

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. Карпинець 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

```
graph TD; A[Елементи системи автентифікації] --> B[Характеристика]; A --> C[Власник системи автентифікації]; A --> D[Суб'єкт]; A --> E[Механізм управління доступом]; A --> F[Механізм автентифікації];
```

Характеристика

Власник
системи
автентифікації

Суб'єкт

Механізм
управління
доступом

Механізм
автентифікації

Методи автентифікації

Парольна
автентифікація

Текстові паролі

Графічні паролі

Апаратна
автентифікація

Електронні
ключі (токени)

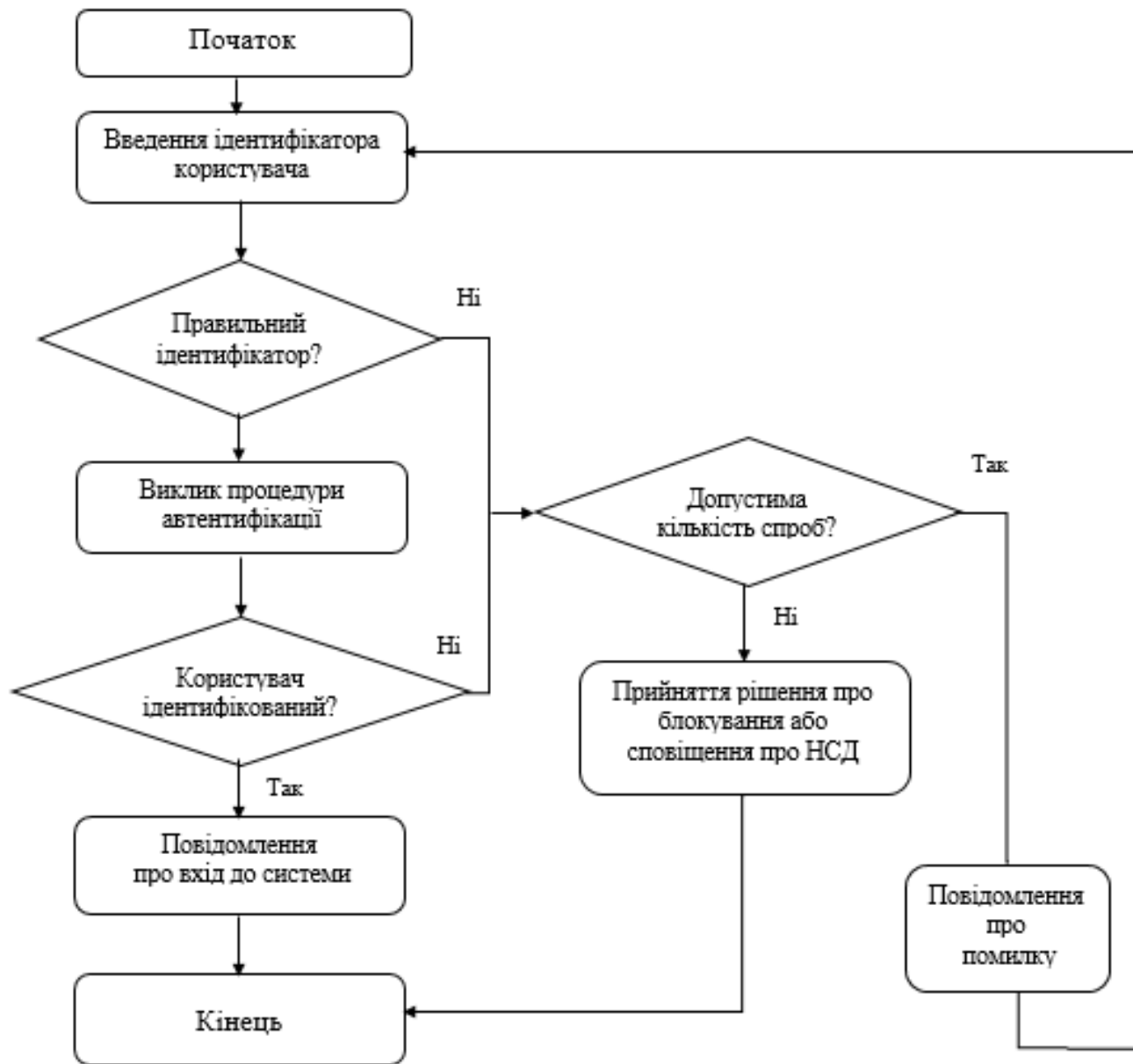
Смарт-карти

Штрих-коди

Біометрична
автентифікація

Статична

Динамічна



Загальна схема процедури автентифікації

Graphical Password Schemes

Drawmetric Schemes

DAS
Passdoodle
Pass-Go
Multi-Grid
DAS
Android Password
PassShapes
Windows 8 Password

