внутрішню ставку дохідності. Значення повинні містити принаймні одне додатне та одне від’ємне число.

Передбачення – це величина, про яку припускається, що вона близька до результату ВСД.

**Приклад**. Витрати інвестиційного проекту становлять 500 000 грн. Очікувані доходи становлять 50 000 грн., 100 000 грн., 300 000 грн., 200 000 грн. протягом наступних 4 років. Потрібно встановити економічну доцільність проекту за внутрішньою нормою дохідності, якщо ринкова норма доходу 12% річних.

Розв’язання. Комірки А1:А5 – масив комірок Microsoft Excel, які містять значення -500, 50, 100, 300, 200. Внутрішня норма дохідності ВСД(А1:А5)=9,25%. Це менше, ніж ринкова норма, тому проект має бути відхилено.

Задачі для лабораторної роботи.

1. Пропонується вкласти 250 000 грн. у цінні папери. Інвестиційний проект розрахований на 15 років. Очікувані доходи такі: протягом перших 4 років по 24 000 грн. на рік, у наступні роки – по 30 000 грн. на рік. Чи варто приймати таку пропозицію, якщо ринкова норма прибутку 8% річних?
2. Є два альтернативних інвестиційних проекти (грн.)

|  |  |  |  |
| --- | --- | --- | --- |
| Проекти | ІС | Р1 | Р2 |
| А | -4000 | 2500 | 3000 |
| Б | -2000 | 1200 | 1500 |

Ранжуйте проекти за критеріями IRR, NPV, якщо j = 10%.

1. Розглядаються два альтернативних інвестиційних проекти (грн.)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Проекти | ІС | Р1 | Р2 | Р3 | Р4 | Р5 |
| А | -50000 | 15625 | 15625 | 15625 | 15625 | 15625 |
| Б | -80000 | - | - | - | - | 140000 |

Зробіть вибір при j = 5% j = 10%.

1. Як Ви оцінюєте доцільність включення проекту до інвестиційного портфелю підприємства, якщо вкладення капіталу в проект становить 110 000 грн., а грошові потоки за роки проекту становлять 30 000 грн., 40 000 грн., 40 000 грн., 50 000 грн., 30 000 грн. Ставка дисконтування 13% річних.
2. Визначте, якими мають бути початкові витрати за проектом, щоб забезпечити такі доходи: 2000 грн., 5000 грн., 6000 грн., 8000 грн., 10000 грн. при нормі доходу за проектом 9% річних.
3. Банк розглядає три можливі проекти

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Проект | Інвестиції, тис. грн. | Річні надходження, тис. грн. | | | |
| 1 | 2 | 3 | 4 |
| А | 400 | 360 | 200 |  |  |
| Б | 400 | 220 | 180 | 160 |  |
| В | 400 | 200 | 200 | 200 | 200 |

Коефіцієнт дисконтування 18% річних. Який проект має перевагу?

**ЛАБОРАТОРНА РОБОТА №9**

**ОФОРМЛЕННЯ РЕГЛАМЕНТНИХ ДОКУМЕНТІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ**

## 9.1. Мета роботи.

Ознайомитися з документацією, яку заповнює адміністратор інформаційної безпеки банку і навчитись її оформлювати.

## 9.2. Методичні вказівки з організації самостійної роботи студентів.

При підготовці до лабораторної роботи необхідно:

- засвоїти лекційний матеріал, який стосується роботи адміністратора інформаційної безпеки банку;

- підготувати відповіді на питання, наведені в методичних вказівках.

## 9.3. Опис лабораторної установки.

Використовується комп’ютер із процесором не нижче ніж Intel 486. У якості програмного забезпечення для виконання роботи використовуються браузер та пакет MS Office.

## 9.4. Регламентовані НБУ форми документації з інформаційної безпеки банку.

Завдання лабораторної роботи базуються на  Постанові Національного банку України [Про затвердження нормативно-правових актів з питань інформаційної безпеки](http://zakon.rada.gov.ua/go/v0829500-15)  
від 26.11.2015 № **829.**

1.     Ознайомтесь із обов’язками адміністратора інформаційної безпеки банку. Заповніть від свого імені зобов’язання адміністратора  інформаційної безпеки вибраного Вами комерційного банку.

### Зобов'язання адміністратора інформаційної безпеки

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  (найменування організації)

|  |
| --- |
| Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, який призначений                                                                   (посада, прізвище, ім'я, по батькові) згідно з внутрішнім документом від "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р. N \_\_\_ адміністратором інформаційної безпеки організації, ознайомлений з правилами використання, зберігання й обліку засобів захисту інформації та інформаційної безпеки під час роботи з електронними банківськими документами і зобов'язуюся:  1. Забезпечувати та контролювати виконання режимних вимог до приміщень, у яких обробляються електронні документи, використовуються і зберігаються засоби захисту інформації Національного банку України.  2. Забезпечувати отримання, зберігання, облік і контроль за використанням засобів захисту інформації Національного банку України.  3. Виконувати правила використання і зберігання засобів захисту інформації Національного банку України та здійснювати контроль за технологією оброблення електронних банківських документів.  4. Знати нормативно-правові акти Національного банку України з питань інформаційної безпеки та здійснювати контроль за їх виконанням відповідальними особами.  5. Надавати інформацію щодо інформаційної безпеки Департаменту інформаційної безпеки Національного банку України на його запити.  6. Підтримувати зв'язок з Департаментом інформаційної безпеки Національного банку України з питань інформаційної безпеки.  7. Передати всі засоби захисту інформації, ключі від сейфів, особисті печатки тощо в установленому порядку в останній день роботи в разі звільнення з роботи.  8. Забезпечувати конфіденційність системи захисту інформації організації, постійно вживати заходів щодо підвищення рівня захищеності інформації в організації.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                     (дата, підпис)  Знання нормативно-правових актів Національного банку України з питань інформаційної безпеки, затверджених постановою Правління Національного банку України від \_\_\_ \_\_\_\_\_\_\_\_\_\_\_ 2015 року N \_\_\_, перевірено. |

|  |  |
| --- | --- |
| Представник Департаменту інформаційної безпеки Національного банку України | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (підпис, ініціали, прізвище) |

2.     Вивчіть регламентовану Національним банком України таблицю суміщення функціональних обов’язків фахівців із банківських інформаційних технологій та інформаційної безпеки.

