Вінницький національний технічний університет
Факультет менеджменту та інформаційної безпеки
Кафедра менеджменту та безпеки інформаційних систем
Кафедра МБІС

Магістерська кваліфікаційна робота
на тему:

«ВДОСКОНАЛЕННЯ МЕТОДУ ЗАХИСТУ ВІД АТАКИ ТИПУ SHOULDER SURFING»

Виконав: ст. гр. УБ-19м
Бондаренко О. В.
Керівник:
к.т.н., доц. Карпінець В. В.

Вінниця
2020

Актуальність теми

Все більш актуальним є питання, яке стосується захисту інформації.

Оскільки ризики злому та отримання конфіденційної інформації зловмисниками збільшуються - виникає необхідність у застосуванні більш досконалих методів захисту.

Для розв’язання даної проблеми користувачам пропонуються альтернативні методи захисту, одним із яких є автентифікації на основі графічних паролів.

Основний недолік для більшості графічних паролів – час введення пароля та вразливість до атаки типу shoulder surfing.

Саме тому актуальним є вдосконалення методу захисту від атаки типу shoulder surfing.

Мета і постановка задачі

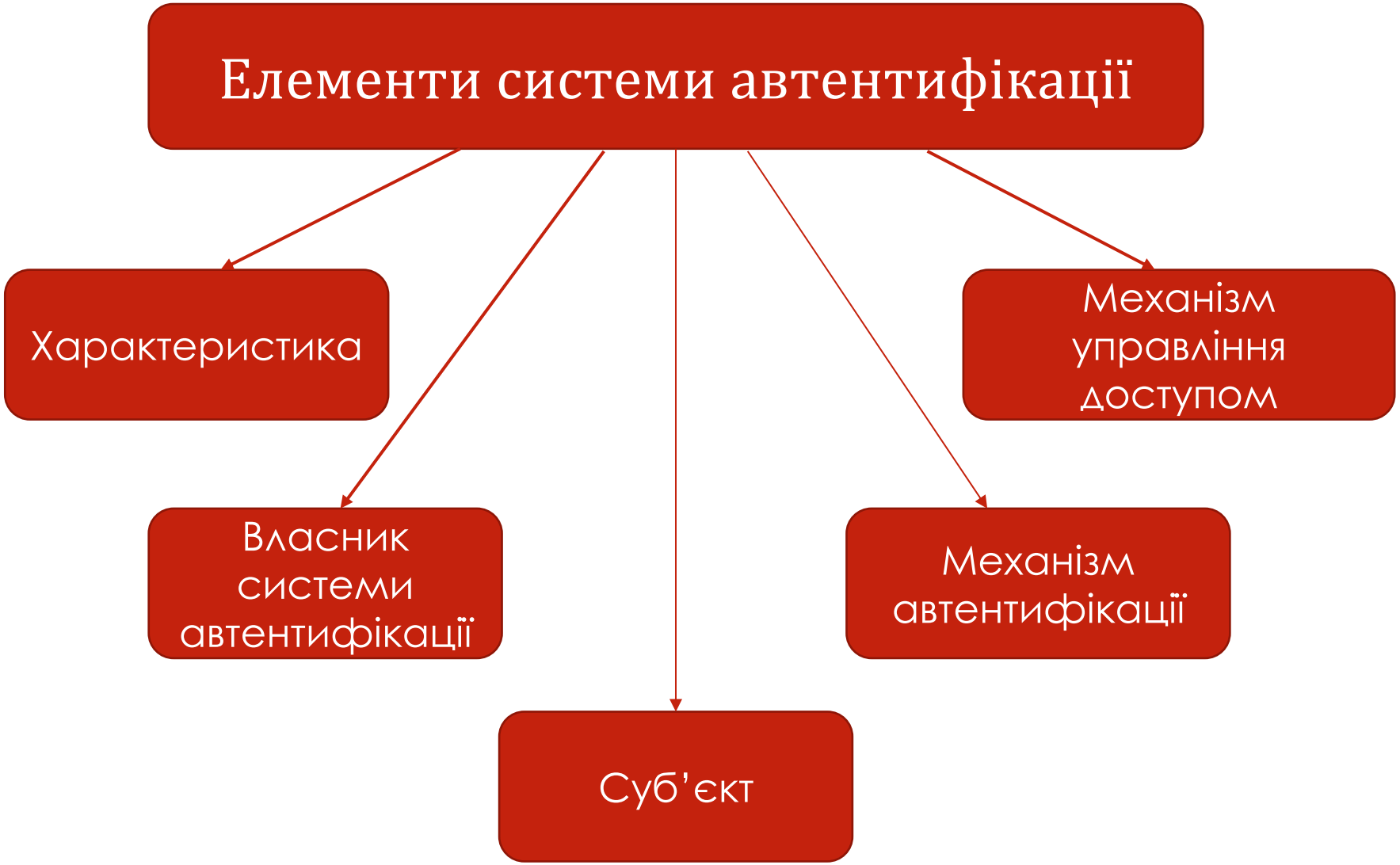
Мета - розробка вдосконаленого методу захисту від атаки типу shoulder surfing

- Провести огляд існуючих методів автентифікації
- Провести аналіз можливих вдосконалень методу графічної автентифікації
- Розробити структуру модуля автентифікації
- Провести програмну реалізацію вдосконаленого методу захисту від атаки типу shoulder surfing на основі графічного пароля