Locimetric Schemes

Blonder
V-Go
PassPoints
VisKey
Suo`s scheme
CCCP

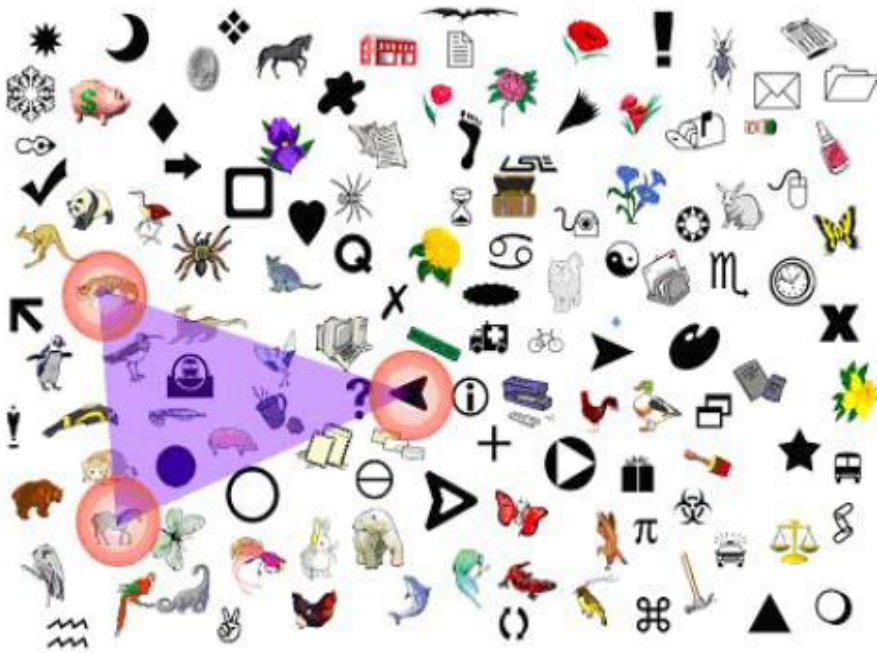
Cognometric Schemes

Deja vu
PassFaces
Awase-E
Picture
Password
CHC
Triangle

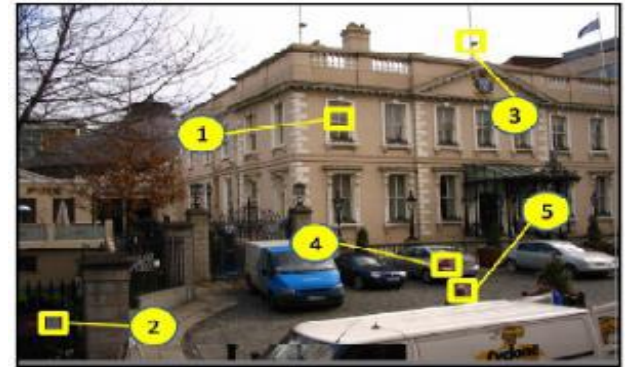
Hybrid Schemes

Man`s scheme
Pass-object
S3PAS
Using
Captcha
Click a secret
PassHands

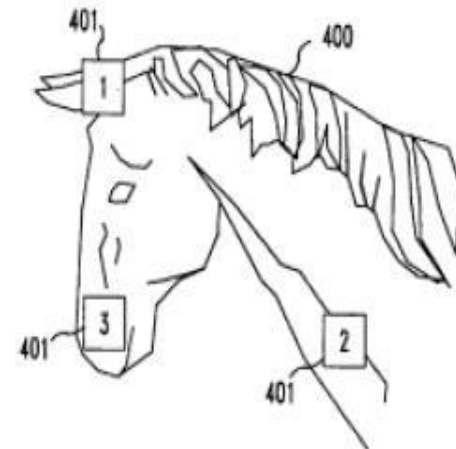
Triangle scheme Sobrado and Birget



PassPoints



Blonder



Функції зручностей використання графічних паролів

Схеми графічних паролів	Методи		Функції зручностей використання графічних паролів																				
	На основі розпізнавання	Відкликання	Запам'ятовуваність																				
			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

```
graph TD; A[Типи атаки типу shoulder surfing] --> B[Тип I: неозброєними очима]; A --> C[Тип II: одноразова відео фіксація процесу автентифікації]; A --> D[Тип III: багаторазова відео фіксація процесу автентифікації];
```