|  |  |
| --- | --- |
|  | Додаток 4  до Правил  (пункт 10 розділу II) |
|  |  |

ТАБЛИЦЯ   
суміщення функціональних обов'язків

| № з/п | Функціональні обов'язки | Адміністратор інформаційної безпеки | Адміністратор АРМ-СЕП/ АРМ-НБУ-інф | Оператор АРМ бухгалтера (ключ типу B) | Оператор АРМ технолога (ключ типу A) | Операціоніст САБ | Оператор АРМ інформаційних задач | Адміністратор САБ | Відповідальний за розроблення САБ | Адміністратор локальної мережі | Адміністратор електронної пошти |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | Адміністратор інформаційної безпеки | - | Х | Х | Х | Х | Х | В | Х | В | В |
| 2 | Адміністратор АРМ-СЕП/АРМ-НБУ-інф | Х | - | Х | В | Д | Д | Х | Х | В | В |
| 3 | Оператор АРМ бухгалтера (ключ типу В) | Х | Х | - | Х | Х | Д | Х | Х | В | В |
| 4 | Оператор АРМ технолога (ключ типу А) | Х | В | Х | - | Х | Д | Д | Х | В | В |
| 5 | Операціоніст САБ | Х | Д | Х | Х | - | Д | Х | Х | В | В |
| 6 | Оператор АРМ інформаційних задач | Х | Д | Д | Д | Д | - | Д | Д | Д | Д |
| 7 | Адміністратор САБ | В | Х | Х | Д | Х | Д | - | В | Д | Д |
| 8 | Відповідальний за розроблення САБ | Х | Х | Х | Х | Х | Д | В | - | Х | Х |
| 9 | Адміністратор локальної мережі | В | В | В | В | В | Д | Д | Х | - | Д |
| 10 | Адміністратор електронної пошти | В | В | В | В | В | Д | Д | Х | Д | - |

|  |  |
| --- | --- |
| Примітки: | Д - суміщення обов'язків дозволено (не більше двох обов'язків одночасно);  В - суміщення можливе як виняток (не більше двох обов'язків одночасно) на час тимчасової відсутності відповідальної особи (хвороба, відпустка), яка виконує ці функції. Якщо суміщення викликано іншими причинами, то необхідно звернутися до Департаменту інформаційної безпеки Національного банку України для отримання відповідного дозволу на таке суміщення;  Х - суміщення обов'язків не дозволено. |

3.     Ознайомтесь із обов’язками адміністратора/оператора АРМ Банку. Кожен працівник банку, який працює з електронними документами, підписує зобов’язання дотримуватись правил інформаційної безпеки. Заповнені зобов’язання зберігаються в адміністратора з інформаційної безпеки. Заповніть два зобов’язання від імені технолога, який є оператором АРМ технолога, та бухгалтера, який є оператором АРМ бухгалтера.

|  |
| --- |
| Додаток 3 до Правил (пункт 7 розділу II) |

### ЗОБОВ'ЯЗАННЯ

|  |
| --- |
| Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, який призначений                                                  (посада, прізвище, ім'я, по батькові)  згідно з внутрішнім документом \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                                                                                    (найменування організації)  від "\_\_\_" \_\_\_\_\_\_\_\_\_ 20\_\_ р. № \_\_\_ виконувати обов'язки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                                                                                               (адміністратора/оператора та назва АРМ)  ознайомлений з правилами використання засобів захисту інформації під час роботи з електронними банківськими документами і зобов'язуюся:  1. Виконувати правила використання та зберігання власних таємних ключів і дотримуватися технології оброблення електронних банківських документів.  2. Не передавати іншим особам власні таємні ключі.  3. Не розголошувати мережеві паролі, паролі входу до системи автоматизації банку, інших програмно-технічно комплексів і пароль власного таємного ключа.  4. У разі спроби інших осіб отримати від мене засоби захисту інформації, підозри щодо втрати контролю за своїми таємними ключами або їх втрати негайно повідомити про це адміністратора інформаційної безпеки організації.  5. У разі звільнення з роботи в останній день роботи повернути адміністратору інформаційної безпеки організації всі засоби захисту інформації, ключі від сейфів, особисті печатки тощо.  6. Дотримуватися вимог щодо забезпечення конфіденційность системи захисту інформації організації.  Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, попереджений про те, що всі                                              (прізвище, ім'я, по батькові)  електронні банківські документи, які мають електронний цифровий підпис, зроблений з використанням мого таємного ключа, уважаються підтвердженими мною, а електронний цифровий підпис - накладеним мною.  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                              (дата, підпис)  Знання правил використання та зберігання таємних ключів перевірено.  Адміністратор інформаційної безпеки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                                                                  (підпис, ініціали, прізвище) |

4. Інформаційну безпеку у СЕП забезпечує Національний банк України. Для цього він забезпечує комерційні банки програмно-апаратними засобами захисту інформації. Заповніть акт передачі/повернення таких засобів.

|  |
| --- |
| Додаток 2 до Положення (пункт 23 розділу III) |

|  |  |
| --- | --- |
| ПОГОДЖЕНО Керівник (заступник керівника)  організації  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_      (підпис, ініціали, прізвище)  "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.  М.П. | ЗАТВЕРДЖЕНО Директор (заступник директора) Департаменту інформаційної безпеки Національного банку України \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_            (підпис, ініціали, прізвище)  "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.  М.П. |

### **АКТ про приймання-передавання апаратних засобів захисту інформації Національного банку України**

|  |  |
| --- | --- |
| м. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р. |
| Представник Департаменту інформаційної безпеки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                                                                                                     (ініціали, прізвище)  та представник \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                                 (найменування організації)                                    (ініціали, прізвище)  відповідно до договору від \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_\_\_\_\_ здійснили передавання  від Національного банку України до \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/                                                                                                 (найменування організації)  від \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ до Національного банку України                                         (найменування організації)  таких засобів захисту інформації Національного банку України:  апаратури криптографічного захисту № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_у комплекті;  смарт-карток № \_\_\_\_\_\_\_\_\_\_\_\_\_.  **Примітка.** Подається перелік засобів захисту інформації Національного банку України, що передаються з наданням номерів, які візуально доступні для зчитування на засобах захисту інформації.  Здав \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                             (підпис, ініціали, прізвище)  Прийняв \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                              (підпис, ініціали, прізвище) | |

5.     Заповніть журнал обліку адміністратора інформаційної безпеки (по три записи у кожній таблиці).

|  |
| --- |
| Додаток 1  до Правил  (підпункт 6 пункту 4 розділу II) |

ЖУРНАЛ   
обліку адміністратора інформаційної безпеки

Розділ I. Перелік відповідальних за роботу із засобами захисту інформації Національного банку України осіб:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № з/п | Прізвище, ініціали відповідальної особи | Функціональні обов'язки | Дата і номер документа про призначення | Дата і номер документа про звільнення від функціональних обов'язків | Причина звільнення |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |

Розділ II. Перелік засобів захисту інформації Національного банку України:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | № з/п | Дата отримання (копіювання) | | Назва | Дата і підпис відповідальної особи про отримання | Дата і підпис відповідальної особи про повернення | Примітки |
|  | 1 | 2 | | 3 | 4 | 5 | 6 |
|  |  |  | |  |  |  |  |
| \_\_\_\_\_\_\_\_\_\_  Примітка. | | | у колонці 6 за потреби робляться короткі робочі записи про факти втрати контролю за засобами захисту інформації тощо. | | | | |
|  |  |  |  |  |  |  |  |

Розділ III. Перелік таємних ключів, що генерувалися в організації відповідальними особами:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № з/п | Назва ТК | Назва файла ТК або номер захищеного носія ТК | Операція (генерація / копіювання / генерація на видалення) | Дата і підпис відповідальної особи, яка генерувала/копіювала та отримала ТК | Дата і підпис відповідальної особи, яка знищувала ТК | Дата і підпис відповідальної особи, яка вилучила ВК з ТВК |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |

Розділ IV. Перелік осіб, які мають допуск до приміщення з АРМ-СЕП/АРМ-НБУ-інф:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № з/п | Прізвище, ініціали особи, яка має допуск до приміщення з АРМ-СЕП/АРМ-НБУ-інф | Функціональні обов'язки | Дата і номер документа про допуск | Дата і номер документа про скасування допуску | Примітки |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |