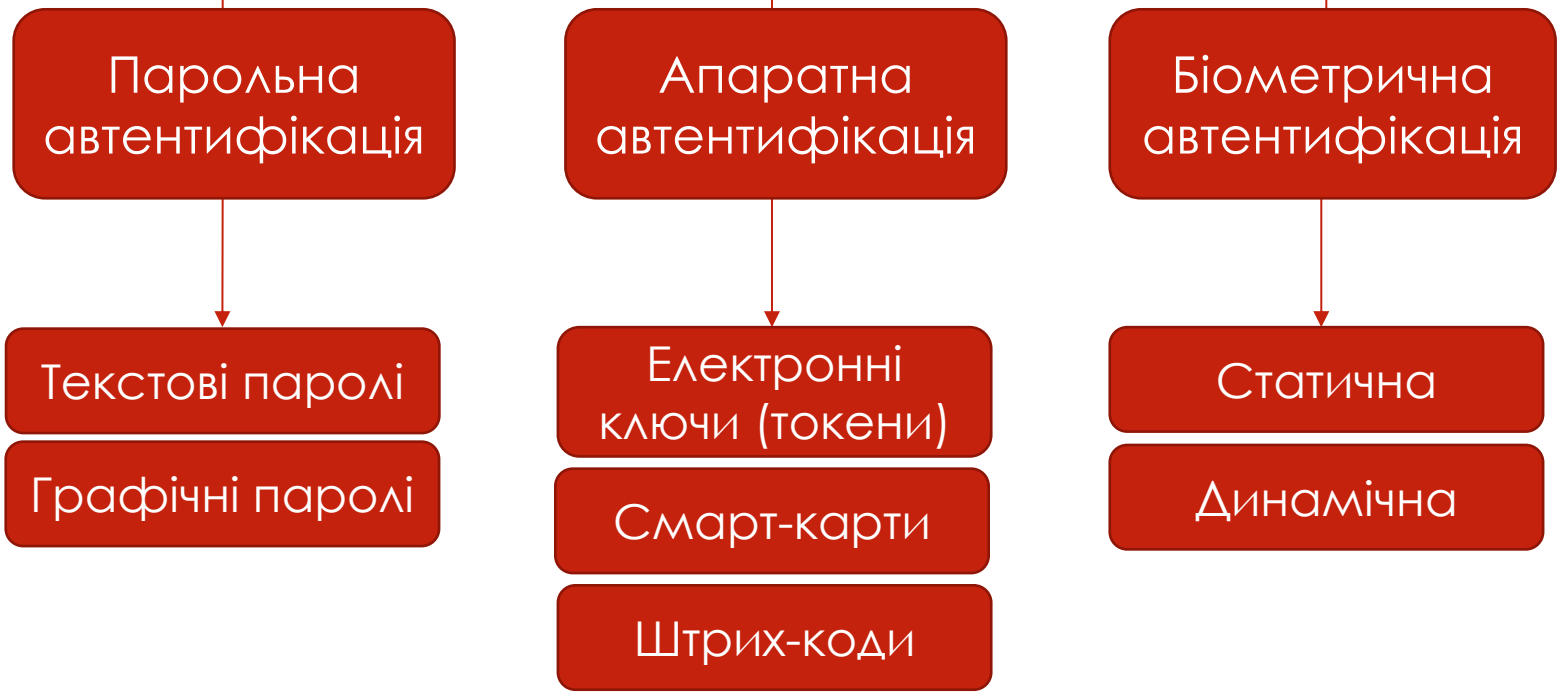
Об'єкт дослідження - процес автентифікації користувача на основі графічного пароля

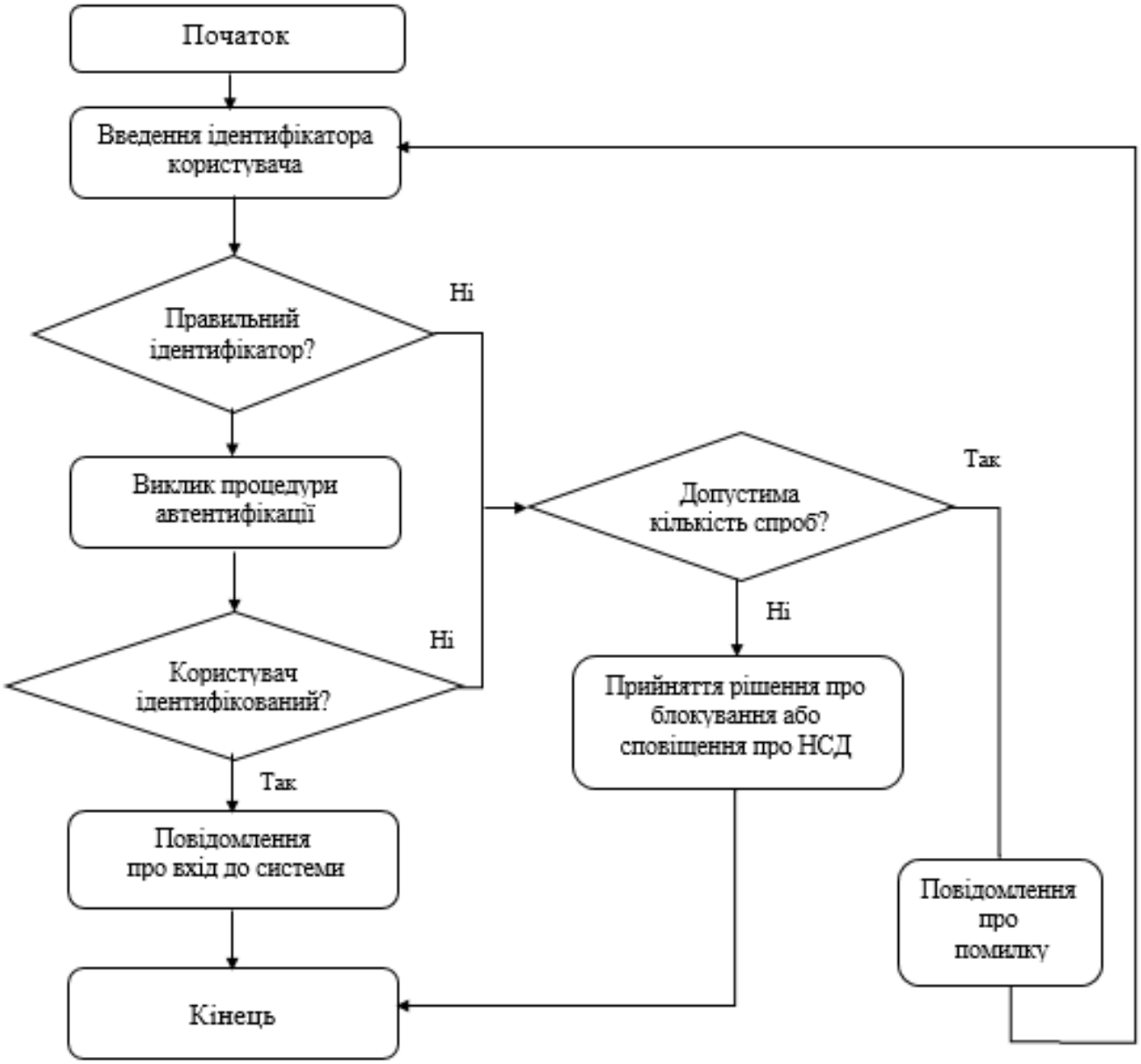
Предмет дослідження - методи та засоби автентифікації користувача із захистом від атаки типу shoulder surfing

Новизна одержаних результатів. Вдосконалено метод захисту від атаки типу shoulder surfing за рахунок використання графічного пароля за схемою Triangle, що дозволило підвищити стійкість до атаки даного типу.


