МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Інститут (факультет) Автоматизації і комп'ютерних систем
Кафедра Інформаційних технологій, штучного інтелекту і кібербезпеки

«До захисту в ЕК»	**«До захисту допущено»**
Директор інституту(декан факультету)	Завідувач кафедри
_____ Андрій ФОРСЮК	_____ Сергій ГРИБКОВ
(підпис) (ім'я та прізвище)	(підпис) (ім'я та прізвище)
«10» червня 2024р.	«10» червня 2024р.

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

зі спеціальності 122 «Комп'ютерні науки»
(код та назва спеціальності)

освітньо-професійної програми Інформаційні системи та штучний інтелект

на тему: «Розроблення програмного модуля для аналізу автентичності фото файлів»

Виконав: здобувач 4 курсу, групи КН-4-4

Франц Святослав Валерійович _____
(прізвище, ім'я, по батькові повністю) (підпис)

Керівник Грама Михайло Петрович _____
(прізвище , ім'я та по батькові повністю) (підпис)

Консультанти _____ _____
(ім'я та прізвище) (підпис)

_____ _____
(ім'я та прізвище) (підпис)

_____ _____
(ім'я та прізвище) (підпис)

Рецензент _____ _____
(ім'я та прізвище) (підпис)

Я як здобувач(ка) Національного університету харчових технологій розумію і підтримую політику університету з академічної доброчесності. Я не надавав(-ла) і не одержував(-ла) недозволеної допомоги під час підготовки цієї роботи. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Здобувач _____
(підпис)

Київ - 2024р.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ХАРЧОВИХ ТЕХНОЛОГІЙ

Інститут (факультет) Автоматизації і комп'ютерних систем
Кафедра Інформаційних технологій, штучного інтелекту і кібербезпеки
Освітній ступінь бакалавр
Спеціальність 122 «Комп'ютерні науки»
Освітньо-професійна програма Інформаційні системи та штучний інтелект

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інформаційних технологій, штучного інтелекту і кібербезпеки
Сергій ГРИБКОВ

" 15 " квітня 2024 року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА

Франц Святослав Валерійович
(прізвище, ім'я, по батькові)

1. Тема роботи «Розроблення програмного модуля для аналізу автентичності фото файлів»

керівник роботи Грама Михайло Петрович, PhD
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від 15 квітня 2024 року № 279-кс
2. Строк подання здобувачем роботи 03.06.2024 р.
3. Вихідні дані до роботи
1) Фото файл

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
1) Системний аналіз об'єкту дослідження та виявлення задач інформатизації
2) Проектування бази даних
3) Проектування програмного модулю
4) Охорона праці та техніка безпеки
5. Перелік графічного матеріалу
1) Фізична модель бази даних
2) Інтерфейс інформаційної системи

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1.	Грама М.П., PhD	15.04.2024	15.04.2024
2.	Грама М.П., PhD	15.04.2024	19.04.2024
3.	Грама М.П., PhD	15.04.2024	20.04.2024

7. Дата видачі завдання 15 квітня 2023 року

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів виконання кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
	Дослідження предметної області та постановка завдання на проектування	05.04.2024 –15.04.2024	Виконано
	Проектування бази даних	15.04.2024 –20.04.2024	Виконано
	Створення програмного модулю	20.04.2024 –15.05.2024	Виконано
	Оформлення пояснювальної записки	15.05.2024 –26.05.2024	Виконано
	Оформлення презентації	26.04.2024 –28.05.2024	Виконано

Здобувач _____ Франц С. В.

(підпис) (прізвище та ініціали)

Керівник роботи _____ Грам М. П.

(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дипломна робота присвячена розробці програмного модулю для аналізу автентичності фото файлів. Метою роботи є полегшення процесу аналізу автентичності фото файлів.

У роботі було проведено аналіз вимог до програмного модулю для аналізу автентичності фото файлів. Було розроблено логічну та фізичну моделі бази даних, інтерфейс користувача та функціональні можливості системи.

Результатом дипломної роботи було функціональний та надійний програмній модуль для аналізу автентичності фото файлів, що сприятиме підвищенню продуктивності та організації роботи. Розроблена система дозволить здійснювати ефективний аналіз зображення та генерувати звіти на основі зроблених висновків.

Дипломна робота складається із 78 сторінок, 8 таблиць, 32 рисунків, 3 додатки та 23 літературних джерел.

Ключові слова: ПРОГРАМНИЙ МОДУЛЬ, АНАЛІЗ ФОТО ФАЙЛІВ, БАЗА ДАНИХ, PYTHON, ІНТРЕФЕЙС КОРИСТУВАЧА, АНАЛІЗ РІВНЯ ПОМИЛОК, МЕТАДАНІ.

SUMMARY

The thesis is devoted to the development of a software module for analysing the authenticity of photo files. The aim of the work is to facilitate the process of analysing the authenticity of photo files.

In the work, the requirements for a software module for analysing the authenticity of photo files were analysed. The logical and physical models of the database, the user interface, and the system's functionality were developed.

The result of the thesis is a functional and reliable software module for analysing the authenticity of photo files, which will help to increase productivity and organise work. The developed system will allow for efficient image analysis and generate reports based on the findings.

The thesis consists of 78 pages, 8 tables, 32 figures, 3 appendices and 23 references.

Keywords: SOFTWARE MODULE, PHOTO FILE ANALYSIS, DATABASE, PYTHON, USER INTERFACE, ERROR RATE ANALYSIS, METADATA.

ЗМІСТ

ВСТУП

У сучасному світі, де проблема кіберзлочинності стає все більш актуальною, аналіз автентичності фото файлів відіграє важливу роль у забезпеченні безпеки та достовірності інформації. Для кіберполіції, яка займається розслідуванням різноманітних кіберзлочинів, наявність ефективного інструменту для виявлення підробок та фальсифікацій є критично важливою.

Ця дипломна робота присвячена розробці програмного модуля для аналізу автентичності фото файлів, який має на меті полегшити процес розслідування кіберзлочинів, спростити аналіз наданих доказів та забезпечити ефективний обмін даними між відповідальними особами. Програмний модуль надає зручні інструменти для аналізу зображень та формування звітів про результати аналізу. В процесі розробки модуля були враховані потреби та вимоги кіберполіції, а також були застосовані сучасні технології та методи, що дозволило створити функціональний та надійний інструмент. Результати дослідження та розробки даного модуля можуть бути використані для покращення організації роботи кіберполіції та підвищення ефективності виявлення кіберзлочинів.

У цій дипломній роботі будуть описані кроки розробки програмного модуля, включаючи аналіз вимог, проектування бази даних, розробку інтерфейсу користувача. Також будуть розглянуті аспекти охорони праці та безпеки, пов'язані з використанням модуля, а також вимоги до інфраструктури та технічного забезпечення.

В результаті успішної реалізації даного програмного модуля, кіберполіція матиме потужний інструмент для аналізу автентичності фото файлів, що сприятиме підвищенню продуктивності та організації роботи, а також забезпечить більш точний аналіз та відстеження кіберзлочинів.

РОЗДІЛ 1. СИСТЕМНИЙ АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Загальна характеристика департаменту кіберполіції національної поліції України

Кіберполіція України була заснована 27 липня 2009 року як відділ боротьби з кіберзлочинністю у складі Департаменту з протидії торгівлі людьми Міністерства внутрішніх справ України [1]. Після цього, у кінці 2012 року, у рамках кримінальної міліції Міністерства був утворений незалежний структурний підрозділ для боротьби з кіберзлочинністю .

13 жовтня 2015 року у структурі Національної поліції України була створена нова Кіберполіція з метою реформування та вдосконалення підрозділів міністерства, а також для підготовки кваліфікованих спеціалістів, здатних використовувати передові технології у боротьбі з кіберзлочинністю[2]. 10 лютого 2016 року міністр Арсен Аваков зазначив, що реформа кіберполіції перебуває в стадії завершення, незважаючи на труднощі.

З вересня 2016 року співробітники кіберполіції проходили курси підвищення кваліфікації в Харківському національному університеті внутрішніх справ, включаючи 760-годинну програму та чотиримісячний курс. Тренінги в Києві за участю експертів з Великобританії також допомогли у підготовці фахівців.

19 липня 2017 року в межах проєкту розбудови потенціалу кіберполіції представники ОБСЄ в Україні передали кіберполіції 194 одиниці спеціалізованого обладнання[3]. У 2023 році кіберполіція супроводжувала понад 6,4 тисяч кримінальних правопорушень, виявила 3,6 тисяч кіберзлочинів та повідомила про підозру 1,7 тисячам осіб.

Основні завдання кіберполіції України включають реалізацію державної політики у сфері протидії кіберзлочинності, а також завчасне інформування населення про новітні кіберзлочини та загрози [1]. Кіберполіція впроваджує програмні засоби для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини, що дозволяє швидше реагувати на такі інциденти. Також важливим завданням є реагування на запити закордонних партнерів, які

надходять через Національну цілодобову мережу контактних пунктів. Кіберполіція активно бере участь у підвищенні кваліфікації працівників поліції, зокрема щодо застосування комп'ютерних технологій у протидії злочинності. Важливою частиною діяльності є участь у міжнародних операціях та співпраця в режимі реального часу з правоохоронцями інших країн. Це забезпечує діяльність мережі контактних пунктів між 90 країнами світу. Кіберполіція також займається протидією кіберзлочинам у сфері використання платіжних систем, таких як скімінг (незаконне копіювання даних банківських карток), кеш-трапінг (викрадення готівки з банкоматів) та кардінг (незаконні фінансові операції з використанням платіжних карток або їх реквізитів).

Види кіберзлочинів, з якими бореться кіберполіція, охоплюють широкий спектр діяльності. Це, зокрема, порушення конфіденційності, цілісності та доступності комп'ютерних даних і систем, які є порушеннями, пов'язаними з комп'ютерами. До таких злочинів належать правопорушення, що стосуються змісту, як наприклад, незаконний доступ до інформації або її зміна. Інша категорія кіберзлочинів включає правопорушення, пов'язані з порушенням авторських та суміжних прав, як наприклад, піратство — незаконне розповсюдження інтелектуальної власності в Інтернеті, або кардшарінг — надання незаконного доступу до перегляду супутникового та кабельного телебачення. Злочини у сфері електронної комерції та господарської діяльності включають фішинг — виманювання у користувачів Інтернету їх логінів та паролів, а також онлайн-шахрайство — заволодіння коштами громадян через інтернет-аукціони, інтернет-магазини та сайти. У сфері використання платіжних систем кіберполіція протидіє таким злочинам, як скімінг, кеш-трапінг та кардінг. Злочини у сфері комп'ютерних технологій включають несанкціоноване втручання в роботу комп'ютерів, створення шкідливого програмного забезпечення, несанкціоноване збирання інформації з обмеженим доступом та порушення правил експлуатації комп'ютерів.

1.2 Організаційна структура департаменту кіберполіції національної поліції України

Управління в кіберполіції України здійснюється через взаємодію між начальником кіберполіції, його заступниками, керівниками відділів, оперативними співробітниками, аналітиками, технічним та адміністративним персоналом. Начальник кіберполіції має відповідальність за організацію роботи підрозділу, встановлення завдань і посадових доручень для співробітників. Кожен співробітник виконує свої відповідні обов'язки, які відповідають їхній спеціалізації.

Керівник департаменту кіберполіції є головою департаменту та відповідає за стратегічне планування та управління всіма аспектами діяльності кіберполіції. Він забезпечує координацію між різними відділами та взаємодію з іншими державними органами та міжнародними партнерами.

Задачі керівника департаменту кіберполіції:

- загальне керівництво та управління кіберполіцією;
- встановлення стратегічних напрямків та пріоритетів роботи;
- координація діяльності всіх підрозділів;
- забезпечення взаємодії з іншими державними органами та міжнародними партнерами;

Відділ оперативно-розшукової діяльності займається розслідуванням кіберзлочинів, збором та аналізом інформації про злочинну діяльність у кіберпросторі. Відділ також проводить оперативні заходи для затримання підозрюваних та вилучення доказів.

Задачі відділу оперативно-розшукової діяльності:

- проведення розслідувань кіберзлочинів;
- збір, аналіз та використання інформації для виявлення злочинної діяльності в кіберпросторі;
- проведення оперативних заходів, включаючи обшуки, вилучення доказів та арешти підозрюваних;
- співпраця з іншими правоохоронними органами для координації

розслідувань;

Відділ аналітики та кібербезпеки відповідає за моніторинг кіберзагроз, аналіз інцидентів та розробку заходів для запобігання кіберзлочинності. Вони також впроваджують програмні засоби для систематизації та аналізу даних про кіберінциденти.

Задачі відділу аналітики та кібербезпеки:

- моніторинг та аналіз кіберзагроз;
- розробка та впровадження заходів для запобігання кіберзлочинності;
- систематизація та аналіз даних про кіберінциденти;
- надання аналітичної підтримки оперативним підрозділам;

Відділ міжнародного співробітництва займається взаємодією з міжнародними правоохоронними органами та організаціями, участю у міжнародних операціях та обміном інформацією і досвідом з іноземними партнерами.

Задачі відділу міжнародного співробітництва:

- взаємодія з міжнародними правоохоронними органами та організаціями;
- обмін інформацією та досвідом з іноземними партнерами;
- координація спільних дій з міжнародними партнерами;

Відділ технічної підтримки забезпечує технічне обладнання та програмне забезпечення для всіх підрозділів кіберполіції. Вони займаються налаштуванням, обслуговуванням та оновленням техніки, а також розробкою нових технічних рішень для протидії кіберзлочинності.

Задачі відділу технічної підтримки:

- забезпечення технічного обладнання та програмного забезпечення для всіх підрозділів кіберполіції;
- налаштування, обслуговування та оновлення техніки;
- розробка нових технічних рішень для протидії кіберзлочинності;
- забезпечення безпеки інформаційних систем кіберполіції;

Адміністративний відділ забезпечує фінансову та кадрову підтримку для роботи підрозділу, веде документацію та організовує роботу офісу.

Задачі адміністративного відділу:

- управління фінансовими та кадровими питаннями;
- ведення документації та забезпечення діловодства;
- організація роботи офісу та підтримка адміністративних процесів;
- координація діяльності з іншими підрозділами Національної поліції України;

Загальну організаційну структуру департаменту кіберполіції національної поліції України зображено на рис.1.1.

Рисунок 1.1- Організаційна структура департаменту кіберполіції національної поліції України

Взаємодія між різними підрозділами та співробітниками кіберполіції України здійснюється через регулярні зустрічі, наради та консультації. Такі зустрічі допомагають вирішувати різні організаційні питання, сприяють координації дій та підвищенню ефективності роботи підрозділу в цілому.

Завдяки таким заходам, кожен підрозділ та співробітник має змогу ефективно виконувати свої обов’язки, співпрацюючи з іншими для досягнення загальних цілей. Взаємодія всіх співробітників кіберполіції забезпечує збалансовану роботу підрозділу та повністю охоплює всі аспекти діяльності,

включаючи оперативно-розшукову, аналітичну, технічну підтримку та міжнародну співпрацю.

Ця координація дозволяє оперативно реагувати на кіберзагрози, проводити ефективні розслідування та підтримувати високий рівень кібербезпеки, забезпечуючи захист національних інтересів України в кіберпросторі.

Основні функції, що виконує департаменту кіберполіції наведені в таблиці 1.1.

Таблиця 1.1. Функції та задачі департаменту кіберполіції

№	**Задачі**	**Функції**
1	Оперативно-розшукова діяльність	- Проведення розслідувань кіберзлочинів; - Збір та аналіз інформації для виявлення злочинної діяльності в кіберпросторі; - Оперативні заходи, включаючи обшуки, вилучення доказів та арешти підозрюваних.
2	Аналітика та кібербезпека	- Моніторинг та аналіз кіберзагроз; - Розробка та впровадження заходів для запобігання кіберзлочинності; - Систематизація та аналіз даних про кіберінциденти; - Надання аналітичної підтримки оперативним підрозділам.
3	Міжнародне співробітництво	- Взаємодія з міжнародними правоохоронними органами та організаціями; - Участь у міжнародних операціях з протидії кіберзлочинності; - Обмін інформацією та досвідом з іноземними партнерами; - Координація спільних дій з міжнародними партнерами.

Продовження таблиці 1.1. Функції та задачі департаменту кіберполіції

4	Технічна підтримка	- Забезпечення технічного обладнання та програмного забезпечення для всіх підрозділів; - Налаштування, обслуговування та оновлення техніки; - Розробка нових технічних рішень для протидії кіберзлочинності; - Забезпечення безпеки інформаційних систем.
5	Адміністративна діяльність	- Управління фінансовими та кадровими питаннями; - Ведення документації та забезпечення діловодства; - Організація роботи офісу та підтримка адміністративних процесів; - Координація діяльності з іншими підрозділами Національної поліції України.

1.3. Аналіз нинішнього стану комп'ютеризації.

Аналізуючи нинішній стан інформатизації в Кіберполіції України, можна стверджувати, що існує певний рівень інформатизації, однак деякі процеси в підрозділі досі не інформатизовані або інформатизовані не повністю.

Зокрема, в Кіберполіції є певні спеціалізовані програмні засоби, які використовуються для виконання окремих завдань. Такими програмними засобами є:

- *система управління інцидентами SIEM* - використовується для моніторингу та аналізу кіберзагроз;
- *система зберігання та обробки даних MySQL* - використовується для зберігання даних, що використовуються в інформаційних системах

кіберполіції;

- *платформа для аналізу великих даних Hadoop* - використовується для аналізу даних, обробки статистики та моделювання;
- *система контролю версій Git* - використовується для зберігання та контролю версій програмного коду;
- *офісні пакети LibreOffice та Microsoft Office* - використовуються для роботи з документами, електронними таблицями та презентаціями;

Ці системи та засоби дозволяють виконувати різні функції та задачі, пов'язані з моніторингом кіберзагроз, зберіганням та обробкою даних, аналізом даних та статистики, розробкою програмного забезпечення та роботою з документами.

Однак, виявлено деякі недоліки та незадовільність наявних інформаційних систем, які потребують вдосконалення та розробки нових систем для забезпечення ефективної роботи кіберполіції. Однією з проблем є відсутність спеціалізованого програмного модуля для аналізу автентичності фото файлів. Без такого модуля керівництво підрозділу не може ефективно перевіряти автентичність наданих фото матеріалів, що може впливати на якість розслідувань та аналітичних робіт.

На основі проведеного аналізу можна зробити висновок, що стан комп'ютеризації в кіберполіції не в повній мірі відповідає сучасному стану інформатизації робіт, оскільки існують деякі проблеми, які потребують вирішення. Тому розробка та впровадження спеціалізованого програмного модуля для аналізу автентичності фото файлів є необхідним кроком у поліпшенні стану комп'ютеризації в підрозділі. Така система дозволить забезпечити ефективний контроль автентичності фото матеріалів та покращити якість роботи всіх працівників кіберполіції, сприяючи підвищенню рівня кібербезпеки в Україні.

