МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

КАФЕДРА КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

# БАКАЛАВРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

## Захист інформації в автоматизованій системі класу 1 від несанкціонованих дій з застосуванням сучасних програмних засобів

Виконав: студент групи БІКС-22 Кучер Б. В.
Спеціальність: 125 «Кібербезпека»
Науковий керівник: к.т.н. доц. Котенко А. М.

КНУБА 2026

# МЕТА, ОБ'ЄКТ, ПРЕДМЕТ, АКТУАЛЬНІСТЬ

| | |
|---|---|
| Мета роботи | Розробка програмного засобу захисту інформації в автоматизованих системах класу 1 від несанкціонованих дій із застосуванням сучасних методів розпізнавання обличчя в реальному часі |
| Об'єкт дослідження | Процеси ідентифікації та контролю доступу персоналу в автоматизованих системах класу 1 |
| Предмет дослідження | Методи та засоби біометричної ідентифікації на основі геометрії обличчя для захисту АС К1 від несанкціонованих дій |
| Актуальність теми | Актуальність теми обумовлена необхідністю розроблення комплексного програмного рішення, що інтегрує функціонал класифікації АС, управління персоналом, біометричної ідентифікації в реальному часі та аудиту подій безпеки відповідно до вимог нормативно-правової бази України у сфері технічного захисту інформації (ТЗІ) |

# ОСНОВНІ ЗАВДАННЯ

Аналіз нормативно-правової бази України у сфері захисту інформації в
АС К1 та класифікаційних вимог

Дослідження сучасних загроз інформаційній безпеці та методів
компрометації автентифікаційних даних

Порівняльний аналіз методів біометричної ідентифікації та
обгрунтування вибору алгоритму розпізнавання обличчя

Проєктування архітектури програмного засобу захисту, бази даних
персоналу та структури біометричних шаблонів

Розробка алгоритмів реєстрації користувачів, верифікації в реальному
часі та блокування несанкціонованих дій

Реалізація криптографічного захисту збережених біометричних даних
та журналів аудиту

Програмна реалізація системи мовою Python з використанням бібліотек
OpenCV та face_recognition

# ПРОБЛЕМАТИКА

Особливу небезпеку становлять інсайдерські загрози та атаки на автентифікаційні дані персоналу, що зумовлює необхідність впровадження засобів неперервної верифікації особи оператора в ході роботи з АС

## Статистика інсайдерських загроз:

| | |
|---|---|
| Частка внутрішніх загроз у всіх інцидентах | 19% |
| Середня вартість одного інсайдерського інциденту | 15,38 млн USD |
| Перевищення вартості над зовнішніми атаками | на 76% |

## Класифікація інсайдерських загроз для АС К1:

| Тип загрози | Мотивація | Механізм реалізації | Превентивні заходи |
|---|---|---|---|
| **Зловмисний інсайдер** | Фінансова вигода, помста, ідеологія | Несанкціоноване копіювання, знищення, передача даних конкурентам або ворожим спецслужбам | Моніторинг поведінки, принцип мінімальних привілеїв, DLP-системи |
| **Необережний інсайдер** | Незнання, недбалість | Помилкова конфігурація, передача даних незахищеними каналами, фішинг | Навчання, технічні блокування, аудит налаштувань |
| **Скомпрометований інсайдер** | Відсутня (жертва атаки) | Використання вкрадених облікових даних, токенів, сесій від імені легітимного користувача | Багатофакторна аутентифікація, безперервна верифікація, аналіз аномалій |
| **Інсайдер-шпигун** | Завдання на користь третіх сторін | Систематичне збирання та передача інформації, розвідка структури системи | Спостереження за патернами доступу, виявлення аномалій об'єму переданих даних |

Критичним недоліком традиційних засобів аутентифікації є відсутність механізму верифікації того, що особа, яка вводить правильний пароль, є тією самою особою, що зареєстрована в системі. Біометрична ідентифікація за геометрією обличчя дозволяє вирішити цю проблему

# НОРМАТИВНО-ПРАВОВА БАЗА ТА КЛАСИФІКАЦІЯ АС

| Документ | Опис |
|---|---|
| **НД ТЗІ 2.5-005-99** | Класифікація автоматизованих систем і стандартні функціональні профілі захищеності |
| **НД ТЗІ 2.5-004-99** | Критерії оцінки захищеності інформації в комп'ютерних системах від НСД |
| **НД ТЗІ 1.1-002-99** | Загальні положення щодо захисту інформації в комп'ютерних системах від НСД |
| **Закон України № 80/94-ВР** | Про захист інформації в інформаційно-комунікаційних системах |

Ключовою особливістю АС К1 з точки зору захисту є вимога обов'язкової ідентифікації та аутентифікації кожного суб'єкта доступу. Автентифікація в АС К1 повинна здійснюватись за допомогою засобів, що забезпечують надійність, яку не може забезпечити проста парольна схема.