Елементи системи автентифікації
Характеристика
Механізм управління доступом
Власник системи автентифікації
Механізм автентифікації
Суб'єкт

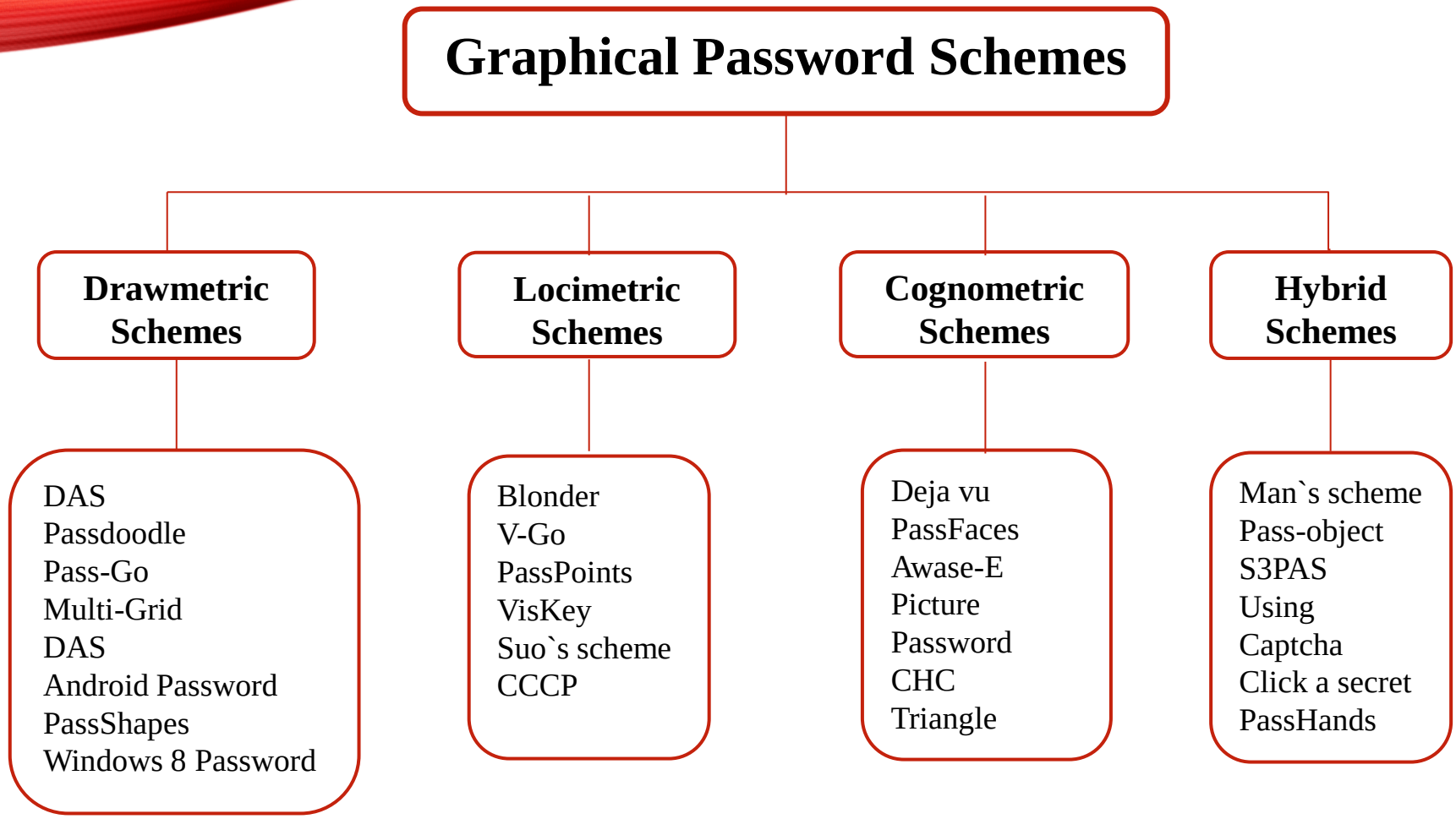
Методи автентифікації



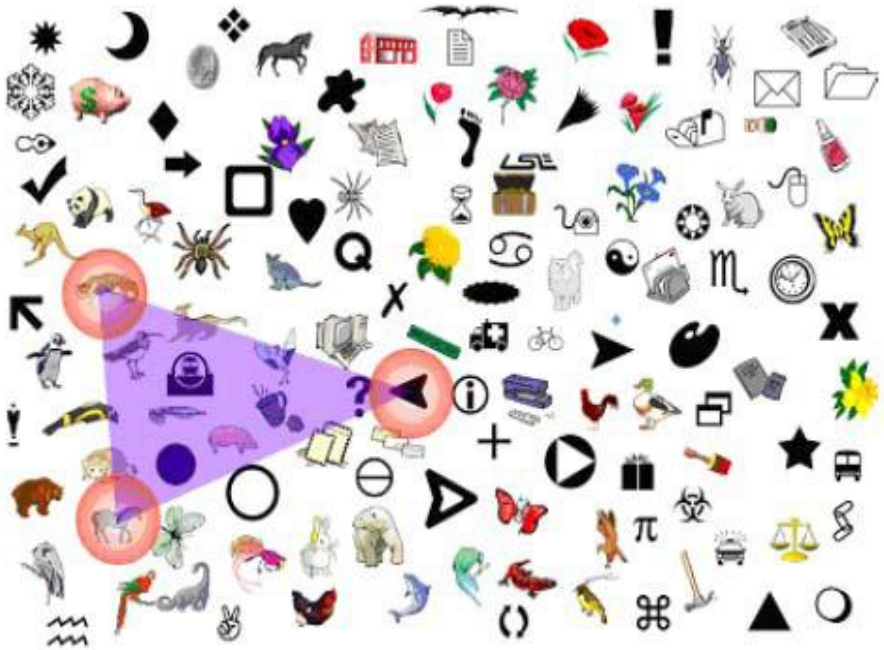


Загальна схема процедури автентифікації

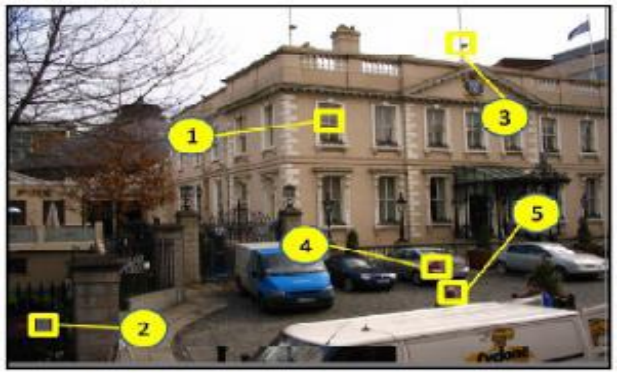
Graphical Password Schemes



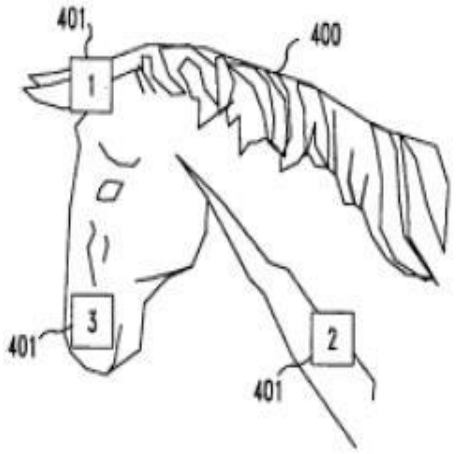
Triangle scheme
Sobrado and Birget



PassPoints



Blonder



Функції зручностей використання графічних паролів

Схеми графічних паролів	Методи		Функції зручностей використання графічних паролів																	
			Запам'ятовуваність																	
	На основі розпізнавання	Відкликання	Змістовність, значущість	Людські обличчя	Впорядковані за темою	Користувач обирає зображ.	На основі іконок	Абстрактні зображення	Вільний вибір	Великий простір пароля	Ефективність	Зображення - приманки	Рандомні призначення	Надійність та точність	Простота створення	Простота виконання	Легкість у використанні	На основі сітки	Кілька раундів	Малювання пароля
Picture Password	√		√		√					X	X	√	√	X	√	√	√	√	X	
PassFaces	√			√		√				X	X	√	√	√	√	√	√	√	√	
Triangle	√						√			√	X	√	√	√	√	√	√		√	
Déjà Vu	√							√		X	X	√	√	√	√		√	√		
Awase-E	√									X			√		√					
