



**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

БАКАЛАВРСЬКА РОБОТА

**«ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ
ВНУТРІШНЬОДЕРЖАВНИХ БАНКІВСЬКИХ ПЛАТІЖНИХ
СИСТЕМ»**

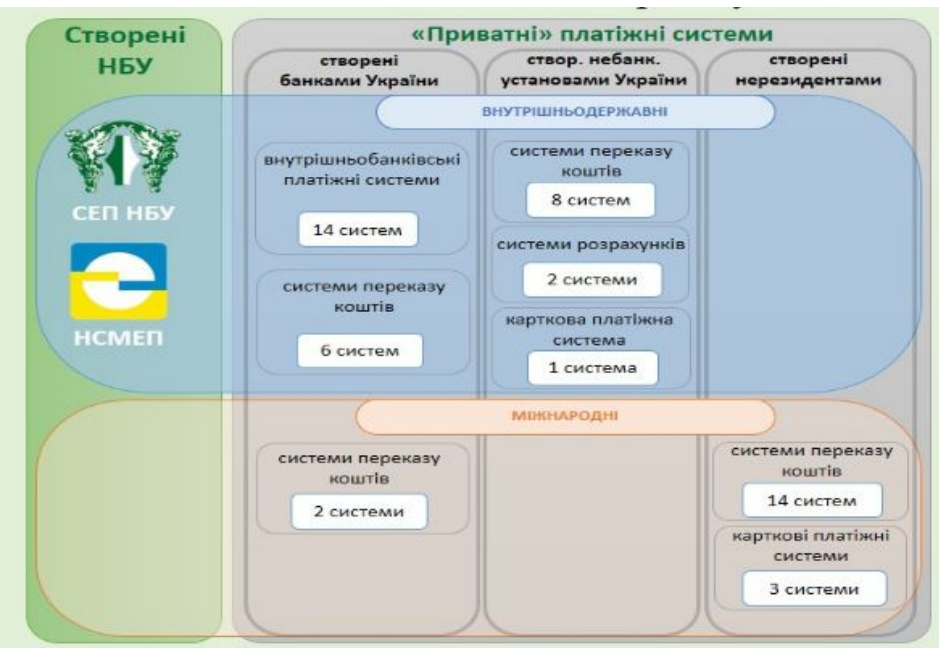
**СТУДЕНТА:
КЕРІВНИК:**

Метою дипломної роботи є розробка рекомендацій щодо підвищення ефективності функціонування внутрішньодержавної банківської платіжної системи.

Для досягнення цієї мети в роботі вирішені такі завдання:

1. Огляд особливостей та компонентів захисту внутрішньодержавних банківських платіжних систем України.
2. Дослідження сучасних методів та засобів захисту внутрішньодержавної банківської платіжної системи.
3. Рекомендації щодо захисту інформації у внутрішньодержавних платіжних системах.

ПЛАТІЖНІ СИСТЕМИ ТА СИСТЕМИ ПЕРЕКАЗУ КОШТІВ



№з/п	Найменування платіжної системи	Найменування платіжної організації	№свідоцтва	Дата видачі свідоцтва	Вид платіжної системи	Ознака платіжної системи
1	"СОФТ"	ПАТ "УКРСОЦБАНК"	7	26.08.2009	система переказу коштів	внутрішньодержавна
2	"FLASHPAY"	ПУБЛІЧНЕ АТ "БАНК ФАМІЛЬНИЙ"	19; 19/1 19/2	14.08.2014; 20.05.2015 31.07.2015	система переказу коштів	внутрішньодержавна
3	"The Money"	ПАТ "КБ "ФІНАНСОВА ІНІЦІАТИВА"	20	06.10.2014	система переказу коштів	внутрішньодержавна
4	"Система термінових переказів" Швидка копійка"	АТ "Ощадбанк"	25	15.07.2015	система переказу коштів	внутрішньодержавна
5	"ПРАВЕКС-ТЕЛЕГРАФ"	ПАТКБ "ПРАВЕКС-БАНК"	26	02.12.2015	система переказу коштів	внутрішньодержавна
6	"IBOX MONEY TRANSFER"	ПАТ "Агрокомбанк"	29	12.05.2016	система переказу коштів	внутрішньодержавна