| Клас АС | Назва | Характеристика | Приклади |
|---|---|---|---|
| **Клас 3** | Однокористувацькі однорівневі системи | Один користувач, один рівень конфіденційності оброблюваної інформації, фізичний захист всього АС | Персональні комп'ютери з конфіденційною інформацією |
| **Клас 2** | Багатокористувацькі системи з рівноцінним доступом | Усі користувачі мають однаковий рівень допуску, але різні повноваження | Корпоративні інформаційні системи, мережі підприємств |
| **Клас 1** | Багатокористувацькі системи з різними рівнями доступу | Різні рівні конфіденційності, обов'язкове розмежування доступу, обробка державної таємниці | Системи обробки державної таємниці, АС органів держвлади |

| Функція захисту | Вимога для АС К1 | Нормативне підґрунтя |
|---|---|---|
| **Ідентифікація та аутентифікація** | Обов'язкова ідентифікація кожного суб'єкта, надійна аутентифікація, ведення списку ідентифікаторів | НД ТЗІ 2.5-005-99, НД ТЗІ 2.5-004-99 |
| **Розмежування доступу** | Мандатне розмежування доступу, ізоляція модулів, захист ресурсів користувача | НД ТЗІ 2.5-005-99, НД ТЗІ 2.5-004-99 |
| **Аудит** | Реєстрація всіх подій НСД, захист журналів аудиту, управління журналами | НД ТЗІ 2.5-005-99 |
| **Криптографічний захист** | Обов'язкове застосування засобів КЗІ для захисту інформації що передається та зберігається | Закон України «Про захист інформації» [1], НД ТЗІ 1.1-003-99 |

# ОГЛЯД МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

| Метод | FAR, % | FRR, % | Пасивність | Реальний час | Вартість обладнання |
|---|---|---|---|---|---|
| **Обличчя (Deep Learning)** | < 0,1 | 0,1–0,5 | Так | Так | Низька (звичайна камера) |
| **Відбиток пальця** | 0,001 | 0,1 | Ні | Так | Помірна (спец. сенсор) |
| **Сітківка ока** | < 0,0001 | 0,05 | Частково | Так | Висока (ІЧ-обладнання) |
| **Голос** | 1–10 | 1–5 | Ні | Так | Низька (мікрофон) |
| **Підпис** | 0,5–3 | 1–5 | Ні | Ні | Помірна (графічний планшет) |
| **Райдужна оболонка** | < 0,001 | 0,1 | Частково | Так | Висока (спец. камера) |

## Метод FaceNet

| Параметр | Значення |
|---|---|
| Точність на LFW | 99,63% |
| Вимірність вектора ознак | 128 |
| Час обробки одного кадру | < 50 мс |
| Базова бібліотека | dlib / face_recognition |

# АРХІТЕКТУРА СИСТЕМИ ТА ВИБІР СТЕКУ ТЕХНОЛОГІЙ

Порівняння мов програмування

| Критерій | Python 3.x | Java | C++ | C# |
|---|---|---|---|---|
| **Екосистема CV/ML** | Відмінна (OpenCV, face_recognition, dlib) | Хороша (JavaCV) | Хороша (OpenCV native) | Хороша (Emgu CV) |
| **Крос-платформеність** | Так (без змін коду) | Так (JVM) | Потребує компіляції | Обмежено (Windows) |
| **Швидкість розробки** | Висока | Середня | Низька | Середня |
| **Продуктивність** | Середня (нативний C для CV) | Висока | Максимальна | Висока |
| **Спільнота та документація** | Найбільша для CV/ML | Велика | Велика | Велика |
| **Підсумок** | Рекомендовано | Альтернатива | Для продуктивних задач | Для Windows-only |

Обґрунтування вибору бібліотек

| Бібліотека | Призначення | Обґрунтування |
|---|---|---|
| **OpenCV 4.x** | Захоплення відеопотоку, обробка зображень | Де-факто стандарт, висока продуктивність (C++ ядро), ліцензія Apache 2.0 |
| **face_recognition** | Детекція облич, обчислення 128-вимірних векторів | Обгортка над dlib, реалізує FaceNet, точність 99,38% на LFW |
| **NumPy** | Ефективні операції з масивами | Векторизовані обчислення евклідових відстаней |
| **Tkinter** | Графічний інтерфейс | Стандартна бібліотека Python, без додаткових залежностей |

# ПРОЄКТУВАННЯ БАЗИ ДАНИХ ПЕРСОНАЛУ ТА БІОМЕТРИЧНИХ ШАБЛОНІВ

Сутність Employee

| Поле | Тип даних | Обов'язкове | Опис |
|---|---|---|---|
| **Id** | String (8 hex) | Так | Унікальний ідентифікатор, MD5-хеш від full_name + timestamp |
| **full_name** | String | Так | Повне ім'я (прізвище, ім'я, по батькові) |
| **position** | String (enum) | Так | Посада зі списку допустимих значень (6 варіантів) |
| **department** | String (enum) | Так | Відділ зі списку допустимих значень (5 варіантів) |
| **access_level** | Integer (1–3) | Так | Рівень доступу: 1 - читання, 2 - запис/читання, 3 - повний |
| **allowed_operations** | Array[String] | Ні | Список дозволених операцій (read_data, write_data, delete_data, тощо) |
| **photo_path** | String (path) | Ні | Абсолютний шлях до фотографії, використовується для формування face encoding |
| **created_at** | String (ISO 8601) | Так (авто) | Дата та час реєстрації у форматі ISO 8601 |
| **active** | Boolean | Так (авто) | Ознака активності: true - активний, false - деактивований (м'яке видалення) |

Структура зберігання біометричних шаблонів

| Характеристика | Значення |
|---|---|
| **Тип шаблону** | 128-вимірний вектор числових значень (face encoding) |
| **Метод обчислення** | face_recognition.face_encodings( ) на основі FaceNet |
| **Зберігання** | Не зберігається у JSON, обчислюється динамічно з фотографій |
| **Формат фото** | JPEG або PNG |
| **Іменування фото** | {employee_id}.jpg |

Формула порівняння векторів

$$d(f_1, f_2) = \sqrt{(\Sigma_i (f_{1i} - f_{2i})^2)}, \qquad i = 1..128$$

# АЛГОРИТМ РЕЄСТРАЦІЇ ТА МАТРИЦЯ ДОСТУПУ

Алгоритм реєстрації нового співробітника:

