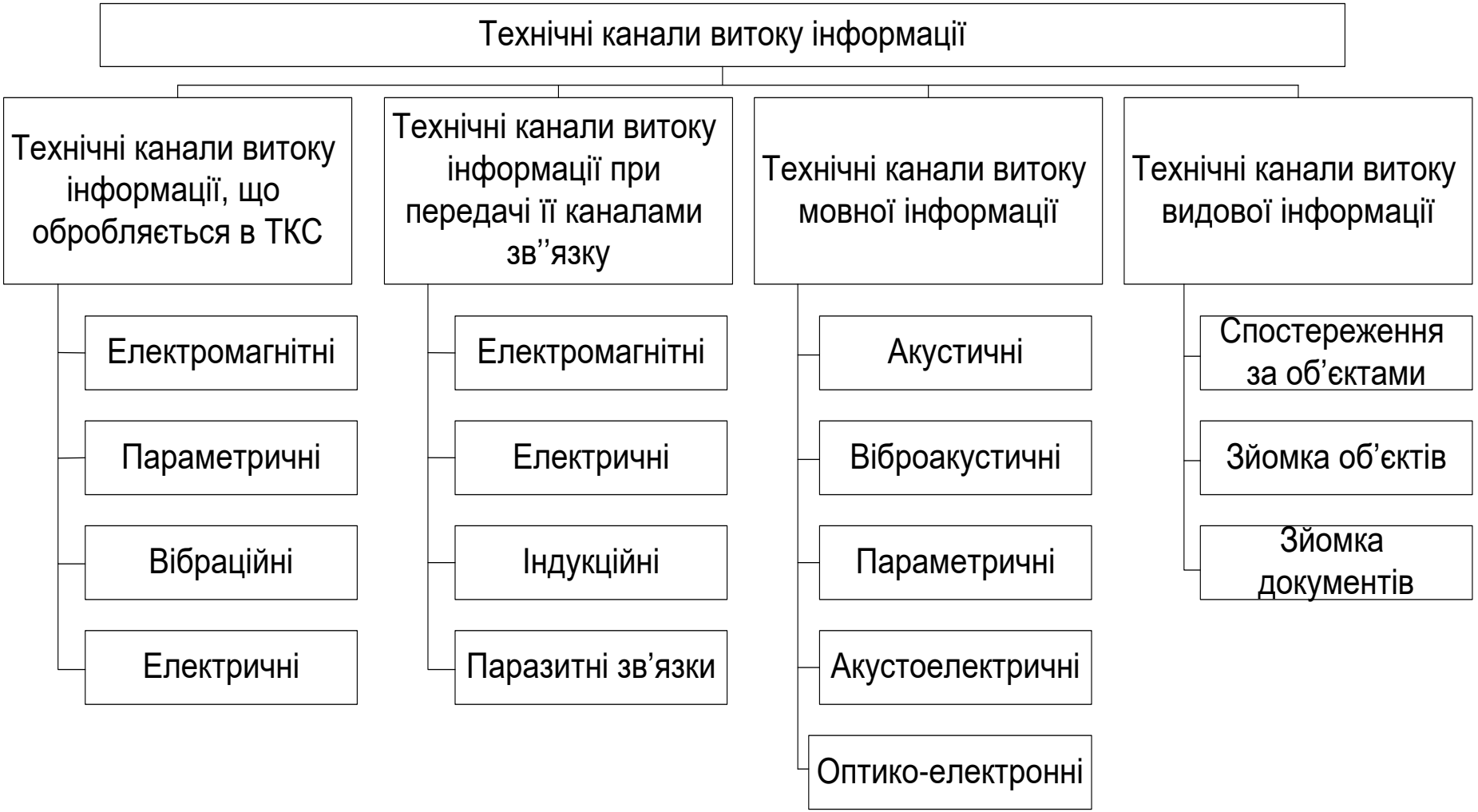
МКР на тему:
“ Аналіз ефективності застосування ЕЦП В ТКС ”