1.4 Розроблення функціональної моделі та аналіз існуючих бізнес процесів

Розробка функціональної моделі разом з аналізом існуючих процесів є важливою складовою впровадження ефективних програмних рішень в організації. Цей процес включає визначення функцій, які повинні виконуватися, встановлення послідовності дій та виявлення можливих проблем і недоліків існуючих процесів.

Для розробки функціональної моделі та аналізу існуючих процесів аналізу автентичності фото файлів необхідно провести детальний огляд поточних процесів.

Огляд поточних процесів:

1. прийом фото для аналізу;
2. аналіз метаданих (декомпозиція процесу наведена в додатку Б.1);
3. аналіз рівня помилок (ELA) (декомпозиція процесу наведена в додатку Б.2);
4. візуальний аналіз (декомпозиція процесу наведена в додатку Б.3);
5. формування звіту;

Після огляду поточних процесів розроблено функціональну модель (рис.1.2) процесу контролю виконання посадових доручень на кафедрі.

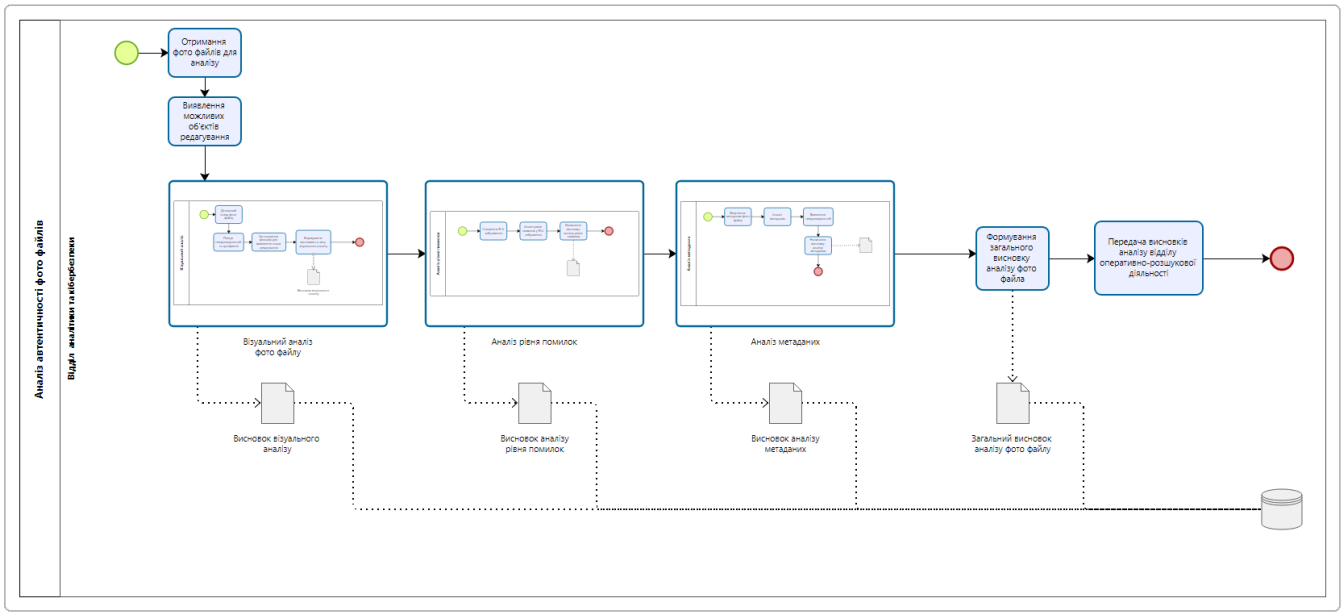


Рисунок 1.2 - Функціональна модель аналізу фото файла

Функціональна модель процесу аналізу автентичності фото файлів містить наступні елементи:

- вхідні дані: фото для аналізу;
- обробка даних: аналіз метаданих, виконання аналізу рівня помилок, візуальний аналіз;
- вихідні дані: звіти про результати аналізу;

Спочатку фото завантажується для аналізу через інтерфейс програмного модуля. Після цього виконується детальний аналіз метаданих, аналіз рівня помилок (ELA), застосування методів візуального аналізу для виявлення можливих підробок. Нарешті, генерується детальний звіт з результатами всіх етапів аналізу, який зберігається в базі даних та може бути експортований для подальшого використання.

Основними функціями, які можна інформатизувати, є процес аналізу метаданих, аналізу рівня помилок, візуальний аналіз, та формування звітів. Інформатизація цих процесів дозволить підвищити точність і швидкість аналізу, зменшити кількість помилок та покращити ефективність роботи кіберполіції.

Виявлені проблеми:

- відсутність єдиної системи для централізованого зберігання та аналізу фото файлів, що призводить до плутанини та втрати даних;
- недостатнє використання сучасних технологій для інформатизації процесів аналізу, що збільшує час та ресурси, необхідні для перевірки автентичності фото;
- відсутність ефективної системи для контролю за процесом аналізу, що ускладнює відстеження виконання завдань і призводить до помилок;

На основі виявлених проблем можна сформулювати наступні задачі інформатизації процесу аналізу автентичності фото файлів:

- розробити та впровадити програмний модуль для централізованого зберігання та аналізу фото файлів, доступний для всіх

відповідальних працівників Кіберполіції;

- забезпечити можливість автоматичного завантаження та обробки фото файлів з різних джерел;
- забезпечити можливість автоматизованого аналізу метаданих, ELA, застосування методів візуального аналізу для виявлення підробок;
- забезпечити інтеграцію з базами даних відомих фейкових зображень для автоматичного виявлення маніпуляцій;
- забезпечити автоматичну генерацію детальних звітів про результати аналізу з можливістю експорту у форматі Word або PDF;
- забезпечити можливість доступу до системи з будь-якого пристрою з доступом до інтернету для ефективного контролю за процесом аналізу;

Загалом, інформатизація процесу аналізу автентичності фото файлів дозволить покращити ефективність виконання завдань, забезпечити точний та швидкий аналіз зображень, підвищити рівень кібербезпеки та сприяти успішному розслідуванню кіберзлочинів.

1.5 Огляд існуючих рішень для розв'язання виявлених проблем

Огляд існуючих рішень для виявлення редагованих фото є важливим етапом у процесі розробки нової системи. Цей етап дозволяє дослідити різноманітні варіанти рішень, а також визначити їхні переваги та недоліки. Огляд існуючих рішень дозволить визначити найбільш оптимальний та ефективний варіант для вирішення проблеми виявлення редагованих фото у кіберполіції.

До аналогів розроблюваної системи входять такі існуючі рішення:

- Amped Authenticate;
- Cognitech FiA 64;
- Forensically Image Verification Tool;
- Photocert;

Amped Authenticate

Amped Authenticate – це спеціалізоване програмне забезпечення для аналізу автентичності зображень та відео, розроблене компанією Amped Software [2]. Цей інструмент використовується для виявлення підробок, аналізу метаданих та підтримки судової експертизи. Інтерфейс Amped Authenticate наведено на рис.1.3.

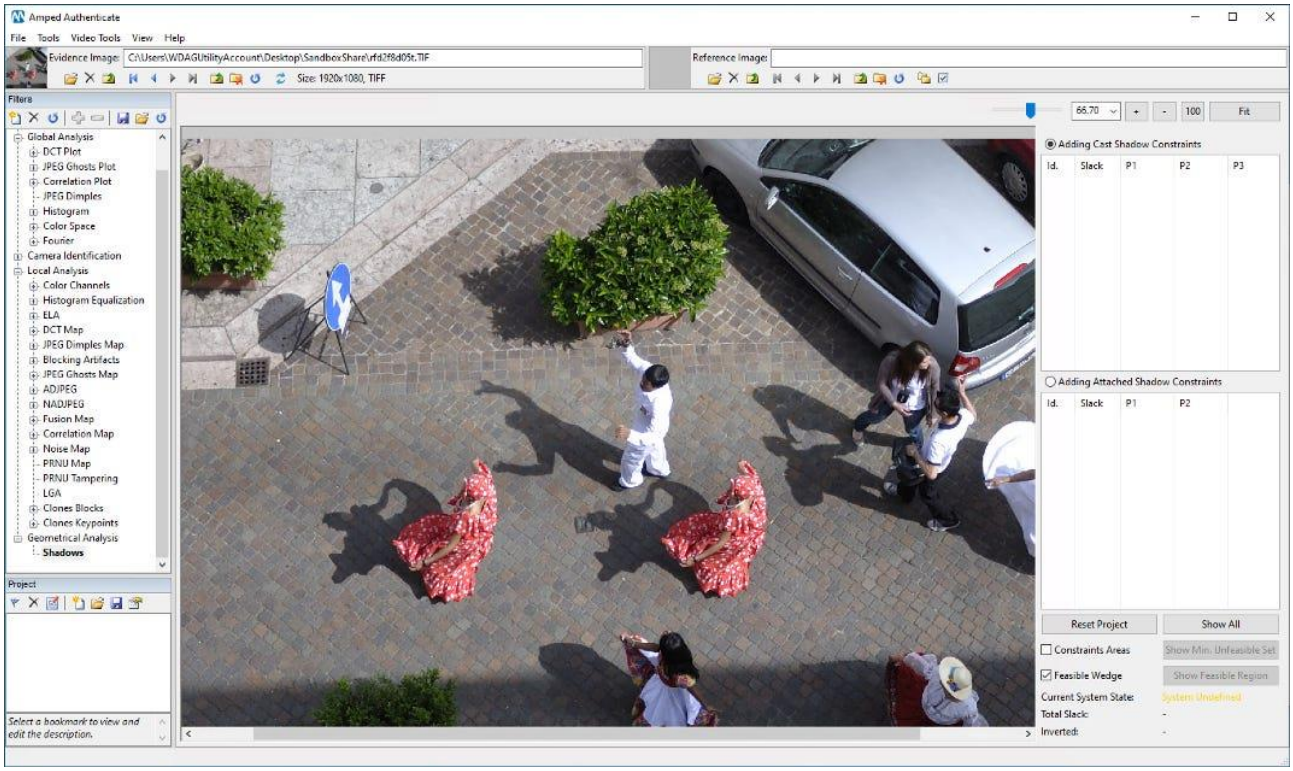


Рисунок 1.3 - Програмне забезпечення Amped Authenticate

Основні функції:

- аналіз автентичності зображень: Система виявляє ознаки підробки, використовуючи різні методи аналізу;
- аналіз метаданих: ПЗ може детально аналізувати метадані зображень, що дозволяє визначити, чи були вони змінені;
- інструменти для судової експертизи: Програма надає функції, що дозволяють створювати звіти, які можуть бути використані в суді;
- можливості порівняння зображень: Включає інструменти для порівняння зображень та виявлення обробки;

Переваги:

- висока точність: Amped Authenticate забезпечує високий рівень точності у виявленні підробок завдяки використанню передових алгоритмів;
- повний аналіз метаданих: програма дозволяє детально аналізувати метадані, що є критично важливим для виявлення маніпуляцій з зображеннями;
- інструменти для судової експертизи: програма розроблена з урахуванням потреб судової експертизи, що робить її придатною для використання у правових процесах;
- широкий спектр функцій: включає різноманітні інструменти для аналізу зображень, що дозволяють комплексно підходити до задачі виявлення підробок;

Вартість річної підписки на Amped Authenticate складає приблизно 2200 доларів США на рік для одного користувача. Це включає доступ до продукту Amped Software та навчання.

Cognitech FiA 64

Cognitech FiA 64 – це потужне програмне забезпечення для аналізу автентичності зображень, розроблене компанією Cognitech [3]. Це ПЗ широко використовується у судовій експертизі для виявлення підробок та маніпуляцій зображеннями. Інтерфейс Cognitech FiA 64 наведено на рис.1.4.

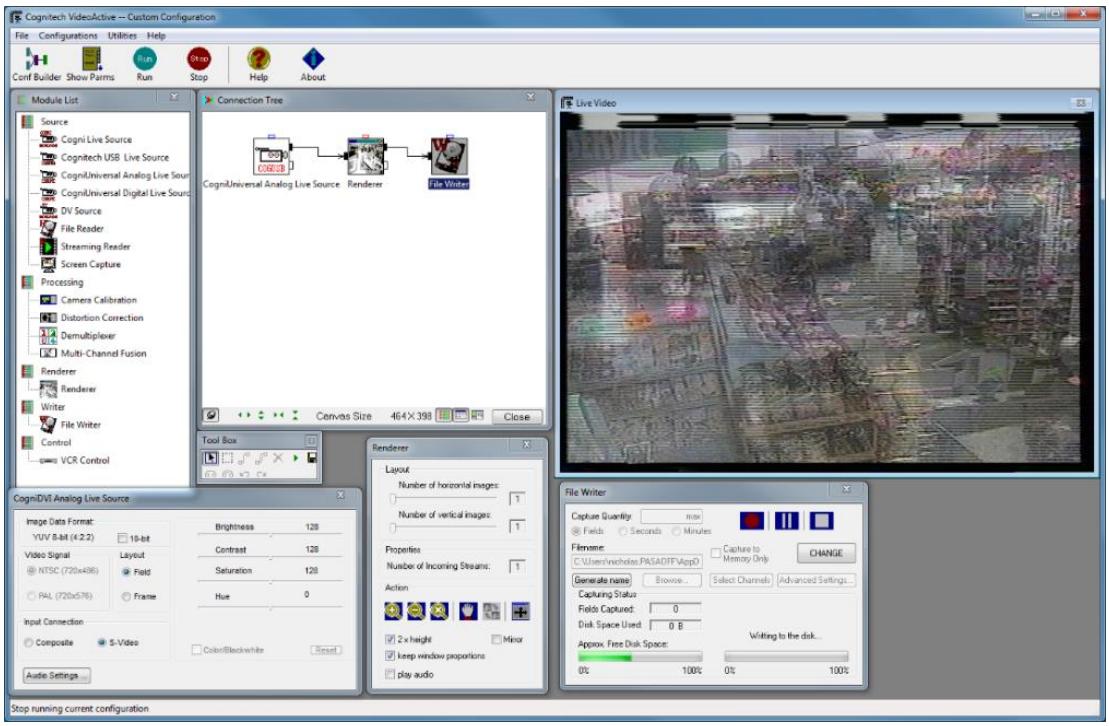


Рисунок 1.4 - Програмне забезпечення Cognitech FiA 64

Основні функції:

- виявлення підробок та маніпуляцій: програма використовує різноманітні методи для виявлення змін у зображеннях, включаючи аналіз рівня компресії JPEG та аналіз метаданих;
- аналіз структури зображення: FiA 64 дозволяє детально аналізувати структуру пікселів, виявляючи ознаки редагування та маніпуляцій;
- аналіз EXIF даних: програма детально аналізує EXIF дані зображень для виявлення змін, що можуть свідчити про підробку;
- диференційні карти: використання диференційних карт для виявлення змін у зображеннях;
- інструменти для судової експертизи: програма створює детальні звіти, які можуть бути використані у судових процесах;

Переваги:

- висока точність: FiA 64 забезпечує високий рівень точності у виявленні підробок завдяки використанню складних алгоритмів аналізу;

- глибокий аналіз зображень: програма дозволяє проводити глибокий аналіз структури зображень, що робить її ефективною для виявлення навіть найменших маніпуляцій;
- інструменти для судової експертизи: програма розроблена спеціально для використання у судових експертизах, що робить її надійним інструментом для правоохоронних органів;
- широкий спектр функцій: включає різноманітні інструменти для аналізу зображень, що дозволяють комплексно підходити до задачі виявлення підробок;

Ціна на Cognitech FiA 64 є високою і уточнюється при запиті до постачальника. Вартість включає доступ до всіх функцій програми та технічну підтримку.

Forensically Image Verification Tool

Forensically Image Verification Tool – це веб-інструмент для цифрової експертизи зображень, розроблений для виявлення підробок та маніпуляцій з фотографіями [4]. Цей інструмент доступний онлайн і не вимагає встановлення програмного забезпечення на комп'ютер користувача. Інтерфейс Forensically Image Verification Tool наведено на рис.1.5.

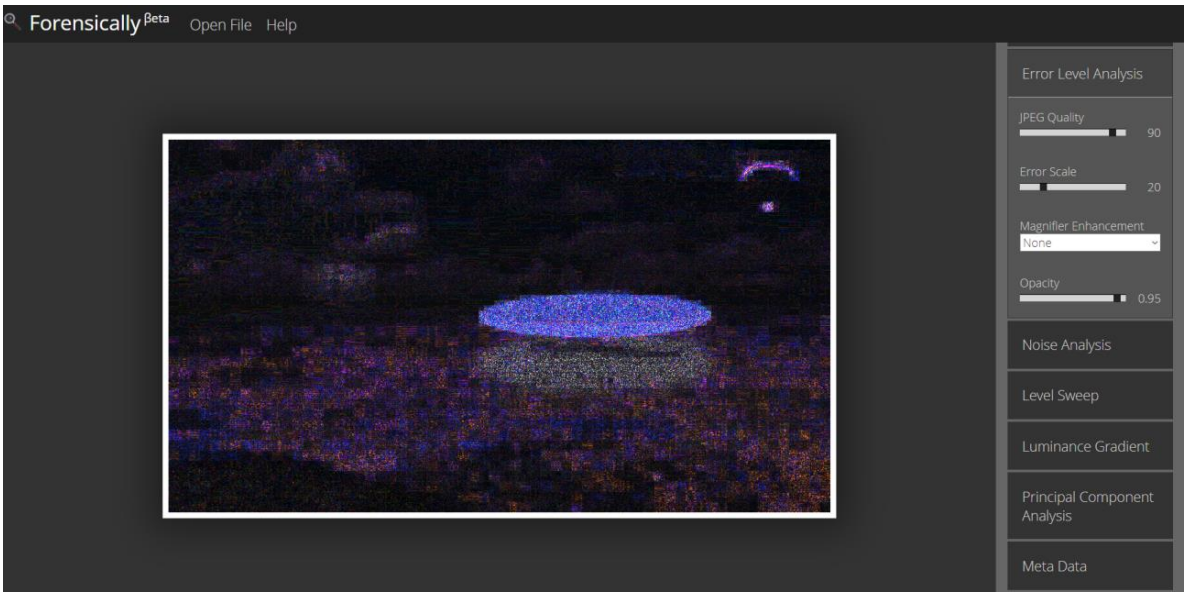


Рисунок 1.5 - Програмне забезпечення Forensically Image Verification Tool

Основні функції:

- збільшення зображення: інструмент дозволяє збільшувати зображення для детального аналізу дрібних деталей;
- аналіз рівня помилок (ELA): інструмент використовує ELA для виявлення змін у зображенні, які можуть свідчити про маніпуляції;
- аналіз метаданих: інструмент дозволяє переглядати та аналізувати метадані зображень, включаючи інформацію про камеру, час зйомки та інші деталі;
- фільтри: інструмент надає можливість застосовувати різні фільтри для підвищення контрасту, виявлення прихованих деталей та покращення видимості потенційних підробок;

Переваги:

- безкоштовність: Forensically є безкоштовним інструментом, доступним для використання онлайн;
- зручність у використанні: інструмент не вимагає встановлення та може використовуватися безпосередньо через веб-браузер;
- різноманітність функцій: Forensically пропонує кілька корисних функцій для аналізу зображень, що дозволяє комплексно підходити до виявлення підробок;
- доступність: інструмент доступний будь-якому користувачеві з доступом до інтернету, що робить його легко доступним для широкої аудиторії;

Forensically Image Verification Tool є безкоштовним інструментом, доступним онлайн. Це робить його привабливим варіантом для користувачів, які не мають бюджетів на придбання дорогого програмного забезпечення, але, в той самий час, це робить небезпечним роботу з Forensically Image Verification Tool у кіберполіції, через недоліки та вразливості веб-інструменту.