Розділ V. Перелік ключів від сейфів (металевих шаф) відповідальних осіб, у яких зберігаються засоби захисту інформації Національного банку України:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № з/п | Призначення ключа | № ключа | Прізвище, ініціали відповідальної особи, яка зберігає ключ | Примітки |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |

Розділ VI. Перелік особистих печаток (штампів, пломбіраторів) відповідальних осіб для опечатування засобів захисту інформації Національного банку України:

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | № печатки (штампів, пломбіраторів) | Прізвище, ініціали відповідальної особи | Примітки |
| 1 | 2 | 3 | 4 |
|  |  |  |  |

Розділ VII. Облік приймання-передавання засобів захисту інформації Національного банку України, за які несе відповідальність адміністратор інформаційної безпеки:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | № з/п | Назва, версія, дата виготовлення засобів захисту інформації | | Дата, час отримання | Підпис адміністратора інформаційної безпеки 1-ї зміни | Дата, час отримання | Підпис адміністратора інформаційної безпеки 2-ї зміни |
|  | 1 | 2 | | 3 | 4 | 5 | 6 |
|  |  |  | |  |  |  |  |
| \_\_\_\_\_\_\_\_\_\_  Примітка. | | | Відмітки про приймання-передавання засобів захисту інформації Національного банку України робляться щодня в разі двозмінної роботи адміністратора інформаційної безпеки або у зв'язку з відсутністю основного адміністратора інформаційної безпеки - відпустка, навчання, хвороба тощо. | | | | |
|  |  |  |  |  |  |  |  |

Розділ VIII. Облік приймання-передавання таємних ключів відповідальних осіб, що зберігаються в адміністратора інформаційної безпеки організації:

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | № з/п | Назва файла ТК або номер захищеного носія ТК | | Дата, час отримання | Підпис відповідальної особи | Дата, час повернення | Підпис адміністратора інформаційної безпеки | Примітки |
|  | 1 | 2 | | 3 | 4 | 5 | 6 | 7 |
|  |  |  | |  |  |  |  |  |
| \_\_\_\_\_\_\_\_\_\_  Примітки: | | | не враховуються таємні ключі тих операторів робочих і технологічних місць САБ, які зберігають власні таємні ключі в особистих сейфах;  якщо оператор (операціоніст) не отримав власного таємного ключа для роботи, то в колонках 3 і 4 ставиться прочерк;  якщо строк дії таємного ключа закінчився, то в колонках 5 і 6 робиться відмітка про це;  у разі потреби допускається ведення не загального обліку таємних ключів, а індивідуального - за кожною відповідальною особою;  допускається зберігання облікових форм у швидкозшивачах. У цьому разі швидкозшивач є додатком до журналу обліку. | | | | | |
|  |  |  |  |  |  |  |  |  |

Розділ IX. Облік перевірок дотримання правил використання і зберігання засобів захисту інформації Національного банку України, проведених адміністратором інформаційної безпеки організації:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № з/п | Дата перевірки | Порушення виявлено/не виявлено | Опис порушення | Підпис адміністратора інформаційної безпеки |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |

6.     Заповніть ЖУРНАЛ приймання-передавання засобів захисту інформації Національного банку України адміністратора АРМ-СЕП/АРМ-НБУ-інф (три записи)

|  |  |
| --- | --- |
|  | Додаток 5  до Правил  (підпункт 12 пункт 12 розділу III) |

ЖУРНАЛ   
приймання-передавання засобів захисту інформації Національного банку України адміністратора АРМ-СЕП/АРМ-НБУ-інф

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № з/ п | Дата | Час отримання засобів захисту з сейфа | | Прізвище, ініціали, підпис адміністратора АРМ-СЕП/ АРМ-НБУ-інф 1-ї зміни | Час отримання засобів захисту від 1-ї зміни | Прізвище, ініціали, підпис адміністратора АРМ-СЕП/ АРМ-НБУ-інф 2-ї зміни | Час повернення засобів захисту до сейфа | Прізвище, ініціали, підпис адміністратора АРМ-СЕП/ АРМ-НБУ-інф 2-ї зміни | № печатки |
| 1 | 2 | 3 | | 4 | 5 | 6 | 7 | 8 | 9 |
|  |  |  | |  |  |  |  |  |  |
| \_\_\_\_\_\_\_\_\_\_  Примітки: | | | Адміністратори АРМ-СЕП/АРМ-НБУ-інф вносять до журналу записи про всі переміщення і зміни засобів захисту інформації Національного банку України АРМ-СЕП/АРМ-НБУ-інф.  Адміністратори АРМ-СЕП мають право не відключати АКЗІ від комп'ютера під час передавання зміни та після закінчення роботи. | | | | | | |
|  |  |  |  |  |  |  |  |  |  |

7.     У випадку розроблення Національним банком України і введення в дію нових засобів захисту інформації старі потрібно знищити. Заповніть відповідний акт.

|  |
| --- |
| Додаток 7 до Правил (пункт 28 розділу V) |

|  |  |
| --- | --- |
|  | ЗАТВЕРДЖЕНО Керівник (заступник керівника) організації \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                    (підпис, ініціали, прізвище)  "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.  М.П. |

### **АКТ про знищення засобів захисту інформації Національного банку України**

|  |  |
| --- | --- |
| м. \_\_\_\_\_\_\_\_\_\_\_\_ | "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р. |

|  |
| --- |
| Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, адміністратор                                                                 (прізвище, ім'я, по батькові)  інформаційної безпеки відповідно до листа Департаменту інформаційної безпеки Національного банку України від "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р. № \_\_\_ знищив програмний модуль генерації ключів та його копію (версія \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, дата виготовлення \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) згідно з Правилами організації захисту електронних банківських документів з використанням засобів захисту інформації Національного банку України, затвердженими постановою Правління Національного банку України від \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2015 року № \_\_\_.  Адміністратор інформаційної безпеки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                                                                                  (підпис, ініціали, прізвище) |

8.     Заповніть ЖУРНАЛ приймання-передавання таємних ключів робочих і технологічних місць (три записи).

|  |  |
| --- | --- |
|  | Додаток 6  до Правил  (підпункт 11 пункту 13 розділу IV) |

ЖУРНАЛ   
приймання-передавання таємних ключів робочих і технологічних місць

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | № з/п | Назва ТК | | Дата, час отримання | Підпис відповідальної особи 1-ї зміни | Дата, час отримання | Підпис відповідальної особи 2-ї зміни |
|  | 1 | 2 | | 3 | 4 | 5 | 6 |
|  |  |  | |  |  |  |  |
| \_\_\_\_\_\_\_\_\_\_  Примітка. | | | Відповідальні особи зобов'язані вносити до журналу записи про приймання-передавання таємних ключів щодня в разі їх двозмінної роботи або у зв'язку з відсутністю основної відповідальної особи - відпустка, навчання, хвороба тощо. | | | | |
|  |  |  |  |  |  |  |  |