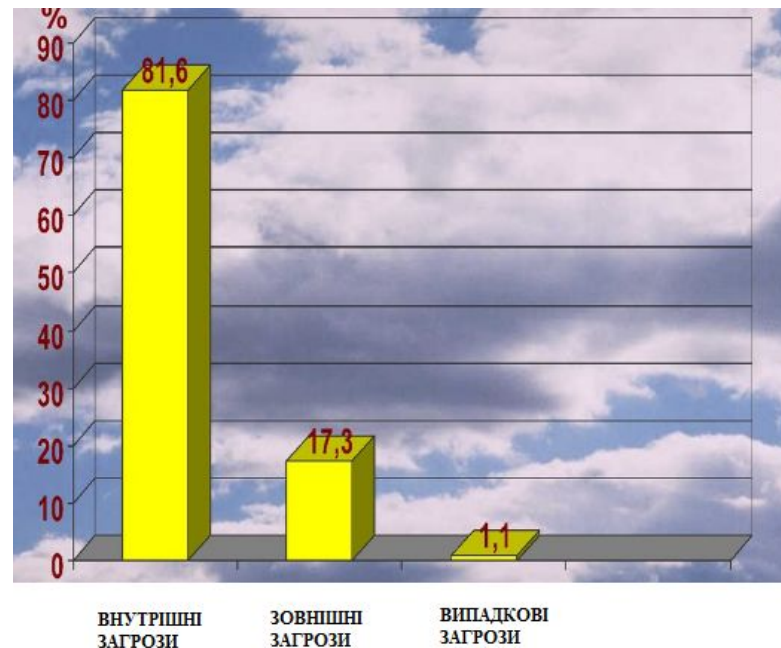
На сьогоднішній день в Україні діє:

- 16 внутрішньобанківських платіжних систем (з них 14 приватних)
- 6 внутрішньодержавних систем переказу коштів.

ОСНОВНИХ ВИДИ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Внутрішні загрози ІБ - будь-які дії з інформацією, які порушують хоча б один з постулатів інформаційної безпеки - цілісність, доступність і конфіденційність, які виходять зсередини інформаційної системи банку і завдають шкоди.

Зовнішні загрози ІБ - це джерела, які існують або можуть існувати поза банком і впливають на його інформаційну безпеку ззовні. Основу зовнішніх загроз, як правило, становить соціальні джерела небезпеки - люди, а також природні явища, лиха, катаклізми.



В ЗАЛЕЖНОСТІ ВІД МЕТИ ВПЛИВУ РОЗРІЗНЯЮТЬ ТРИ ОСНОВНИХ ТИПИ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕКИ ПЛАТІЖНИХ СИСТЕМ:

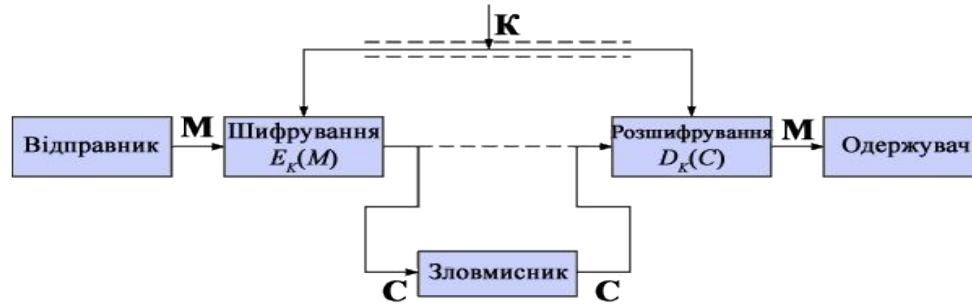
Загрози порушення **доступності** - спрямовані на створення таких ситуацій, коли певні навмисні дії або знижують працездатність апаратних засобів обробки інформації, або блокують доступ до деяких її ресурсів.

Загрози порушення **цілісності** інформації - спрямовані на її зміну або спотворення, що приводить до порушення її якості або повного знищення.

Загрози порушення **конфіденційності** - спрямовані на розголошення конфіденційної або секретної інформації.

КРИПТОГРАФІЯ

Криптографія є одним з найкращих засобів забезпечення конфіденційності і контролю цілісності інформації.