Порівняння систем аналогів

Враховуючи вищеописані параметри, переваги та недоліки існуючих рішень, було створено таблицю порівнянь.

Таблиця 1.2. Порівняння систем аналогів

Параметр	Amped Authenticate	Cognitech FiA 64	Forensically Image Verification Tool
Мова	Англійська	Англійська	Англійська
Метадані	Так	Так	Так
ELA (Error Level Analysis)	Так	Так	Так
Фільтри	Так	Так	Так
Ціна	Приблизно 2200 доларів на рік (річна підписка)	Висока, уточнюється при запиті	Безкоштовно
Безкоштовний період	Немає	Немає	Так
Безпечність	Висока, використовується в судовій експертизі	Висока, використовується в судовій експертизі	Відносно висока (веб-інструмент)

1.6 Обґрунтування доцільності проектування й розроблення системи для контролю виконання посадових доручень на кафедрі

Розроблення та впровадження програмного модуля для аналізу автентичності фото файлів має численні переваги, що забезпечують ефективну роботу кіберполіції України.

- аналізуючи фото файли на автентичність за допомогою автоматизованого інструменту, можна значно підвищити ефективність розслідувань. Використання спеціалізованих алгоритмів дозволяє швидко виявляти редаговані зображення, що скорочує час на перевірку та аналіз матеріалів.

Це зменшує навантаження на співробітників та підвищує швидкість реагування на кіберзагрози;

- забезпечення зручного контролю автентичності фото матеріалів дозволяє оперативно виявляти підробки, що сприяє підтримці високого рівня кібербезпеки. Це також допомагає уникати поширення неправдивих новин та дезінформації, що є критично важливим для захисту національних інтересів України;
- програмний модуль для аналізу автентичності фото файлів сприяє покращенню комунікації та взаємодії між співробітниками кіберполіції. Використання спільного інструменту для аналізу дозволяє співробітникам обмінюватися інформацією у режимі онлайн, що підвищує координацію дій та ефективність роботи підрозділу;
- централізоване зберігання даних, яке забезпечується програмним модулем, дозволяє зберігати всі документи та аналізовані матеріали в одному місці. Це забезпечує швидкий доступ до необхідної інформації та покращує організацію роботи, що сприяє ефективнішому проведенню розслідувань;
- автоматизація процесів, пов'язаних з аналізом фото файлів, зменшує кількість ручної роботи та підвищує точність виконання завдань. Це дозволяє знизити кількість помилок та покращити загальну ефективність роботи кіберполіції, що є важливим кроком у підвищенні рівня кібербезпеки в країні;

Можна зробити висновок, що розроблення та впровадження програмного модуля для аналізу автентичності фото файлів є доцільним, оскільки цей інструмент дозволить покращити ефективність та точність розслідувань, забезпечить зручний контроль автентичності матеріалів, сприятиме покращенню комунікації між співробітниками та забезпечить централізоване зберігання даних. Інформатизація процесів також допоможе зменшити кількість помилок та покращити загальну ефективність роботи кіберполіції України.

1.7 Концептуальна модель системи

Концептуальна модель системи матиме вигляд аналогічний до функціональної моделі роботи Кіберполіції під час аналізу автентичності фото файлів. Для автоматизації цього процесу пропонується запровадити програмний модуль, який забезпечить автоматичне виконання деяких блоків функціональної моделі.

До таких блоків входить:

- *аналіз метаданих* - система автоматично аналізуватиме метадані фото, щоб визначити інформацію про камеру, дату та час зйомки, місцезнаходження та інші важливі деталі. Будуть виявлятися зміни у метаданих, що можуть свідчити про маніпуляції.
- *аналіз рівня помилок (ELA)* - виконання ELA буде автоматизоване для виявлення областей зображення, де була проведена обробка або редагування. Результати ELA будуть відображатися для подальшого візуального аналізу експертами.
- *візуальний аналіз* - програмний модуль застосовуватиме різні фільтри для підвищення контрасту, різкості та виділення кольорів. Функція зум-аналізу дозволить детально переглядати окремі частини зображення для виявлення підозрілих деталей.
- *формування звітів* - звіти будуть автоматично формуватися з результатами всіх етапів аналізу. Вони будуть зберігатися в базі даних та можуть бути експортовані у форматі Word або PDF для подальшого використання.

Структура цього програмного модуля буде розроблена з можливістю вдосконалення та розширення. У подальшому, в системі можна реалізувати такі функції, як створення нагадувань для всього колективу про заплановані зустрічі, засідання та обговорення, а також терміни їх проведення.

1.8 Розрахунок економічного ефекту від впровадження системи

Оцінка економічного ефекту від впровадження модуля має велике значення, оскільки це є основою для техніко-економічного обґрунтування розробки автоматизованої системи.

Визначення розміру оплати праці розробників:

Для визначення розміру оплати праці потрібно враховувати тип системи, ступінь новизни розроблюваних завдань і складність алгоритму. При цьому важливо враховувати організацію управління працею та кадрами.

Ступінь новизни для розроблюваної системи - "В", це означає, що розробка здійснюється на основі змінених типових проектних рішень. Група складності алгоритмів, що використовуватимуться в процесі розробки - "З", це вказує на використання стандартних методів рішень без застосування складних числових або логічних методів.

Таблиця 1.3. Узагальнені дані для вхідної та вихідної інформації для системи координації проєкту

Вид інформації	**Позначення**	**К-сть наборів даних**
Змінна інформація	ЗІ	m=4
Нормативно – довідкова інформація	НДІ	n=2
Банк(база) даних	БД	p=1
Обробка в режимі реального часу	РЧ	Так
Забезпечення телекомунікаційної обробки даних і управління віддаленими об’єктами	ТОУ	Ні

Використовуючи надані вихідні дані, можна розрахувати прогнозований час, необхідний для розробки системи координації проекту, як показано в таблиці 1.4.

Таблиця 1.4. Визначення витрат часу

Вид системи	Стадія розробки системи	
	Ескізний проект	Технічне завдання
	В	В
Комп'ютерна майстерня. Управління та контроль за виконання замовлення, обліком та видачею замовлення; оптимізація процесів роботи.	T_1=50	T_2=31

Визначимо витрати часу на стадіях «технічний проект», «робочий проект» і «впровадження».

Вхідними даними для визначення є:

- кількість форм вхідної інформації 5;

- кількість форм вихідної інформації 4;

- базове значення витрат часу для стадії «Технічний проект» $T_{Б3}$=60

- базове значення витрат часу для стадії «Робочий проект» $T_{Б4}$=75

- базове значення витрат часу для стадії «Впровадження» $T_{Б5}$=35

Базове значення витрат часу ТБ коригується за допомогою поправочних коефіцієнтів для всіх стадій розробки автоматизованої системи.

Визначення витрат часу для стадії «Технічний проект» (T_3).

Для розрахунку витрат часу на стадії "технічний проект" T_3 було використано наступну формулу (формула 1.1)

$$T_3 = T_{Б3} * k_п * k_о \quad (1.1)$$

Для розрахунку $k_п$ використовувалась наступна формула (формула 1.2)

$$k_n = \frac{k_1 * m + k_2 * n + k_3 * p}{m+n+p} \quad (1.2)$$

Таблиця 1.5. Коефіцієнти ступеню новизни проєкту, ko

Стадія розробки проєкту	Вид обробки	Ступінь новизни
		В
Технічний проєкт	РЧ	1.26
Робочий проєкт	РЧ	1.32
Впровадження	РЧ	1.21

Таблиця 1.6. Коефіцієнти k1 (ЗІ), k2 (НДІ), k3 (БД) для стадії «Технічний проект»

Вид використаної інформації	Ступінь новизни
	В
k_1 (ЗІ)	1.0
k_2 (НДІ)	0.72
k_3 (БД)	2.08

$$k_n = \frac{(1 * 4 + 0.72 * 2 + 2.08 * 1)}{(4 + 2 + 1)} = 1.074$$

Отже,

$$T_3 = 60 * 1.074 * 1.26 = 81.19$$

Визначення витрат часу на стадії “робочий проєкт” (Т4).

Для розрахунку витрат часу на стадії “ робочий проєкт” T_4 було використано наступну формулу (формула 1.3)

$$T_4 = T_{Б4} * k_п * k_о * k_с \quad (1.3)$$

Для визначення часу на стадії “робочий проєкт”, потрібно скористатись формулою розрахунку коефіцієнту $k_п$ (формула 1.2)

Таблиця 1.7. Коефіцієнти k_1, k_2, k_3 для стадії «Робочий проект»

Вид використаної інформації	Ступінь новизни
	В
k1(ЗІ)	1.1
k2(НДІ)	0.50
k3(БД)	0.47

$$k_{\text{п}} = \frac{(1.1 * 4 + 0.50 * 2 + 0.47 * 1)}{(4 + 2 + 1)} = 0.839$$

Для визначення значення kc у формулі ідентифікуємо складність контролю вхідної та вихідної інформації. Зауважимо, що вхідна інформація має подібний формат і зміст. Так само друк документів має подібну форму і зміст.

Тобто $k_{\text{с}} = 1.4$

$$T_4 = 75 * 0.839 * 1.32 * 1.4 = 116.29$$

Визначення витрат часу на стадії «впровадження» (Т5).

Для розрахунку витрат часу на стадії "впровадження" T_5 було використано наступну формулу (формула 1.4)

$$T_5 = T_{\text{Б5}} * k_{\text{п}} * k_{\text{о}} * k_{\text{с}} \quad (1.4)$$

$$T_5 = 35 * 0.839 * 1.21 * 1.4 = 49.744$$

Загальні витрати були обчислені за формулою (формула 1.5):

$$\text{T}_{\sum} = \text{T}_1 + \text{T}_2 + \text{T}_3 + \text{T}_4 + \text{T}_5 \quad (1.5)$$

$$\text{T}_{\sum} = 50 + 31 + 81.19 + 116.29 + 49.744 = 328.224$$

На розробку проєкту виділено Ф = 40 днів. Тоді кількість місяців із розрахунку 25 робочих днів: М = Ф/25 = 40/25 = 1.6 місяці

Отже, для виконання такого проекту потрібно така чисельність виконавців Ч, яка обраховується за формулою: Ч = 328.224/45 = 8 виконавців

Приймемо розмір заробітної плати програміста - 25000 грн, тоді загальна сума заробітних плат програмістів складає:

$$\text{V}_1' = \text{Ч} * \text{М} * \text{ЗП} = 8 * 2 * 25000 = 400000 \text{ грн}$$

Витрати, пов'язані з розробкою програми на ПК

- Розрахунок річного фонду часу роботи ПК:

Дійсний річний фонд часу ПК у годинах дорівнює числу робочих годин у році для оператора, за винятком часу на технічне обслуговування і ремонт ПК (в середньому 5год/міс + 6 роб.днів/рік).

$$\text{T}_{\text{ПК}} = 2000 - (6 * 8 + 5 * 12) = 1892 \text{ год.}$$

Оскільки під час виконання курсової роботи здобувач в середньому витрачає 450 год. машинного часу, то величина фонду часу ПК дорівнює

$$Т'_{ПК} = 1892 * (450/2000) = 425.7 \text{ год}$$

Поточні витрати на експлуатацію V":

Балансована вартість ПК, де $Ц_Р$ - ринкова вартість ПК, орієнтовно складає 50000 грн, $К_{УН}$ – коефіцієнт, що враховує витрати на установку ПК. $k_{УН} = 0{,}12$

$$Ц_{ПК} = Ц_Р * (1 + k_{УН}) = 50000 * (1 + 0{,}12) = 56000 \text{ грн}$$

Для обчислення амортизаційних відрахувань за використання ПК, використовувалась наступна формула (формула 1.6):

$$З_{АМ} = \frac{Ц_{ПК}}{Н_А} \quad (1.6)$$

$$З_{АМ} = \frac{56000}{5} = 11200 \text{ грн}$$

Загальні витрати на розробку програмного забезпечення комп'ютерної системи розраховуються за формулою(формула 1.7):

$$V_1'' = ЗОП + ЗАМ + ЗЕЛ + Зр + ЗМАТ \quad (1.7)$$

Для обчислення витрати на електроенергію ($З_{ЕЛ}$) , споживану ПК, використовувалась наступна формула: $З_{ЕЛ} = Р_{ПК} * Т_{ПК} * Ц_{ЕЛ} * А$, де потужність ПК, $Р_{ПК}$ = 0.5 кВт; фонд корисного часу роботи ПК, $Т_{ПК} = 435.16$ год, вартість 1 кВт електроенергії для підприємств, $Ц_{ЕЛ}$ = 2,64 грн/кВт, коефіцієнт інтенсивного використання ПК, А = 0.9.

$$З_{ЕЛ} = 0.5 * 425.7 * 2.56 * 0.9 = 490.4 \text{ грн}$$

Витрати на поточний ремонт і технічне обслуговування ПК ($З_Р$)визначаються як 6% від балансової вартості ПК, $Ц_{ПК}$ (формула 1.8).

$$З_р = Ц_{ПК} * 0.06 \quad (1.8)$$

$$З_р = 56000 * 0.06 = 3360 \text{ грн}$$

Непрямі витрати, пов’язані з експлуатацією ПК, визначаються як 5% від балансової вартості ПК $Ц_{ПК}$ (формула 1.9)

$$З_{МАТ} = Ц_{ПК} * 0.05 \quad (1.8)$$

$$З_{МАТ} = 56000 * 0.05 = 2800 \text{ грн}$$

Заробітна плата обслуговуючого персоналу складає в середньому - 15000

Тож, поточні витрати на експлуатацію, V_1'', грн, складають:

$$V_1'' = 15000 + 11200 + 490.4 + 3360 + 2800 = 32850.4 \text{ грн}$$

А, загальні витрати на розробку програмного забезпечення комп’ютерної системи складуть:

$$V_1 = V_1' + V_1'' = 400000 + 32850.4 = 432850.4 \text{ грн}$$

Оскільки підрозділи Кіберполіції вже обладнані необхідними комп'ютерами, а кожен співробітник має свій персональний комп’ютер, то витрати на придбання і установку нових комп’ютерів становитимуть:

$$V_2 = 0$$

Оскільки немає необхідності у підготовці спеціальних приміщень, то: $V_3 = 0$

Також співробітники повинні пройти навчання для роботи з новим програмним модулем. В середньому навчання триватиме 5 днів, тому витрати на навчання складуть: $V_3 = 2500$ грн

Загальна вартість розробки і впровадження системи вираховується за формулою (формула 1.10):

$$V_\Sigma = V_1 + V_2 + V_3 + V_4 \quad (1.10)$$

$$V_\Sigma = 432850.4 + 0 + 0 + 2500 = 435350.4 \text{ грн}$$

Оскільки норма амортизаційних втрат для комп’ютерних систем НА = 5, то для обрахування річного економічного ефекту слід брати до розгляду величину $V_р$ (формула 1.11)

$$V_{\text{р}} = \frac{V_{\Sigma}}{\text{Н}_{\text{А}}} \tag{1.11}$$

$$V_{\text{р}} = \frac{435350.4}{5} = 87070.08 \text{ грн}$$

Оскільки Кіберполіція не має власного прибутку і не здійснює розподіл фінансів, то впровадження даного програмного модуля матиме переважно соціальний ефект. Соціальний ефект, в свою чергу, буде досягнуто за рахунок автоматизації та оптимізації процесу аналізу автентичності фото файлів, а саме завдяки автоматизації таких задач: аналіз метаданих, візуальний аналіз зображень, автоматичне формування звітів про результати аналізу.

Програмний модуль також забезпечить швидкий доступ до інформації в будь-який момент часу та покращить організацію процесу аналізу та моніторинг за станом виконання завдань. Це дозволить оперативно реагувати на підозрілі фото та підвищить ефективність роботи Кіберполіції у боротьбі з кіберзлочинністю.

1.9. Висновок до розділу 1

У даному документі проведено детальний системний аналіз предметної області діяльності департаменту кіберполіції України, який включає історію становлення та розвитку підрозділу, його організаційну структуру, сучасний стан комп'ютеризації, а також потреби та можливості подальшої інформатизації. Було зазначено, що кіберполіція України виконує широкий спектр завдань у боротьбі з кіберзлочинністю, таких як розслідування кіберзлочинів, моніторинг та аналіз кіберзагроз, а також міжнародне співробітництво. Проте, існуючі процеси потребують вдосконалення та більшої інформатизації, зокрема у сфері аналізу автентичності фото файлів.

Запропонована функціональна модель включає автоматизований аналіз метаданих, рівня помилок (ELA), візуальний аналіз та формування звітів. Впровадження такого програмного модуля дозволить підвищити точність і швидкість аналізу, зменшити кількість помилок та покращити ефективність роботи кіберполіції.

Огляд існуючих рішень на ринку показав, що існує низка програмних продуктів для аналізу автентичності зображень, кожен з яких має свої переваги та недоліки. Проте, жодне з цих рішень не повністю задовольняє потреби кіберполіції України, що підкреслює необхідність розробки власного програмного модуля.

Економічний аналіз показав, що розробка та впровадження даної системи є доцільними та економічно обґрунтованими. Очікувані витрати на розробку та впровадження системи, включаючи заробітну плату розробників, експлуатаційні витрати та навчання персоналу, будуть компенсовані підвищенням ефективності та зменшенням часу на перевірку автентичності фото матеріалів.

Таким чином, впровадження спеціалізованого програмного модуля для аналізу автентичності фото файлів є необхідним кроком у підвищенні ефективності роботи кіберполіції України, що сприятиме покращенню національної кібербезпеки та підвищенню рівня захисту від кіберзлочинів.