Authenti-Graph	√									X			√		√					
Blonder		√	√			√			√	√	X		X		√	X				
PassPoints		√	√			√			√	√	√		X	√	√	X	√	√		
DAS		√	√							√			X	X	√	X		√		√
VisKey		√	√			√			√	X	X			√	√					
Passlogix		√	√		√					X	X			X	√		√			
√ - Да X – Ні Пусто – не визначено																				

Порівняльний аналіз схем графічної автентифікації

Назва методу	Назва атаки	
	Стійкі	Нестійкі
Awase-E	Brute Force, Shoulder surfing	Description, Guessing
PassFaces	Spyware, Description	Dictionary, Guessing, Shoulder Surfing, Brute Force,
Déjà vu	Description, Dictionary, Spyware	Guessing, Shoulder Surfing,
Blonder	Dictionary, Spyware, Description,	Brute Force, Guessing, Shoulder Surfing
PassPoint	Dictionary, Spyware, Description	Brute Force, Guessing, Shoulder Surfing
Draw A-Secret	Dictionary, Shoulder Surfing	Brute Force, Spyware, Description, Guessing,
Triangle	Dictionary, Shoulder Surfing, Description	Brute Force
Pass-Go	Brute Force, Guessing	Description
Picture Password	Brute Force, Guessing,	Shoulder Surfing, Spyware

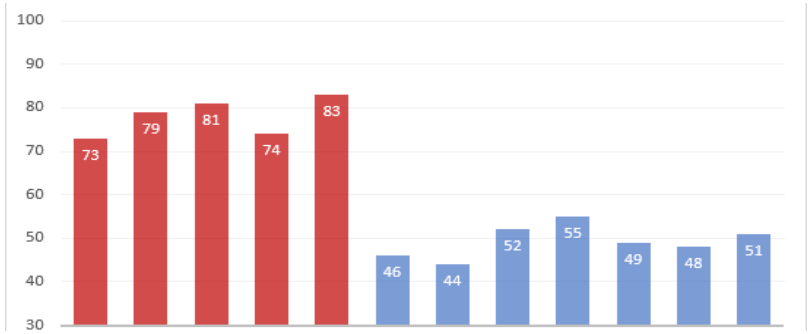
Типи атаки типу shoulder surfing

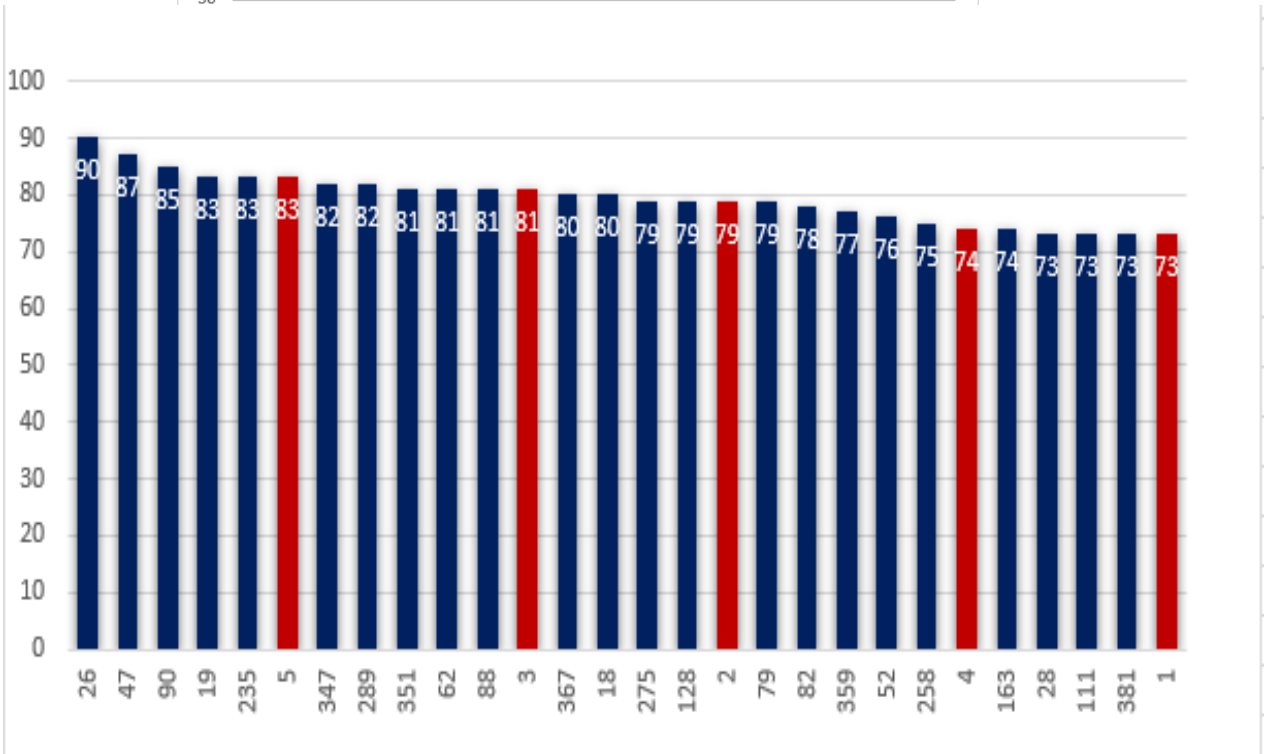
- Тип I: неозброєними очима
- Тип II: одноразова відео фіксація процесу автентифікації
- Тип III: багаторазова відео фіксація процесу автентифікації

