Вінницький національний технічний університет
НАЗВА ІНСТИТУТУ
НАЗВА КАФЕДРИ

Дипломна робота
на тему:

Розробка системи захисту електронного документообігу підприємства від втручань через глобальну мережу

Виконала: Павлік Марія Миколаївна
Науковий керівник: **посада, ім’я**

Тема дипломної роботи:

Розробка системи захисту електронного документообігу підприємства від втручань через глобальну мережу

Мета дипломної роботи:

Дослідження можливості захисту електронного документообігу підприємства від втручань через глобальну мережу

Для досягнення поставленої мети необхідно дослідити такі задачі:

1. *Провести техніко-економічне обґрунтування доцільності розробки WEB-сервісу захисту електронного документообігу;*
2. *Проаналізувати основні поняття електронного цифрового підпису та сучасних систем електронного документообігу;*
3. *Проаналізувати існуючі засади безпеки електронного документообігу та можливості для розробки захисту обміну документами засобами мережі Інтернет;*
4. *Розробити та описати засіб захисту електронного документообігу підприємства через глобальну мережу;*
5. *Розрахувати економічний ефект від впровадження інноваційного рішення.*

Наукова новизна та практичне значення одержаних результатів

Наукова новизна одержаних результатів.
До захисту виноситься науковий результат, що являє собою розроблений WEB-сервіс, що виконує захист електронного документообігу підприємства від втручань через глобальну мережу за допомогою ЕЦП.

Практичне значення одержаних результатів.
Розроблено WEB-сервіс для захисту електронного документообігу підприємства від втручань через глобальну мережу.

Поняття електронного документу

Електронний документ *– документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.*

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа *є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.*

Поняття електронного підпису

Електронний цифровий підпис *– вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.*

Властивості електронного підпису:

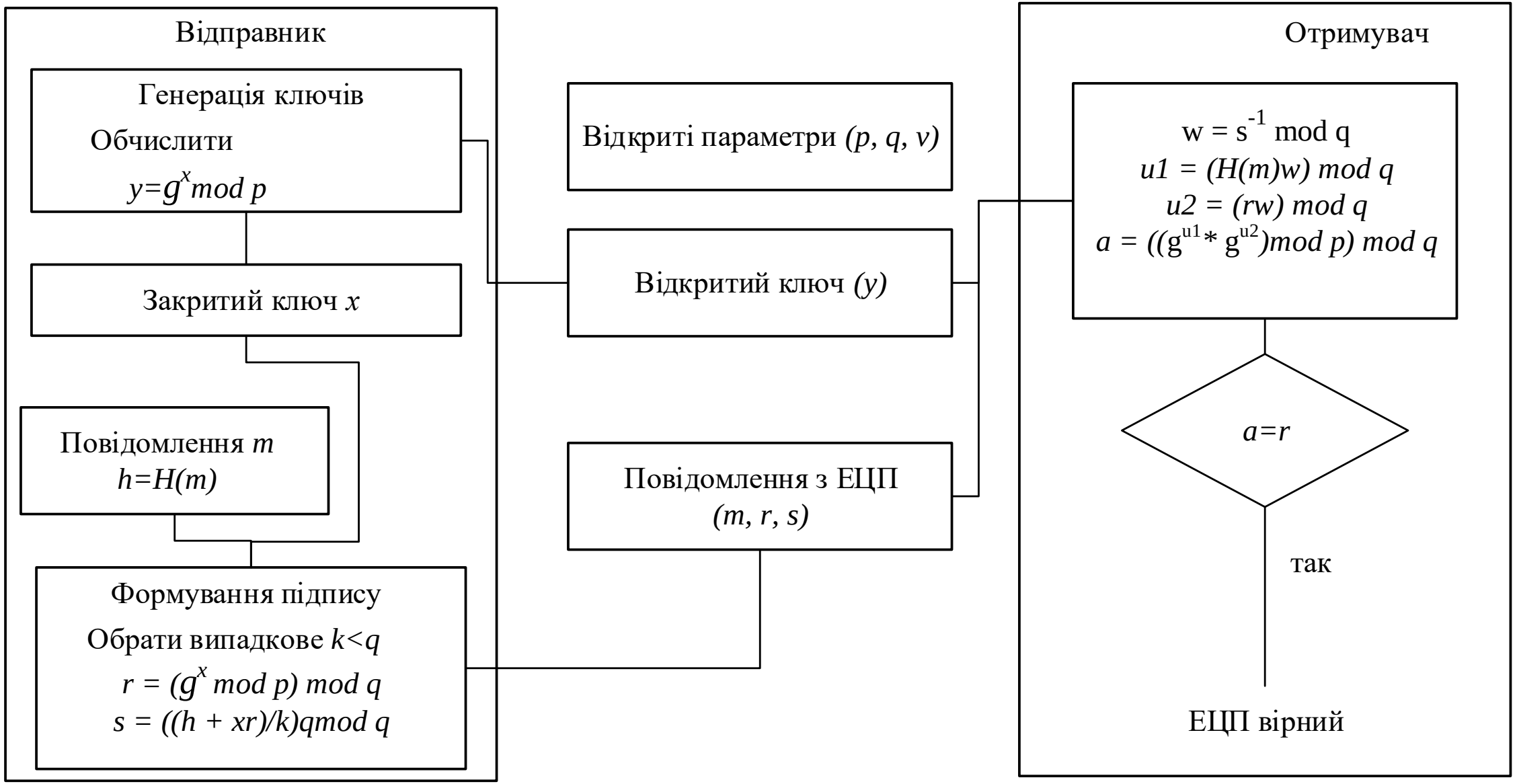
1) Достовірність, що дозволяє переконатися у тому, що саме адресат підписав документ.