- Введення персональних даних (ПІБ, посада, відділ, рівень доступу)
- Завантаження фотографії (JPEG, PNG)
- Валідація фотографії (виявлення обличчя)
- Генерація ідентифікатора (MD5, 8 символів hex)
- Збереження фотографії у photos/{employee_id}.ext
- Збереження запису у data/personnel.json
- Реєстрація події у журналі аудиту

Матриця прав доступу

| Операція | Рівень 1 | Рівень 2 | Рівень 3 | Опис |
|---|---|---|---|---|
| **read_data (Читання даних)** | ✓ (за дозволом) | ✓ | ✓ | Читання файлів та баз даних АС |
| **write_data (Запис даних)** | ✗ | ✓ (за дозволом) | ✓ | Запис та модифікація інформаційних ресурсів |
| **delete_data (Видалення даних)** | ✗ | ✗ | ✓ | Видалення записів із підтвердженням операції |
| **view_logs (Журнал аудиту)** | ✗ | ✓ (за дозволом) | ✓ | Перегляд журналу подій безпеки |
| **export_data (Експорт)** | ✗ | ✓ (за дозволом) | ✓ | Вивантаження даних у зовнішні формати |
| **system_config (Конфігурація)** | ✗ | ✗ | ✓ | Зміна параметрів системи (вимагає верифікації) |
| **manage_users (Персонал)** | ✗ | ✗ | ✓ | Реєстрація, редагування, деактивація співробітників |
| **classify_system (Класифікація АС)** | ✗ | ✗ | ✓ | Визначення класу захисту АС (лише для адміністраторів) |

# НЕПЕРЕРВНА ВЕРИФІКАЦІЯ ТА КРИПТОЗАХИСТ

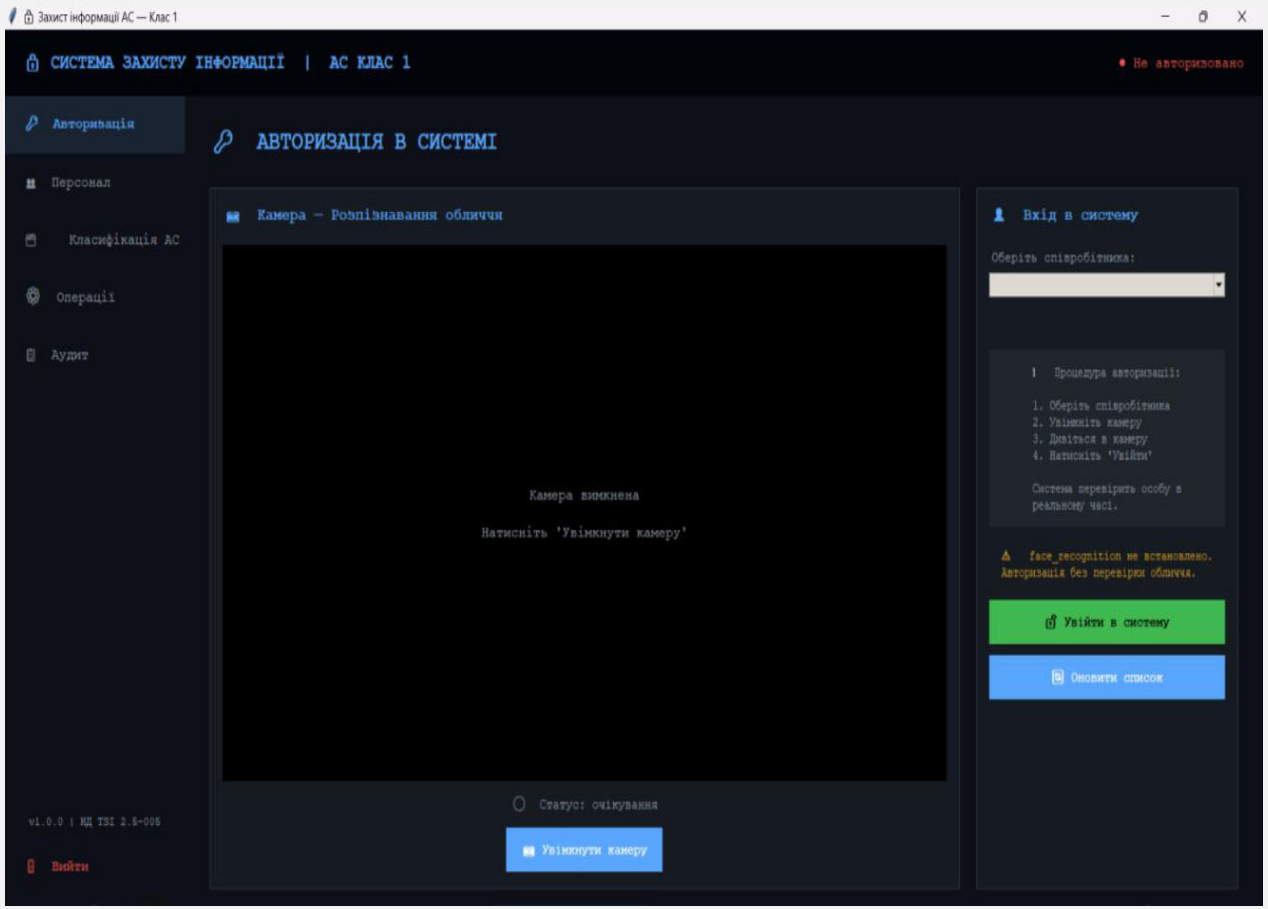
## Режими роботи

| Режим | Опис | Дія при невідповідності |
|---|---|---|
| **Авторизація** | Вхід у систему (вибір ID + розпізнавання обличчя) | Відмова у доступі |
| **Неперервна** | Перевірка перед кожною операцією | Блокування операції + запис CRITICAL |