Тип I:
неозброєними
очима

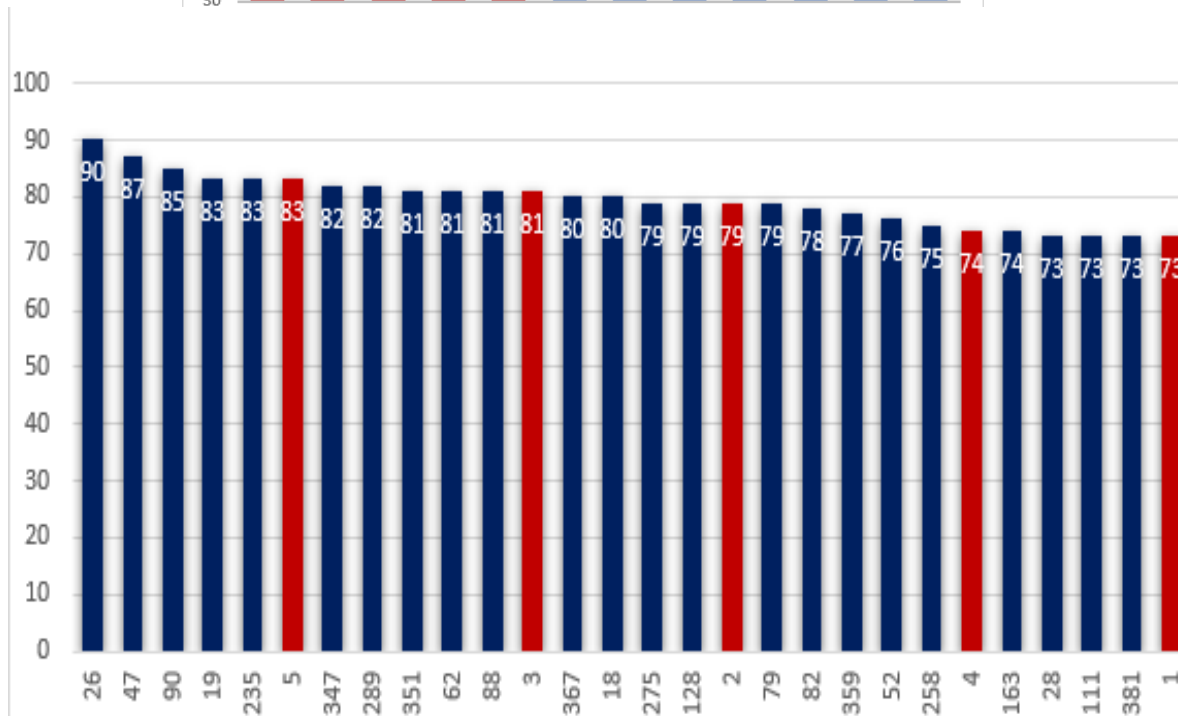
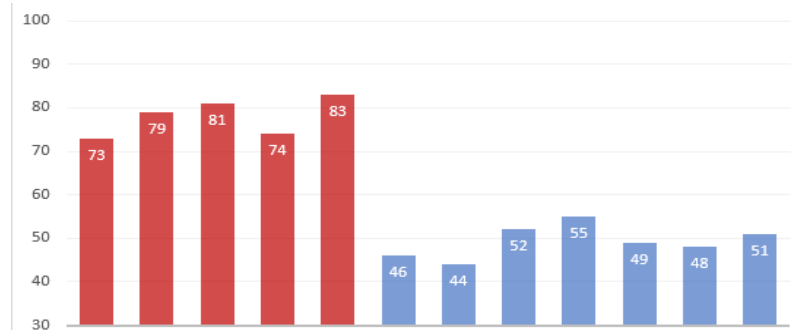
Тип II:
одноразова
відео фіксація
процесу
автентифікації