2) Унікальність, так як і ручний підпис – частина документа, яку не можна перемістити на інші документи. Тобто у будь-якого окремого документа буде свій унікальний цифровий підпис.

3) Цілісність підписаного документа, тобто неможливість зміни підписаного документа.

4) Неспростовність від авторства або вмісту документа – від підпису в подальшому не можна відмовитися.

Принцип функціонування ЕЦП



Алгоритм роботи модуля створення ЕЦП

1. Вибір випадкового числа $k \in (0, q)$;
2. Обчислення:

$$r = \left(g^k mod\ p\right) mod\ q$$

3. Обчислення:

$$s = k^{-1}(H(m) + x \cdot r)\ mod\ q$$

4. Вибір іншого k, якщо виявилося, що $r = 0$ або $s = 0$.

Підписом є пара чисел (r, s), загальна довжина підпису $2 \cdot N$.

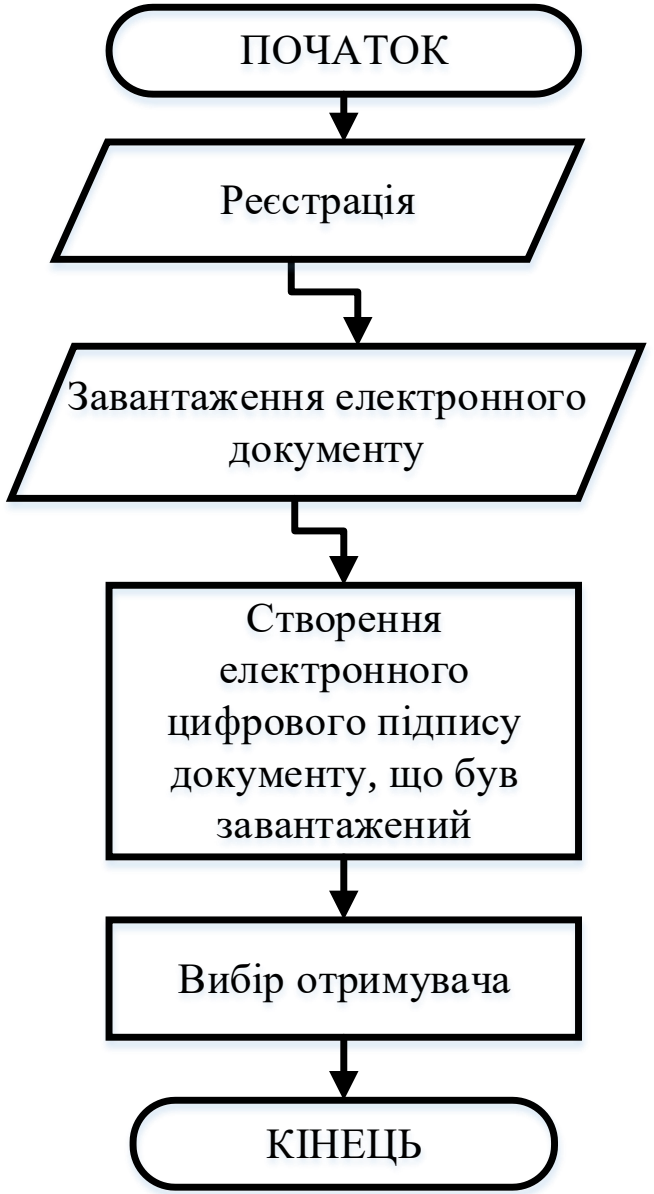
Модуль створення ЕЦП

Крок 1 *– Реєстрація нового користувача в сервісі.*

Крок 2 *– Завантаження нового електронного документа.*

Крок 3 *– Створення електронного цифрового підпису завантаженому електронному документу.*

Крок 4 *– Вибір Отримувача, якому буде надано доступ до завантаженого документу.*



Алгоритм перевірки ЕЦП

1. Обчислення:

$$w = s^{-1} mod\ q$$

2. Обчислення:

$$U_1 = H(m) \cdot w\ mod\ q$$

3. Обчислення:

$$U_2 = r \cdot w\ mod\ q$$

4. Обчислення:

$$U = (g^{U1} \cdot y^{U2}\ mod\ p) mod\ q$$

Підпис вірний, якщо $v = r$.

Модуль перевірки ЕЦП

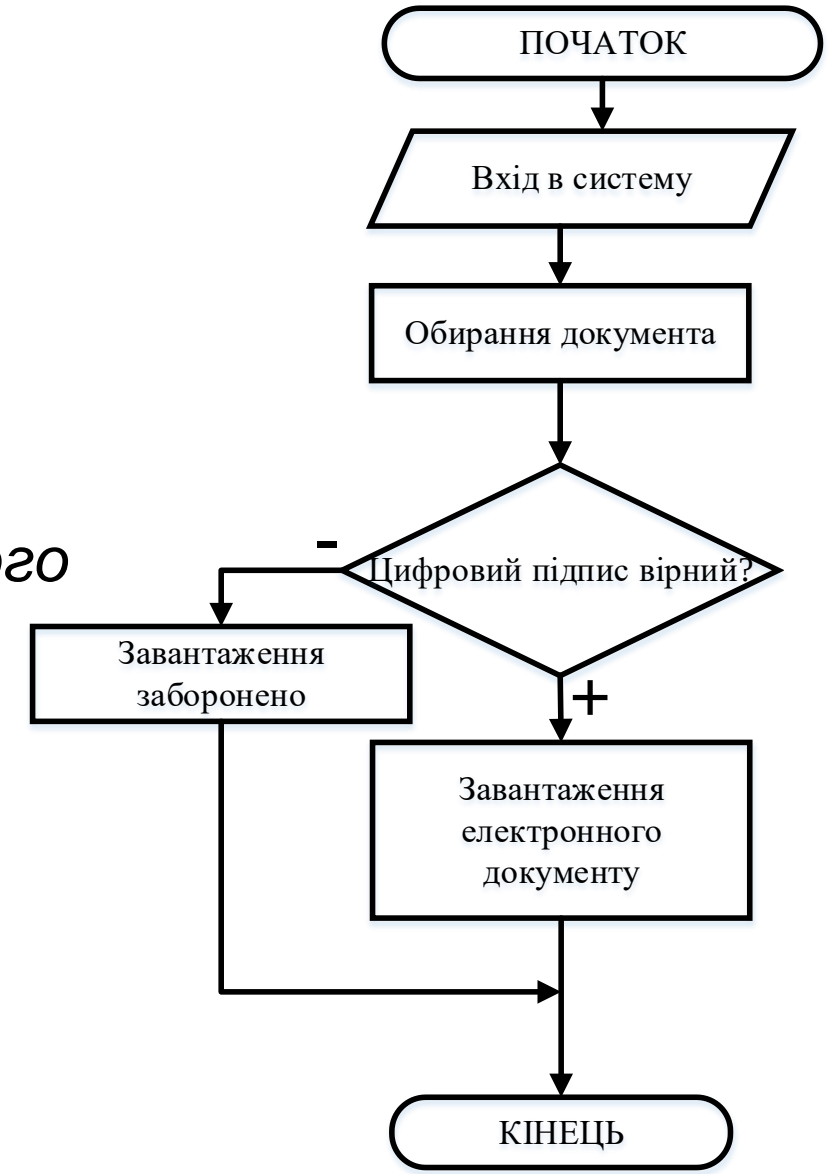
Крок 1 *– Вхід в систему раніше зареєстрованого користувача.*