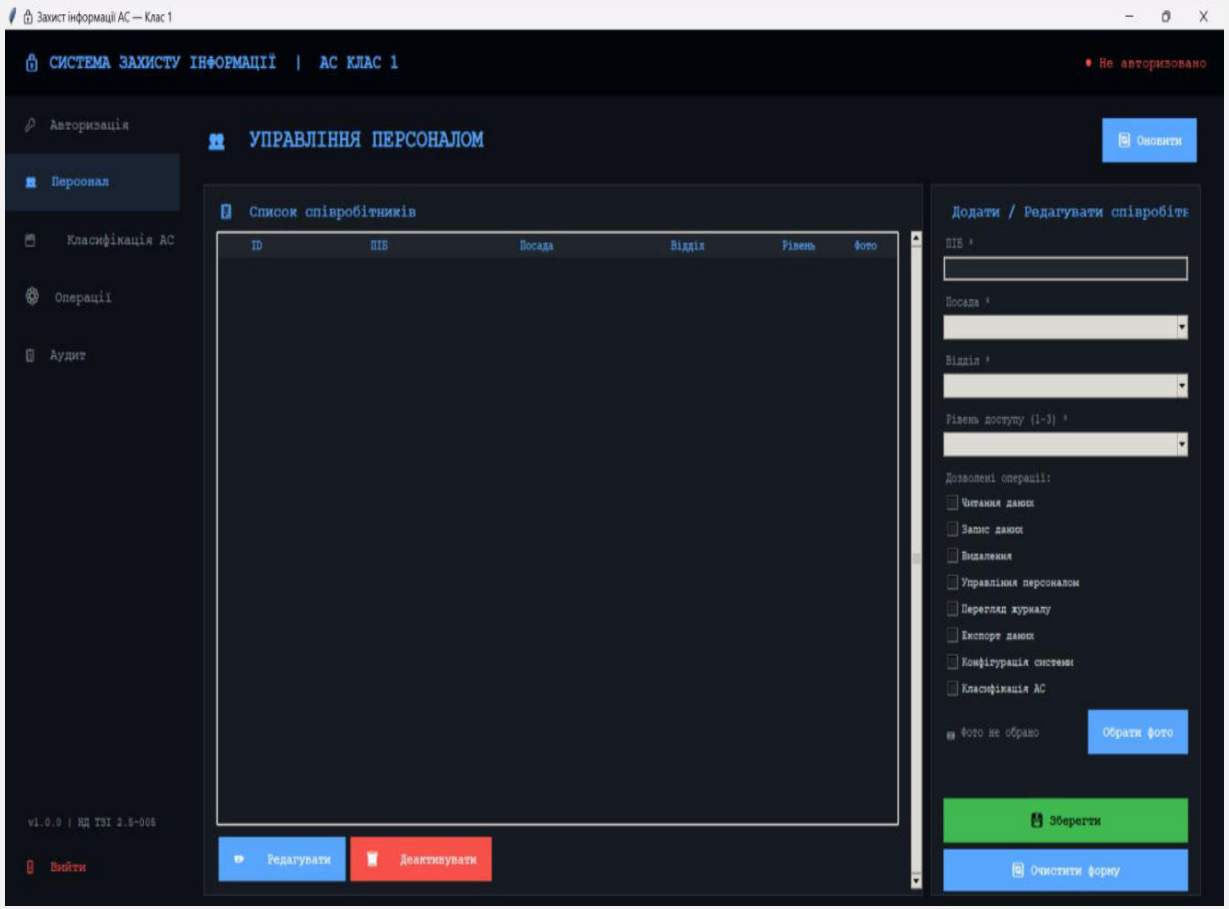
## Криптографічний захист

| Категорія даних | Алгоритм шифрування | Алгоритм цілісності | Обґрунтування |
|---|---|---|---|
| **Фотографії персоналу** | AES-256-GCM | GMAC (вбудований) | GCM забезпечує автентифіковане шифрування (AEAD), стійкість до tamper attacks |
| **Файл personnel.json** | AES-256-CBC | HMAC-SHA256 | Стандарт для шифрування файлів конфігурації, підтримується бібліотекою cryptography |
| **Журнал аудиту (audit.json)** | Без шифрування (відкритий) | SHA-256 chaining | Відкритість журналу для перегляду адміністратором, цілісність забезпечується хешуванням |
| **Ключ шифрування** | HSM / OS Keyring | - | Апаратне або системне захищене сховище, ключ ніколи не зберігається поряд із даними |
| **Передача даних (майбутнє)** | TLS 1.3 | HMAC-SHA384 | При реалізації мережевого режиму для централізованого управління або SIEM-інтеграції |