Залежність можливих комбінацій пароля від загальної кількості зображень та від кількості парольних зображень

k \ n	300	350	400	450	500
4	$0{,}29*10^9$	$0{,}61*10^9$	$1{,}1*10^9$	$1{,}68*10^9$	$2{,}47*10^9$
5	$19*10^9$	$42*10^9$	$82*10^9$	$150*10^9$	$254*10^9$
6	$0{,}95*10^{12}$	$2{,}38*10^{12}$	$5{,}42*10^{12}$	$11{,}1*10^{12}$	$20{,}08*10^{12}$

Частота попадань зображень в згенерований набір





Ймовірність попадання в область трикутника

$$P_{\text{попад.}} = \frac{S_{\text{трик.}}}{S_{\text{заг.}}},$$

де $S_{\text{трик.}}$ – площа парольних картинок;

$S_{\text{заг.}}$ – загальна площа екрану, де розташовані графічні об’єкти.

$S_{max.\text{трик.}} = \frac{1}{2} S_{\text{заг.}}$,

тоді $P_{\text{попад.}} = \frac{1}{2}$

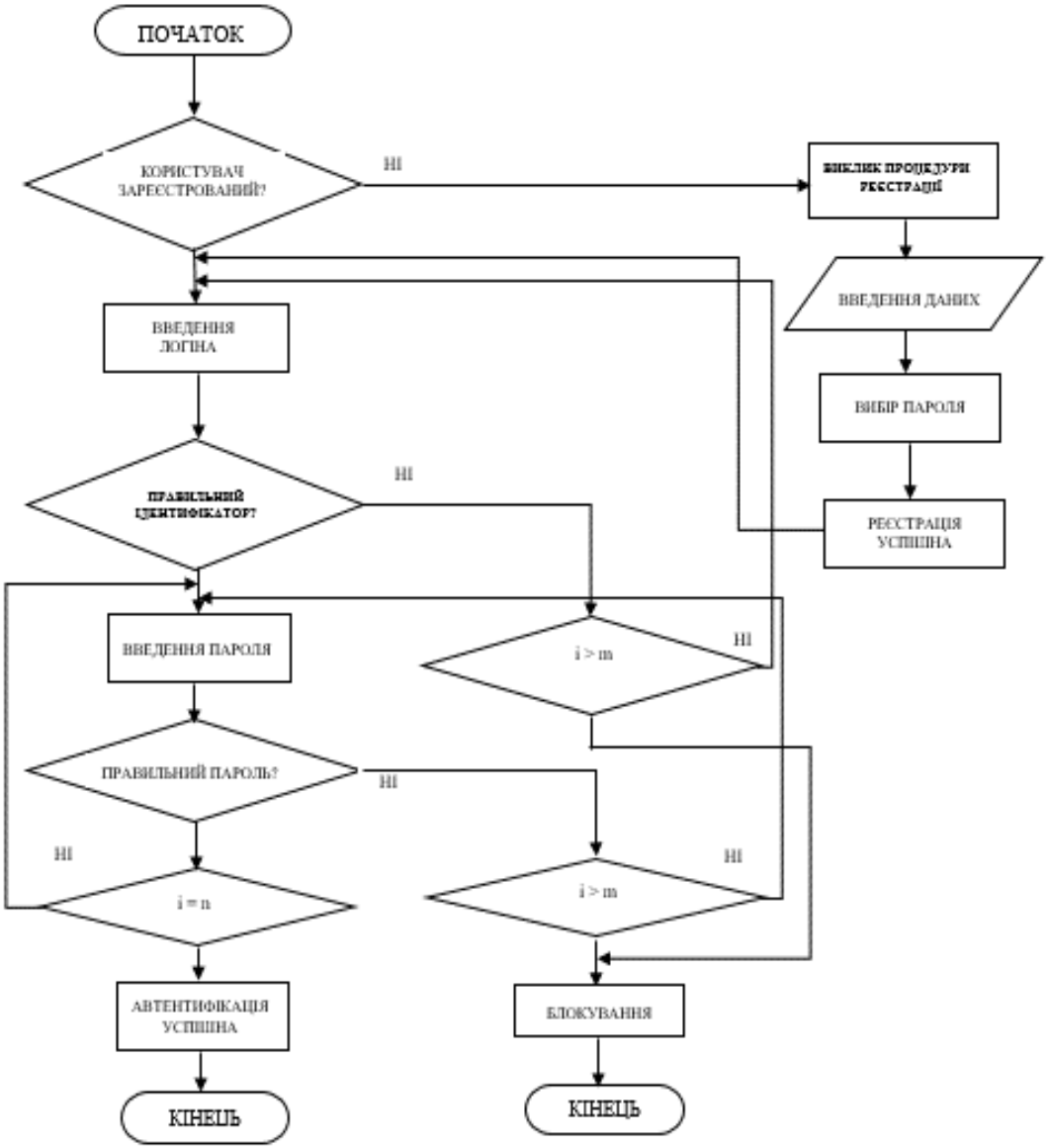
Ймовірність вгадування пароля

$$p = \frac{1}{n} \sum_{i=1}^{n} \frac{S_i}{S},$$

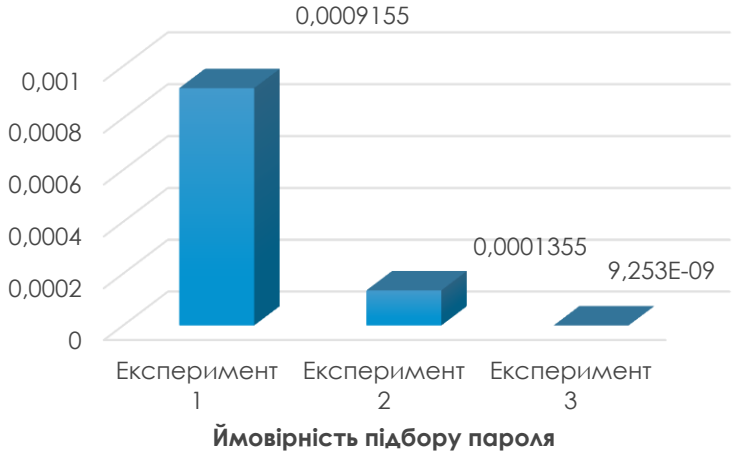
де S_i (i=1…n) - площа і-го трикутника;