Крок 2 *– Вибір електронного документу, який користувач бажає завантажити.*

Крок 3 *– Перевірка цифрового підпису електронного документу.*

Крок 4 *– Якщо підпис вірний – відбувається завантаження електронного документу.*

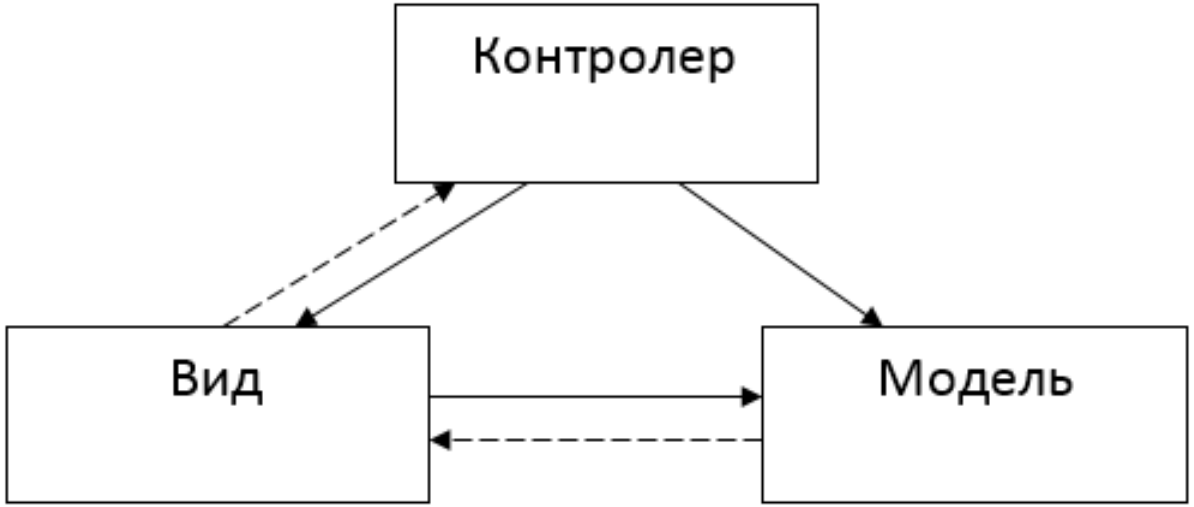
Крок 5 *– Якщо ЕЦП не вірний – заборона завантажувати даний документ даному користувачеві сервісу.*