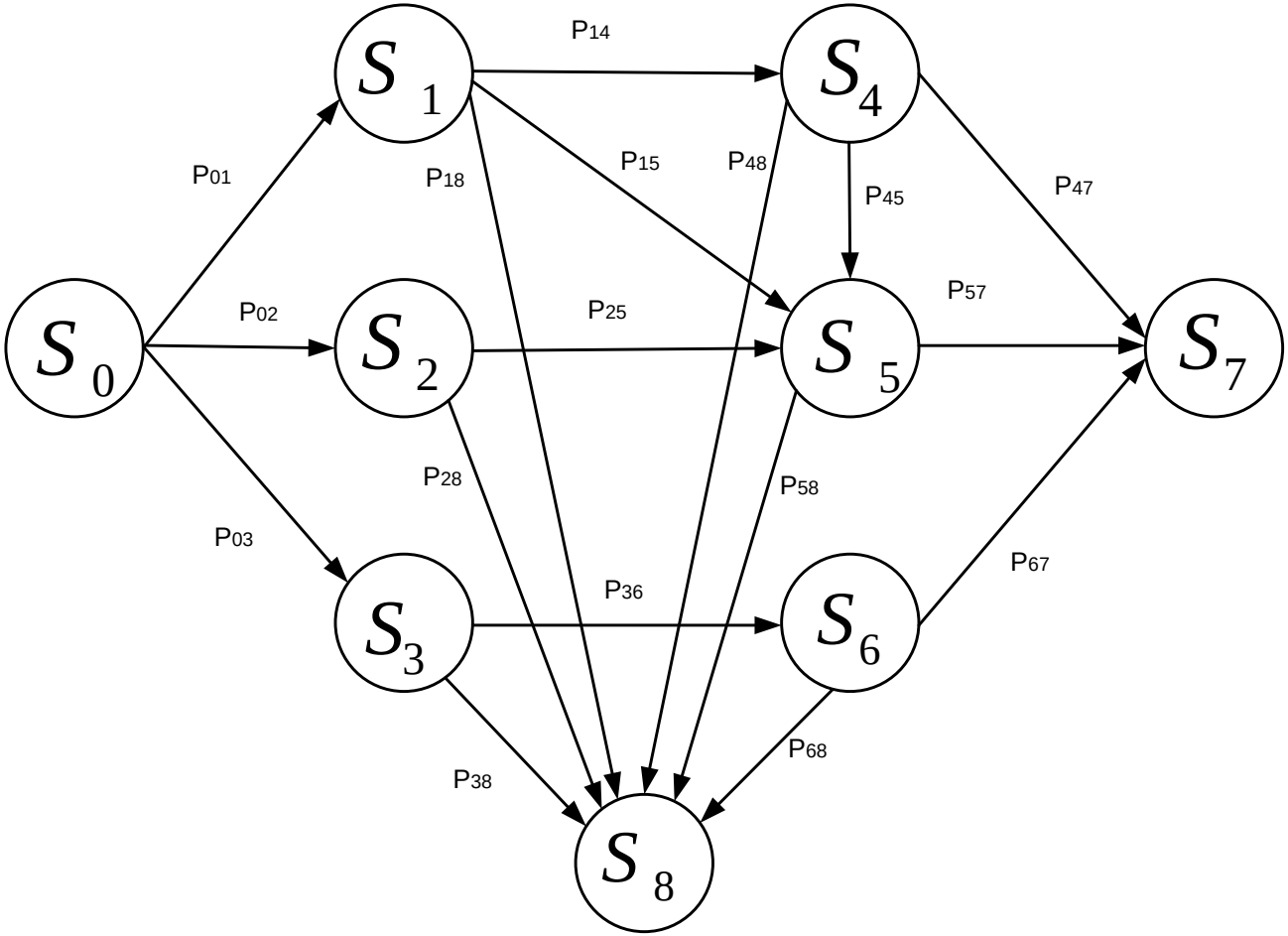
Виконала:
ст. гр. ТСМ-15м
Номировська В.В.
Науковий керівник:
к. т. н., доцент кафедри ТКСТБ
Стальченко О.В.