9.     У зв'язку зі зміною моделі обслуговування консолідованого кореспондентського рахунку банку втрачається необхідність у засобах захисту інформації за попередньою моделлю обслуговування. Заповніть акт повернення до НБУ засобів захисту інформації та передавання журналів в архів.

|  |
| --- |
| Додаток 3 до Положення (пункт 29 розділу III) |

|  |  |
| --- | --- |
| ПОГОДЖЕНО Директор (заступник директора) Департаменту інформаційної безпеки Національного банку України \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_              (підпис, ініціали, прізвище)  "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.  М.П. | ЗАТВЕРДЖЕНО Керівник (заступник керівника) організації   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                    (підпис, ініціали, прізвище)  "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.  М.П. |

### **АКТ про повернення до Департаменту інформаційної безпеки Національного банку України, знищення, передавання до архіву засобів захисту інформації Національного банку України, справ і журналів обліку**

|  |  |
| --- | --- |
| м. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р. |
| У зв'язку з припиненням роботи \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                                                                           (найменування організації)  з "\_\_\_" \_\_\_\_\_ 20\_\_ р. у СЕП/інформаційних задачах Національного банку України і дії договору про використання засобів захисту інформації Національного банку України від "\_\_\_" \_\_\_\_\_ 20\_ р. № \_\_\_\_\_\_\_  або:  У зв'язку зі зміною моделі обслуговування консолідованого кореспондентського  рахунку банку \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                                                                (найменування організації)  у СЕП з "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р. і припиненням договору про використання засобів захисту інформації Національного банку України від "\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р. № \_\_\_\_\_\_ нами вжито таких заходів:  1. До Департаменту інформаційної безпеки Національного банку України повернуто:  апаратуру криптографічного захисту інформації № \_\_\_\_\_\_\_\_ у комплекті;  смарт-картки № \_\_\_\_\_\_\_\_\_\_\_\_;  2. Знищені на місці:  програмний модуль генерації ключів та його копія (версія \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  дата виготовлення \_\_\_\_\_\_\_\_\_\_\_\_);             таємний ключ АРМ-СЕП s\_\*300.\*;             копія таємного ключа АРМ-СЕП s\_\*300.\*;             таємні ключі АРМ бухгалтера  s\_\*.\* (перелік усіх ключів) - усього \_\_\_\_\_ ключів;             копії таємних ключів АРМ бухгалтера  s\_\*.\* (перелік усіх ключів) - усього \_\_\_\_\_ ключів;            таємні ключі операціоністів - усього \_\_\_\_\_ ключів;            програмний комплекс АРМ-СЕП;            таємний ключ АРМ-НБУ-інф s\_\*500.\*;            копія таємного ключа АРМ-НБУ-інф s\_\*500.\*;            програмний комплекс АРМ-НБУ-інф;            таємні ключі інформаційних задач - усього \_\_\_\_ ключів;  відкриті ключі АРМ-СЕП/АРМ-НБУ-інф, АРМ бухгалтера САБ, таблиці відкритих ключів АРМ-СЕП/АРМ-НБУ-інф, АРМ бухгалтера та інших робочих місць САБ, файли сертифікатів відкритих ключів для роботи в СЕП.  3. Передані в архів \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_:                                                                          (найменування організації)  справи і журнали обліку адміністратора інформаційної безпеки;  журнали обліку АРМ-СЕП/АРМ-НБУ-інф;  електронні архіви електронних платежів і відкритих ключів операціоністів.  4. Копій знищених і переданих документів, програм, засобів захисту інформації Національного банку України немає.  Адміністратор інформаційної безпеки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                                                                                   (підпис, ініціали, прізвище) | |

10. Згідно і Інструкцією НБУ «Про [міжбанківський переказ коштів в Україні в національній валюті](http://zakon.rada.gov.ua/go/z1035-06)» від 16.08.2006 № **320**

**п.** 10. Кожний учасник СЕП веде журнал обліку встановлення та заміни програмно-технічних засобів, що використовуються для роботи в СЕП, у якому зазначаються дата та час їх установлення (заміни), а також компоненти, що замінюються, їх назва, підстава для заміни, нова версія, прізвище, ініціали та підпис виконавця.

Обов'язковій реєстрації в журналі підлягають установлення та заміна таких компонентів:

прикладного програмного забезпечення СЕП, системи ЕП;

комп'ютера та його компонентів;

мережевої плати та/або мережевого клієнта;

системного програмного забезпечення;

апаратних засобів захисту інформації, а також настройка комп'ютера.

Розробіть форму такого журналу та внесіть 5 записів (по одному для кожного компонента ІС, що передбачений переліком НБУ).

11.  У зв'язку із звільненням (переведенням на іншу посаду) адміністратора інформаційної безпеки або у зв'язку з утратою чи компрометацією діючого ПМГК потрібно електронною поштою звернутись до НБУ із проханням видати новий ПГМК. Заповніть такий лист.

|  |
| --- |
| Додаток 8 до Правил (пункт 30 розділу V) |

### **ЕЛЕКТРОННА ПОШТА**

|  |  |
| --- | --- |
| Найменування організації | Національний банк України Департамент інформаційної безпеки |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                         (дата, № документа) |  |

|  |
| --- |
| Просимо надати новий програмний модуль генерації ключів у зв'язку із звільненням (переведенням на іншу посаду) адміністратора інформаційної безпеки \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                                                                                                                               (ініціали, прізвище)  (або у зв'язку з утратою чи компрометацією діючого ПМГК. Після вивчення всіх обставин копії матеріалів службового розслідування будуть надіслані на вашу адресу). |

|  |  |
| --- | --- |
| Керівник (заступник керівника) організації | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (підпис, ініціали, прізвище) |
| Виконавець \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_                              (ініціали, прізвище)  роб. тел. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

# Питання для захисту лабораторної роботи

1. Назвіть обов’язки адміністратора інформаційної безпеки.
2. Функціональні обов’язки яких посад може виконувати за сумісництвом адміністратор інформаційної безпеки банку?
3. Функціональні обов’язки яких посад може виконувати за сумісництвом адміністратор АРМ-СЕП/АРМ-НБУ-інф?
4. Із якими посадовими обов’язками може суміщати свої оператор АРМ бухгалтера?
5. Із якими посадовими обов’язками може суміщати свої оператор АРМ технолога?
6. Із якими посадовими обов’язками може суміщати свої операціоніст САБ?
7. Із якими посадовими обов’язками може суміщати свої оператор АРМ інформаційних задач?
8. Із якими посадовими обов’язками може суміщати свої адміністратор САБ?
9. Із якими посадовими обов’язками може суміщати свої відповідальний за розроблення САБ?
10. Із якими посадовими обов’язками може суміщати свої адміністратор локальної мережі?
11. Із якими посадовими обов’язками може суміщати свої адміністратор електронної пошти?
12. Функціональні обов’язки скількох посад можуть суміщати фахівці інформаційних технологій банку?
13. У яких випадках дозволяється виняткове суміщення посадових обов’язків без отримання дозволу НБУ?
14. Хто перевіряє виконання адміністраторами/операторами АРМ правил інформаційної безпеки?
15. Які аспекти роботи адміністраторів/операторів АРМ перевіряються у процесі моніторингу інформаційної безпеки банку?
16. Хто надає адміністратору інформаційної безпеки апаратні засоби захисту інформації у СЕП?
17. Які апаратні засоби використовуються для захисту інформації у СЕП?
18. Що означає примітка до Акту про приймання-передавання апаратних засобів захисту інформації НБУ: «Подається перелік засобів захисту інформації Національного банку України, що передаються з наданням номерів, які візуально доступні для зчитування на засобах захисту інформації»?
19. Назвіть програмні та апаратні засоби захисту інформації у СЕП.
20. Які події зобов’язаний протоколювати у журналі обліку встановлення та заміни програмно-технічних засобів, що використовуються для роботи в СЕП адміністратор інформаційної безпеки банку?