# ІНТЕРФЕЙС ПРОГРАМИ (МОДУЛЬ АДМІНІСТРАТОРА)

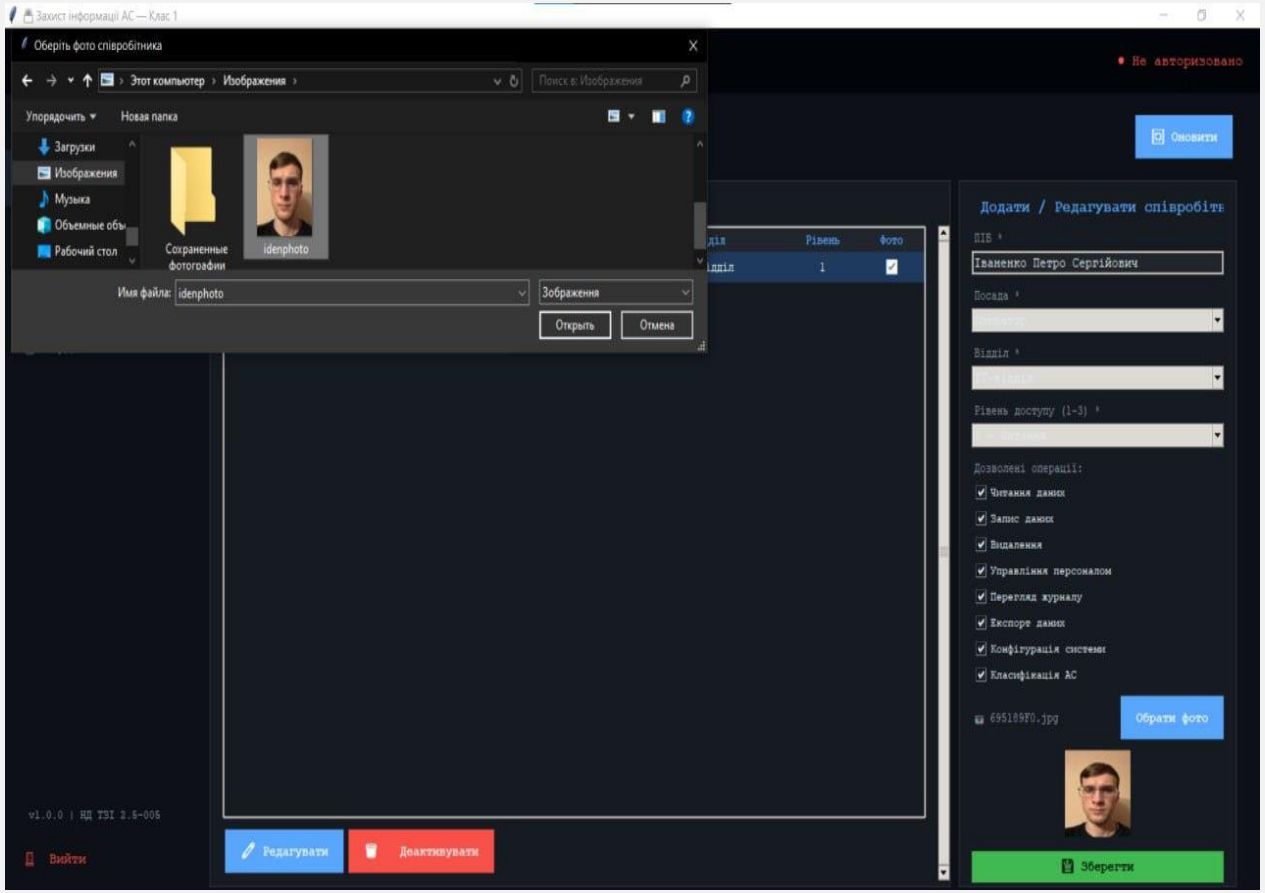



Загальний вигляд інтерфейсу модуля адміністратора

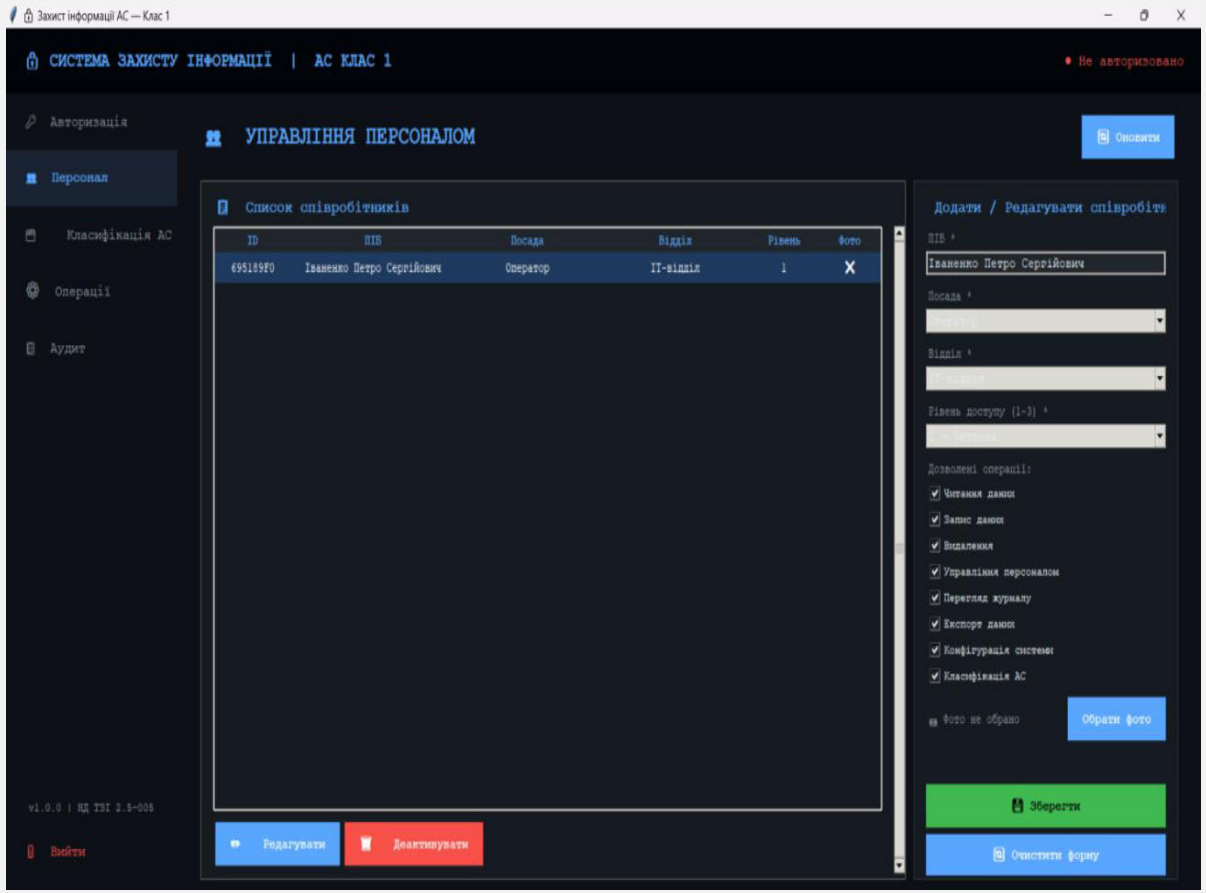



Форма додавання нового співробітника

# ІНТЕРФЕЙС ПРОГРАМИ

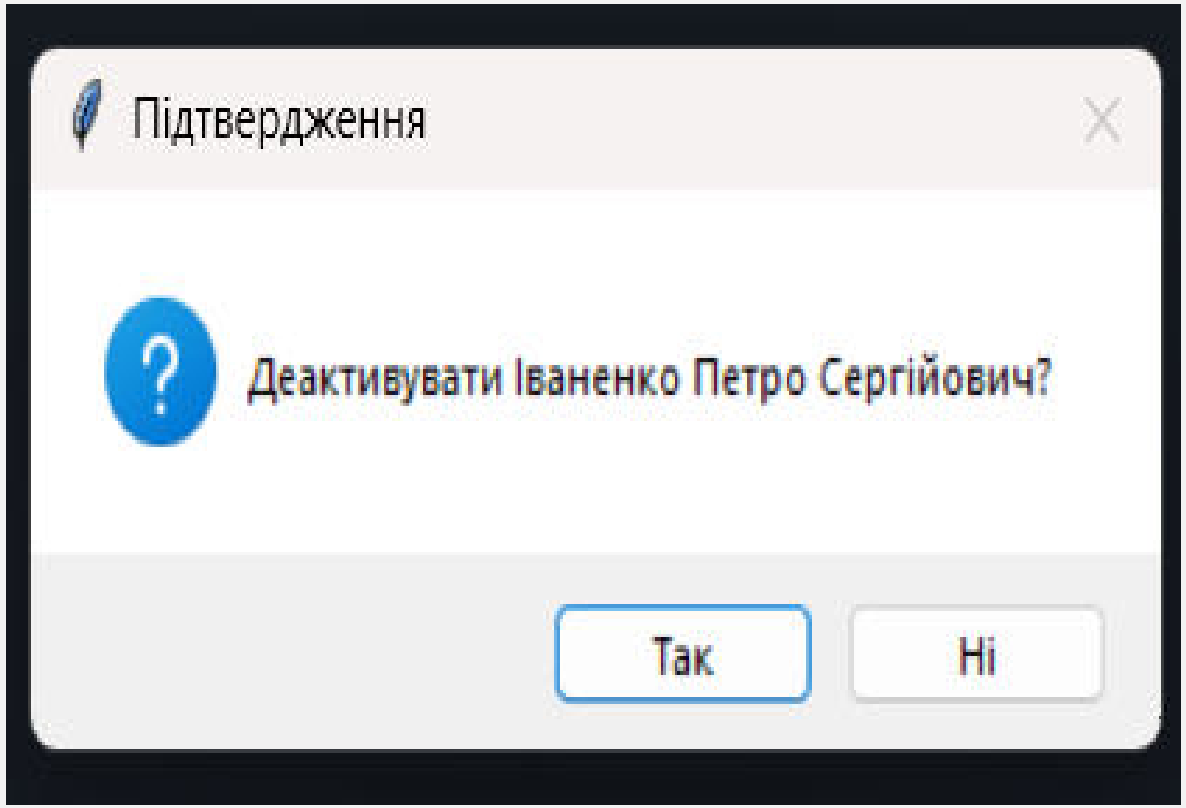



Завантаження фотографії

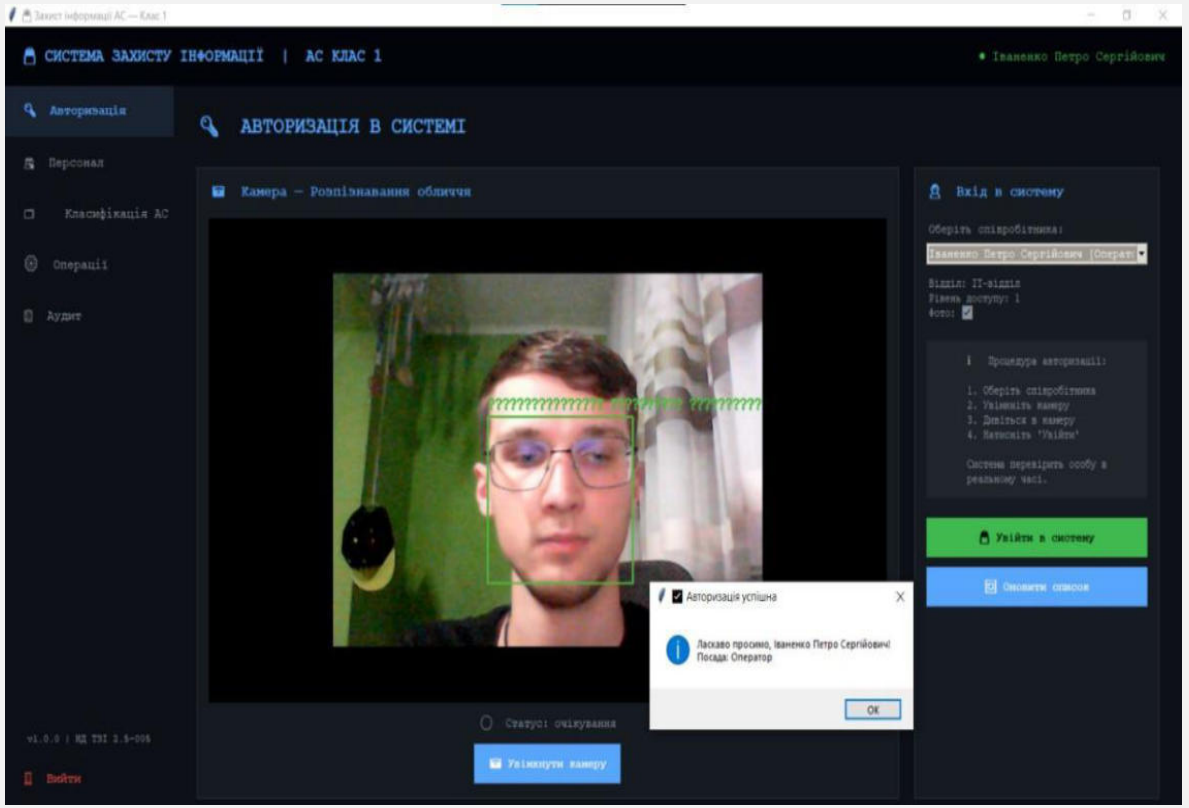



Редагування існуючого співробітника

# ІНТЕРФЕЙС ПРОГРАМИ

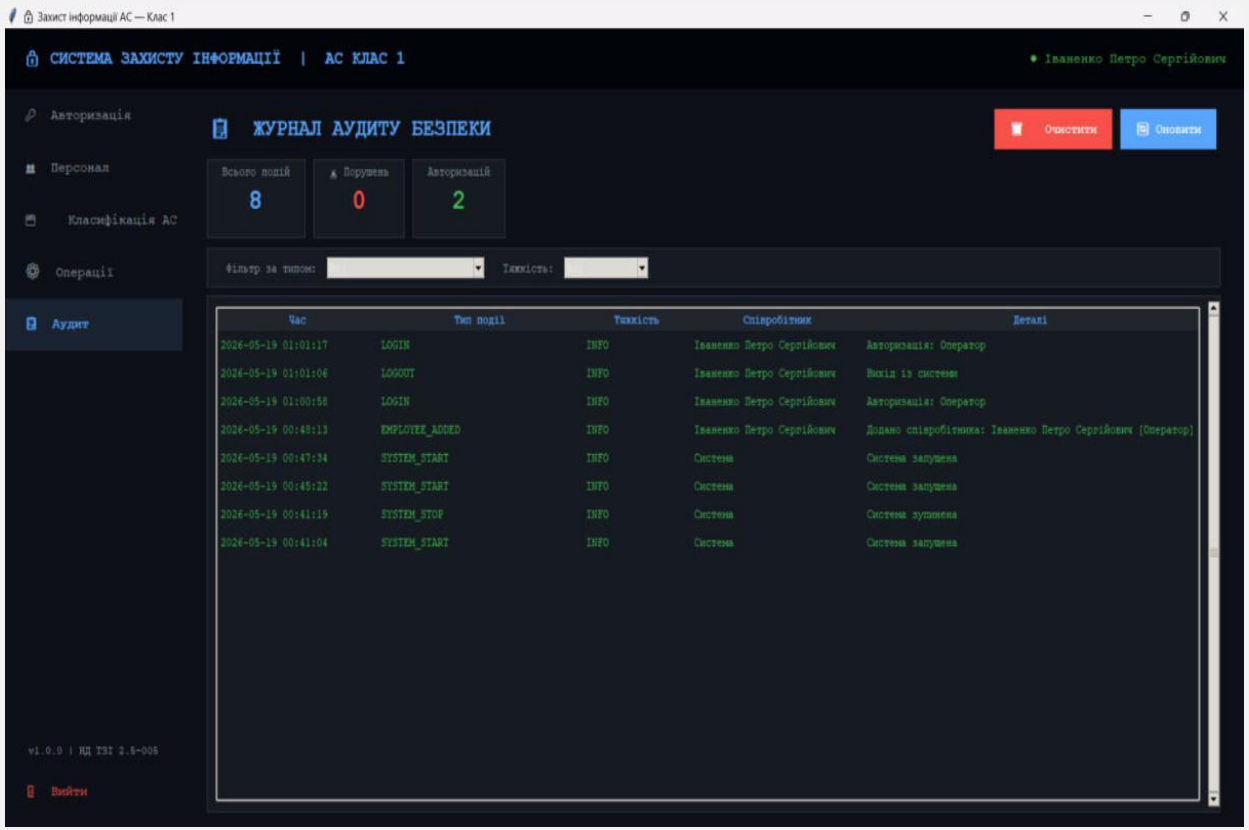



Деактивація співробітника

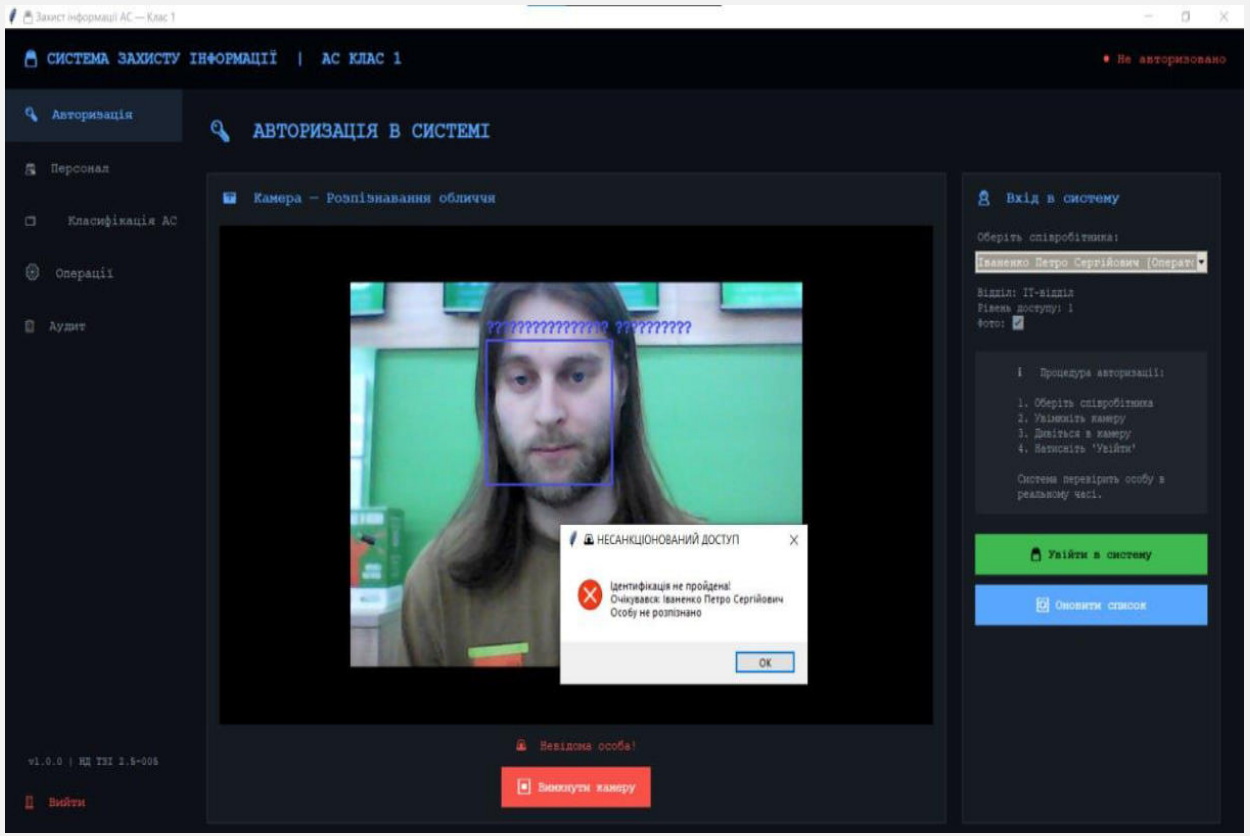



Розпізнавання та авторизація

# ІНТЕРФЕЙС ПРОГРАМИ




Запис у журнал аудиту