- Актуальність теми: у зв’язку зі стрімким розвитком інфокомунікацій, глобальним охопленням і транснаціональним характером Internet, зростанням швидкості обміну інформацією і необхідністю боротьби зі збільшенням числа і розмаїття загроз (віруси, черв’яки, троянські коні, спуфінг, крадіжка ідентичності, спам та інші форми кібератак) існують проблеми забезпечення інформаційної безпеки.

- Основна мета дипломної роботи — підвищення захищеності інформації в телекомунікаційних системах.


Технічні канали витоку інформації
Технічні канали витоку інформації, що обробляється в ТКС
Електромагнітні
Параметричні
Вібраційні
Електричні
Технічні канали витоку інформації при передачі її каналами зв''язку
Електромагнітні
Електричні
Індукційні
Паразитні зв'язки
Технічні канали витоку мовної інформації
Акустичні
Віброакустичні
Параметричні
Акустоелектричні
Оптико-електронні
Технічні канали витоку видової інформації
Спостереження за об'єктами
Зйомка об'єктів
Зйомка документів

Приклад графа станів системи



Ймовірність подолання рубежу захисту при досягненні порушником цілі визначається:

$$g_l^f = \left(1 - e^{-\omega^f}\right) \prod_{m \in N_j^f} \left(1 - r_{jm}^f x_{jm}\right)$$

Залежність загроз інформаційної безпеки відносно стану системи

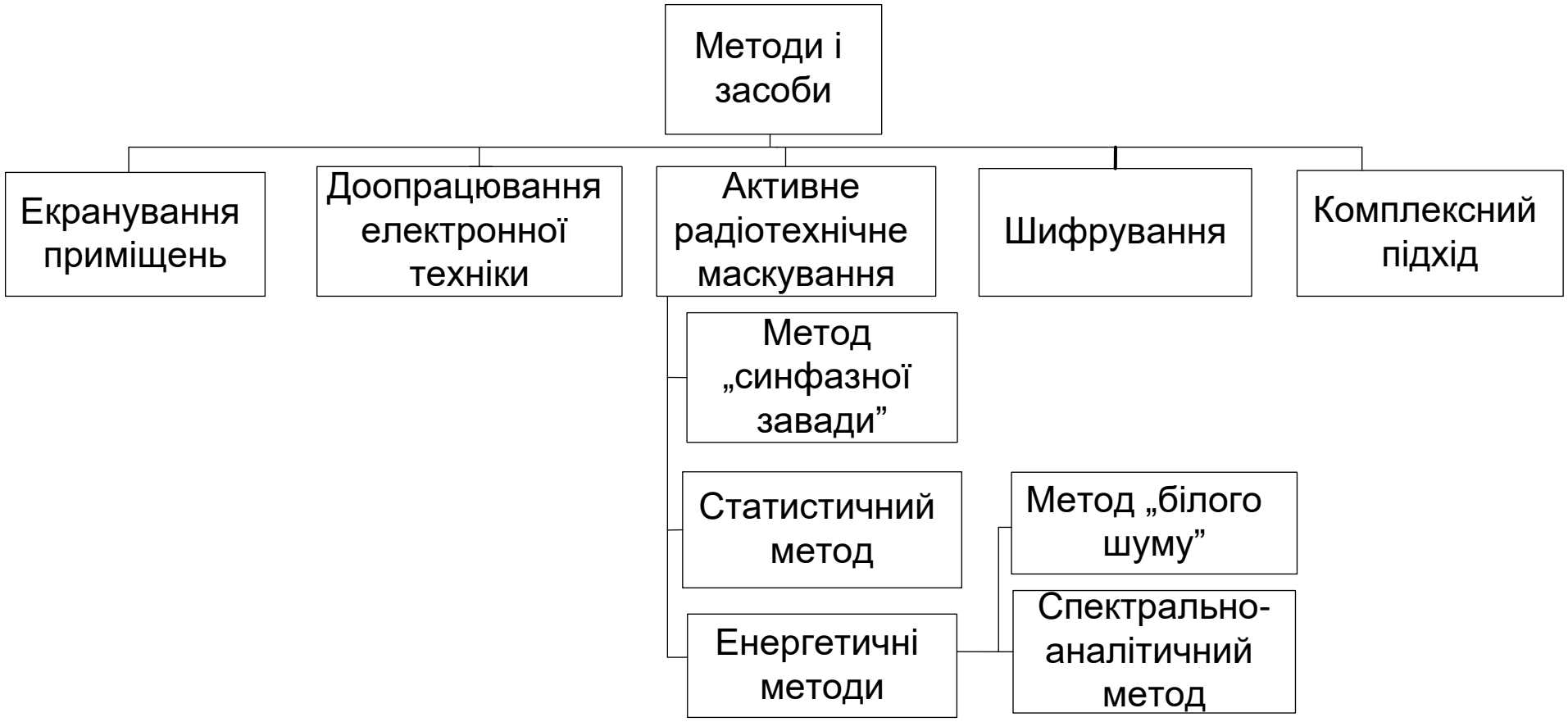
Стан системи	Загрози безпеки
$a_0 \,\&\, a_1 \,\&\, b$	К, Ц, Д
$a_0 \,\&\, \overline{a_1} \,\&\, b$	К, Д
$a_0 \,\&\, \overline{a_1} \,\&\, \overline{b}$	Потенційна загроза К
$a_0 \,\&\, a_1 \,\&\, \overline{b}$	Потенційна загроза К, Д
$\overline{a_0} \,\&\, a_1 \,\&\, b$	Ц, Д
$\overline{a_0} \,\&\, \overline{a_1} \,\&\, b$	Д
$\overline{a_0} \,\&\, \overline{a_1} \,\&\, \overline{b}$	Захист
$\overline{a_0} \,\&\, a_1 \,\&\, \overline{b}$	Потенційна загроза Ц