**ЛАБОРАТОРНА РОБОТА №10**

**ТЕРМІН ОКУПНОСТІ ІНВЕСТИЦІЙНОГО ПРОЕКТУ**

## 10.1. Мета роботи.

Навчитись визначати термін окупності інвестиційного проекту, тобто період, за який повернуться вкладення.

## 10.2. Методичні вказівки з організації самостійної роботи студентів.

При підготовці до лабораторної роботи необхідно:

- засвоїти лекційний матеріал, який стосується інвестування;

- вивчити і засвоїти основні поняття і визначення підрозділу 10.4;

- опрацювати приклади розв’язання задач.

## 10.3. Опис лабораторної установки.

Використовується комп’ютер із процесором не нижче ніж Intel 486. У якості програмного забезпечення для виконання роботи використовуються браузер та пакет MS Office.

## 10.4. Теоретичні відомості та практика їх застосування.

Функція КПЕР розраховує загальну кількість періодів виплат як єдиної суми вкладу (позики), так і для періодичних виплат на основі постійної процентної ставки та приведеної вартості інвестиції.

**КПЕР(ставка; плт; пс; бс; тип).**

**Значення аргументів:**

Ставка – відсоткова ставка за період;

Плт – фіксована виплата, яка здійснюється кожного періоду;

Пс – приведена вартість (сума, яка на поточний момент рівноцінна  ряду майбутніх платежів);

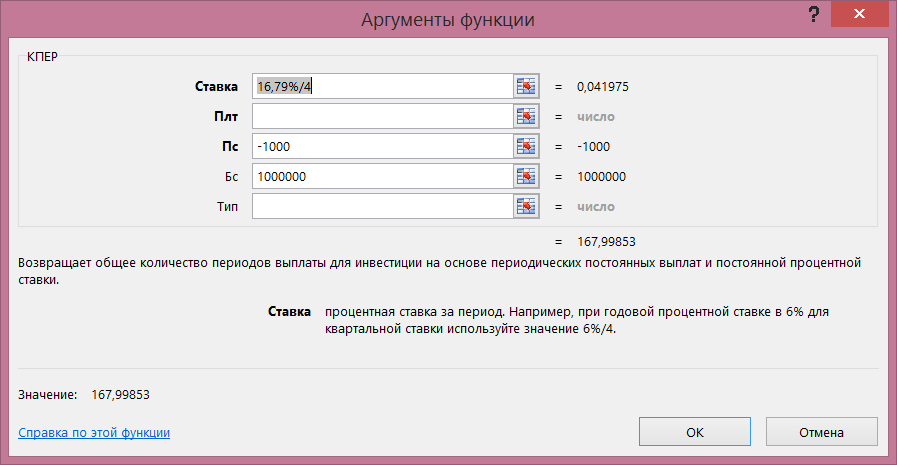
Бс – майбутня вартість;

Тип – число 0 – виплата вкінці періоду або 1 – виплата напочатку періоду. Якщо аргумент не вказаний, він дорівнює 0.

**Значення функції** обчислює термін окупності інвестиційного проекту, тобто кількість розрахункових періодів, через яку сума дисконтованих доходів дорівнюватиме величині інвестицій.

**Приклад 1.**

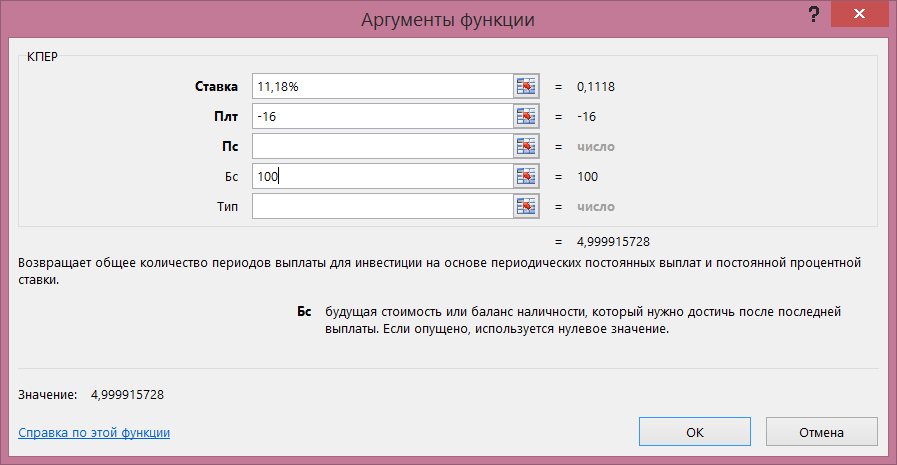
Розрахуйте, через скільки років вклад 1 тис. грн. досягне величини 1 млн. грн., якщо річна ставка за вкладом 16,79%, нарахування відсотків проводиться щокварталу.



Значення функції становить приблизно 168 кварталів або 42 роки.

**Приклад 2.**

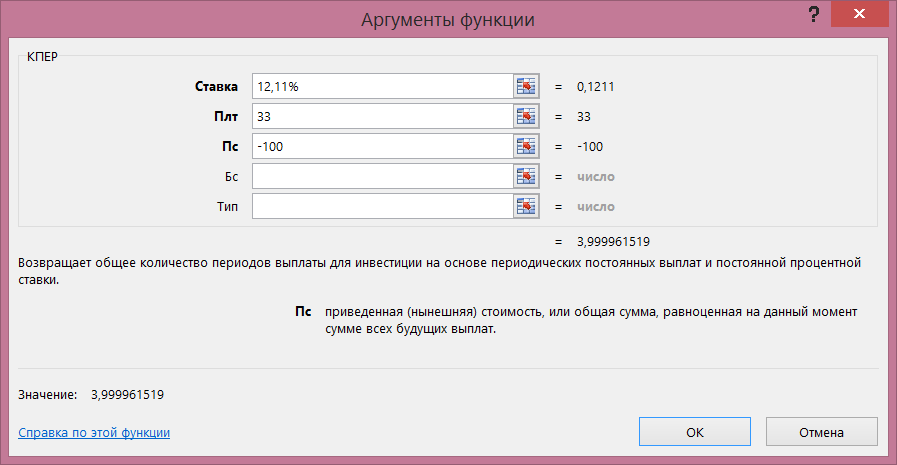
Для забезпечення майбутніх витрат створюється фонд – раз на рік вкладається 16 тис. грн. Кошти лежать на депозиті і на них нараховується 11,18% річних. Визначте, через скільки років обсяг фонду становитиме 100 тис. грн.



Відповідь: обсяг фонду 100 тис. грн. буде досягнуто через 5 років.