РОЗДІЛ 2. ТЕХНІЧНЕ ЗАВДАННЯ

2.1. Загальні положення

2.1.1. Найменування системи: «Програмний модуль для аналізу автентичності фото файлів»

2.1.2. Оформлення та передача результатів роботи зі створення системи здійснюється відповідно до вимог ДСТУ, встановлених для кожного етапу розробки. Конкретний порядок оформлення та передачі результатів визначається залежно від змісту та календарного плану проекту.

2.1.3. Під час подальших етапів роботи над створенням системи можуть виникати потреби в додатковому уточненні та розвитку окремих положень.

2.2. Призначення і цілі створення системи

2.2.1. Призначення системи.

Система призначена для покращення ефективності та точності аналізу автентичності фото файлів. Вона дозволяє визначати та виявляти ознаки редагування зображень. Система повинна спрощувати процес аналізу фото файлів, надаючи зручні інструменти для виявлення можливих фальсифікацій, а також для написання звітів про результати аналізу. Це забезпечує користувачам легкий доступ до інформації про автентичність зображень, покращує здатність експертів до ефективного моніторингу та оцінки зображень, а також підвищує загальний рівень довіри до візуальних даних.

2.2.2. Цілі створення системи.

Основною метою створення системи є підвищення точності та ефективності аналізу автентичності фото файлів, спрощення процесу виявлення фальсифікацій та полегшення написання звітів про результати аналізу. Це включає в себе надання інструментів для аналізу зображень, оперативний доступ до цих інструментів, контроль стану автентичності фото

файлів. Система забезпечує точне виявлення маніпуляцій з зображеннями, покращує якість та швидкість аналізу, і підвищує загальний рівень довіри до візуальних даних.

2.3. Характеристика об’єкта інформатизації

2.3.1. Короткі відомості про об’єкт інформатизації.

Об’єктом інформатизації є процес аналізу автентичнсті фото файлів.

2.4. Вимоги до системи

2.4.1. Вимоги до системи у цілому:

- Нативний інтерфейс: Програмний модуль має бути простим для освоєння та користування.
- Функції обробки та аналізу зображень: Користувачі модуля можуть переглядати, редагувати наявними інструментами та зберігати редаговані зображення.

2.4.2. Вимоги до функцій (завдань), що виконуються системою

2.4.2.1. Загальна функціональність

Функціонал програмного модуля для аналізу автентичності фото файлів повинен включати наступні завдання та функції:

- Відкриття зображення: Забезпечення роботи з різними форматами фото, такими як JPEG, JPG, PNG;
- Збереження зображення: Програмний модуль має зберігати редаговані зображення без втрати якості та зміни метаданих.
- Error Level Analysis (ELA): Визначення областей, що піддавалися повторній компресії, що може свідчити про редагування;
- Аналіз метаданих: Читання та аналіз метаданих EXIF для визначення оригінальності фото;
- Приближення (Зум): Можливість збільшення певних ділянок зображення для більш деталізованого аналізу і виявлення маніпуляцій;
- Фільтри: Регулювання параметрів зображення, таких як контраст, кольори, чіткість та яскравість;

- Конвертація зображень: Підтримка конвертації фото у різні формати, такі як 1, L, RGB, RGBA, CMYK, LAB, HSV, roll, R, G, B;
- Обрізання та поворот зображень: Можливість обрізати та повертати зображення;
- Меню з формами введення звітів: Форми для введення звітів для візуального аналізу, аналізу рівня помилок, аналізу метаданих та загального аналізу з можливістю введення, видалення та оновлення даних у базі даних;
- Формування звітів: Генерація звітів з інформацією щодо всіх видів аналізу та формування Word файлу звіту;
- Довідка: Інструкція користувача з детальним описом функціоналу програми;

2.4.2.2. Вимоги до функції відкриття та збереження файлів:

- Підтримка форматів: Підтримка зображень у форматах JPEG та PNG, у тому числі різних варіантів JPEG, таких як JPG;
- Відкриття файлів: Безпомилкове відкриття файлів без зміни вмісту та метаданих;
- Збереження файлів: Забезпечення збереження файлів у вихідному форматі без додаткової компресії чи втрати даних;

2.4.2.3. Вимоги до функції Error Level Analysis (ELA):

- Налаштування чутливості: Можливість користувача регулювати параметри ELA;
- Візуалізація результатів: Надання інтуїтивно зрозумілого візуального представлення результатів ELA, з чітким позначенням потенційно змінених областей;
- Підтримка форматів файлів: Підтримка аналізу зображень у форматах JPEG, JPG;

2.4.2.4. Вимоги до функції аналізу метаданих у програмному модулі:

- Вилучення метаданих: Здатність точно вилучати метадані з різних типів файлів зображень;

- Аналіз EXIF: Детальний аналіз метаданих EXIF для ідентифікації даних про камеру, дату зйомки, параметри зображення та історії редагувань;
- Підтримка форматів: Підтримка всіх поширених форматів зображень, таких як JPEG, JPG і PNG, та сумісність з їхніми варіантами метаданих;

2.4.2.5. Вимоги до функції приближення (зуму) в програмному модулі:

- Гнучке масштабування: Можливість масштабування зображень без втрати якості;
- Інтерактивність: Легке використання функції зуму з можливістю вибору різних рівнів приближення;

2.4.2.6. Вимоги до фільтрів:

- Контраст: Можливість регулювання контрасту зображення;
- Кольори: Налаштування насиченості та балансу кольорів;
- Чіткість: Підвищення чіткості зображення;
- Яскравість: Регулювання яскравості зображення;

2.4.2.7. Вимоги до конвертації зображень:

- Підтримка форматів: Конвертація зображень у формати 1, L, RGB, RGBA, CMYK, LAB, HSV, roll, R, G, B;

2.4.2.8. Вимоги до функції обрізання та повороту зображень:

- Обрізання зображень: Можливість обрізання зображень для видалення небажаних частин;

2.4.2.9 Функція повороту зображення:

- Поворот зображень: Можливість повороту зображень на заданий кут;

2.4.2.10. Вимоги до меню з формами введення звітів:

- Форми введення звітів: Форми для введення звітів для візуального аналізу, аналізу рівня помилок, аналізу метаданих та загального аналізу;

- Функціонал введення, видалення та оновлення: Можливість введення, видалення даних у базі даних через форми;

2.4.2.11. Вимоги до формування звітів:

- Генерація звітів: Формування звітів з інформацією щодо всіх видів аналізу;
- Формування Word файлів: Генерація звітів у форматі Word;

2.4.2.12. Вимоги до довідки:

- Інструкція користувача: Детальна інструкція користувача з описом всіх функцій та можливостей програми;

2.4.2.13. Можливість модифікації:

- Вся виконана робота має бути задокументована та описана (Коментарі у коді, пояснювальні записки);

2.4.2.14.

Інформація яка буде вводитися та яка буде формуватися:

Таблиця 2.1 . Перелік функцій, вхідної та вихідної інформації

№	Підсистема	Вхідна інформація	Вихідна інформація
1	Відкритя зображення	Зображення	Створення вкладки зображення на вивід на екран
2	Збереження зображення	Зображення	Збереження зображення у обраній директорії

Продовження таблиці 2.1. Перелік функцій, вхідної та вихідної інформації

№	Підсистема	Вхідна інформація	Вихідна інформація
3	ELA аналіз	Зображення, рівень стискання	Створення ELA зображення у директорії оригінального зображення, створення вкладки та виведення створеного ELA зображення на екран
4	Приближення (Зум)	Зображення	Виведення на екран приближеного зображення
5	Фільтри	Зображення, коефіцієнт фільтру	Виведення на екран зображення з неакладеним фільтром
6	Конвертація	Зображення	Вивід на екран конвертованого зображення
7	Обрізання	Зображення, область обрізання	Обрізане за областю зображення

Продовження таблиці 2.1. Перелік функцій, вхідної та вихідної інформації

№	Підсистема	Вхідна інформація	Вихідна інформація
8	Формування та введення загального висновку аналізу	Таблиці AppUser, Image Шлях зображення, висновок аналізу, інформація щодо редагування	Форма з загальним висновком
9	Формування та введення висновку ELA аналізу	Таблиці AppUser, Image, Image_analysis Шлях ELA зображення, висновок аналізу	Форма з висновком ELA аналізу
10	Формування та введення висновку візуального аналізу	Таблиці AppUser, Image, Image_analysis зображення, висновок аналізу	Форма з висновком візуального аналізу
11	Формування та введення висновку аналізу метаданих	Таблиці AppUser, Image, Image_analysis метадані зображення, висновок аналізу	Форма з висновком аналізу метаданих
12	Формування звіту аналізу	Таблиці AppUser, Image, Image_analysis, ELA_analysis, MetaData_analysis, Visual_analysis	Звіт у вигляді документу Word

2.4.3. Вимоги до доступності програми:

- Сумісність: Програма повинна бути сумісна з усіма поточними версіями Windows 64-біт, включаючи останні оновлення безпеки та функціональні пакети;
- Підтримка: Підтримка користувачів через документацію та оновлення з рекомендаціями для оптимізації продуктивності під ОС Windows 64-біт;

2.4.4. Вимоги до стандартизації та уніфікації:

В процесі розробки та впровадження системи необхідно керуватися:

- державними стандартами України (ДСТУ);
- нормативними та керівними документами органів законодавчої та виконавчої влади;
- відповідними відомчими нормативними та керівними документами;
- міжнародними стандартами і нормативними документами.

2.4.5. Ліцензійні вимоги

Система повинна використовувати лише ліцензійне програмне забезпечення.

Спеціалізоване ПЗ, що розробляється власними силами виконавця, повинне використовувати ліцензійні компоненти (бібліотеки) і засоби розробки.

2.5. Склад і зміст робіт під час створення системи.

1. Аналіз і визначення вимог:
   - Збір і аналіз вимог щодо системи від користувачів та зацікавлених сторін.
   - Визначення функціональних і нефункціональних вимог до системи.
   - Розробка специфікацій вимог.

   Дата: 21.04.2024
2. Моделювання бази даних:
   - Створення структури бази даних, включаючи таблиці, поля, ключі, індекси та відносини між таблицями.
   - Визначення типів даних для кожного поля в базі даних.

- Розробка логічної та фізичної моделей бази даних.

Дата: 30.04.2024

3. Розгортання структури бази даних:
   - Створення фізичної бази даних на сервері або хмарному середовищі.
   - Встановлення необхідного програмного забезпечення для управління базою даних.
   - Завантаження початкових даних та встановлення доступів до бази даних для користувачів та додатків.

   Дата: 01.05.2024
4. Проектування:
   - Розробка архітектури системи.
   - Визначення структури бази даних і логічної моделі даних.
   - Розробка дизайну користувацького інтерфейсу.
   - Вибір технологій і інструментів для розробки.

   Дата: 05.05.2024
5. Реалізація:
   - Розробка програмного забезпечення та бази даних.
   - Інтеграція компонентів системи.
   - Тестування окремих модулів і функцій.

   Дата: 10.05.2024
6. Тестування:
   - Виконання різних видів тестування, включаючи тестування елементів системи, тестування системи у цілому, дослідну експлуатацію та інші види тестів, які були зазначені в попередньому описі.
   - Виправлення і видалення помилок.

   Дата: 20.05.2024

7. Впровадження:
   - Впровадження системи в робоче середовище.
   - Навчання користувачів і персоналу, який буде працювати з системою.

Дата: 22.05.2024

2.6. Порядок контролю і приймання системи

2.6.1. Види, склад, об’єми і методи випробувань системи та її складових частин

У процесі розробки системи виконуються наступні види випробувань:

- тестування елементів системи;
- тестування системи у цілому;
- дослідна експлуатація;

Крім того, при впровадженні комплексної системи захисту інформації, проводяться додаткові випробування, передбачені інструкціями ДСТЗІ.

2.6.2. Загальні вимоги до приймання робіт за стадіями

- Після закінчення відповідного етапу робіт формується комплект документації, передбаченої п.5;
- Завершення етапу фіксується відповідним протоколом між Виконавцем і Замовником.

2.7. Вимоги до складу і змісту робіт із підготовки до впровадження системи

Підготовка до запуску системи в дію передбачає виконання ряду правил і вимог для забезпечення успішної і ефективної роботи системи. Правила та вимоги включають:

- укомплектування та підготовка технічних засобів;
- перед запуском системи необхідно провести повне тестування, включаючи функціональне тестування, тестування на відмовостійкість та продуктивність;
- проведення інструктажу з використання системи, ознайомлення користувачів із функціональністю системи та правилами експлуатації;

2.8. Вимоги до документації

Документування системи повинне виконуватися у відповідності з

вимогами ГОСТ 34.201-89.

Спеціалізовані елементи системи, що поставляються підрядними організаціями, повинні супроводжуватися відповідним комплектом документації, а також (коли застосовано) сертифікатами відповідності.

2.9. Джерела розробки

2.9.1. При розробленні технічного завдання на систему використано наступні документи:

1. ДСТУ ISO/IEC/IEEE 12207:2018. Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення.
2. ДСТУ ISO/IEC/IEEE 29119-1:2017. Інженерія систем і програмних засобів. Тестування програмних засобів. Частина 1. Поняття та визначення (ISO/IEC/IEEE 29119-1:2013, IDT).
3. ДСТУ ISO/IEC 29155-1:2015. Розроблення систем і програмного забезпечення. Платформи для тестування проектів з розроблення інформаційних систем. Частина 1. Концепції та визначення.
4. ДСТУ ISO/IEC 12207:2016. Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення.

РОЗДІЛ 3. ОПИС КОМПЛЕКСУ ЗАДАЧ АВТОМАТИЗАЦІЇ

3.1. Інформаційне забезпечення системи

Для розробки програмного модулю використано наступні технології:

- середовище розробки: VS Code;
- мова програмування: Python;
- бібліотеки: Pillow, TKinter, pyodbc, docx;
- програмне забезпечення для проектування та документування баз даних: AllFusion ERWin Data Modeler;
- СКДБ: Microsoft SQL Server 2022;

Для створення бази даних, що підтримує необхідні функції системи, було розроблено логічно-фізичну модель даних (рис.3.1 та додаток А.1) за допомогою CASE-засобу AllFusion ERWin Data Modeler. В цій моделі визначені ключові сутності, їх атрибути та встановлені взаємозв'язки між сутностями.

Логічна схема містить наступні сутності:

Користувач (AppUser) – містить інформацію про користувача, таку як логін, пароль, ім’я, призвище та посаду. Ця інформація необхідна для авторизації, роботі з фото файлами та формування звіту. Дана таблиця пов’язана з таблицею “Image” зв’язком типу “один до багатьох”.

Картинка (Image) – містить шлях до картинки та інформацію про те, чи відкрита вона користувачем. Ця інформація необхідна для збереження інформацію про картинку, для подальшого аналізу картинки та для відкриття картинки автоматично, якщо вона не була закрита користувачем у застосунку. Дана таблиця пов’язана з таблицею “ Image_analysis” зв’язком типу “один до багатьох”.

Аналіз картинки (Image_analysis) – містить основний висновок щодо аналізу картинки та бінарне значення редагування. Ця інформація потрібна для аналізу картинки та подальшого формування звіту. Дана таблиця пов’язана з таблицями “ELA_analysis”, “MetaData_analysis”, “Visual_analysis”, зв’язками типу “один до багатьох”.

Аналіз рівня помилок (ELA_analysis) - містить висновок аналізу рівня

помилок та шлях до зображення з рівнем помилок. Ця інформація потрібна для аналізу картинки та подальшого формування звіту.

Аналіз метаданих (MetaData_analysis) - містить висновок аналізу метаданих та основні метадані фото. Ця інформація потрібна для аналізу картинки та подальшого формування звіту.

Візуальний аналіз (Visual_analysis) - містить висновок візуального аналізу фото. Ця інформація потрібна для аналізу картинки та подальшого формування звіту.

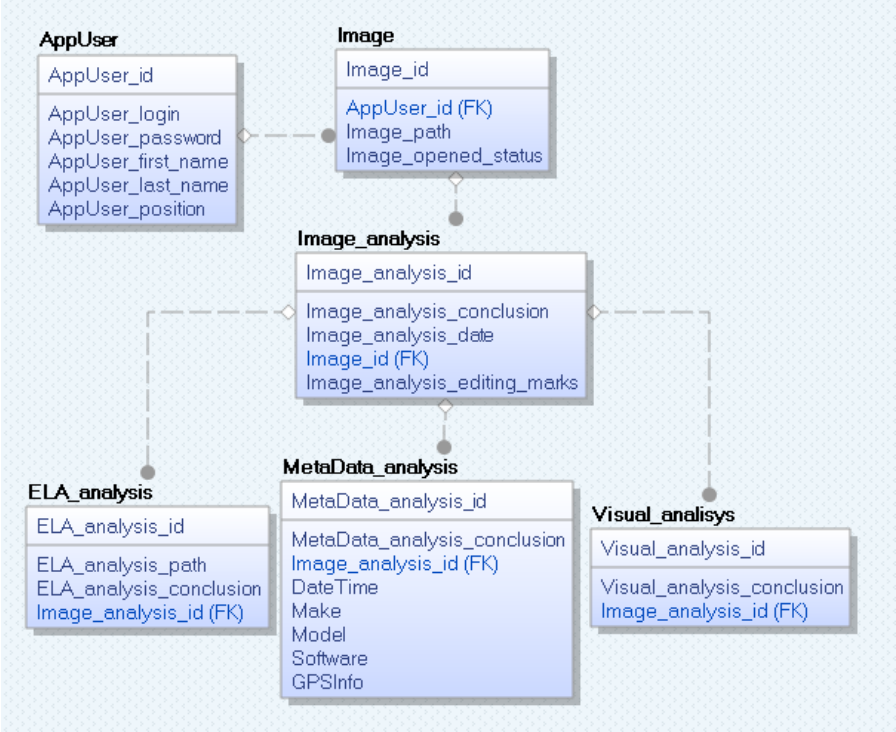


Рисунок 3.1 - Логічна модель бази даних

На основі розробленої логічної моделі бази даних створено фізичну модель (додаток А.1), яка визначає методи зберігання та організації даних на рівні операційної системи та апаратного забезпечення. У цій моделі встановлено типи даних для кожного атрибута сутності. Структура БД в СКБД MS SQL Server 2022 зображена на рис. 3.2.

