

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

**Навчально-науковий інститут телекомунікаційних систем
Кафедра: Інформаційних технологій в телекомунікаціях**

«На правах рукопису»
УДК 004.02

«До захисту допущено»
Завідувач кафедри
Марія СКУЛИШ
“ ” 2025 р.

Магістерська дисертація

зі спеціальності 172 Електронні комунікації та радіотехніка
на тему: Удосконалений метод виявлення та захисту приватних відеоданих

Виконала: студентка VI курсу, групи ЦІ-41мп,
Солоденко Марія Андріївна

(підпис)

Науковий керівник:
Старший викладач кафедри ІТТ НН ІТС, кандидат технічних наук
Педан Станіслав Ігорович

(підпис)

Рецензент:
Доцент кафедри ІБ НН ФТІ, доктор технічних наук
Прогонов Дмитро Олександрович

(підпис)

Засвідчую, що у цій магістерській
дисертації немає запозичень з праць
інших авторів без відповідних посилань.
Студентка _____

Київ – 2025 року

**Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»**

**Навчально-науковий інститут телекомунікаційних систем
Кафедра: Інформаційних технологій в телекомунікаціях**

Рівень вищої освіти – другий магістерський за освітньо-професійною програмою Інформаційно-комунікаційні технології
Спеціальність – 172 Електронні комунікації та радіотехніка

ЗАТВЕРДЖУЮ

Завідувач кафедри

Марія СКУЛИШ

«__» _____ 2025 р.

**ЗАВДАННЯ
на магістерську дисертацію студентці
Солоденко Марії Андріївні**

1. Тема дисертації: «Удосконалений метод виявлення та захисту приватних відеоданих» науковий керівник дисертації Педан Станіслав Ігорович старший викладач кафедри ІТТ НН ІТС, кандидат технічних наук затверджені наказом по університету від «3» листопада 2025 р. №4772-с.
2. Строк подання студенткою дисертації: «12» грудня 2025 р.
3. Об'єкт дослідження Процес безпечної передачі відеоданих.
4. Предмет дослідження (Вихідні дані – для магістерської дисертації за освітньо-професійною програмою) Методи виявлення та захисту приватних атрибутів користувача під час передачі відеоданих.
5. Перелік завдань, які потрібно зробити:
 1. Аналіз сучасного стану забезпечення приватності користувачів при передачі відеоданих.
 2. Дослідження проблеми законодавчого регулювання приватності даних користувачів.
 3. Дослідження методів виявлення та захисту приватних даних користувачів.
 4. Розробка удосконаленого методу для захисту приватності користувачів при передачі відеоданих.

5. Оцінка запропонованого удосконалення методу для захисту приватності користувачів при передачі відеоданих.
6. Розробка стартап проєкту запропонованого удосконалення методу для захисту приватності користувачів при передачі відеоданих.
6. Перелік графічного (ілюстративного) матеріалу:
 - Слайд №1 Титульний слайд;
 - Слайд №2 Мета дослідження;
 - Слайд №3 Актуальність дослідження;
 - Слайд №4 Основні задачі дослідження;
 - Слайд №5 Об'єкт та предмет дослідження. Наукова новизна та практичне значення отриманих досліджень;
 - Слайд №6 Методи шифрування відеоданих;
 - Слайд №7 Технології анонімізації відеоданих;
 - Слайд №8 Порівняння GDPR, ССРА та Закону «Про захист персональних даних»;
 - Слайд №9 Основні атрибути приватності даних користувачів;
 - Слайд №10 Аналіз суміжних робіт з захисту приватних даних;
 - Слайд №11-15 Опис удосконаленого методу виявлення та захисту приватних відеоданих;
 - Слайд №16 Оцінка запропонованого удосконаленого методу виявлення та захисту приватних відеоданих;
 - Слайд №17-19 Стартап проєкт удосконаленого методу виявлення та захисту приватних відеоданих;
 - Слайд №20 Публікації;
 - Слайд №21 Висновки.
7. Орієнтовний перелік публікацій:
 1. «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРИТС 2025.
 2. "Перспективи телекомунікацій" ПТ-2025.
8. Дата видачі завдання 05 жовтня 2024 року