**Приклад 3.**

Очікується, що щорічні доходи від реалізації проекту становитимуть 33 тис. грн. Визначте термін окупності проекту, якщо інвестиції становлять 100 тис. грн., а норма дисконтування 12,11 %.



Відповідь: Проект окупиться через 4 роки.

**Задачі**

1. Позика розміром 66000 грн., яка видана під 36% річних, погашається щомісячними платежами по 6630 грн. Розрахуйте термін погашення позики.
2. Фірма створює резервний фонд і для цього щомісяця переводить у банк 8 тис. грн. Річна процентна ставка становить 16%. Визначте, через який час на рахунку буде 300 тис. грн.
3. Щомісяця сім’я робить внесок у банк 1 тис. грн. Річна відсоткова ставка депозиту 18%, нарахування відсотків щомісячне. Через який час сума накопичень буде достатньою для купівлі автомобіля вартістю 258 000 грн.?
4. Щомісяця пенсіонер автоматично перераховує на депозит «Копілка» 200 грн. під 16% річних із щомісячним нарахуванням відсотків. Через який час накопичиться сума, достатня для придбання холодильника вартістю 8 000 грн.?
5. На який термін був виданий кредит розміром 300 тис. грн. під 60% річних, якщо для погашення кредитор повернув у банк 380 тис. грн.?
6. Розрахуйте, через скільки років позика розміром 500 тис. грн. буде погашена щоквартальними виплатами по 100 тис. грн. при ставці 15% річних?
7. Розрахуйте, через скільки років вклад розміром 500 тис. грн. досягне розміру 1 млн. грн. при щомісячному нарахуванні процентів за ставкою 15,18% річних.

# ЛАБОРАТОРНА РОБОТА №11

# ВИЗНАЧЕННЯ ПРОЦЕНТНОЇ СТАВКИ У MS EXCEL

## 11.1. Мета роботи.

Навчитись обчислювати процентну ставку інвестування, необхідну для досягнення поставленої мети інвестора.

## 11.2. Методичні вказівки з організації самостійної роботи студентів.

При підготовці до лабораторної роботи необхідно:

- засвоїти лекційний матеріал, який стосується інвестицій;

- опрацювати приклади розв’язання задач.

## 11.3. Опис лабораторної установки.

Використовується комп’ютер із процесором не нижче ніж Intel 486. У якості програмного забезпечення для виконання роботи використовуються браузер та пакет MS Office.

## 11.4. Теоретичні відомості та їх застосування на практиці.

Функція СТАВКА визначає значення процентної ставки за один період. Для визначення річної процентної ставки отримане значення потрібно помножити на число періодів, які становлять рік.

СТАВКА (кпер; плт; пс; бс; тип; предположение)

Кпер – загальне число періодів платежів;

Плт – виплата, яка здійснюється кожного періоду;

Пс – приведена вартість, тобто загальна сума рівноцінна ряду майбутніх платежів;

Бс – майбутня вартість;

Тип – число 0 або 1, яке означає, коли повинна здійснюватись виплата: 1 – напочатку періоду, 0 – вкінці. Якщо аргумент не вказаний, він приймається рівним 0.

Предположение – передбачувана величина ставки (найчастіше не вказується).

Якщо потрібно розрахувати процентну ставку при відомій поточній вартості пс, майбутній вартості бс, числі періодів кпер, то формула набуде вигляду

СТАВКА (кпер; ; пс; бс; ; предположение)

При наявності періодичних платежів формула має вигляд

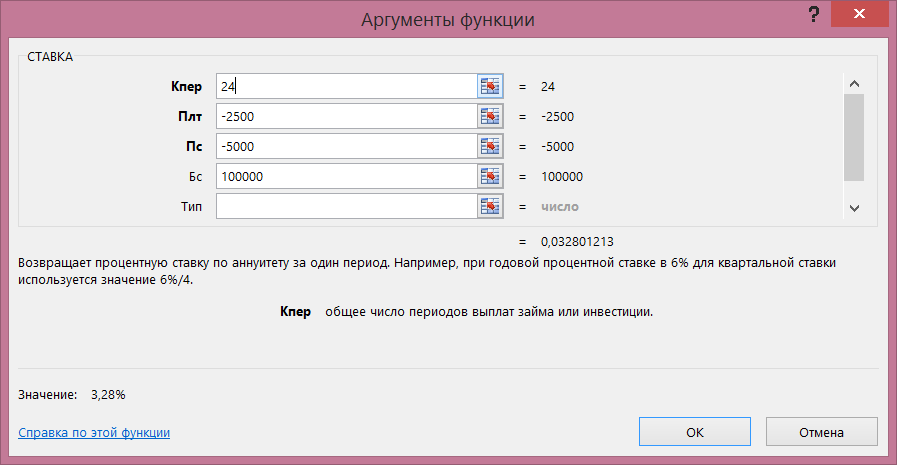
СТАВКА (кпер; ; плт; бс; тип; предположение)

Розрахунок процентної ставки розміром пс при рівномірному погашенні періодичними платежами ведеться за формулою

СТАВКА (кпер; плт; пс; ; ; предположение)

## Приклад

Компанії через 2 роки буде потрібно 100 000 грн. Компанія готова вкласти 5000 грн. відразу і по 2500 грн. кожного наступного місяця. Яким повинен бути процент на інвестиційні ресурси, щоб отримати необхідну суму в кінці другого року?



Отже, ставка за місяць становить 3,28%, а річна ставка 3,28%\*12=39,36%

## Задачі

1. Передбачається шляхом щоквартальних внесків постнумерандо (виплати вкінці періоду) по 35000 грн. протягом 3 років створити фонд розміром 500 000 грн. Якою повинна бути річна процентна ставка?
2. Поточна вартість ренти, яка має щомісячні рівні внески вкінці кожного місяця на термін 3 роки, дорівнює 100 000 грн. Нарощена вартість становить 300 000 грн. Визначте річну процентну ставку.
3. Визначте процентну ставку за місяць, яку потрібно встановити фінансовій компанії, щоб кредит у $2000 за 84 дні мав прибуток $120.
4. Якою повинна бути річна процентна ставка за вкладом 800000 грн., якщо його величина до кінця року становитиме 1 200 000 грн, проценти нараховуються щомісяця.
5. Розрахуйте процентну ставку для 3-річної позики розміром 5000 грн. із щоквартальним погашенням по 500 грн.
6. Ви маєте 20000 грн. і хочете подвоїти цю суму через 2 роки. Яке потрібно мінімальне значення процентної ставки?
7. Через рік син буде вступати до університету на платне навчання. Ціна освіти $5600. У батьків зараз є $4000. Під яку процентну ставку треба інвестувати гроші, щоб накопичити потрібну суму?
8. За виконану роботу підприємець повинен отримати 60000 грн. Замовник не має можливості розрахуватися зараз і пропонує відкласти строк оплати на 2 роки, після закінчення яких він зобов’язується виплатити 70000 грн. Чи вигідна підприємцю така пропозиція, якщо прийнятна норма прибутку становить 10% річних?

**ЛАБОРАТОРНА РОБОТА №12**

**РОЗРАХУНОК ПЕРІОДИЧНИХ ПЛАТЕЖІВ В EXCEL**

## 12.1. Мета роботи.

Зрозуміти суть основних і процентних виплат по кредиту та навчитись їх обчислювати засобами фінансових функцій Microsoft Excel.