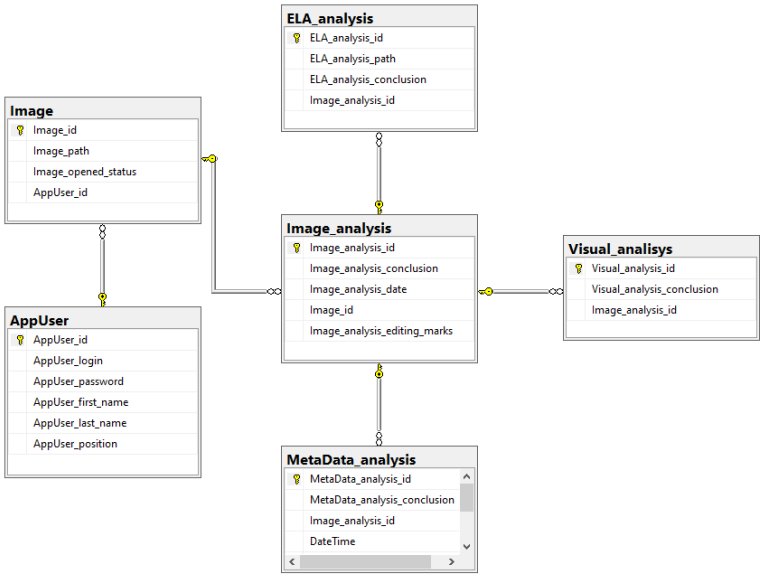


Рисунок. 3.2 - Структура БД в СКБД MS SQL Server 2022

3.2. Алгоритмізація та реалізація комплексу задач програмного модулю

Перш за все, було розроблено вікно авторизації (додаток В), яке викликається в основному класі програми та повертає у клас user_id, для подальшої роботи з таблицями. Вікно авторизації (рис. 3.3.) має поля Ім'я користувача та пароль, також на у вікні є кнопка Увійти. Для продовження роботи необхідно авторизуватись.

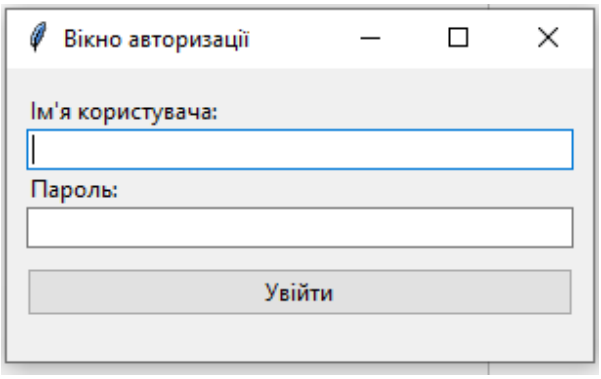


Рисунок. 3.3 - Вікно авторизації.

При натискані кнопки Увійти, виконується підключення до бази даних та виконується запит на виведення AppUser_id, з таблиці AppUser, де відповідні AppUser_login та AppUser_password.

cursor.execute("SELECT AppUser_id FROM AppUser WHERE AppUser_login = ? AND AppUser_password = ?", (username, password))

Якщо AppUser_id знайдено, то вікно авторизації закривається, та відкривається головне вікно програми, якщо AppUser_id не знайдено, то виводиться помилка (рис. 3.4.)

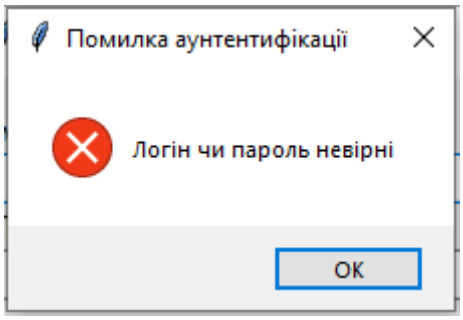


Рисунок. 3.4 - Помилка авторизації.

Після успішної авторизації, відкривається головне вікно програми (рис. 3.5.)

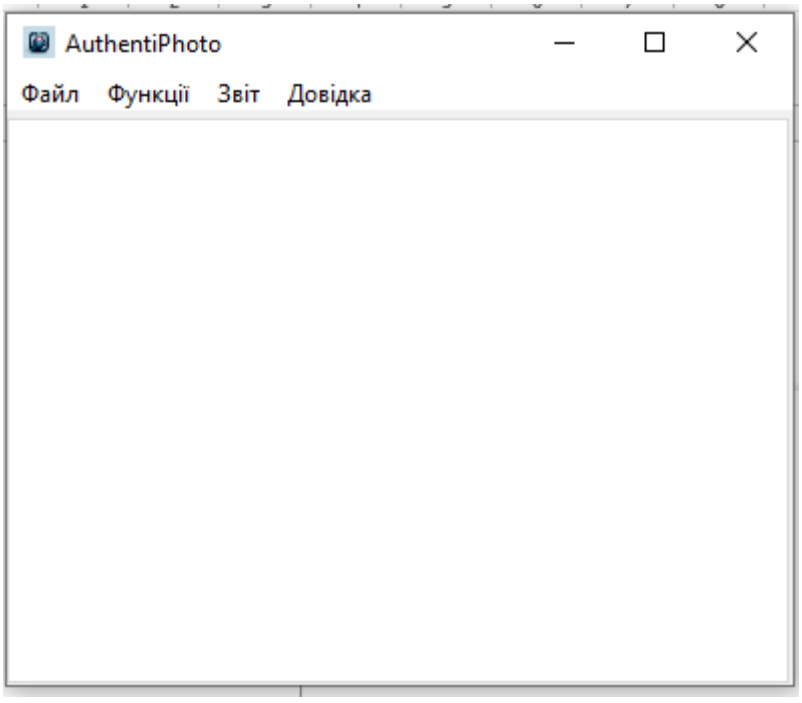


Рисунок. 3.5 - Головне вікно програми.

Для роботи з фото файлами, було створено меню Файл (рис. 3.6.), де додані такі функції як відкрити, зберегти, зберегти як, зберегти все, закрити картинку, видалити картинку та вихід.

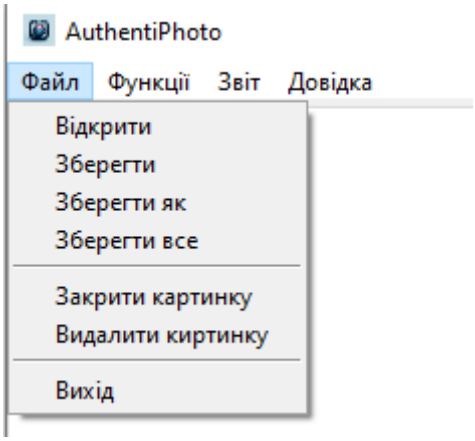


Рисунок. 3.6 - Меню Файл.

Код функції відкриття зображення має такий вигляд :

```
def open_new_images(self):
    image_paths = fd.askopenfilenames(filetypes=(("Images",
"*.jpeg;*.jpg;*.png"), ))
    for image_path in image_paths:
        self.add_new_image(image_path)
def add_new_image(self, image_path=None, image=None, load_from_bd =
None):
    if image is None and image_path is not None:
        image = Image.open(image_path)
    image_tab = Frame(self.image_tabs)
    image_info = ImageInfo(image, image_path, image_tab)
    self.opened_images.append(image_info)
    image_tab.rowconfigure(0, weight=1)
    image_tab.columnconfigure(0, weight=1)
    canvas = Canvas(image_tab, highlightthickness=0)
    canvas.grid(row=0, column=0, sticky='nsew')
    image_info.set_canvas(canvas)
    self.image_tabs.add(image_tab, text=image_info.filename())
    self.image_tabs.select(image_tab)
    if load_from_bd == None:
        self.update_image_status(image_path)
```

Після відкриття картинки, створиться вкладка з назвою картинки, де буде відображатись сама картинки (рис. 3.8.).

Рисунок. 3.8 - Відображення відкритої картинки у застосунку.

Для аналізу зображення було творено функції, у меню Функції (рис. 3.8.), такі як: конвертація, фільтр, обрізати, повернути, ELA та Metadata.

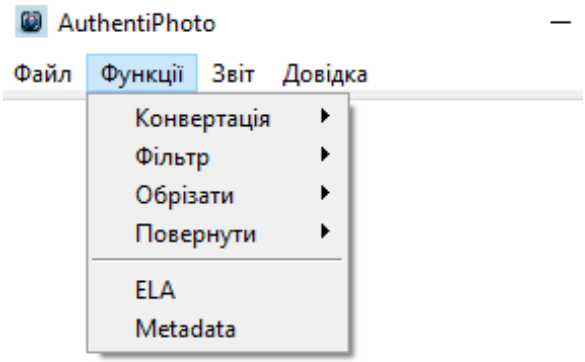


Рисунок. 3.8 - Меню Функції.

Для візуального аналізу було розроблено логіку зуму та переміщення картинки у програмі. Максимальний рівень приближення був обмежений, для

коректної роботи бібліотеки tkinter з пам’яттю та попередження помилок memory error, які можуть виникнути через великий зум.

```
def _zoomed_with_wheel(self, event):
        x = self.canvas.canvasx(event.x)
        y = self.canvas.canvasy(event.y)
        bbox = self.canvas.bbox(self.zoom_container)
        image_area = Rect(*bbox)
        if not (image_area.x0 < x < image_area.x1 and image_area.y0 < y < image_area.y1) : return
        scale = 1.0
        #       лінукс       він мак
        if event.num == 5 or event.delta == -120:
          i = min(self.image.width, self.image.height)
           if int(i * self.imscale) < 256: return
           self.imscale /= self.zoom_delta
           scale /= self.zoom_delta
        if event.num == 4 or event.delta == 120:
           if 2.5 < self.imscale:  # зум не більше
              return
           self.imscale *= self.zoom_delta
           scale *= self.zoom_delta
        self.canvas.scale('all', x, y, scale, scale)
        self._show_zoomed_image()
```

Аналіз рівня помилок (ELA, Error Level Analysis) – це методика, яка використовується для виявлення маніпуляцій з цифровими зображеннями. Вона базується на аналізі помилок, які виникають при повторному стисненні зображення у форматі JPEG. Ключова ідея полягає у тому, що при кожному стисненні JPEG зображення втрачає певну кількість даних через втратний характер стиснення. Внаслідок цього, різні частини зображення, які стискались різну кількість разів, будуть відрізнятися за рівнем помилок.

Принцип роботи ELA:

- Повторне стиснення: зображення зберігається знову у форматі JPEG з певним рівнем якості. Частини зображення, які раніше не зазнавали стиснення, після цього будуть стиснуті вперше і, таким чином, покажуть вищий рівень помилок стиснення. В той же час, частини, які були вже редаговані або стиснуті, втратять менше інформації при повторному стисненні, показуючи нижчий рівень помилок;
- Аналіз різниці: за допомогою програмного забезпечення порівнюється оригінальне зображення та його повторно стиснута версія. Результатом є зображення, яке відображає рівень помилок — чим більша різниця між двома версіями, тим більше помилок в тій області;
- Візуалізація: отримане зображення часто підсилюється за яскравістю або контрастом, щоб краще виділити області з високим рівнем помилок, що може вказувати на потенційні маніпуляції;

Також, слід зазначити що, ELA може давати помилкові позитивні результати, особливо у випадках, коли зображення має високий рівень шуму, або було стиснуте з дуже низькою якістю в оригіналі. Також важливо розуміти, що ELA не може точно вказати, що зображення було змінено, а лише показує потенційні області для подальшої перевірки.

Для аналізу рівня помилок було розроблену функцію яка створює, у директорії аналізованого фото, ELA зображення (рис. 3.9.) за алгоритмом:

```
def ela_analysis(self, quality):
    if self.path is None:
        raise ValueError("No file path provided for ELA analysis")
    directory = os.path.dirname(self.path)
    filename, ext = os.path.splitext(os.path.basename(self.path))
    temp_filename = os.path.join(directory, f"{filename}_temp{ext}")
    self.image.save(temp_filename, 'JPEG', quality=quality)
    temp_image = Image.open(temp_filename)
    ela_image = ImageChops.difference(self.image, temp_image)
```

```
            max_diff = max(extrema[1] for extrema in ela_image.getextrema())
            scale = 255.0 / max_diff
            ela_image = ImageEnhance.Brightness(ela_image).enhance(scale)
            counter = 0
            ela_image_path = os.path.join(directory, f"{filename}_ElaImage{ext}")
            while os.path.exists(ela_image_path):
                ela_image_path = os.path.join(directory,
f"{filename}_ElaImage{counter}{ext}")
                counter += 1
            ela_image.save(ela_image_path)
            os.remove(temp_filename)
            return ela_image_path
```

Рисунок. 3.9 - ELA зображення.

Для зручності аналізу, була написана функція фільтрів насичесності кольорів, контрасності, яскравості та різкості. Код застосування фільтру виглядає так:

```
        enhance_menu = Menu(func_menu, tearoff=0)
            enhance_menu.add_command(label="Колір", command=lambda:
self.enhance_current_image("Колір", ImageEnhance.Color))
            enhance_menu.add_command(label="Контраст", command=lambda:
```

```
self.enhance_current_image("Контраст", ImageEnhance.Contrast))
        enhance_menu.add_command(label="Яскравість", command=lambda:
self.enhance_current_image("Яскравість", ImageEnhance.Brightness))
        enhance_menu.add_command(label="Різкість", command=lambda:
self.enhance_current_image("Різкість", ImageEnhance.Sharpness))

    def enhance_current_image(self, name, enhance):
        image = self.current_image()
        if not image:
            return
        SliderWindow(self.root, name, enhance, image,
self.update_image_inside_app)

    def value_changed(self, value):
        image = self.enhancer.enhance(self.factor.get())
        self.image_info.set_image(image)
        self.image_info.update_image_on_canvas()
```

Для аналізу метаданих було створено функцію яка автоматично виводить дані з EXIF файлу. Код функції виведення метаданих:

```
    def get_metadata(self, image_path):
        image = Image.open(image_path)
        exifData = image.getexif()
        metadata = {}
        for tag_id in exifData:
            tag = TAGS.get(tag_id, tag_id)
            data = exifData.get(tag_id)
            if isinstance(data, bytes):
                try:
                    data = data.decode()
                except UnicodeDecodeError:
```

```
                data = data.decode('iso-8859-1')
            metadata[tag] = data
        return metadata
```

EXIF (Exchangeable Image File Format) – це стандарт для зберігання метаданих в зображеннях і аудіофайлах, які були створені цифровими камерами, смартфонами та іншими пристроями. Метадані – це додаткова інформація, яка додається до файлу зображення або аудіо і містить деталі про умови зйомки, налаштування камери та інші важливі параметри. EXIF-дані включають різноманітні типи інформації. Наприклад, технічні характеристики зображення, такі як дата і час зйомки, виробник і модель камери, а також використані налаштування камери (витримка, діафрагма, ISO, фокусна відстань тощо). Окрім цього, EXIF-дані можуть містити інформацію про саме зображення, зокрема його розміри (ширина і висота в пікселях), роздільну здатність і формат файлу. Також ці дані можуть включати геолокаційні дані, такі як широта і довгота місця зйомки, висота над рівнем моря та напрямок компасу. Важливою складовою EXIF-даних є і дані про авторські права, що можуть містити ім'я фотографа та інформацію про авторські права. EXIF-дані можуть допомагати виявляти фальсифікації зображень, адже зміни або видалення метаданих можуть вказувати на можливу маніпуляцію. Соціальні мережі та сервіси для обміну фотографіями також використовують геолокаційні дані для автоматичного додавання тегів з місцями зйомки, що полегшує ідентифікацію та організацію зображень. Вікно виведення метаданих має наступний вигляд (рис. 3.10.)

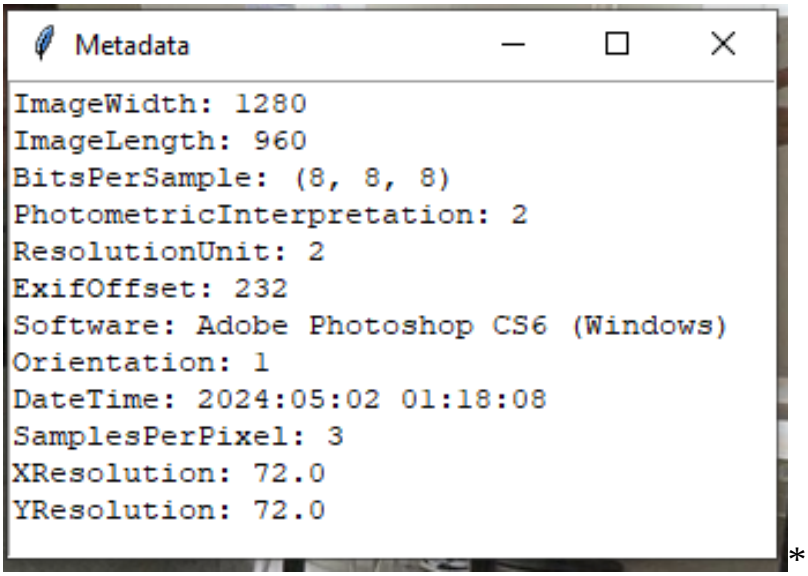


Рисунок. 3.10 - Вікно виведення метаданих.

Також, для зручного використання фільтрів та визначення ступеню стискання для аналізу рівня помилок, було створено додаткове вікно (рис.3.11.) SliderWindow.

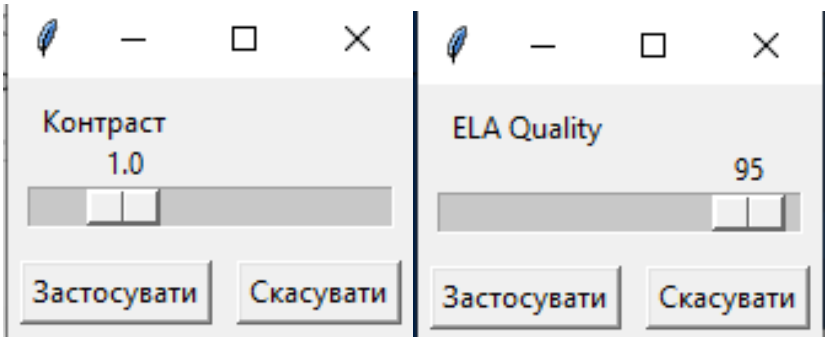


Рисунок. 3.11 - Вікно SliderWindow.

Вікно було запрограмовано адаптивним під різні функції. Для фільтрів діапазон значення є від 0.0 до 5.0 з шагом зміни значення у 0.1. Для ELA аналізу діапазон значень станговить від 0 до 100 з шагом у 1.

Для роботи з базою даних, було створено меню Звіт (рис. 3.12.), який має функції звітів для візуального аналізу, ELA аналізу, аналізу метаданих, та загального аналізу, також реалізована функція експорту звіту у форматі docx.