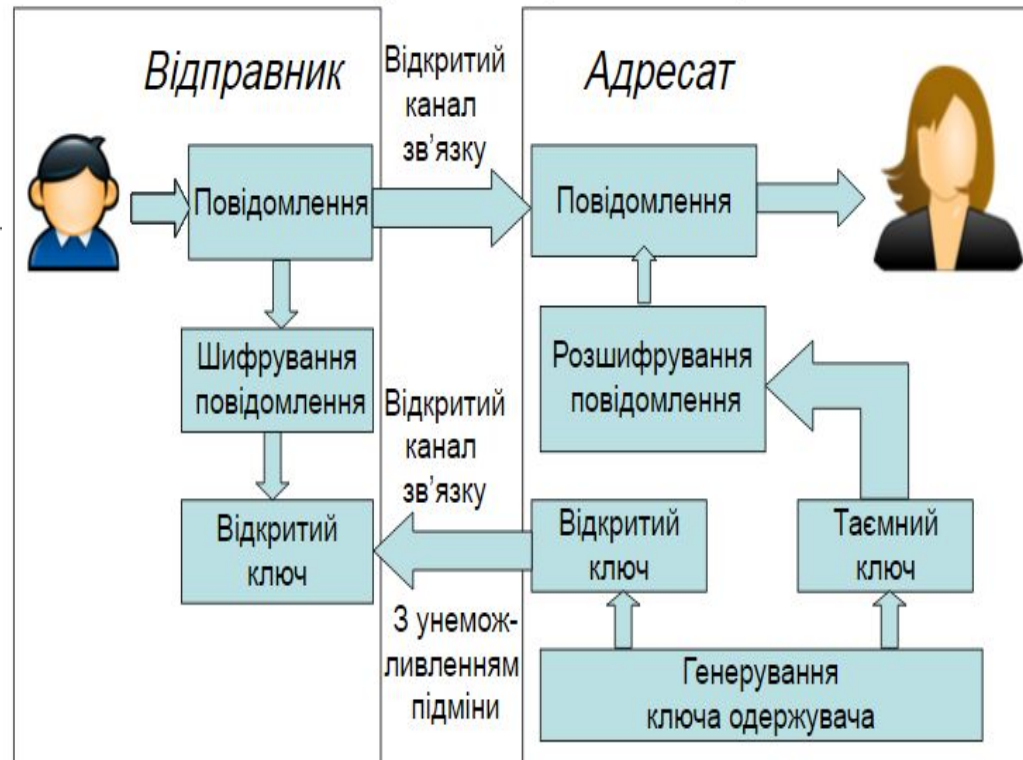
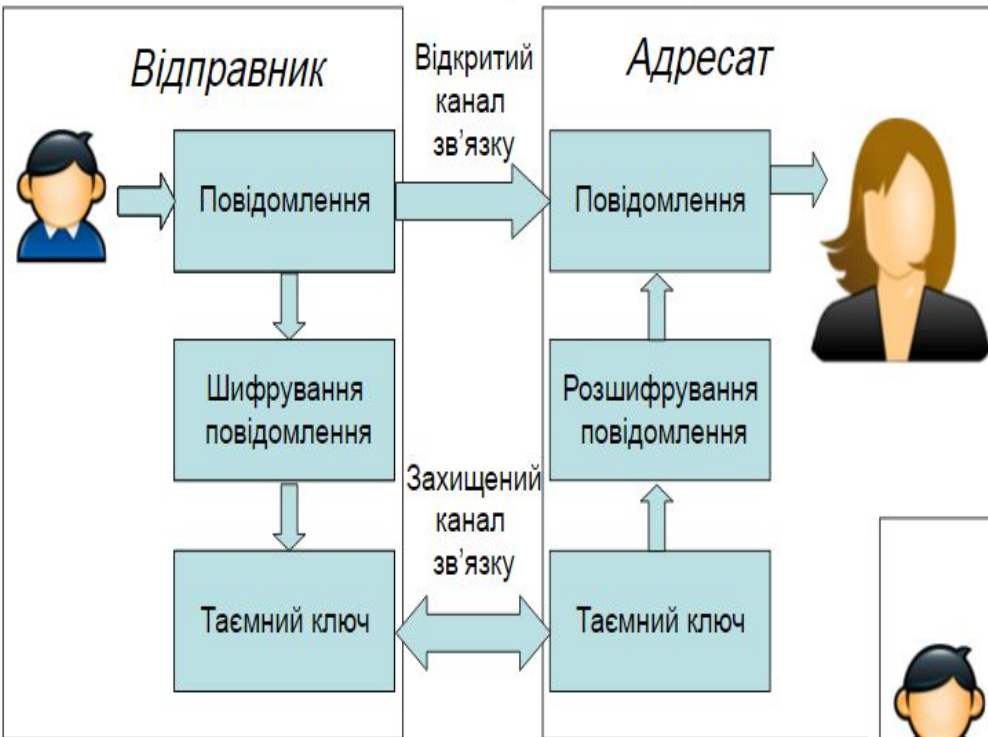