К — загроза конфіденційності;

Ц — загроза цілісності;

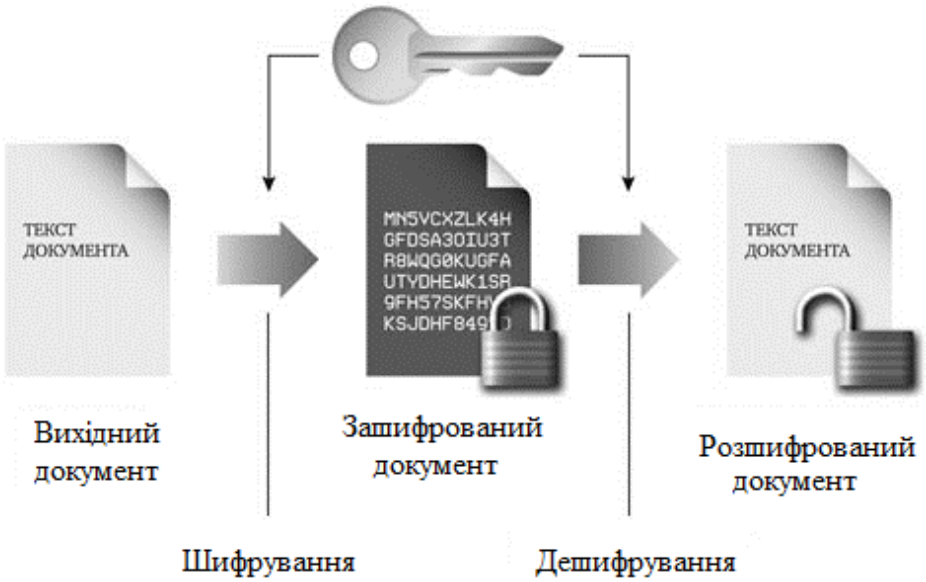
Д — загроза доступності.