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	$0,29 \cdot 10^9$	$0,61 \cdot 10^9$	$1,1 \cdot 10^9$	$1,68 \cdot 10^9$	$2,47 \cdot 10^9$
5	$19 \cdot 10^9$	$42 \cdot 10^9$	$82 \cdot 10^9$	$150 \cdot 10^9$	$254 \cdot 10^9$
6	$0,95 \cdot 10^{12}$	$2,38 \cdot 10^{12}$	$5,42 \cdot 10^{12}$	$11,1 \cdot 10^{12}$	$20,08 \cdot 10^{12}$

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.

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

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

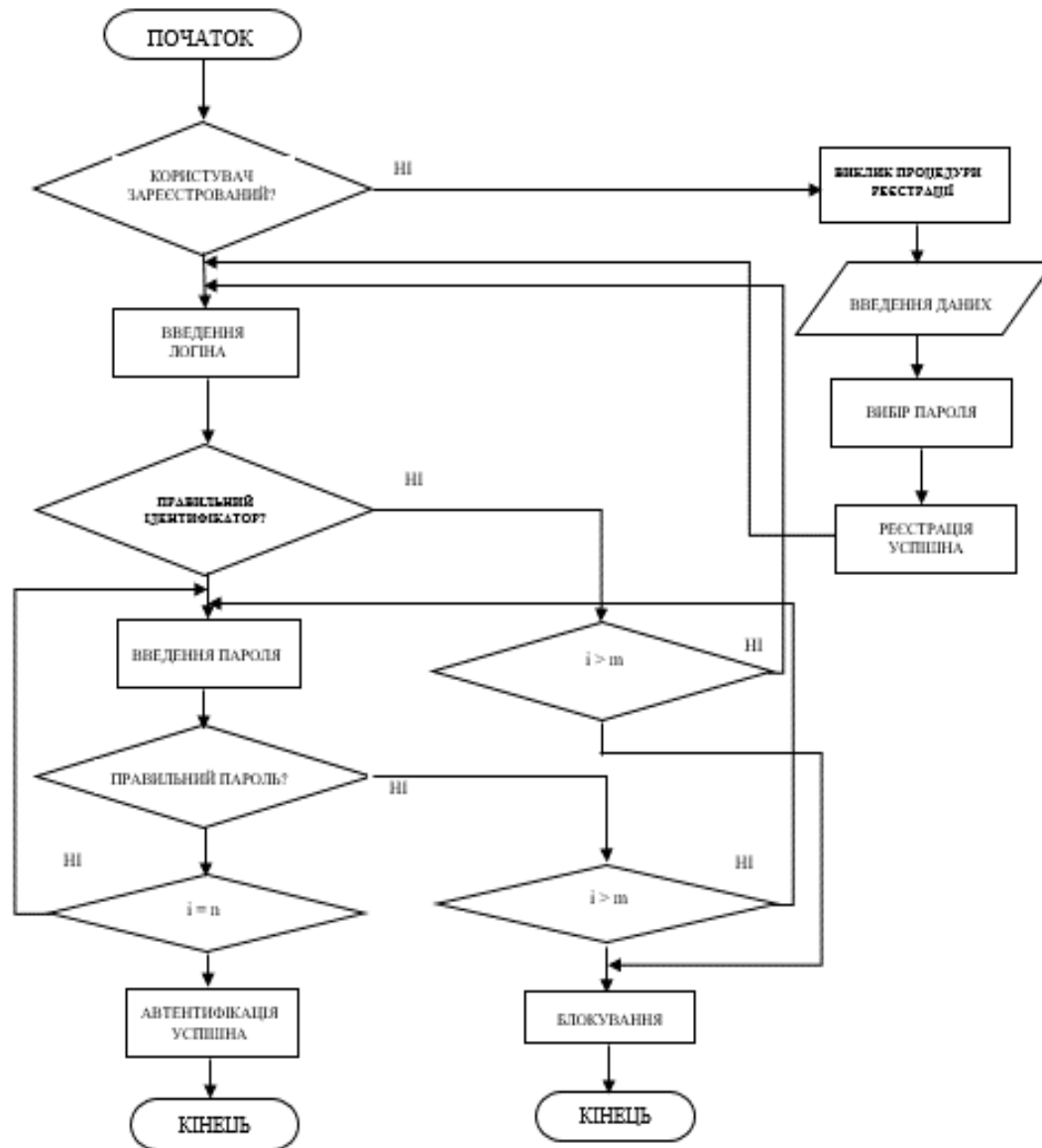
Ймовірність вгадування пароля

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

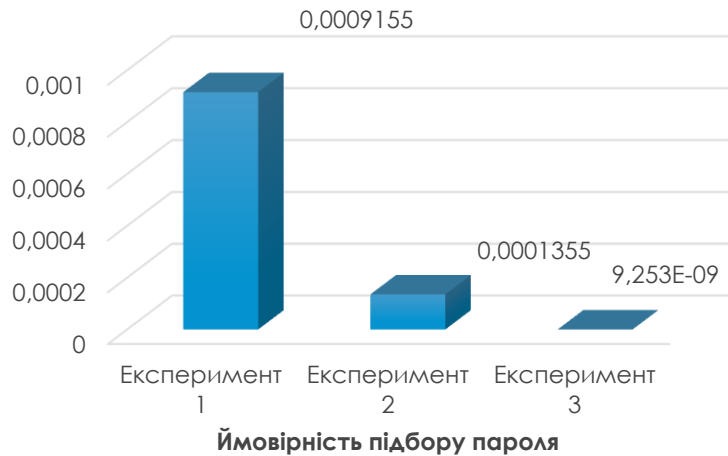
де $S_i (i=1 \dots n)$ - площа i -го трикутника;

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 .

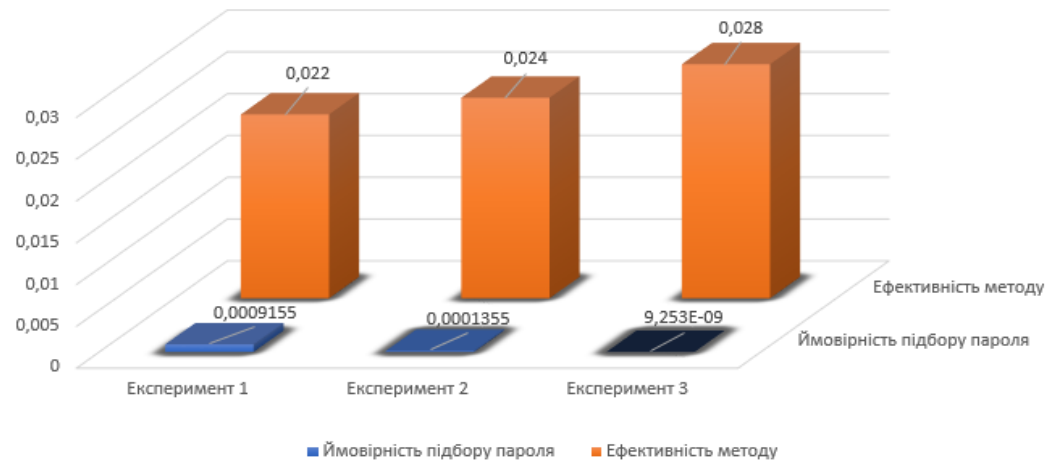
Ефективність визначають за формулою

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

де E – ефективність графічної автентифікації;

P – оцінка стійкості пароля;