Вікно введення висновків ELA аналізу (рис. 3.13.) містить, назву фото файлу над яким проводиться аналіз, назву ELA зображення та поле введення тексту, також є три кнопки: ввести, скасувати та видалити, які виконують відповідні функції. Слід зазначити що, для застереження помилок та

невідповідних даних, ввести висновок до ELA аналізу можна лише за умови що у директорії, де знаходиться аналізуйме фото

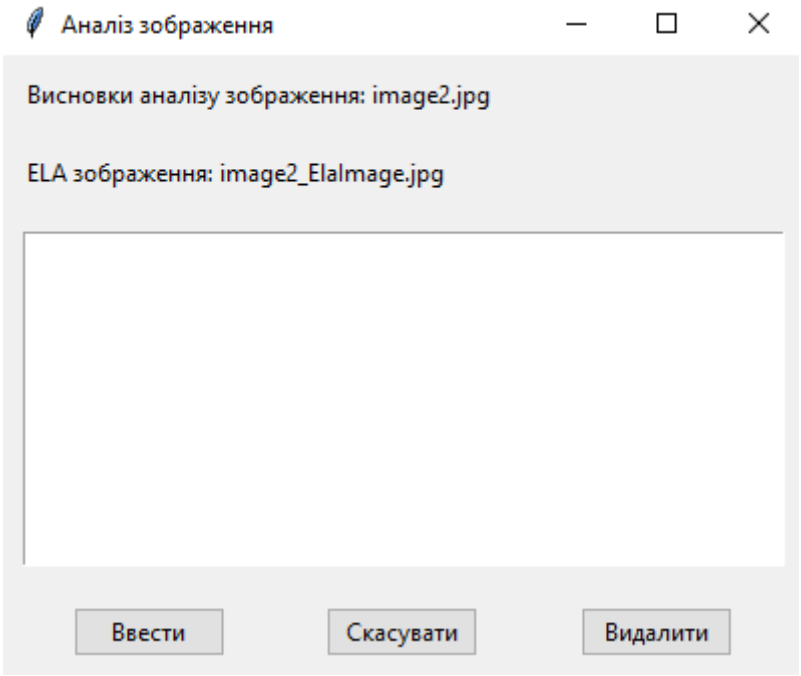


Рисунок. 3.13 - Вікно введення висновків ELA аналізу.

Вікно введення висновків візуального аналізу (рис. 3.14.) містить назву аналізуємого фото та поле введення тексту, аналогічно до попереднього вікна, має три кнопки.

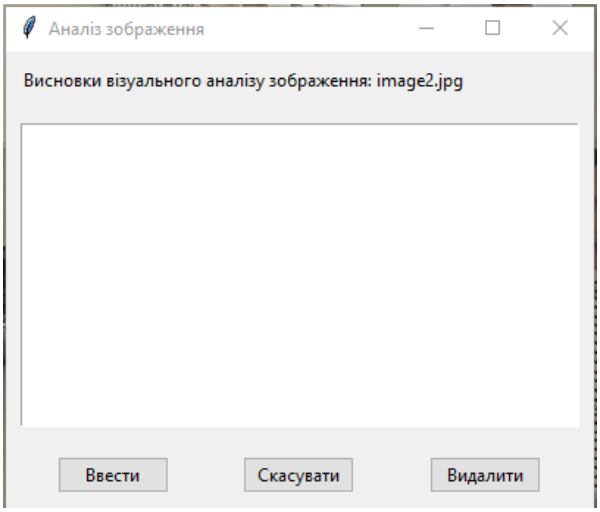


Рисунок. 3.14 - Вікно введення висновків візуального аналізу.

Вікно введення висновків аналізу метаданих (рис. 3.15.) містить назву аналізуємого фото, поле введення тексту, таблицю метаданих та кнопки введення, скасування та видалення. Таблиця метаданих заповнюється автоматично при натисканні кнопки Ввести. Якщо метаданих не буде виявлено,

то виведеться відповідна помилка і метадані не будуть введені.

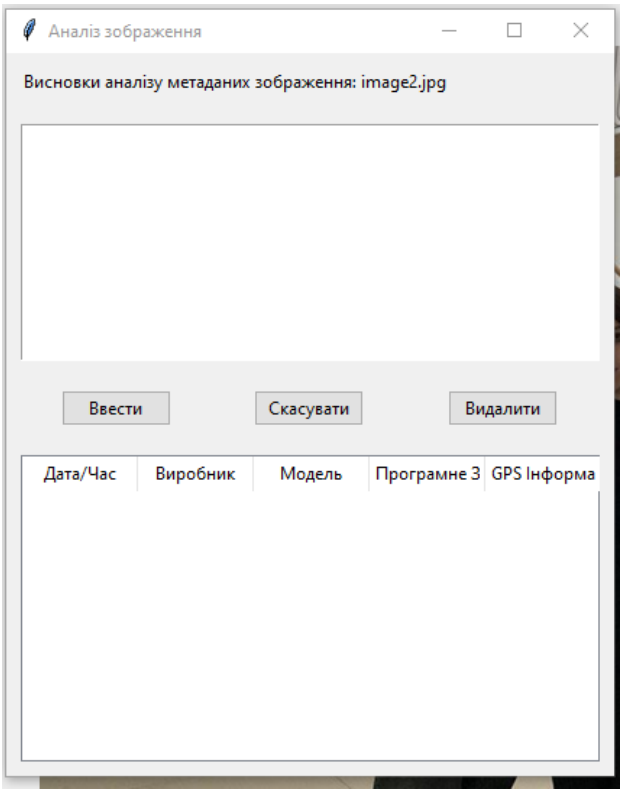


Рисунок. 3.15 - Вікно введення висновків візуального аналізу.

Вікно загального висновку аналізу (рис. 3.16.) містить містить назву аналізуємого фото, поле введення тексту, прапорець статусу редагування фото та кнопки видалення, введення, скасування.

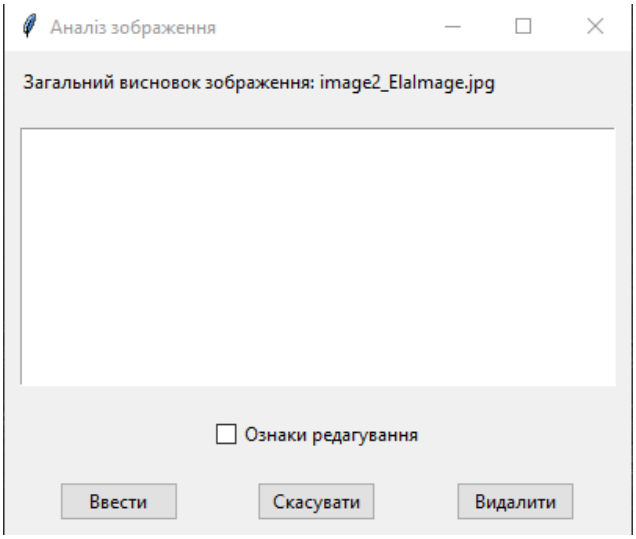


Рисунок. 3.16 - Вікно введення висновків візуального аналізу.

Вікно загального висновку є основним, та автоматично створюється при введенні будь якого з висновків вище. Також, при видаленні загального висновку, будуть видалені і всі інші висновки до цього фото (рис. 3.17.).

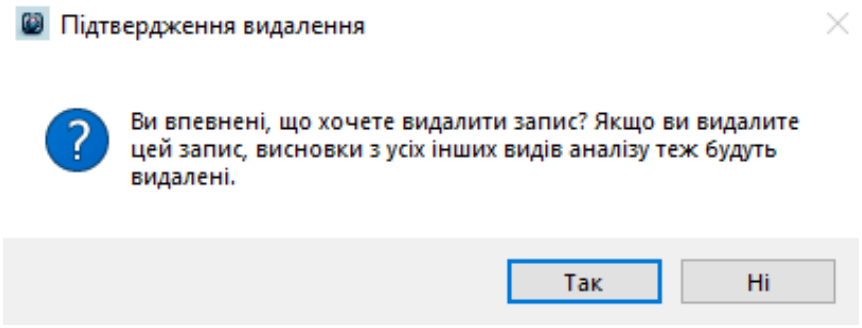


Рисунок. 3.17 - Повідомлення щодо видалення загального висновку.

При успішному введені даних до висновків, буде з’являтись повідомлення про успіх (рис. 3.18.).

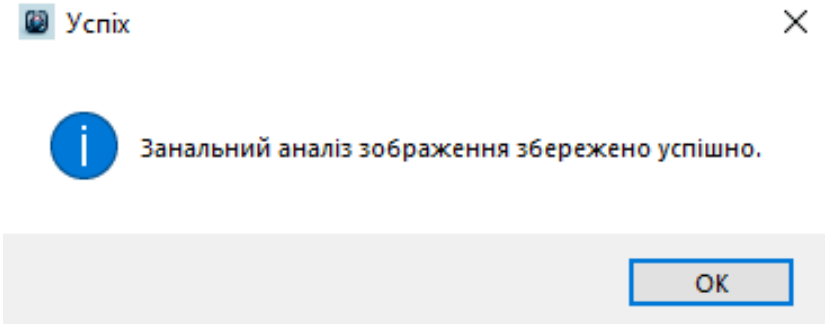


Рисунок. 3.18 - Повідомлення про успішне введення даних.

Будь які помилки при роботі з висновками будуть виводити повідомлення та детальний опис помилки.

Для експортування звіту, потрібно натиснути відповідну кнопку («Звіт» -> «Експортувати звіт») та обрати папку (рис. 3.19.), у якому буде збережений файл звіту.

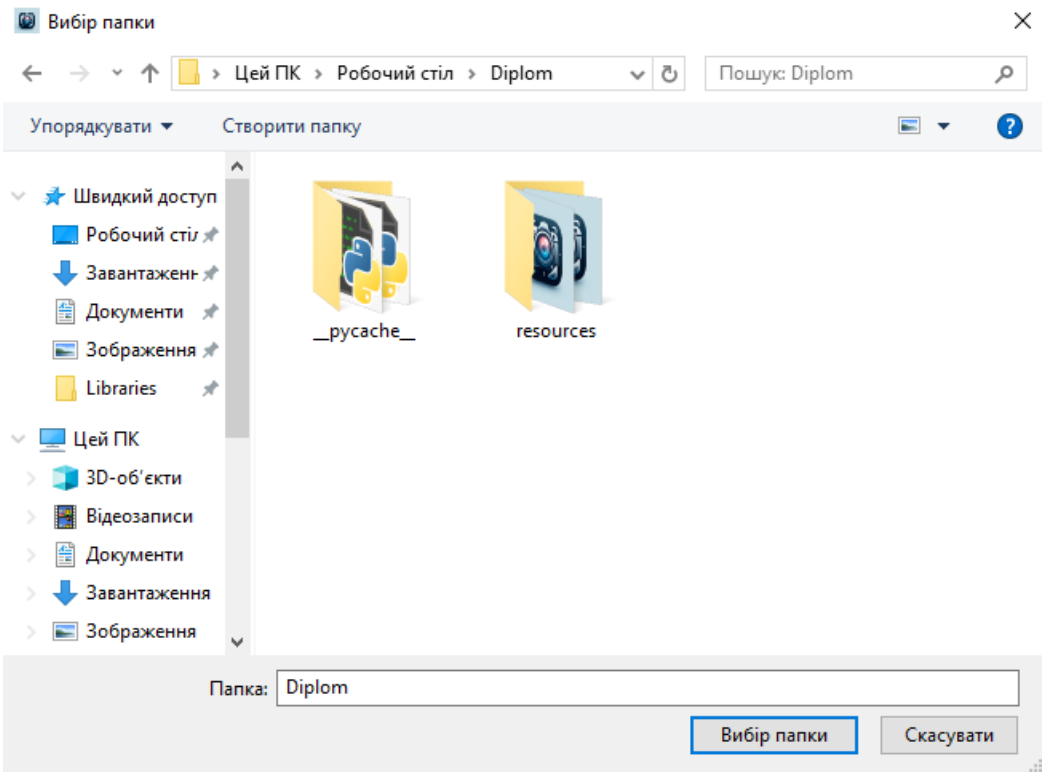


Рисунок. 3.19 - Вибір директорії збереження звіту.

Після успішного збереження, буде повідомлення що звіт збережено (рис. 3.20.).

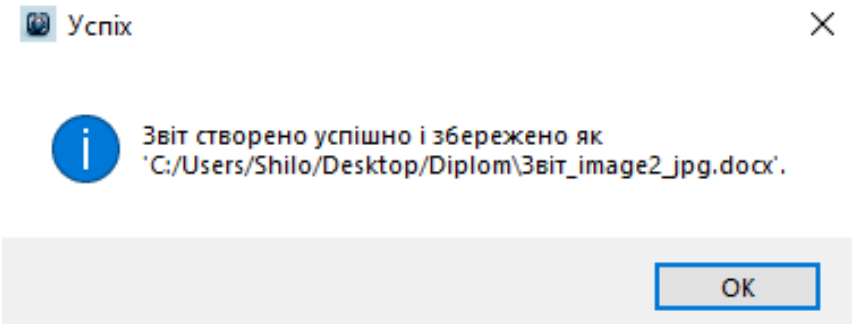
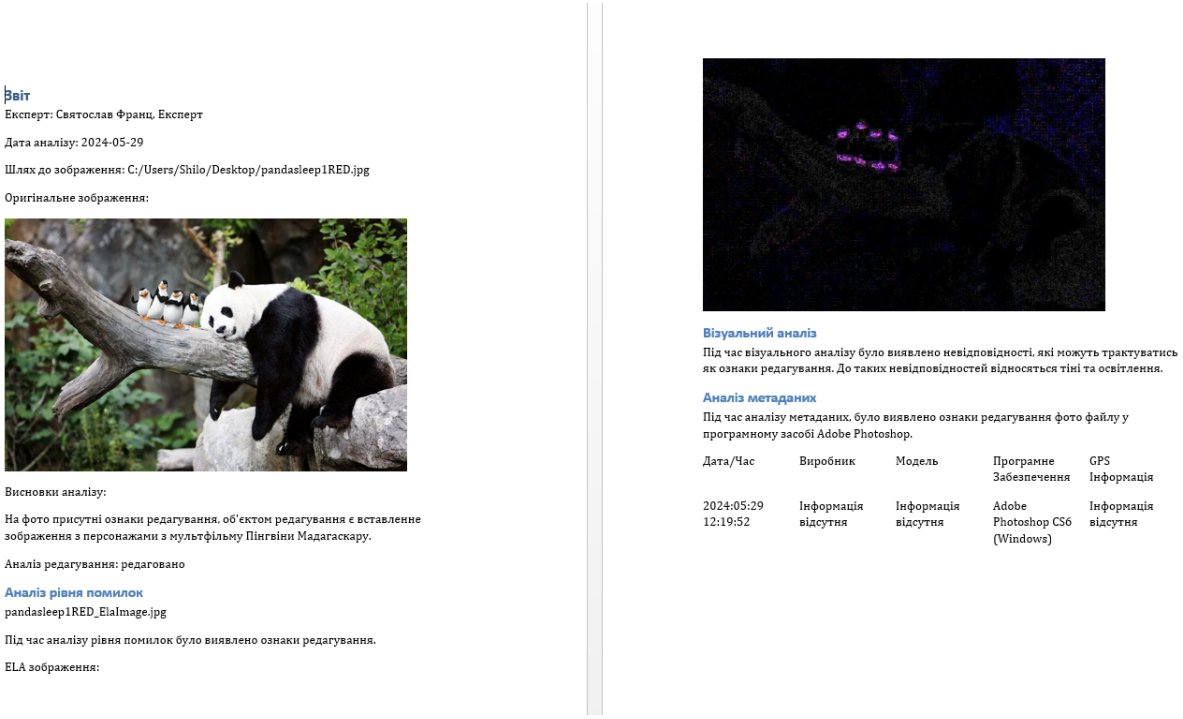


Рисунок. 3.20 - Повідомлення про успішне збереження звіту.

Експортований звіт має наступний вигляд (рис. 3.21.)



Звіт

Експерт: Святослав Франц, Експерт

Дата аналізу: 2024-05-29

Шлях до зображення: C:/Users/Shilo/Desktop/pandasleep1RED.jpg

Оригінальне зображення:

Висновки аналізу:

На фото присутні ознаки редагування, об'єктом редагування є вставленне зображення з персонажами з мультфільму Пінгвіни Мадагаскару.

Аналіз редагування: редаговано

Аналіз рівня помилок

pandasleep1RED_ElaImage.jpg

Під час аналізу рівня помилок було виявлено ознаки редагування.

ELA зображення:

Візуальний аналіз

Під час візуального аналізу було виявлено невідповідності, які можуть трактуватись як ознаки редагування. До таких невідповідностей відносяться тіні та освітлення.

Аналіз метаданих

Під час аналізу метаданих, було виявлено ознаки редагування фото файлу у програмному засобі Adobe Photoshop.

Дата/Час	Виробник	Модель	Програмне Забезпечення	GPS Інформація
2024:05:29 12:19:52	Інформація відсутня	Інформація відсутня	Adobe Photoshop CS6 (Windows)	Інформація відсутня

Рисунок. 3.21 - Експортований звіт.

Для зручності роботи з обліковими записами користувачів, було розроблено окремий додаток, який має функціонал додавання, редагування та видалення облікових записів користувачів (рис. 3.22). Цей додаток має використовуватись лише спеціальними працівниками, які будуть мати доступ до роботи з базами даних.

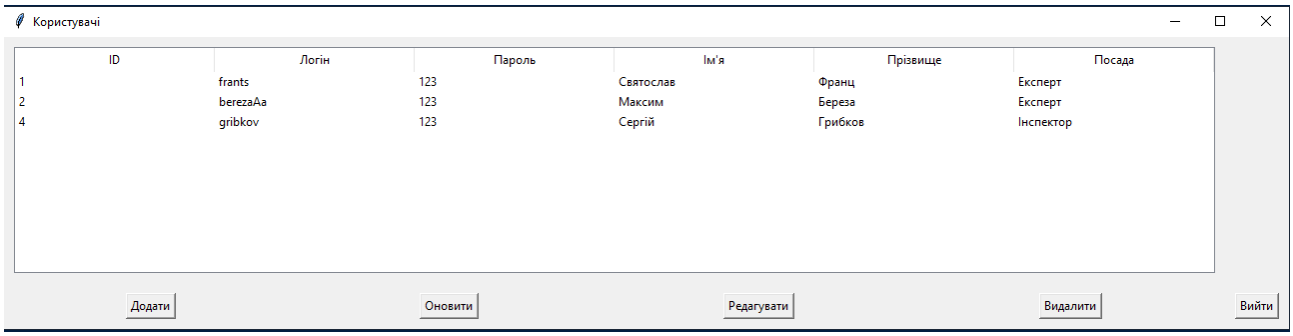


Рисунок. 3.22 – Вікно роботи з обліковими записами користувачів.

При внесенні будь яких змін у фото, накладання фільтрів, конвертації зображення, обрізання або повороту зображення, у вкладці зображення, після назви, буде мітка * (рисунок 3.23), яка слугує міткою незбережених змін, при збережені фото будь яким методом, мітка зникне.

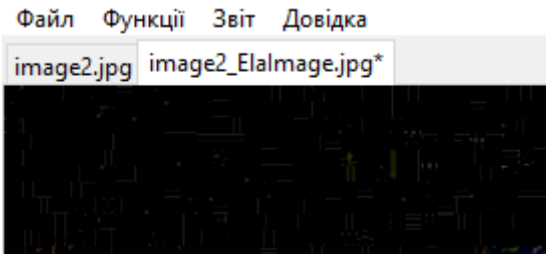


Рисунок. 3.23 – Мітка не збережених змін.