## 12.2. Методичні вказівки з організації самостійної роботи студентів.

При підготовці до лабораторної роботи необхідно:

- засвоїти лекційний матеріал, який стосується банківського кредитування;

- опрацювати приклади розв’язання задач.

## 12.3. Опис лабораторної установки.

Використовується комп’ютер із процесором не нижче ніж Intel 486. У якості програмного забезпечення для виконання роботи використовуються браузер та пакет MS Office.

## 12.4. Теоретичні відомості та практика їх застосування.

Функція ПЛТ розраховує **суму періодичного платежу для ануїтету на основі постійності сум платежів і процентної ставки**.

**ПЛТ (ставка; кпер; пс; бс; тип)**

Аргументи функції:

Ставка – процентна ставка за період;

Кпер – загальна кількість періодів ануїтету;

Пс – приведена до поточного моменту вартість, яка рівноцінна ряду майбутніх платежів;

Бс – необхідне значення майбутньої вартості;

Тип – число 0 (виплата вкінці періоду), 1 (виплата напочатку періоду).

Якщо позика погашається неповністю, то потрібно вказати аргумент бс, який дорівнюватиме непогашеному залишку позики.

**Приклад.**

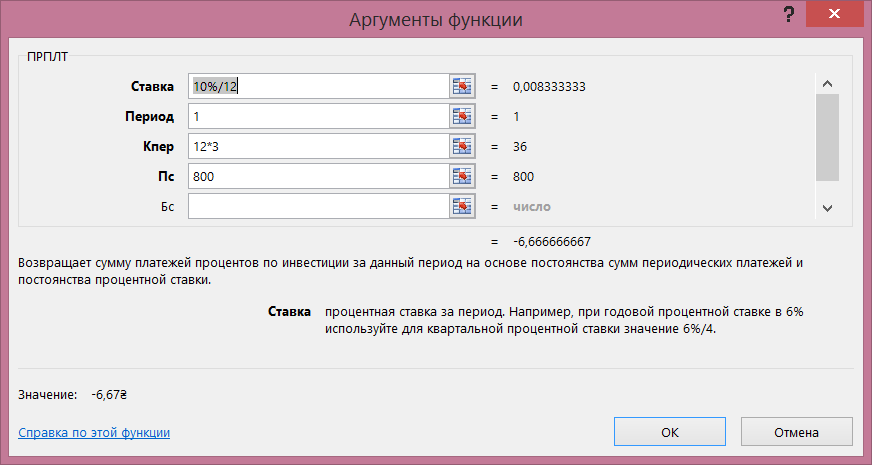
Потрібно накопичити 4000 грн. за 3 роки, відкладаючи однакову суму вкінці кожного місяця. Якою повинна бути ця сума, якщо ставка 12% річних?

**Платежі за процентами за заданий період за умови однакових періодичних виплат і постійної процентної ставки** розраховуються за допомогою функції ПРПЛТ.

**ПРПЛТ (ставка; період; кпер; пс; бс; тип)**

**Приклад.**

Розрахуйте платежі за процентами за перший місяць від трирічної позики у 800 тис. грн. при ставці 10% річних.



Отже, у перший місяць погашення позики потрібно сплатити 6667 грн. для погашення процентів.

**Сума основного платежу за позикою на вказаний період розраховується за допомогою функції ОСПЛТ.**

**ОСПЛТ (ставка; период; кпер; пс; бс; тип)**

Аргументи:

Ставка – процентна ставка за період;

Період – період, за який потрібно дізнатись суму основного платежу, діапазон допустимих значень [1; кпер];

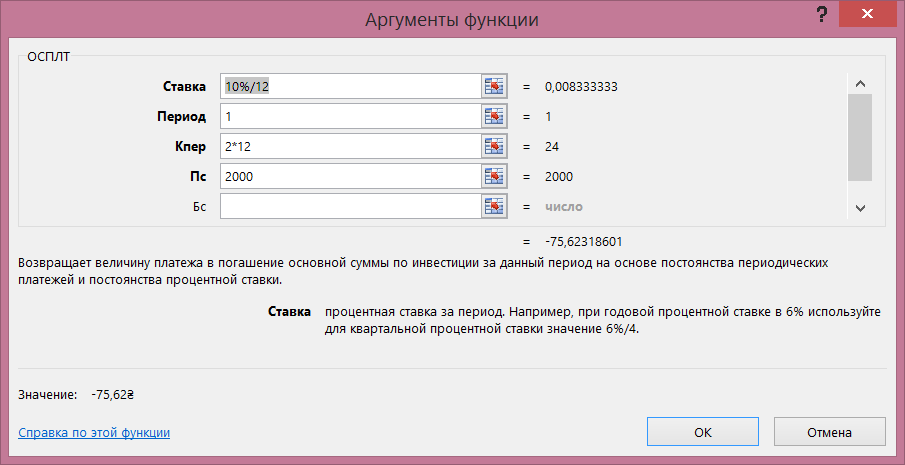
Кпер – загальна кількість періодів виплат;

Пс – теперішня вартість;

Тип - число 0 (виплата вкінці періоду), 1 (виплата напочатку періоду).

**Приклад.**

Визначте суму основного платежу з дворічної позики 2000 грн за перший місяць при ставці 10% річних. Нарахування процентів щомісяця.



Отже, платіж для погашення основної суми позики із заданими параметрами становить 75,62 грн.

**Накопичену суму платежів по процентах між двома періодами виплат обчислює функція ОБЩПЛАТ.**

ОБЩПЛАТ (ставка; кол\_пер; Нз; нач период; кон период; тип),

Ставка – процентна ставка за період;

Нач Период – номер першого періоду, включеного до обчислення. Періоди нумеруються з 1;

Кон Период – номер останнього періоду, включеного до обчислення;

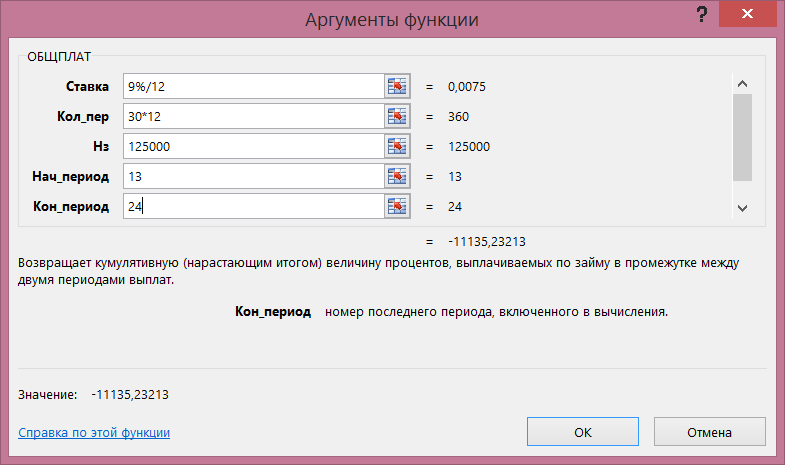
Кол\_пер – загальна кількість періодів виплат;