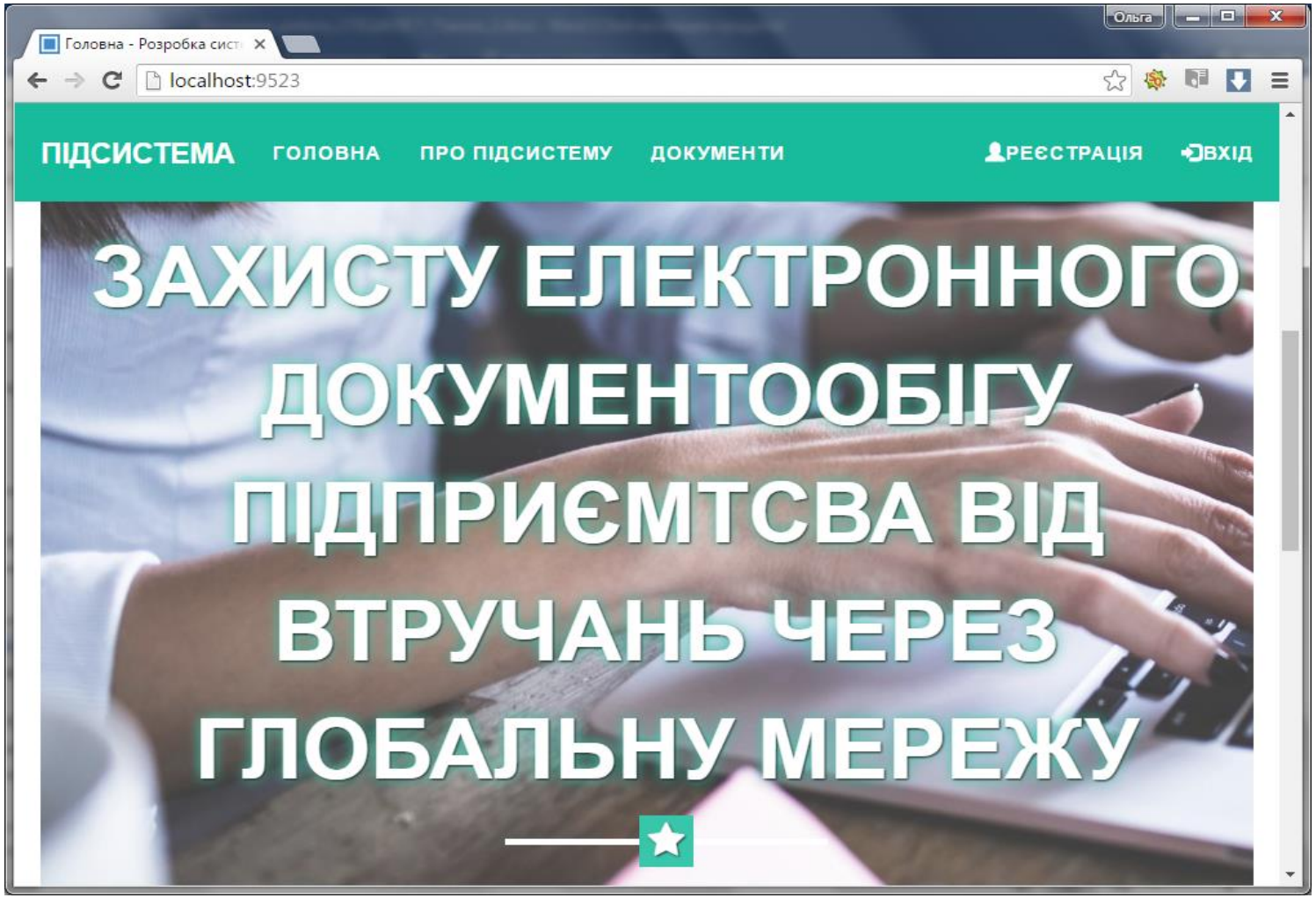
Вибір мови програмування

Програмна реалізація системи захисту електронного документообігу підприємства від втручань через глобальну мережу буде виконуватись засобами мови програмування ASP .NET MVC5. Для цифрового підпису було обрано алгоритм DSA.

Архітектурний шаблон поділяє систему на три частини: модель даних, представлення (вигляд) даних та керування. Застосовується для відокремлення даних (моделі) від інтерфейсу користувача (вигляду) так, щоб зміни інтерфейсу користувача мінімально впливали на роботу з даними, а зміни в моделі даних могли здійснюватися без змін інтерфейсу користувача.



Програмна реалізація



Адреса web-сервісу: http://diplomasignature.azurewebsites.net/

Економічні розрахунки

*НовийWEB-сервіс є **економічно доцільним** для споживача, оскільки:*

- *витрати на розробку - В = 12571,93 грн.;*
- *виробнича собівартість - $S_в$= 828,63 грн.;*
- *ціна реалізації - $Ц_р$= 1293 грн.;*
- *експлуатаційні витрати - E_2 = 1001 грн./рік;*
- *обсяг робіт - Q = 1020 шт./рік;*
- *чистий прибуток від реалізації - П = 30775,75 грн;*
- *термін окупності витрат - То = 0,41 року;*
- *річний економічний ефект - ΔE = 800,4 грн./рік.;*
- *економічний ефект для споживача на ціні - $\Delta Ц$ = 507 грн.*

Таким чином, отримані результати доводять корисність та необхідність нової розробки.

Дякую за увагу !