Узагальнена схема криптосистеми



Класифікація криптоалгоритмів

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ

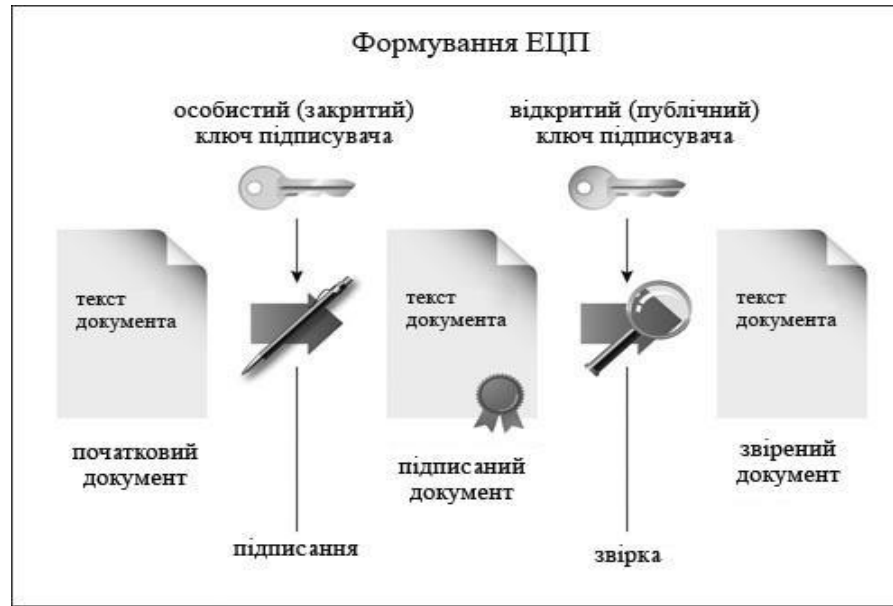


ПОРІВНЯННЯ МЕТОДІВ ШИФРУВАННЯ

Симетричне шифрування		Асиметричне шифрування	
Переваги • швидкість (на 3 порядки) • простота реалізації • менша довжина ключа для визначення стійкості	Недоліки • складність управління ключами • складність обміну ключами	Переваги • відсутність необхідності захищеного каналу • наявність тільки одного секретного ключа • число ключів в мережі менше і не росте в квадратичній залежності	Недоліки • складність проведення зміни алгоритму • неможливість шифрування ID відправника та адресата • велика довжина ключа, порівняно із симетричним шифруванням

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЇ В ПЛАТІЖНИХ СИСТЕМАХ

Цілісність інформації в платіжних системах забезпечується криптографічними методами та в першу чергу за допомогою електронного цифрового підпису.



- електронний цифровий підпис отриманий в результаті криптографічного перетворення інформації з використанням закритого ключа
- ЕЦП використовується для створення сертифікатів і підписів транзакцій
- в механізмі ЕЦП використовуються два криптографічних ключі: відкритий і закритий, які генеруються автором повідомлення.

ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ІНФОРМАЦІЇ В ПЛАТІЖНИХ СИСТЕМАХ

Доступність - це властивість інформації при її обробці технічними засобами, що забезпечує безперешкодний доступ до неї для проведення санкціонованих операцій ознайомлення, модифікації або знищення.

Призначення засобів боротьби з загрозами доступності в платіжних системах - забезпечити своєчасний доступ користувачів до необхідної їм інформації та ресурсів інформаційної системи. Завдання забезпечення доступності - комплексна, для її вирішення застосовуються як методи захисту від несанкціонованого доступу, так і спеціалізовані методи захисту від руйнівних програмних дій.

Регулярне резервування всієї зберігається в банку інформації - абсолютно необхідний захід. На сьогодні існують три типи продуктів, покликаних мінімізувати ризики, пов'язані з несанкціонованим доступом до резервних копій.