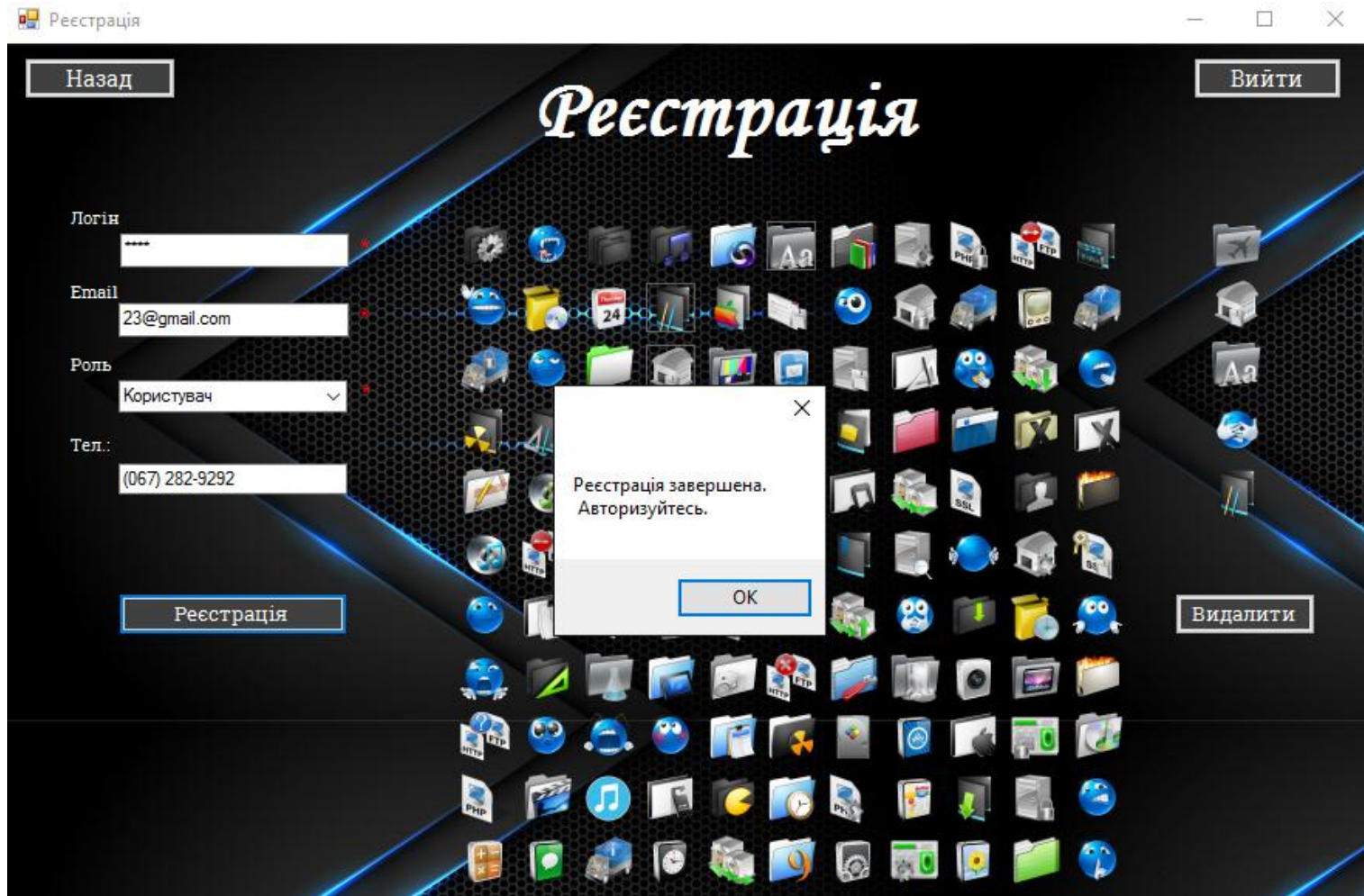
T – час необхідний для проходження автентифікації.