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Строк виконання етапів магістерської дисертації	Примітка
1	Отримання завдання	05.10.2024	Виконано
2	Аналіз теоретичної інформації	07.10.2024 – 13.12.2024	Виконано
3	Аналіз законодавчих аспектів захисту приватної інформації	15.12.2024 – 17.02.2025	Виконано

4	Аналіз технічних аспектів захисту приватної інформації	20.02.2025 – 24.04.2025	Виконано
5	Дослідження суміжних робіт про захист приватної інформації	25.04.2025 – 27.06.2025	Виконано
6	Розробка удосконаленого методу виявлення та захисту приватних відеоданих	28.06.2025 – 01.09.2025	Виконано
7	Оцінка удосконаленого методу виявлення та захисту приватних відеоданих	02.09.2025 – 31.10.2025	Виконано
8	Розробка стартап проекту	03.11.2025 – 17.11.2025	Виконано
9	Оформлення магістерської дисертації	18.11.2025 – 08.12.2025	Виконано

Студентка _____

Марія СОЛОДЕНКО

Науковий керівник дисертації _____

Станіслав ПЕДАН

РЕФЕРАТ

Тема магістерської дисертації «Удосконалений метод виявлення та захисту приватних відеоданих». Робота містить 87 сторінок, 18 рисунків, 11 таблиць, використано 42 літературних джерела.

Актуальність теми дослідження полягає в потребі забезпечення безпеки та приватності при передачі відеоданих через активний перехід до дистанційної роботи та онлайн-навчання.

Метою роботи є підвищення безпеки користувача при передачі відеоданих шляхом розпізнавання та захисту приватних текстових даних на відео кадрах в режимі реального часу.

Об'єктом дослідження є процес безпечної передачі відеоданих.

Предметом дослідження є методи виявлення та захисту приватних атрибутів користувача під час передачі відеоданих.

Методи дослідження: аналітичний огляд сучасних рішень, літератури та законодавчих аспектів, удосконалення методу виявлення та захисту приватних відеоданих, експериментальна оцінка удосконаленого методу виявлення та захисту приватних відеоданих.

Наукова новизна отриманих результатів: удосконалено метод виявлення приватної інформації у відеоданих. На відміну від існуючих підходів, що фокусуються переважно на обличчях та інших приватних візуальних об'єктах, запропонований метод базується на динамічному розпізнаванні та семантичному аналізі текстових атрибутів, присутніх на відео кадрах (на документах, екранах, записах) у режимі реального часу, що дозволяє підвищити точність виявлення приватних даних. Також набув подальшого розвитку алгоритм адаптивного маскування відеокадрів, що забезпечує баланс між швидкістю обробки кадрів, рівнем безпеки та мінімізацією втрати корисної візуальної інформації при передачі даних, що є критичним для систем відеоконференцз'язку.

Практичне значення отриманих результатів: розроблено програмний прототип захисту відеоданих, що в автоматичному режимі визначає та

приховує приватні текстові дані, що може бути інтегровано в існуючі платформи для дистанційної роботи та навчання. В рамках стартап-проєкту обґрунтовано комерційний потенціал розробки шляхом проведення аналізу ринку та розробки бізнес-моделі впровадження запропонованого методу, що підтверджує економічну доцільність його використання.

Ключові слова: ПРИВАТНА ІНФОРМАЦІЯ, АНОНІМІЗАЦІЯ, ВИЯВЛЕННЯ ПРИВАТНОЇ ІНФОРМАЦІЇ, ЗАХИСТ ПРИВАТНОЇ ІНФОРМАЦІЇ, ОПТИЧНЕ РОЗПІЗНАВАННЯ ТЕКСТУ.

ABSTRACT

The topic of the master's thesis is «Improved method for detecting and protecting private video data». The work contains 87 pages, 18 figures, 11 tables, 42 sources were used.

The relevance of the research topic lies in the need to ensure security and privacy when transmitting video data due to the active transition to remote work and online learning.