Якщо користувач закриє застосунок, а у відкритих зображеннях будуть незбережені зміни, то буде виведене повідомлення, про незбережені зміни (рисунок 3.24).

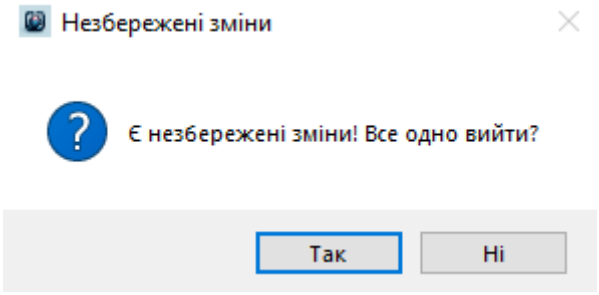


Рисунок. 3.24 – Мітка не збережених змін.

Також, була створена довідка користувача у застосунку. При натисканні кнопки «Довідка», відкривається нове вікно, де описані функції та інструкція користувача (рисунок 3.25)

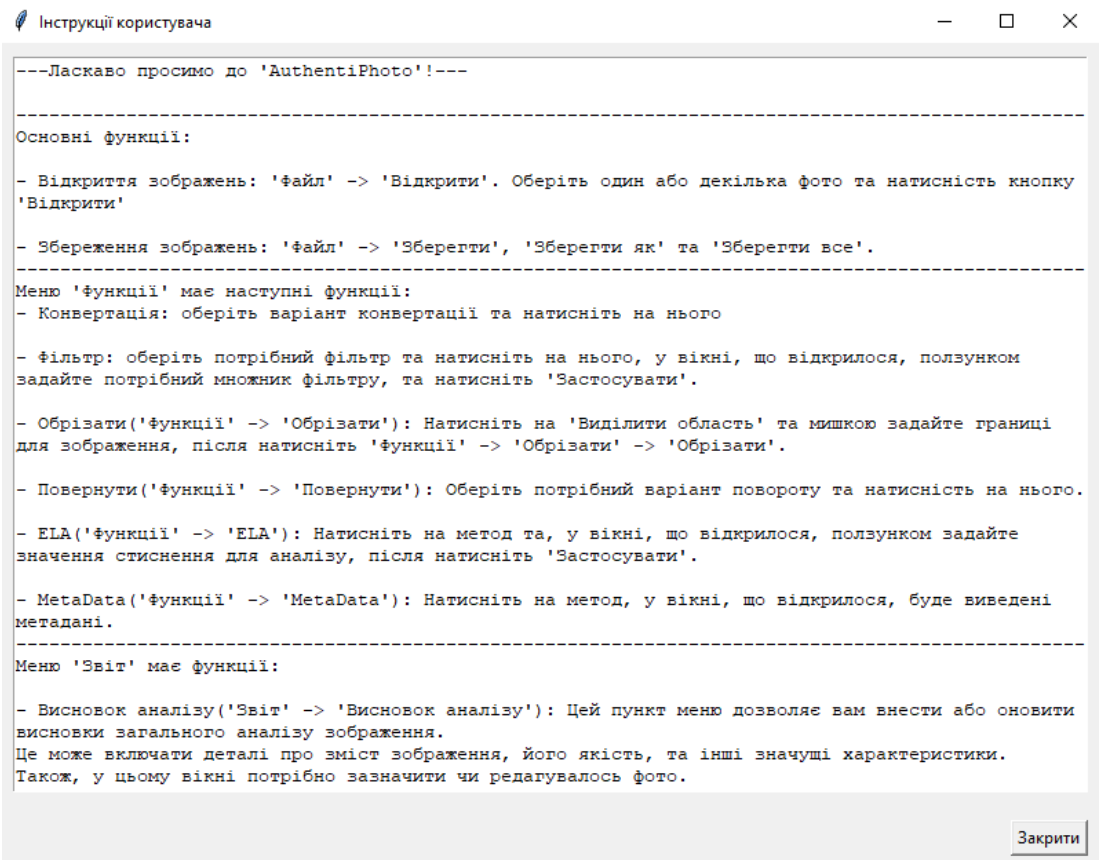


Рисунок. 3.25 – Вікно інструкції користувача.

3.3. Інструкція користувача

Меню Файл (рисунок 3.26):

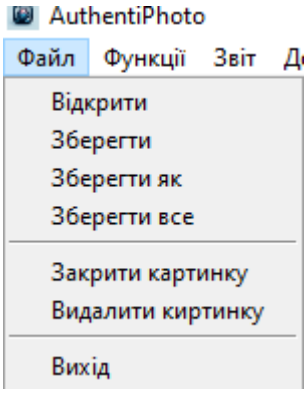


Рисунок. 3.26 – Меню Файл.

- Відкриття зображень: Перейдіть у меню 'Файл -> Відкрити. Оберіть одне або декілька фото та натисніть кнопку Відкрити.
- Збереження зображень: Перейдіть у меню Файл -> Зберегти, Зберегти як або Зберегти все.
- Закрити картинку: Перейдіть у меню Файл -> Закрити картинку

- Видалити картинку: Перейдіть у меню Файл -> Видалити картинку
- Для виходу з програми можна декількома способами:
  1. Файл -> Вихід
  2. Сполученням клавіш Alt + F4
  3. Натисканням крестику виходу у вікні

Меню Функції (рисунок 3.27):

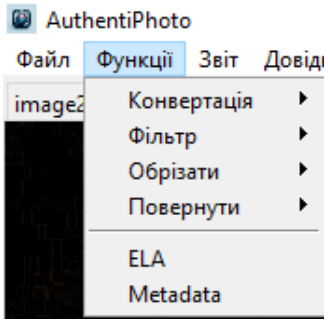


Рисунок. 3.27 – Меню Функції.

- Конвертація: Оберіть варіант конвертації та натисніть на нього.
- Фільтр: Оберіть потрібний фільтр та натисніть на нього. У вікні, що відкрилося, ползунком задайте потрібний множник фільтру, та натисніть Застосувати.
- Обрізати (Функції -> Обрізати): Натисніть на Виділити область та мишкою задайте границі для зображення, після натисніть Функції -> Обрізати -> Обрізати.
- Повернути (Функції -> Повернути): Оберіть потрібний варіант повороту та натисніть на нього.
- ELA (Функції -> ELA): Натисніть на метод та, у вікні, що відкрилося, ползунком задайте значення стиснення для аналізу, після натисніть Застосувати.
- MetaData (Функції -> MetaData): Натисніть на метод, у вікні, що відкрилося, буде виведено метадані.

Меню Звіт (рисунок 3.28):

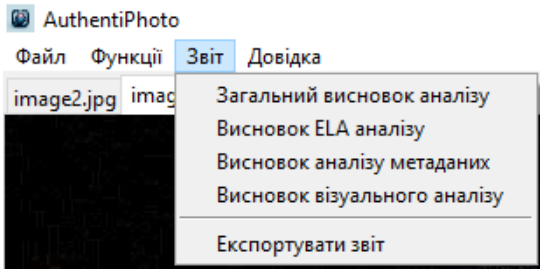


Рисунок. 3.28 – Меню Звіт.

- Висновок аналізу (Звіт -> Висновок аналізу): Дозволяє внести або оновити висновки загального аналізу зображення. Це може включати деталі про зміст зображення, його якість та інші значущі характеристики. У цьому вікні потрібно зазначити, чи редагувалось фото.
- Висновок ELA аналізу (Звіт -> Висновок ELA аналізу): Висновок ELA аналізу можна зробити лише після створення ELA зображення (Функції -> ELA). Цей пункт дозволяє записувати висновки про результати ELA аналізу, які можуть вказувати на потенційні маніпуляції з зображенням.
- Висновок аналізу метаданих (Звіт -> Висновок аналізу метаданих): У цьому пункті вводиться висновок аналізу метаданих зображення.
- Висновок візуального аналізу (Звіт -> Висновок візуального аналізу): Дозволяє записати висновки візуального аналізу.
- Експортувати звіт (Звіт -> Експортувати звіт): Після завершення внесення даних аналізу можна сформувати Word документ, який автоматично створиться у обраній директорії.

Важливо:

- До однієї фотографії можна зробити лише один висновок кожного виду аналізу.
- Якщо висновок вже зроблений та збережений, наступні введення будуть оновлювати висновок.
- Назва зображень не має змінюватись під час написання висновків.
- Для збереження висновків потрібно натискати виключно Ввести. Якщо ввести дані та просто закрити вікно, дані збережені не будуть.
- Переконайтеся, що перед закриттям програми збережено всі зміни.

РОЗДІЛ 4. ОХОРОНА ПРАЦІ

В даному розділі розглядаються питання охорони праці та техніки безпеки, які необхідно враховувати при розробці та впровадженні програмного забезпечення для інтернет-магазину молочної продукції. Забезпечення безпечних умов праці є невід'ємною частиною успішної роботи підприємства, оскільки це допомагає запобігти нещасним випадкам та знизити ризики для здоров'я працівників.

4.1 Організація охорони праці

При використанні програмного модуля для аналізу автентичності фото файлів у кіберполіції повинна бути організована система охорони праці, яка включає в себе:

- проведення інструктажів з техніки безпеки для всіх працівників: інструктажі мають проводитися регулярно та охоплювати всі аспекти безпечної роботи з програмним модулем, включаючи основи роботи з комп'ютерною технікою та правила використання системи;
- регулярне проведення навчальних занять та тренінгів з питань охорони праці: це дозволяє постійно підвищувати рівень обізнаності працівників щодо можливих ризиків, пов'язаних з використанням програмного забезпечення, та методів їх уникнення. Працівники повинні бути ознайомлені з процедурами безпечного аналізу фото файлів та захисту даних;
- розробка та впровадження заходів для зниження ризиків при роботі з програмним модулем: важливо впроваджувати інноваційні рішення для захисту даних, запобігання втраті інформації та забезпечення безпеки працівників під час роботи з фото файлами;
- забезпечення працівників необхідними засобами індивідуального захисту: для роботи з комп'ютерною технікою це може включати ергономічні засоби, такі як підставки для зап'ясть, спеціальні стільці для комфортної роботи;

Організація охорони праці при використанні програмного модуля для

аналізу автентичності фото файлів допоможе забезпечити безпеку та здоров'я працівників, а також запобігти можливим ризикам та проблемам, пов'язаним з використанням системи.

4.2 Техніка безпеки при роботі з комп'ютерним обладнанням

Для працівників кіберполіції, які працюють з програмним модулем для аналізу автентичності фото файлів, необхідно забезпечити наступні умови:

- зручні робочі місця з ергономічними стільцями та столами: це допоможе уникнути проблем зі спиною та зменшити стомлюваність під час тривалого використання комп'ютерів. Ергономічні стільці та столи повинні бути регульованими для забезпечення оптимальної посадки та підтримки тіла;
- відповідне освітлення робочого місця: освітлення повинно бути оптимальним для запобігання перевтомі очей. Рекомендується м'яке та рівномірне освітлення, яке не створює блисків на моніторах та не спричиняє додаткове навантаження на зір;
- дотримання правил користування комп'ютерною технікою: важливо забезпечити регулярні перерви для відпочинку, щоб уникнути перевтоми та зниження продуктивності. Рекомендується кожні 1-2 години робити короткі перерви, протягом яких працівники можуть відпочити від екрану;
- захист від електромагнітного випромінювання: використання захисних екранів-фільтрів та відповідних налаштувань моніторів допоможе зменшити негативний вплив електромагнітного випромінювання на здоров'я працівників. Це включає оптимальну яскравість та контрастність моніторів, а також розташування робочого місця для мінімізації впливу випромінювання;

Забезпечення цих умов допоможе покращити здоров'я та добробут працівників, а також підвищити їх продуктивність і ефективність під час використання програмного модуля для аналізу автентичності фото файлів.

4.3 Пожежна безпека

З метою забезпечення пожежної безпеки в приміщеннях, де використовується програмний модуль для аналізу автентичності фото файлів,

необхідно:

- оснащення приміщень первинними засобами пожежогасіння: приміщення повинні бути обладнані вогнегасниками, пожежними кранами та іншими засобами пожежогасіння. Вогнегасники повинні бути доступними в кожному приміщенні, де використовується комп'ютерна техніка.
- забезпечення наявності вільних шляхів евакуації та їх правильне маркування: важливо, щоб всі працівники знали розташування евакуаційних виходів та мали доступ до них у разі надзвичайної ситуації. Евакуаційні шляхи повинні бути вільними від перешкод та належним чином позначеними.
- проведення регулярних навчань з евакуації у разі пожежі: регулярні тренування дозволять працівникам діяти швидко та впевнено під час надзвичайних ситуацій, забезпечуючи їх безпеку. Навчання має включати інструктажі щодо правильних дій у разі пожежі та практичні заняття з евакуації.
- установка пожежної сигналізації та систем автоматичного пожежогасіння: для підвищення рівня безпеки приміщення повинні бути обладнані сучасними системами пожежної сигналізації та автоматичного пожежогасіння. Це дозволить швидко виявляти пожежу та оперативно реагувати на загрозу.

Дотримання цих заходів допоможе забезпечити пожежну безпеку працівників та приміщень, де використовується програмний модуль для аналізу автентичності фото файлів, а також мінімізувати ризики виникнення та поширення пожежі.

4.4 Електробезпека

Забезпечення електробезпеки в приміщеннях, де використовується програмний модуль для аналізу автентичності фото файлів, включає:

- використання електрообладнання відповідно до вимог нормативних документів: Всі електроприлади, що використовуються в процесі аналізу, повинні відповідати стандартам безпеки та мати відповідні сертифікати;

- регулярну перевірку та технічне обслуговування електричних мереж та пристроїв: Це допоможе уникнути коротких замикань та інших електричних аварій. Регулярні перевірки дозволять своєчасно виявляти та усувати потенційно небезпечні несправності;
- забезпечення працівників інструкціями з безпечного користування електроприладами: Інструкції повинні бути чіткими та доступними для розуміння, містити основні правила безпеки при роботі з електрообладнанням та поради щодо дій у разі аварійної ситуації;
- встановлення захисного заземлення та пристроїв захисного вимкнення: Це забезпечить додатковий рівень захисту від ураження електричним струмом. Захисне заземлення та пристрої захисного вимкнення повинні бути встановлені відповідно до вимог безпеки та регулярно перевірятися на працездатність;

Дотримання цих заходів допоможе забезпечити безпеку працівників під час роботи з електрообладнанням та програмним модулем для аналізу автентичності фото файлів, а також запобігти можливим електричним аваріям.

4.5 Психофізіологічний комфорт працівників

Для підтримання психофізіологічного комфорту працівників Кіберполіції, які працюють з програмним модулем для аналізу автентичності фото файлів, необхідно:

- організація перерв для відпочинку та розслаблення: це може включати облаштування кімнат для відпочинку з комфортними умовами, де працівники можуть відпочити від роботи, розслабитися та відновити свої сили;
- створення сприятливого психологічного клімату в колективі: важливо підтримувати позитивну атмосферу та взаємоповагу між працівниками. Сприятливий психологічний клімат допомагає зменшити стрес та підвищити ефективність роботи;
- забезпечення можливості фізичних вправ протягом робочого дня: працівникам слід надавати можливість займатися фізкультурою або

робити прості вправи для розслаблення. Це може включати організацію коротких фізичних активностей або встановлення зон для вправ у приміщенні;

Дотримання цих заходів допоможе підтримати психофізіологічний комфорт працівників, що, в свою чергу, сприятиме підвищенню їхньої продуктивності та загального задоволення роботою.

4.6 Впровадження заходів для зменшення стресу

Зменшення стресу є важливою складовою охорони праці для працівників кіберполіції, які працюють з програмним модулем для аналізу автентичності фото файлів. Для цього необхідно:

- організація тренінгів з управління стресом: це допоможе працівникам навчитися справлятися зі стресовими ситуаціями, які можуть виникати під час роботи з кіберзлочинами та аналізу фото файлів. Тренінги можуть включати техніки релаксації, дихальні вправи та методи ефективного управління часом;
- проведення командоутворюючих заходів: це сприяє зміцненню колективу та покращенню взаємодії між працівниками. Командні заходи допомагають створити позитивну робочу атмосферу та підвищити рівень довіри між колегами;
- надання психологічної підтримки: працівники повинні мати доступ до консультацій психологів за потреби. Психологічна підтримка може включати індивідуальні або групові сесії, де працівники можуть обговорити свої проблеми та отримати професійну допомогу;

Дотримання цих заходів допоможе зменшити рівень стресу серед працівників, підвищити їхню продуктивність та забезпечити комфортні умови праці під час використання програмного модуля для аналізу автентичності фото файлів.

ВИСНОВКИ

У кваліфікаційній роботі був успішно створений програмний модуль для аналізу автентичності фото файлів, призначений для використання кіберполіцією. Всі поставлені задачі, визначені у технічному завданні, були повністю виконані. Розроблений модуль демонструє високу ефективність та надійність у виявленні фальсифікацій, аналізі метаданих та проведенні візуального аналізу зображень, що значно покращує процес розслідування кіберзлочинів.

У процесі розробки програмного модуля були враховані всі вимоги, встановлені у технічному завданні, та забезпечено їх повне виконання. Була створена логічна та фізична моделі бази даних, розроблені необхідні інтерфейси та функціональні можливості модуля.

Також було проведено ретельне тестування програмного модуля перед впровадженням в експлуатацію, що дозволило виявити та виправити всі помилки та недоліки. Результатом є функціональний і стабільний модуль, який відповідає всім поставленим вимогам і задовольняє потреби користувачів.

Отже, у кваліфікаційній роботі реалізовано програмний модуль для аналізу автентичності фото файлів, який може бути використаний кіберполіцією для підвищення ефективності розслідування кіберзлочинів. Результати дослідження та розробки можуть бути використані для покращення організації роботи кіберполіції та забезпечення надійного аналізу автентичності зображень.