S – площа вікна для введення пароля.

Блок-схема алгоритму ідентифікації та автентифікації



Аналіз стійкості вдосконаленого методу захисту



Кількісна оцінка стійкості парольного захисту з параметрами, які пов’язані за формулою

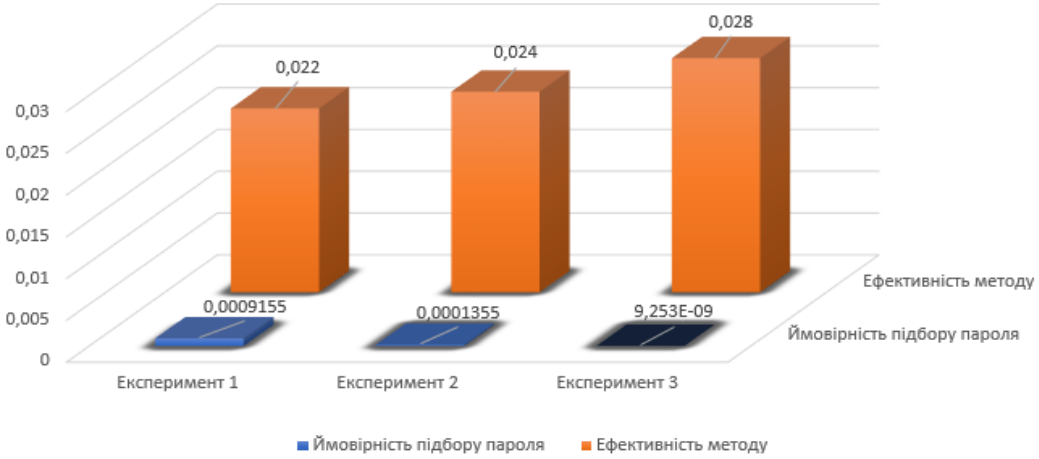
$$P = \frac{V \cdot T}{A^l},$$

де P – ймовірність підбору пароля протягом його часу дії
V – швидкість перебору зловмисником паролів;
T – максимальний термін дії пароля;
A – потужність алфавіту пароля;
l – довжина пароля;
A^l – кількість можливих паролів довжиною l, отриманих за допомогою символів алфавіту A.