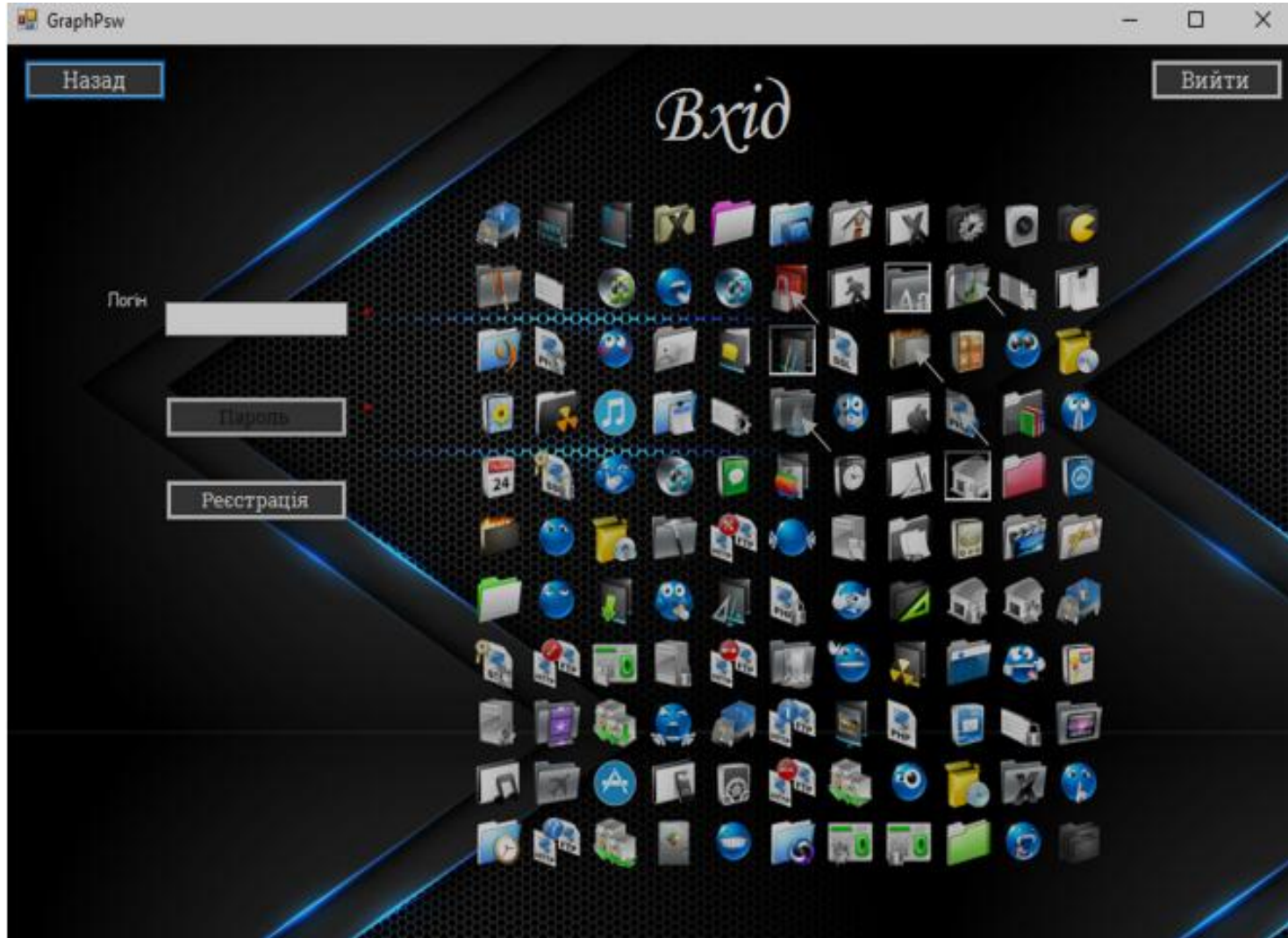
Головне вікно програми



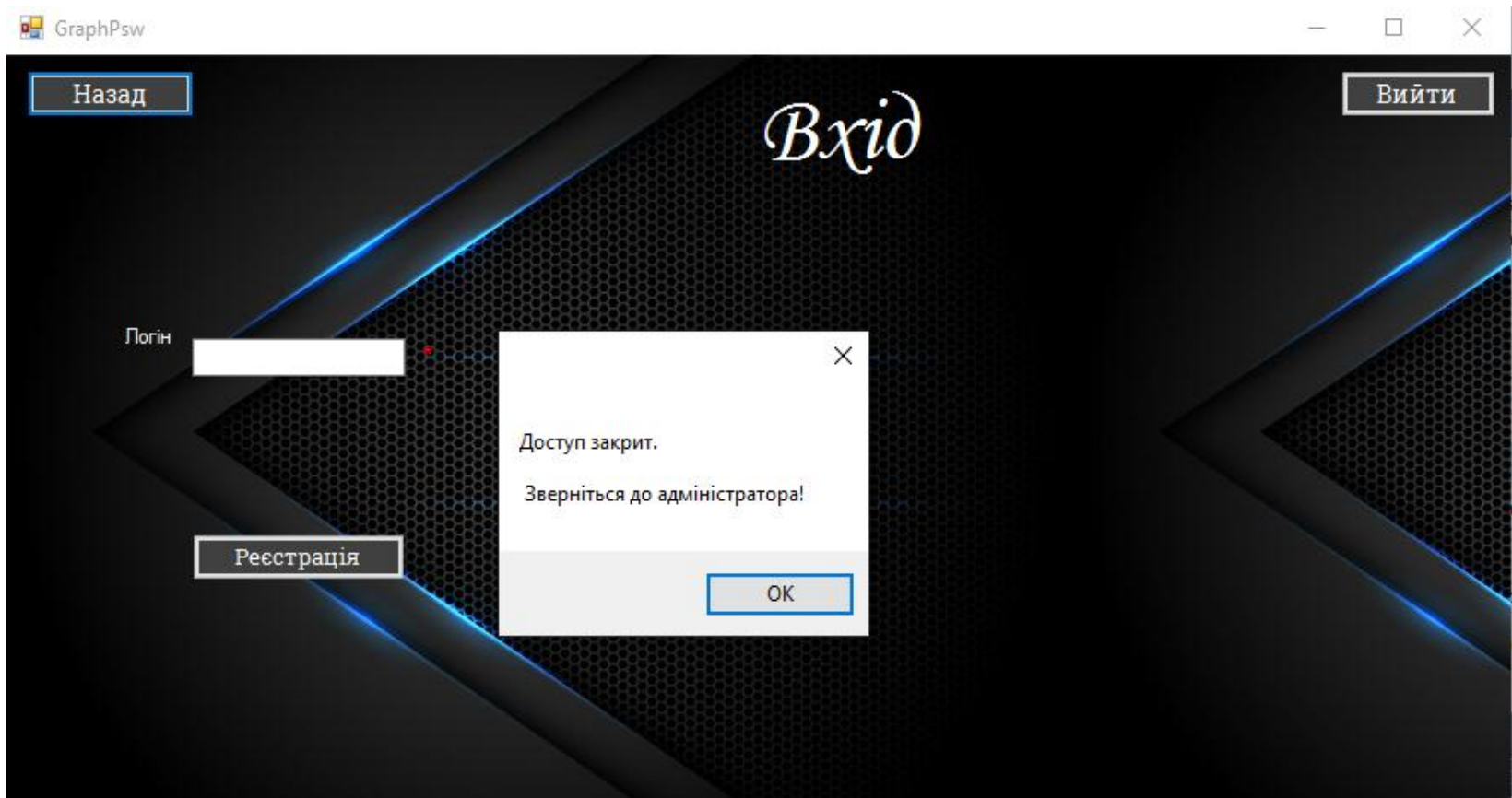
Форма реєстрації



Форма входу користувачів



Повідомлення про блокування користувача



Сторінки входу користувачів з різними типами ролей

GraphPsw

Клієнти "Gbyanecnet"

Вийти

id	Ім'я	Прізвище	Серія паспорта	Номер паспорта	Телефон
1	Олександра	Мороз	AA	23476123	(098)-65-42-337
3	Ірина	Асауленко	AB	91827361	(092)-87-36-269
4	Артем	Лук'янов	CA	81726350	(099)-81-76-209
5	Володимир	Гудзенко	AC	29871092	(096)-82-87-635
7	Валерія	Пастух	AB	82763819	(096)-73-62-558

id:

Ім'я:

Прізвище:

Серія паспорта:

Номер паспорта:

Телефон:

1 для 12

Додати Видалити Зберегти

GraphPsw

Користувачі

Вийти

Id	Логін	Email	Телефон	Роль	Дата активації	Блокування	Дата блокування
17	admin	admin@jhg.com	(078) 987-8798	Адміністратор	10.06.2019 21:24	false	
18	user	user@sqh.com	(016) 276-2728	Адміністратор г...	10.06.2019 21:27	false	
19	daha	daha@hgafg.com	(028) 272-6438	Користувач	10.06.2019 21:30	false	
20	qawa	qaw@kjl.com	(098) 989-8989	Користувач	10.06.2019 23:03	true	10.06.2019 23.0...
21	auto	aut@kjh.com	(019) 181-8919	Користувач	11.06.2019 8:13	false	
22	adam	adam@gmail.com	(092) 898-2982	Користувач	11.06.2019 15:46	false	

Id:

Логін:

Email:

Роль:

Дата активації:

Тел.:

Блокування:

Дата блокування:

1 для 6

Додати Видалити Зберегти

Економічна частина.

Розрахунок ефективності вкладених інвестицій 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 оцінку 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 !