БІБЛІОГРАФІЧНИЙ СПИСОК

1. Кіберполіція України // wikipedia. URL: https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%BF%D0%BE%D0%BB%D1%96%D1%86%D1%96%D1%8F_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8#cite_note-2 (дата звернення: 27.05.24).
2. Про утворення територіального органу Національної поліції: Постанова Кабінету Міністрів України від 13.10.2015 № 831 // Урядовий кур'єр 2015 — № 195 С. 1.
3. Кіберполіція отримала 194 одиниці спеціального обладнання для протидії кіберзагрозам // Урядовий портал. URL: https://www.kmu.gov.ua/news/250149450 (дата звернення: 27.05.24).
4. Демедюк С. В. ДОСВІД РОБОТИ ТА МІЖНАРОДНОЇ СПІВПРАЦІ КІБЕРПОЛІЦІЇ УКРАЇНИ. *Сучасні проблеми правового, економічного та соціального розвитку держави.* : наук. конф., м. Харків, 30 листоп. 2018 р. Харків, 2018. С. 124–127.
5. Управління ІТ проектами [Електронний ресурс] : методичні рекомендації до самостійної роботи для здобувачів освітнього ступеня «Бакалавр» спеціальності 122 «Комп’ютерні науки» освітньо-професійних програм «Комп’ютерні науки» та «Інформаційні системи та штучний інтелект» денної та заочної форм навчання ⁄ укладачі : С. В. Грибков, О. Л. Сєдих ; Національний університет харчових технологій. – Київ : НУХТ, 2022 – 25 с.– № 51.64.
6. Управління ІТ проектами [Електронний ресурс]: лабораторний практикум для студентів напряму підготовки 6.050101 "Комп'ютерні науки" денної та заочної форм навч. / уклад. О. А. Хлобистова, М. В. Гладка. - К. : НУХТ, 2013. – 108 с.. URL: http://library.nuft.edu.ua/ebook/file/51.07A.pdf.

7. Управління ІТ проектами [Електронний ресурс]: методичні рекомендації до виконання курсової роботи для студентів напряму підготовки 6.050101 «Комп’ютерні науки» денної та заочної форм навч. / уклад. М. В. Гладка,О. А. Хлобистова. – К. : НУХТ, 2014.– 91 с.. URL: http://library.nuft.edu.ua/ebook/file/51.13.pdf.

8. Проектування інформаційних систем [Електронний ресурс]: конспект лекцій для студентів освітнього ступеня «Бакалавр» спеціальності 122 «Комп’ютерні науки» денної та заочної форм навчання. Уклад.: О. М. М’якшило, О. В. Харкянен: НУХТ, 2018. – 47 с.

9. Проектування інформаційних систем. [Електронний ресурс]: лабораторний практикум для студ. освітнього ступеню "бакалавр" спец. 122 “Комп'ютерні 99 науки ” денної і заочної форм навчання.Частина 1 / Уклад.: О.М. М’якшило, О.В. Харкянен – К.: НУХТ, 2017 – 33 с.

10. Проектування інформаційних систем. [Електронний ресурс]: лабораторний практикум для студ. освітнього ступеню "бакалавр" спец. 122 “Комп'ютерні науки ” денної і заочної форм навчання.Частина 2 "Проектування клієнтського додатку" / Уклад.: О.М. М’якшило, О.В. Харкянен – К.: НУХТ, 2017 – 33 с.

11. Проектування інформаційних систем [Електронний ресурс]: методичні рекомендації до виконання курсового проекту для студентів освітнього ступеня «Бакалавр» спеціальності 122 «Комп’ютерні науки» денної та заочної форм навчання./Уклад.: О. М. М’якшило, О. В. Харкянен: НУХТ, 2018. – 24 с.

12. Кіберполіція. Національна Поліція України : вебсайт. URL: https://cyberpolice.gov.ua/ (дата звернення: 27.05.24).

13. Офіційна сторінка python: вебсайт. URL: https://www.python.org (дата звернення: 27.05.24).

14. Документація до бібліотеки tkinter: вебсайт. URL:

https://docs.python.org/uk/3/library/tkinter.html (дата звернення: 27.05.24).

15. Документація до бібліотеки Pillow : вебсайт. URL: https://pillow.readthedocs.io/en/stable/ (дата звернення: 27.05.24).
16. Документація до бібліотеки pyodbc : вебсайт. URL: https://github.com/mkleehammer/pyodbc/wiki (дата звернення: 27.05.24).
17. Нотація BPMN PostgreSQL [Електронний ресурс] – Режим доступу до ресурсу: https://iampm.club/ua/blog/shho-take-bpmn-diagrama-i-navishho-vona-potribna-z-prikladami-2/
18. Побудова бізнес-процесів за допомогою Bizagi PostgreSQL [Електронний ресурс] – Режим доступу до ресурсу: https://www.ba.in.ua/2022/11/25/typovi-pomylky-pry-modelyuvanni-biznes-proczesiv-v-notacziyi-bpmn-ch-1/
19. М'якшило О.М. CASE-технології у проектуванні інформаційних систем: електронний навчальний посібник для студ. вищих навч. закладів / О.М. М'якшило, Л.Г. Загоровська,– К.: НУХТ, 2017. – 190 с.
20. ДСТУ ISO/IEC/IEEE 12207:2018. Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення. [Чинний від 15.08.2018].
21. ДСТУ ISO/IEC/IEEE 29119-1:2017. Інженерія систем і програмних засобів. Тестування програмних засобів. Частина 1 Поняття та визначення (ISO/IEC/IEEE 29119-1:2013, IDT). [Чинний від 01.01.2019].
22. ДСТУ ISO/IEC 29155-1:2015. Розроблення систем і програмного забезпечення. Платформи для тестування проектів з розроблення інформаційних систем. Частина 1. Концепції та визначення. [Чинний від 01.01.2019].
23. ДСТУ ISO/IEC 12207:2016. Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення. [Чинний від 01.01.2018].

24. Кожевніков О. А. ДОСЛІДЖЕННЯ ЦИФРОВИХ ФОТОЗОБРАЖЕНЬ З МЕТОЮ ВИЯВЛЕННЯ ОЗНАК МОНТАЖУ. Актуальні питання досудового розслідування та тенденції розвитку криміналістичної методики : наук. конф., м. Харків, 21 листоп. 2018 р. Харків, 2018. С. 91–93.

25. Державні санітарні норми виробничого шуму, ультразвуку та інфразвуку [Електронний ресурс]: ДСН 2.3.6.037-99, затверджені постановою Головного державного санітарного лікаря України від 01.12.99 р. № 37 URL: https://ips.ligazakon.net/ document/view/MOZ641?ed=1999_12_01.

ДОДАТКИ

Додаток А. Фізична модель БД

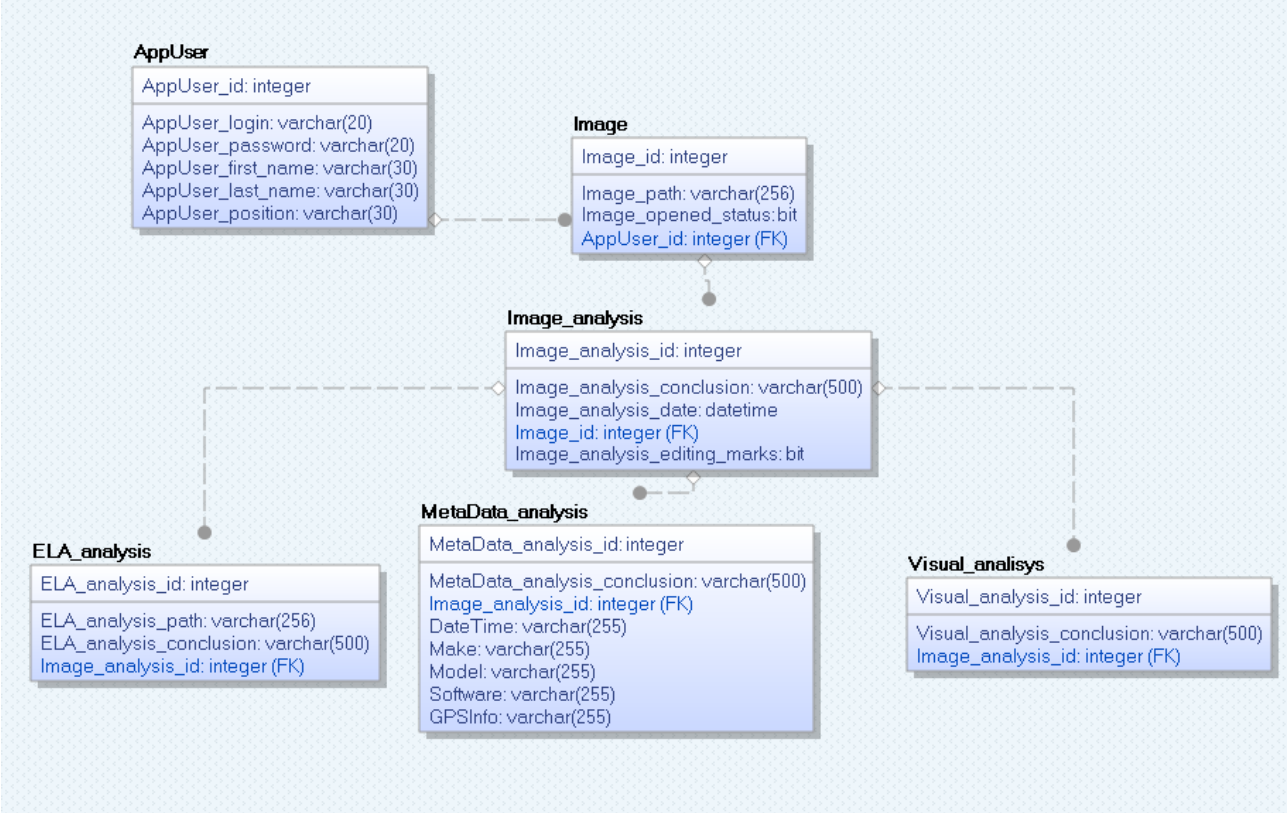


Рисунок А.1 - Фізична модель БД

Додаток Б. Функціональна модель процесу аналізу фото файлу

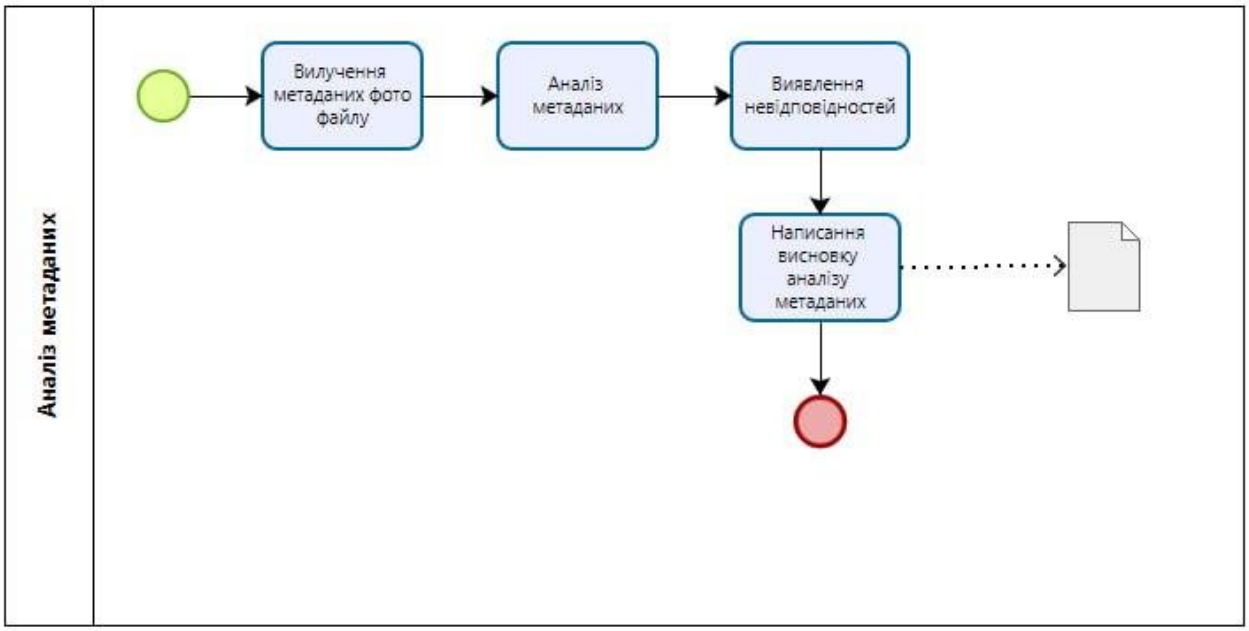


Рисунок Б.1 – Функціональна модель аналізу метаданих фото файлу

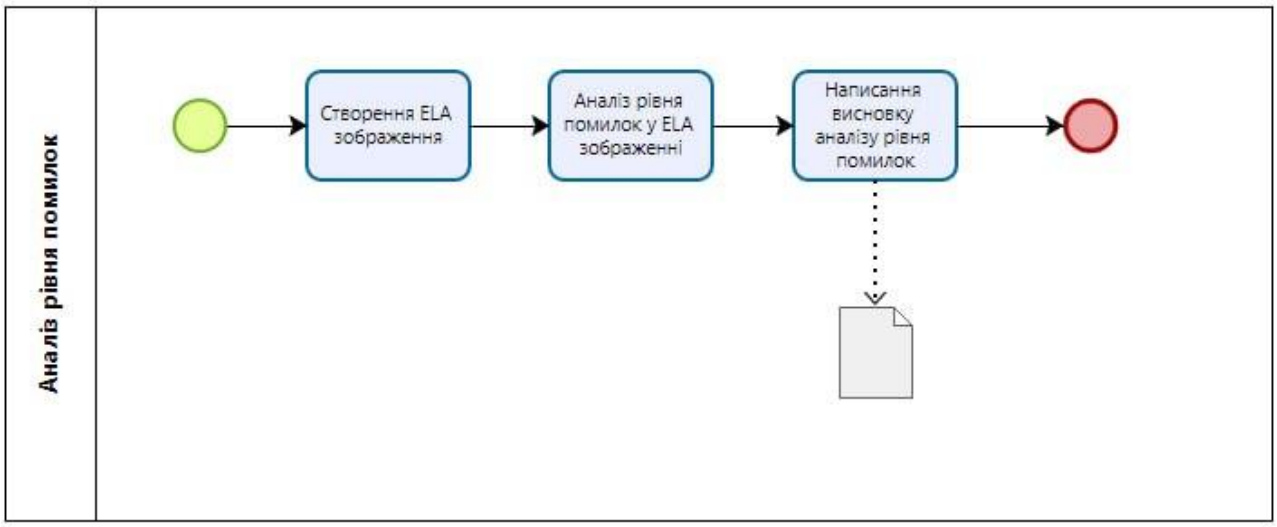


Рисунок Б.2 – Функціональна модель аналізу рівня помилок фото файлу

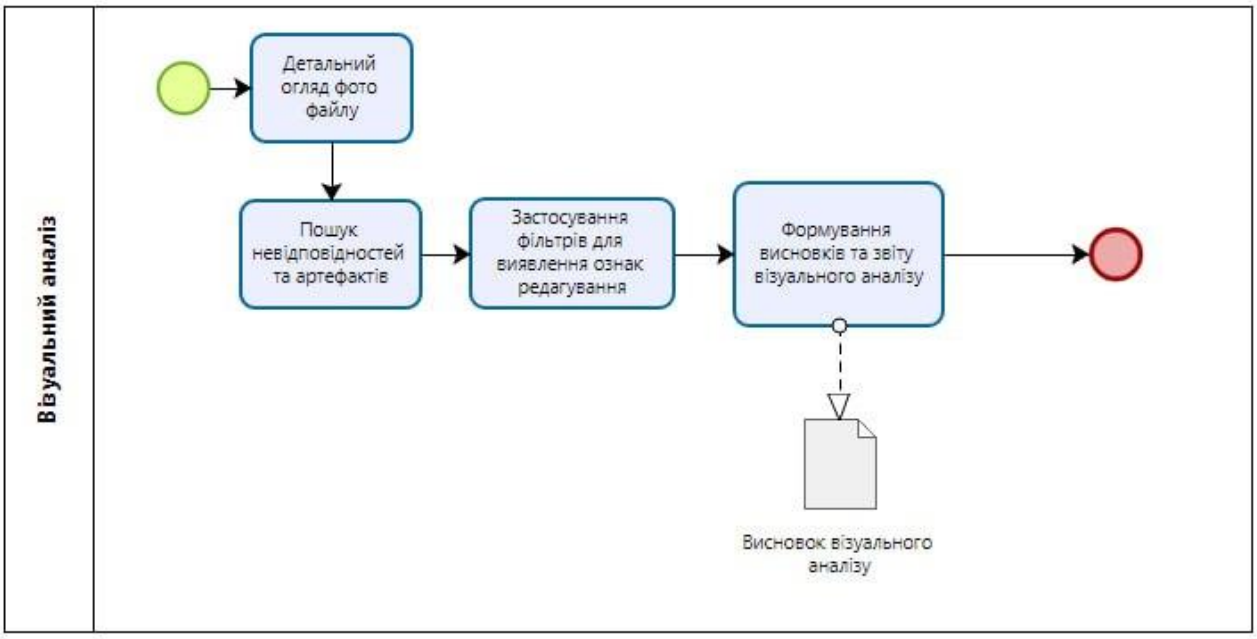


Рисунок Б.3 – Функціональна модель візуального аналізу фото файлу

Додаток В. Код вікна авторизації

```
def authenticate_user():
    user_id = None
    def on_login_clicked():
        nonlocal user_id
        username = username_entry.get()
        password = password_entry.get()
        if username and password:
            try:
                connection = pyodbc.connect('DRIVER={ODBC Driver 17 for SQL Server};SERVER=DESKTOP-BEJ89H1;DATABASE=Diplom;Trusted_Connection=yes;')
                cursor = connection.cursor()
                cursor.execute("SELECT AppUser_id FROM AppUser WHERE AppUser_login = ? AND AppUser_password = ?", (username, password))
                user_id = cursor.fetchone()
                cursor.close()
                connection.close()
                if user_id:
                    root.destroy()
                    return user_id[0]  # Повертає ID користувача
                else:
                    mb.showerror("Помилка аунтентифікації", "Логін чи пароль невірні")
            except Exception as e:
                mb.showerror("Помилка", f"Сталася помилка під час підключення до бази даних: {e}")
        else:
            mb.showerror("Помилка вводу", "Будь ласка, введіть ім'я користувача та пароль")
```

```
    root = tk.Tk()
    root.title("Вікно авторизації")
    root.geometry("300x150")
    frame = ttk.Frame(root)
    frame.pack(padx=10, pady=10, fill='x', expand=True)
    username_label = ttk.Label(frame, text="Ім'я користувача:")
    username_label.pack(fill='x', expand=True)
    username_entry = ttk.Entry(frame)
    username_entry.pack(fill='x', expand=True)
    username_entry.focus()
    password_label = ttk.Label(frame, text="Пароль:")
    password_label.pack(fill='x', expand=True)
    password_entry = ttk.Entry(frame, show="*")
    password_entry.pack(fill='x', expand=True)
    login_button = ttk.Button(frame, text="Увійти", command=on_login_clicked)
    login_button.pack(fill='x', expand=True, pady=10)
    root.mainloop()
    if 'user_id' in locals():
        return user_id[0]
    else: # Якщо ID користувача не визначено після закриття root, повертаємо
None
        return None
```