Хибна ідентифікація (НСД)

# РЕЗУЛЬТАТИ ТЕСТУВАННЯ ТА МЕТРИКИ ЕФЕКТИВНОСТІ

Показники швидкодії

| Показник | Значення | Цільове значення |
|---|---|---|
| **Час холодного старту** | 4.2 с | ≤ 5 с |
| **Час обробки одного кадру** | 92 мс | ≤ 150 мс |
| **Кадрів за секунду (FPS)** | 10.8 | ≥ 8 |
| **Час відгуку на операцію** | 180 мс | ≤ 300 мс |
| **Споживання RAM (пік)** | 385 МБ | ≤ 512 МБ |
| **Завантаження CPU (середнє)** | 22% | ≤ 30% |
| **Розмір на диску** | 118 МБ | - |
| **Об'єм одного запису у журналі** | ≈ 320 байт | - |

Основні метрики точності

| Метрика | Значення | Норма для класу 1 | Висновок |
|---|---|---|---|
| **FAR (False Acceptance Rate)** | 0.69% | ≤ 1% | Відповідає |
| **FRR (False Rejection Rate)** | 2.40% | ≤ 5% | Відповідає |
| **APCER (атаки фото на папері)** | 0.00% | ≤ 5% | Відповідає |
| **APCER (атаки фото на екрані)** | 1.33% | ≤ 5% | Відповідає |
| **APCER (атаки відео)** | 2.00% | ≤ 10% | Відповідає |
| **APCER (маска)** | 0.00% | ≤ 10% | Відповідає |
| **BPCER** | 2.40% | ≤ 5% | Відповідає |
| **EER (точка перетину)** | ≈ 1.5% | - | Високий рівень |
| **Доступність системи** | 99.6% | ≥ 99% | Відповідає |

# ВИСНОВКИ

У дипломній роботі виконано аналіз нормативно-правової бази, сучасних загроз та методів біометричної ідентифікації, на основі чого розроблено програмний засіб захисту автоматизованих систем класу 1 з використанням безперервного розпізнавання обличчя в реальному часі.

- Система повністю відповідає вимогам НД ТЗІ 2.5-005-99
- FAR = 0,69%, FRR = 2,40%, стійкість до фотоатак – 98,7-100%
- Час обробки кадру – 92 мс, частота – ≈10,8 FPS
- Реалізовано повнофункціональний журнал аудиту

Розроблений програмний засіб є сучасним, ефективним рішенням, що суттєво підвищує рівень захисту інформації в АС класу 1 та рекомендується до впровадження на об'єктах критичної інфраструктури.

# ДЯКУЮ ЗА УВАГУ!