Класифікація способів і методів захисту інформації

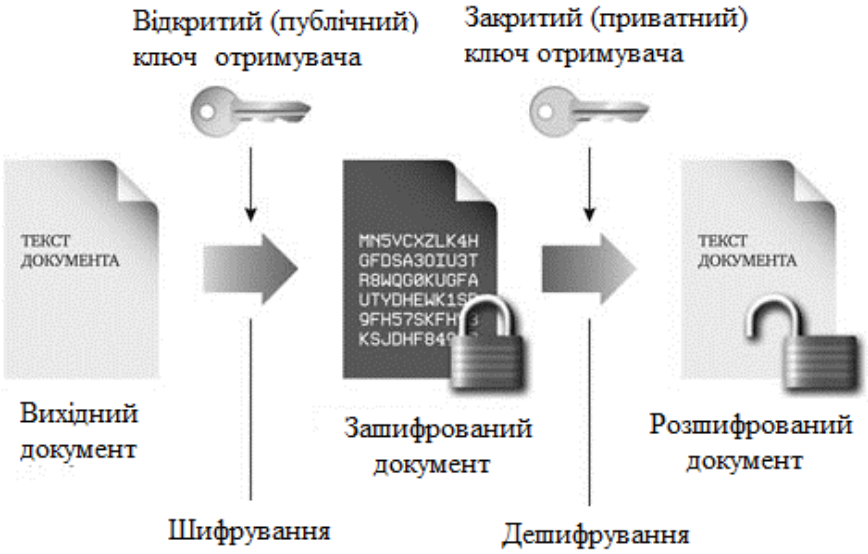


Схеми створення ЕЦП

- Симетрична



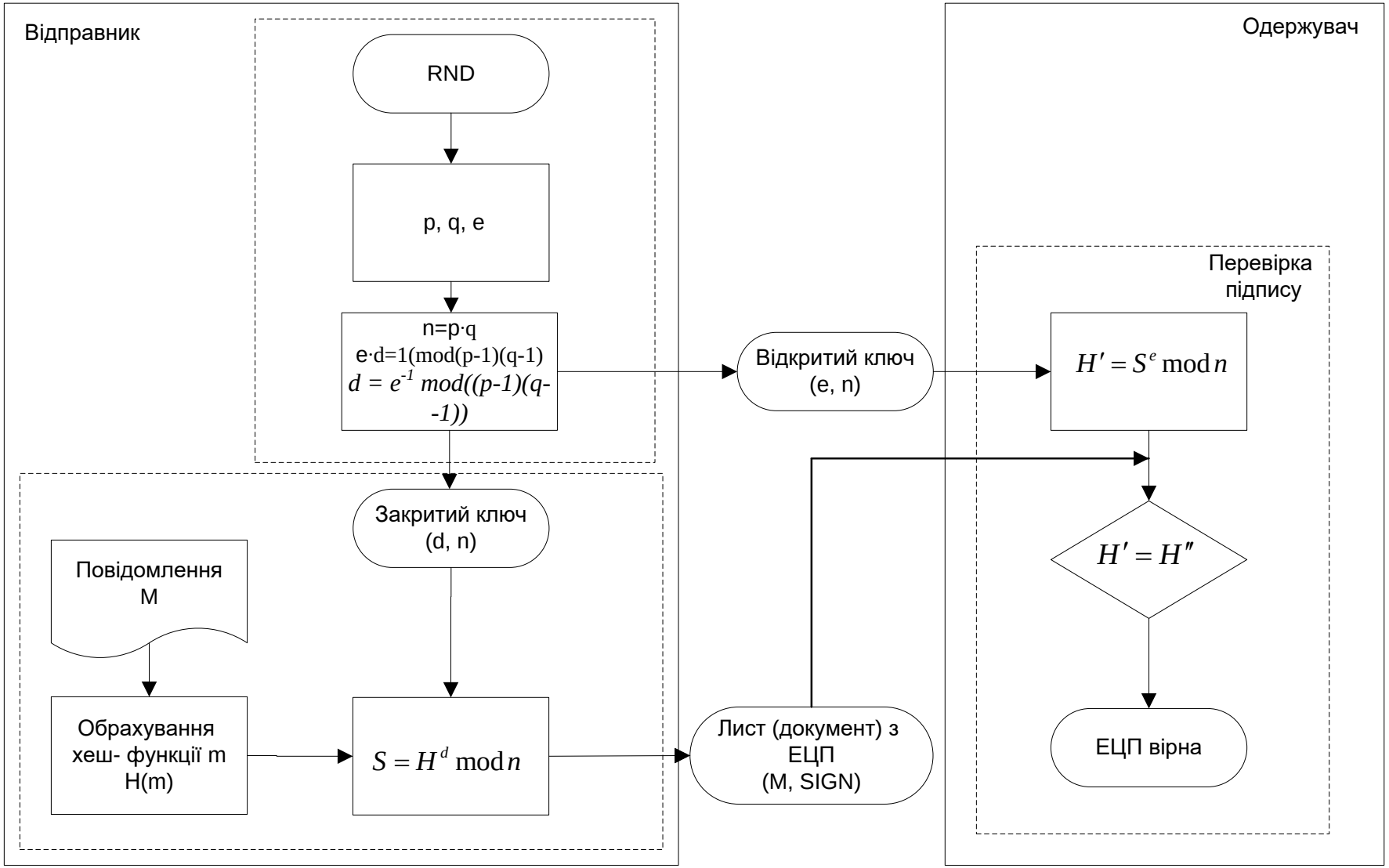
- Асиметрична