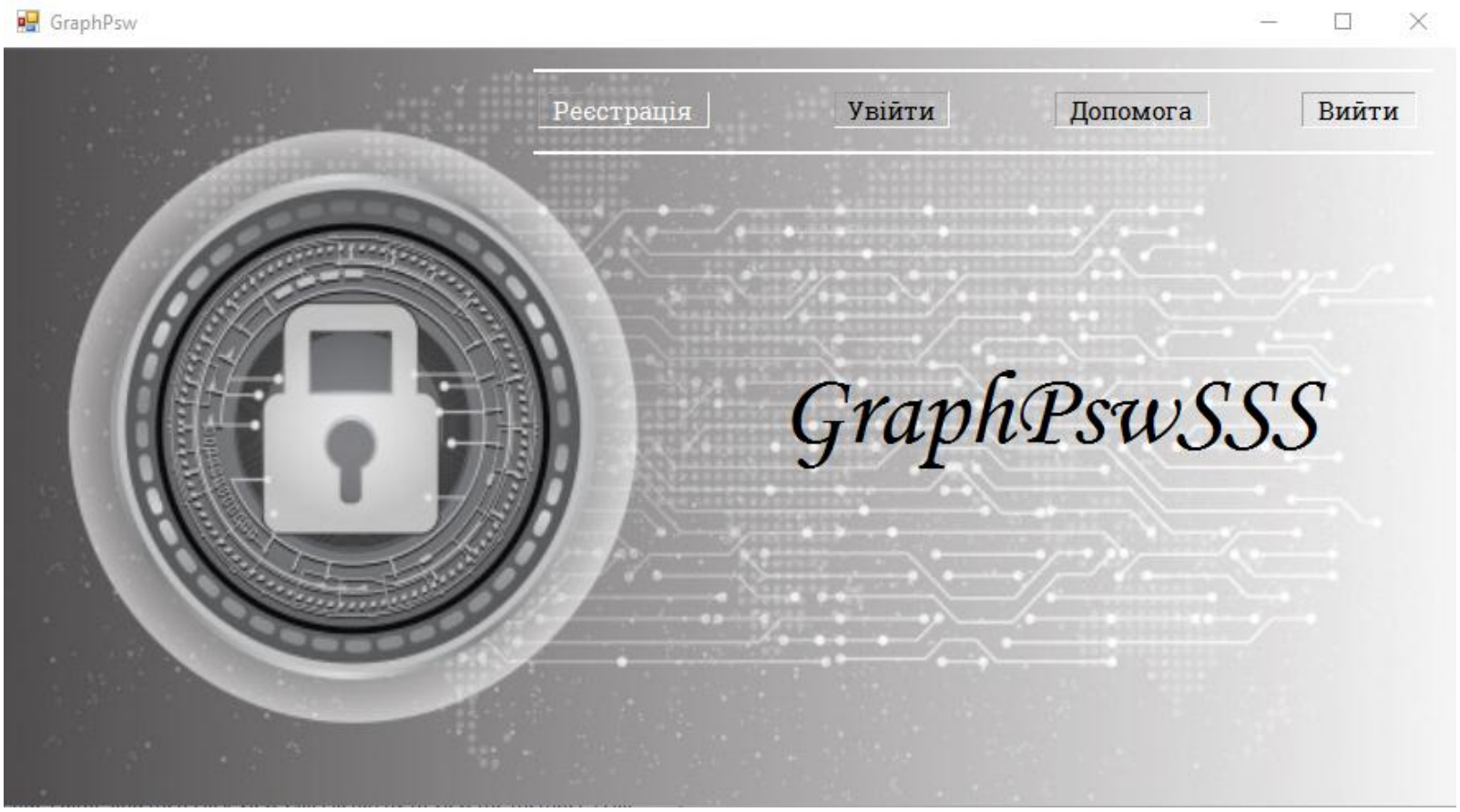
Ефективність визначають за формулою

$$E = \frac{P}{T},$$

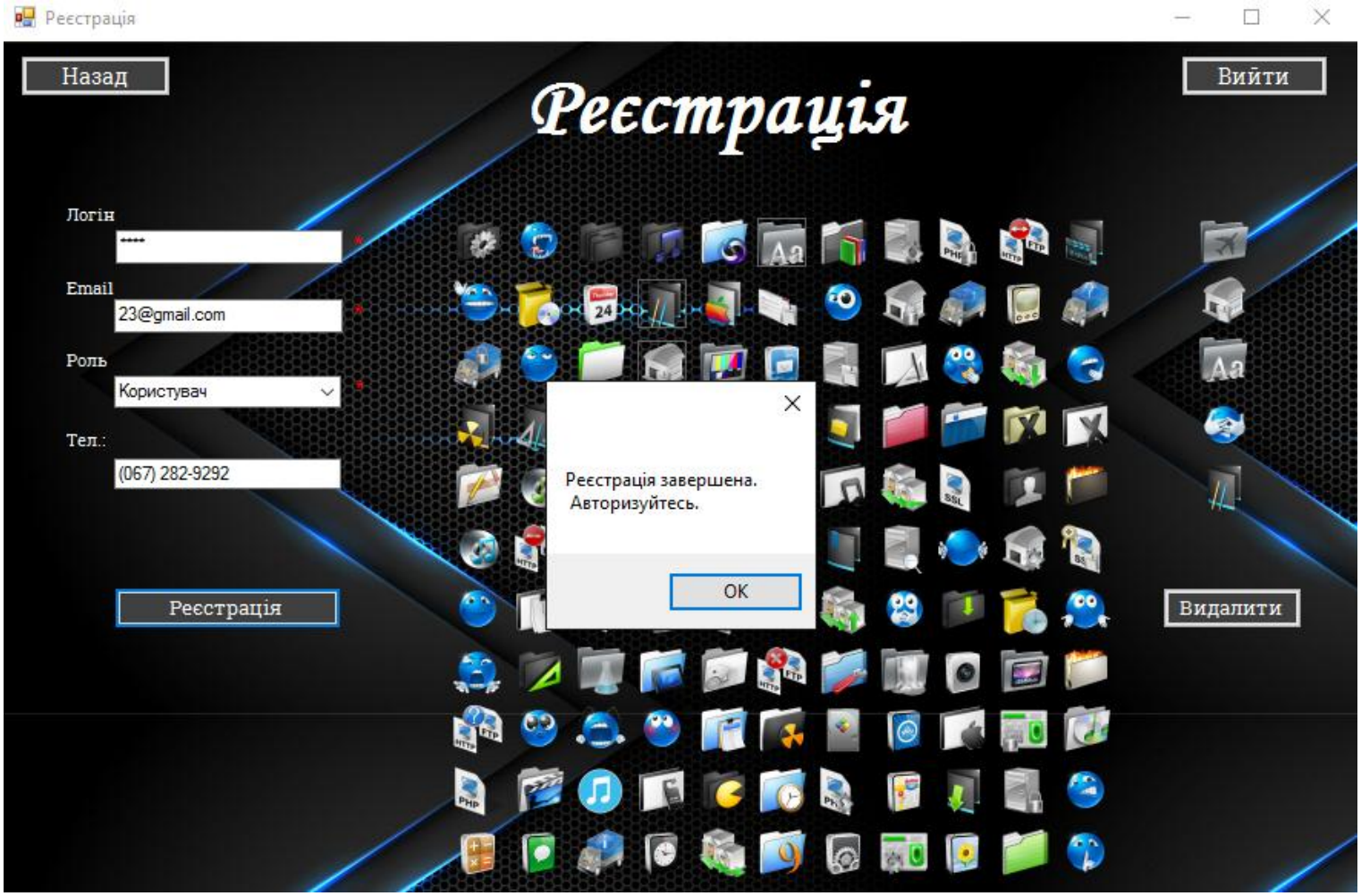
де E – ефективність графічної автентифікації;
P – оцінка стійкості пароля;
T – час необхідний для проходження автентифікації.