1. Спеціальні пристрої
2. Модулі ArcServe, Veritas Backup Exec і ін.
3. Спеціально розроблені програмні, програмно-апаратні та апаратні продукти, не прив'язані до конкретних систем архівування даних

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ПАРОЛЯ ДЛЯ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧА

Схема звичайної аутентифікації за допомогою пароля

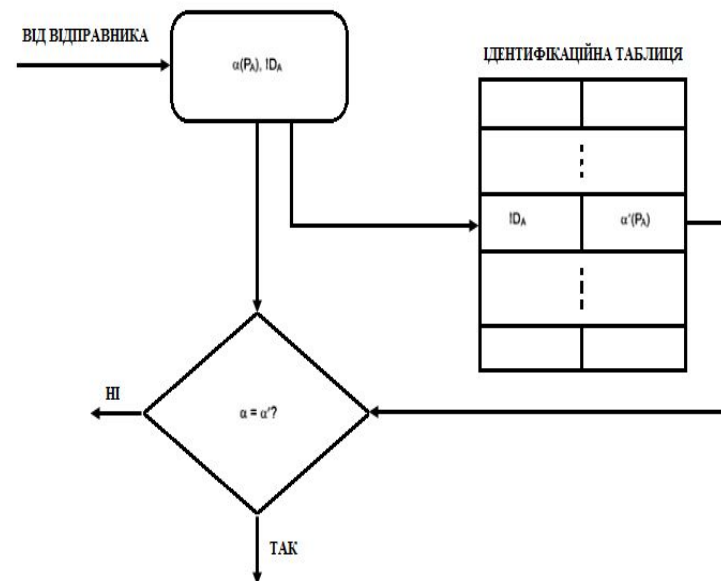
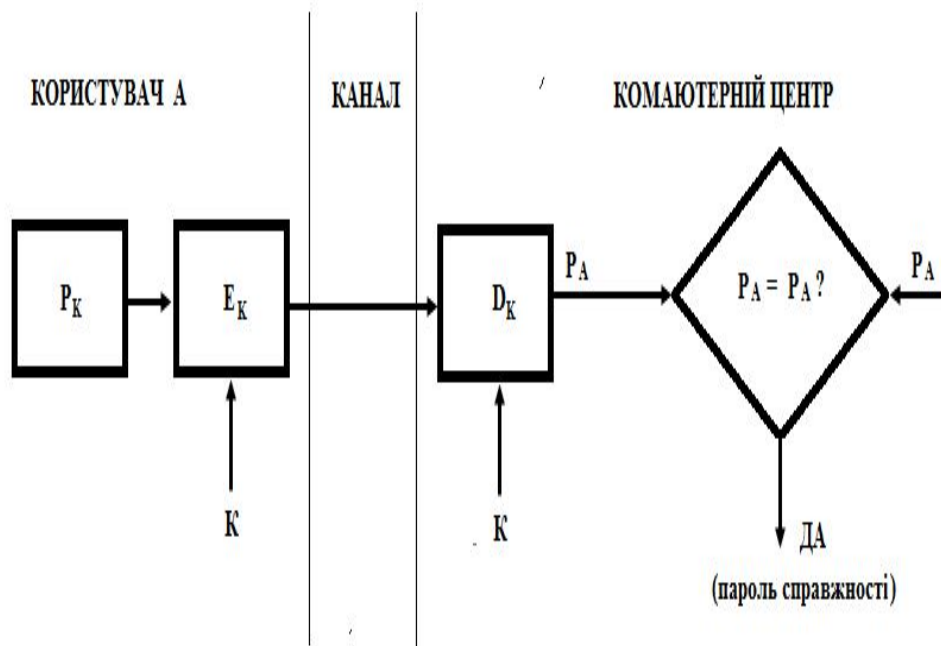


Схема аутентифікації за допомогою пароля з використанням ідентифікаційної таблиці

ВИСНОВОК

Для забезпечення безпеки банківських платіжних систем на сьогоднішній день в Україні використовуються криптографічні симетричні і асиметричні алгоритми шифрування, які пройшли стандартизацію і сертифікацію на державному рівні.

Однак відсутність національних стандартів по спеціальним механізмам забезпечення інформаційної безпеки (шифрування, цілісність даних, аутентифікація) істотно впливає на рівень забезпечення інформаційної безпеки банківських транзакцій і надійності платіжних систем в цілому.