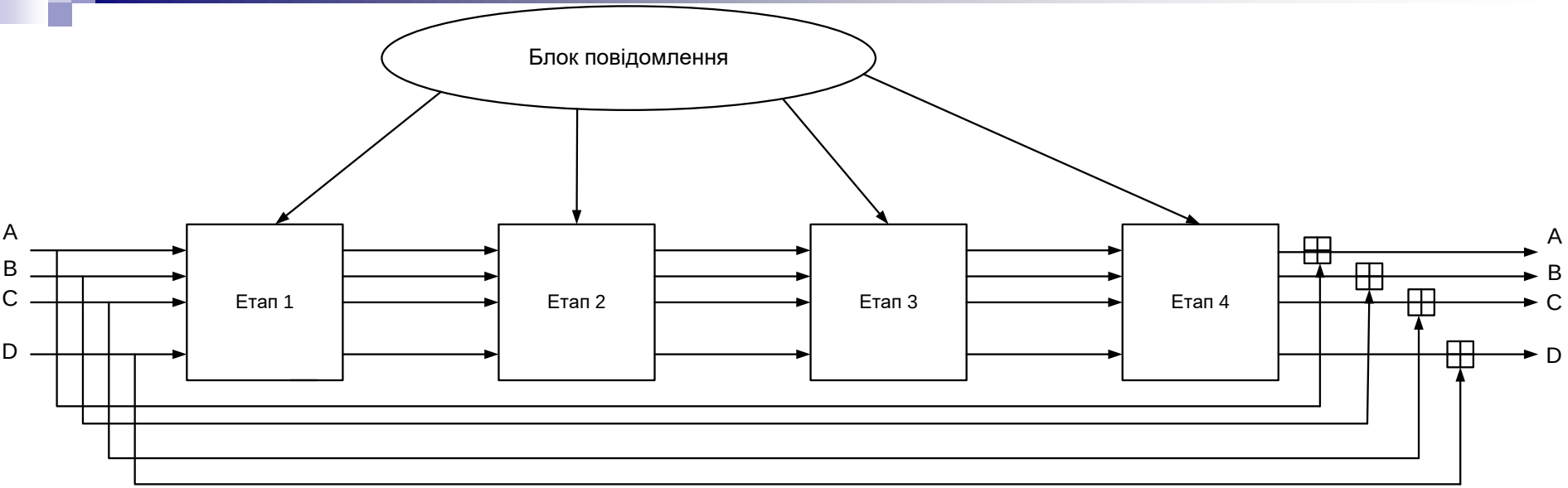


Алгоритми ЕЦП та хеш-функції, що використовуються

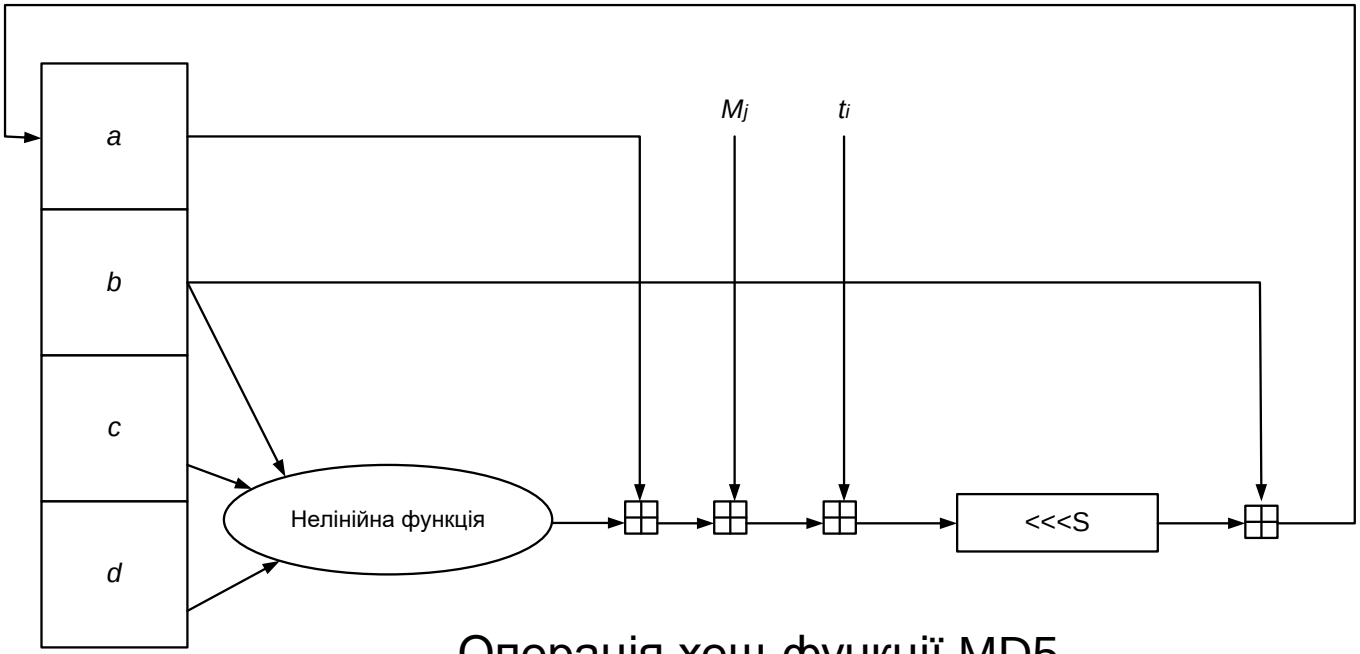
- Алгоритм RSA
- Алгоритм ElGamal
- Алгоритм DSS
- Стандарт цифрового підпису ГОСТ 334.10-9427
- Стандарт цифрового підпису ДСТУ 4145-2002
- Хеш-функція MD5
- Хеш-функція SHA
- Хеш-функція RIPEMD-160
- Хеш-функція PKCS#5
- Хеш-функція Tiger
- Хеш-функція Whirlpool