Головне вікно програми

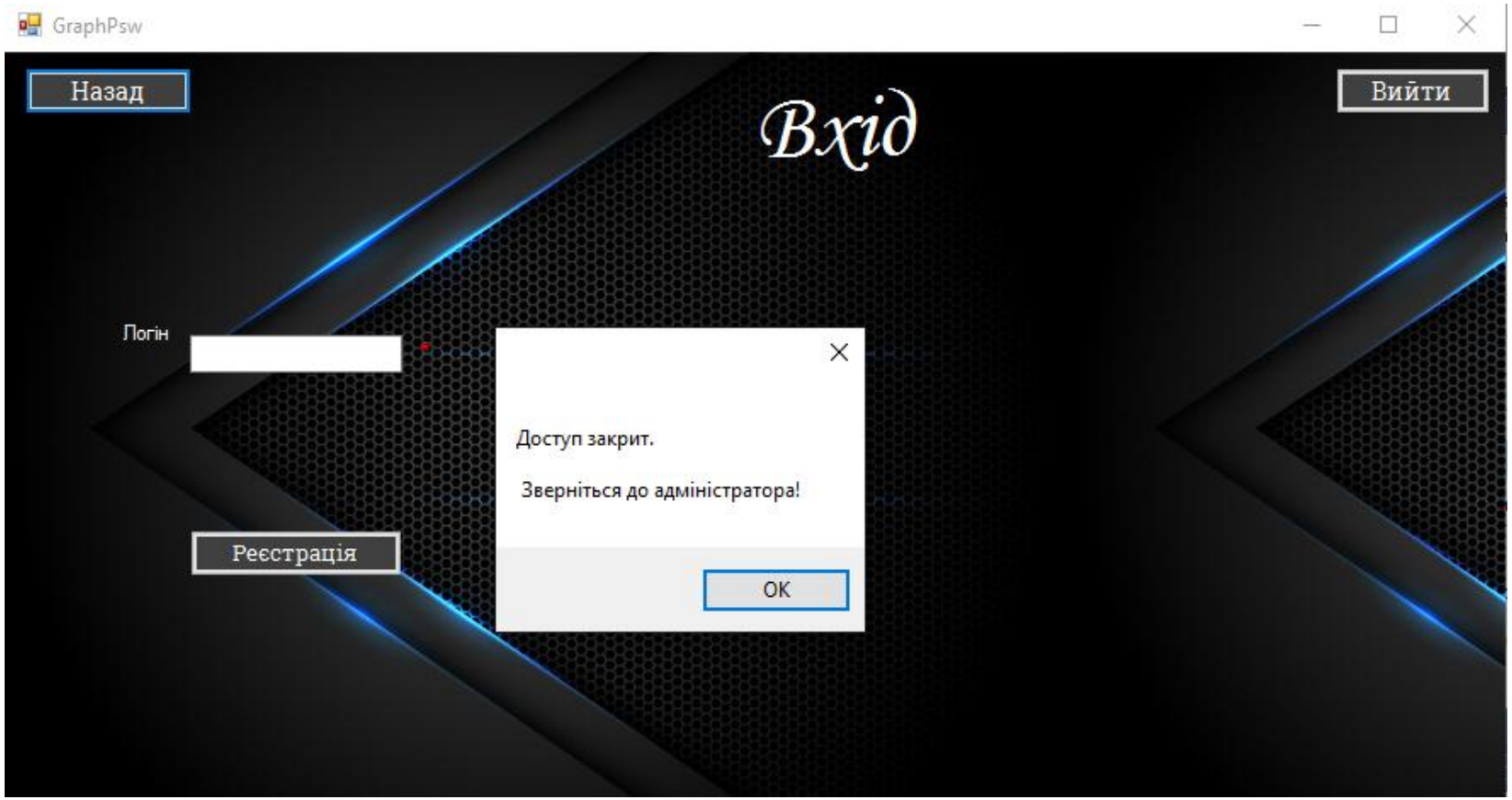


Форма реєстрації

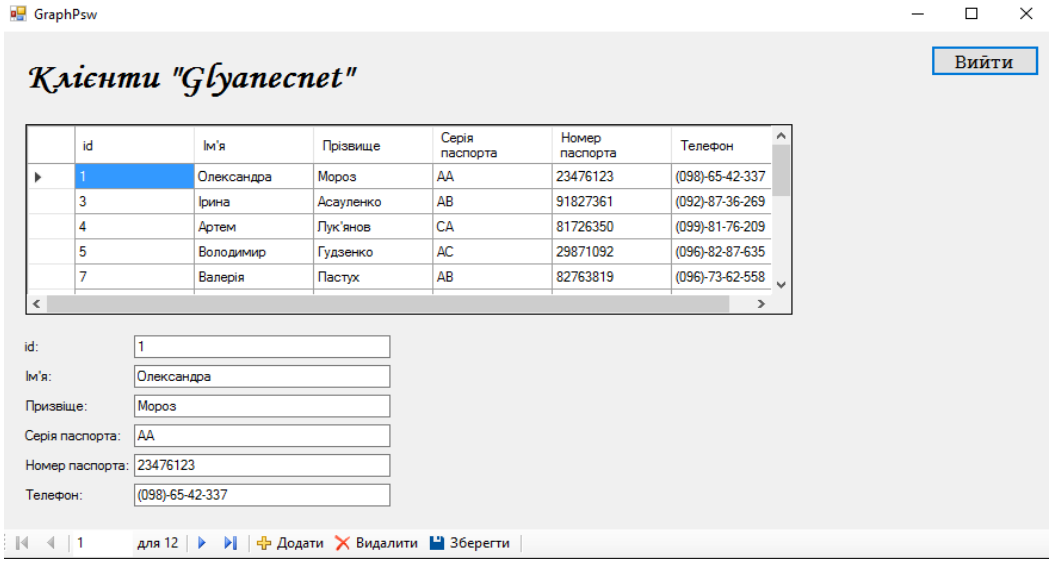


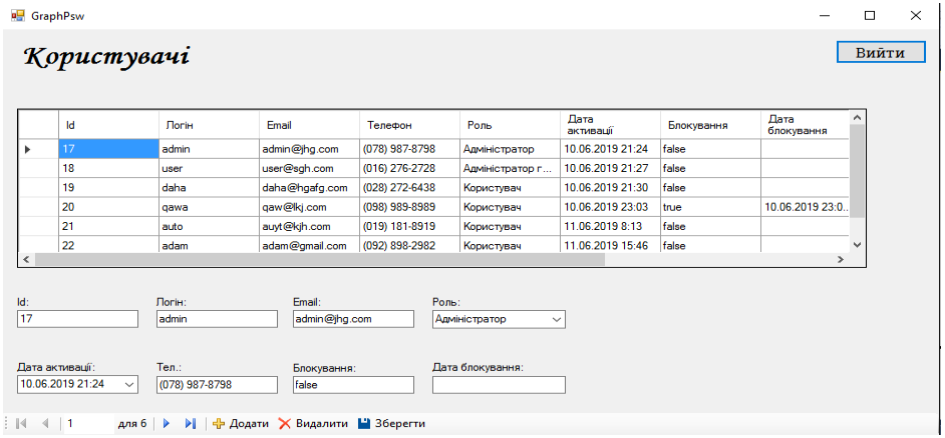
Форма входу користувачів

Повідомлення про блокування користувача



Сторінки входу користувачів з різними типами ролей





Економічна частина.
Розрахунок ефективності вкладених інвестиції та періоду їх окупності

Проведено оцінку комерційного потенціалу розробки програмного продукту.

Спрогнозовано загальні витрати на розробку і впровадження, які складають 72806,96 грн.

Розраховано абсолютна ефективність вкладених інвестицій, яка становить 321971,85 грн., що свідчить про отримання прибутку інвестором від комерціалізації розробки.

Термін окупності вкладених у реалізацію проекту інвестицій становить 1,31 року

Висновки

Проаналізовано існуючі методи автентифікації на основі графічного пароля

Проведено аналіз можливих вдосконалень методу захисту від атаки типу shoulder surfing

Розроблено алгоритм вдосконаленого методу захисту

Проведено оцінка стійкості вдосконаленого методу захисту до атаки типу shoulder surfing

Програмна реалізація вдосконаленого методу захисту від атаки типу shoulder surfing на основі графічного пароля

Тестування роботи програмного додатку

Дякую за увагу !