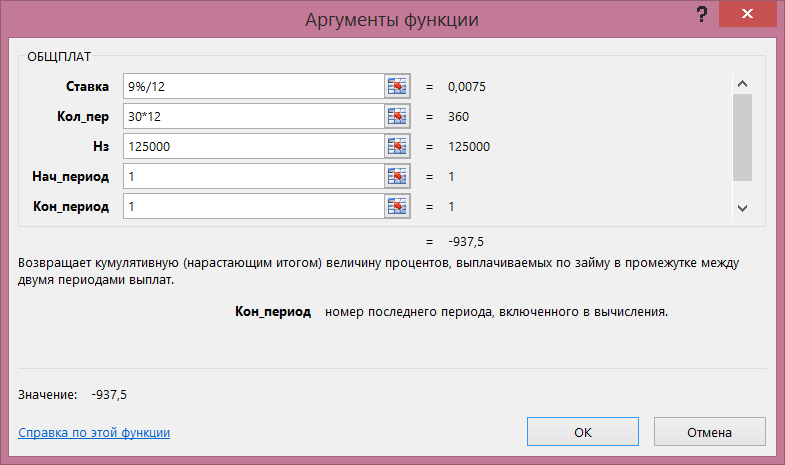
Нз – поточна вартість інвестиції;

Тип - число 0 (виплата вкінці періоду), 1 (виплата напочатку періоду).

**Приклад.**

Видана позика розміром 125 000 грн. для купівлі нерухомості терміном на 30 років під 9% річних, проценти нараховуються щомісяця. Визначити величину основних виплат: а) за другий рік, б) за перший місяць.





**Функція ОБЩДОХОД розраховує кумулятивну (наростаючим підсумком) суму, яка виплачується в погашення основної суми позики в проміжку між двома періодами.**

**ОБЩДОХОД (ставка; кол\_пер; Нз; нач период; кон период; тип),**

Ставка – процентна ставка за період;

Нач Период – номер першого періоду, включеного до обчислення. Періоди нумеруються з 1;

Кон Период – номер останнього періоду, включеного до обчислення;

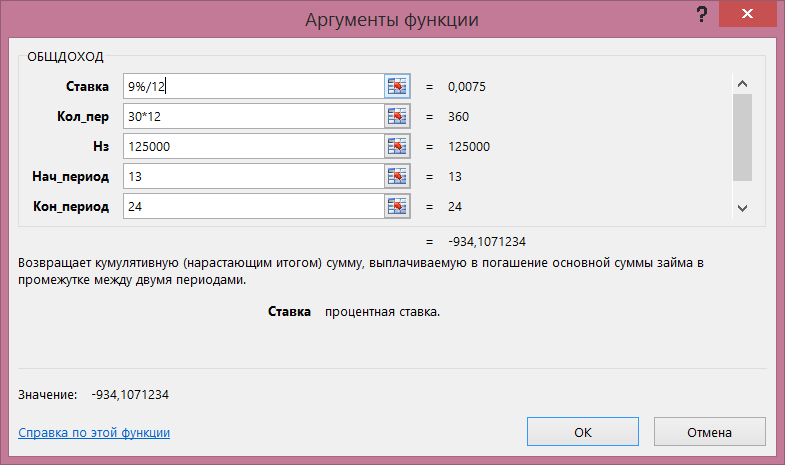
Кол\_пер – загальна кількість періодів виплат;

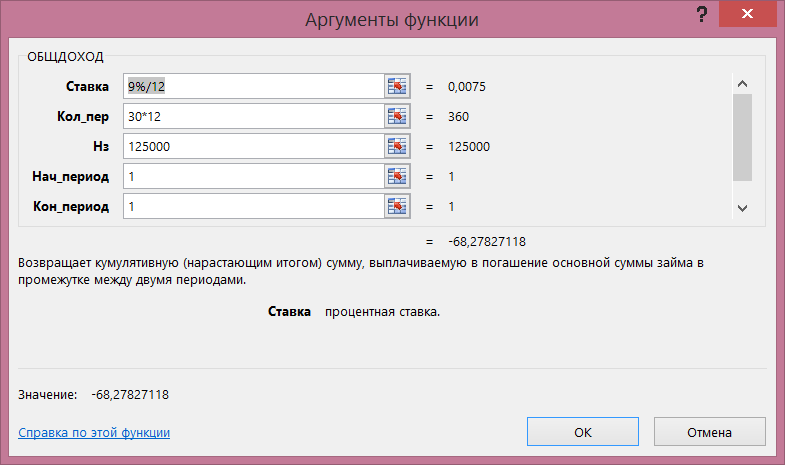
Нз – поточна вартість інвестиції;

Тип - число 0 (виплата вкінці періоду), 1 (виплата напочатку періоду).

**Приклад.**

Видана позика розміром 125 000 грн. для купівлі нерухомості терміном на 30 років під 9% річних, проценти нараховуються щомісяця. Визначити величину основних виплат: а) за другий рік, б) за перший місяць.





**Задачі.**

1. Банк видав позику 200 тис. грн на 4 роки під 18% річних. Позика видана напочатку року, а погашення починається вкінці року однаковими платежами. Потрібно визначити величину щорічного погашення позики.
2. За рахунок щорічних відрахувань протягом 6 років був сформований фонд 500 тис. грн. Треба розрахувати, який дохід приносили вкладення власнику за останній рік, якщо річна ставка становила 17,5%.
3. Батько хоче зробити подарунок 8000 доларів тринадцятирічному синові на момент його повноліття (18 років). Для цього він уклав договір з банком, згідно з яким робитиме щоквартальні внески (схема пренумерандо), на які банк буде щороку нараховувати відсотки за ставкою 8%. Визначте суму внеску. Яку суму потрібно було б покласти в банк одноразово, щоб досягти тієї ж мети?
4. Підприємство придбало будинок за 20000 доларів за таких умов: 25% вартості сплачується негайно; частина, що залишилась, погашається щорічними однаковими платежами протягом 10 років з нарахуванням 12% річних. Визначте величину річного платежу.
5. Позичальник позичив на 5 років 12000 грн. під 12% річних. Повертати борг потрібно однаковими сумами вкінці кожного року. Визначте, яка сума тіла кредиту буде погашена за перші два роки.
6. Позичальник позичив 10000 грн на 5 років під 8% річних. Повертати борг потрібно рівними сумами вкінці кожного року. Визначте загальну суму процентів до виплати.
7. Потрібно накопичити 25000 грн. за 8 років. Яким повинен бути щорічний внесок у банк при ставці 10% річних? Розгляньте схеми постнумерандо та пренумерандо. Яку суму потрібно одноразово покласти в банк сьогодні, щоб досягти тієї ж мети?
8. Підприємство отримало кредит 500 000 грн. на 3 роки. Річна процентна ставка за користування кредитом 16%. Визначте 1) величину разового платежу та 2) загальну вартість кредиту при сплаті: а) щорічними однаковими виплатами вкінці кожного року; б) щорічними рівними внесками вкінці кожного місяця.
9. Надано позику 129 000 грн під процентну ставку 9% річних на 30 років. Проценти нараховуються щомісяця. Знайдіть суму виплат за процентами за 2-й рік і за 1-й місяць позики.
10. Позику 1 млн грн видано на 6 років під 15% річних, проценти нараховуються щокварталу. Визначте величину основних виплат за п’ятий рік.