Схема реалізації алгоритму RSA



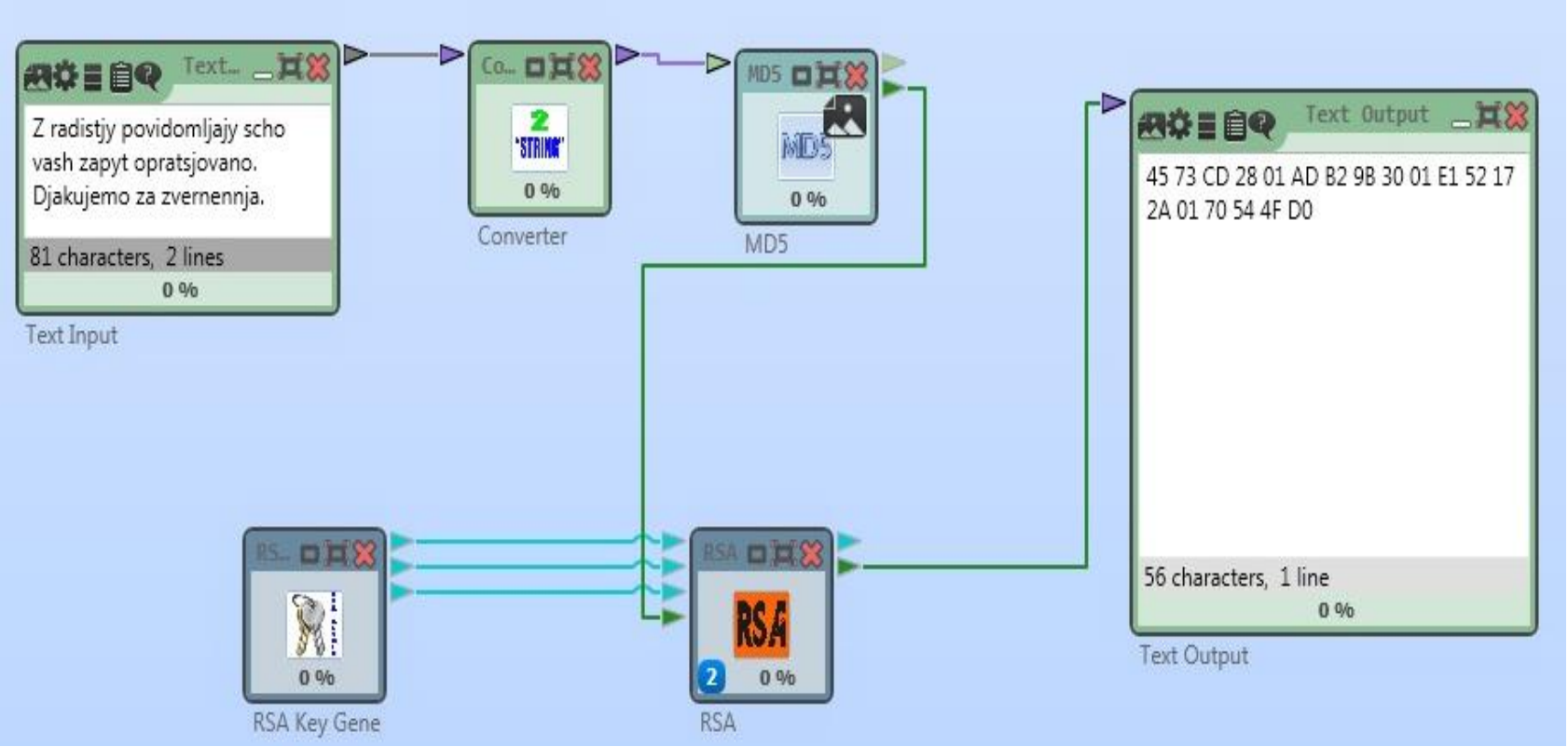


Головний цикл хеш-функції MD5



Операція хеш-функції MD5

Схема моделювання з використанням хеш-функції MD5



Результати моделювання