The goal of the work is to improve user's security during the transmission of video data by recognizing and protecting private textual data in video frames in real time.

The object of research is the process of secure transmission of video data.

The subject of research is methods for detecting and protecting user private attributes during the transmission of video data.

Research methods: analytical review of modern solutions, literature and legislative aspects, improvement of the method for detecting and protecting private video data, experimental evaluation of the improved method for detecting and protecting private video data.

Scientific novelty of the results: the method for detecting private information in video data has been improved. Unlike existing approaches, which focus mainly on faces and other private visual objects, the proposed method is based on dynamic recognition and semantic analysis of text attributes present in video frames (on documents, screens, recordings) in real time, which increases the accuracy of private data detection. The algorithm for adaptive masking of video frames has also been further developed, ensuring a balance between frame processing speed, security level and minimization of loss of useful visual information during data transmission, which is critical for video conferencing systems.

Practical significance of the results: a software prototype for video data protection has been developed that automatically identifies and hides private text data, which can be integrated into existing platforms for remote work and learning. As part of the start-up project, the commercial potential of the development has been

substantiated by conducting market analysis and developing a business model for implementing the proposed method, which confirms the economic feasibility of its use.

Keywords: PRIVATE INFORMATION, ANONYMIZATION, DETECTION OF PRIVATE INFORMATION, PROTECTION OF PRIVATE INFORMATION, OPTICAL CHARACTER RECOGNITION.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	11
ВСТУП	13
РОЗДІЛ 1. СУЧАСНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ ПРИ ПЕРЕДАЧІ ВІДЕОДАНИХ.....	16
1.1 Основи захисту приватності відеоданих.....	16
1.2 Методи шифрування відеоданих	18
1.3 Технології анонімізації відеоданих	21
Висновок	23
РОЗДІЛ 2. ЗАКОНОДАВЧІ АСПЕКТИ ЗАХИСТУ ПРИВАТНОСТІ ПРИ ПЕРЕДАЧІ ВІДЕОДАНИХ.....	24
2.1 Регуляторна база ЄС	24
2.2 Регуляторна база США	27
2.3 Регуляторна база України	31
2.4 Порівняння підходів до законодавчого регулювання	35
Висновок	37
РОЗДІЛ 3. МЕТОДИ ВИЯВЛЕННЯ ТА ЗАХИСТУ ПРИВАТНИХ ДАНИХ..	39
3.1 Категорії приватних даних	39
3.2 Технології для розпізнавання тексту на зображеннях.....	40
3.3 Аналіз суміжних робіт з захисту приватних даних	42
Висновок	45
РОЗДІЛ 4. РОЗРОБКА УДОСКОНАЛЕНОГО МЕТОДУ ДЛЯ ЗАХИСТУ ПРИВАТНИХ ДАНИХ КОРИСТУВАЧА ПРИ ПЕРЕДАЧІ ВІДЕОДАНИХ ...	47
4.1 Опис удосконаленого методу для захисту приватності користувача при передачі відеоданих.....	47
4.2 Особливості реалізації удосконаленого методу для захисту приватності користувача при передачі відеоданих.....	48
4.3 Опис реалізації удосконаленого методу для захисту приватності користувача при передачі відеоданих.....	55
Висновок	57
РОЗДІЛ 5. ОЦІНКА РОЗРОБЛЕНОГО УДОСКОНАЛЕНОГО МЕТОДУ ДЛЯ ЗАХИСТУ ПРИВАТНИХ ДАНИХ КОРИСТУВАЧА ПРИ ПЕРЕДАЧІ ВІДЕОДАНИХ.....	59

5.1 Тестування удосконаленого методу для захисту приватності користувача при передачі відеоданих.....	59
5.2 Аналіз удосконаленого методу для захисту приватності користувача при передачі відеоданих.....	69
Висновок	71
РОЗДІЛ 6. РОЗРОБКА СТАРТАП ПРОЄКТУ	73
6.1 Опис стартап проєкту	73
6.2 Оцінка стартап проєкту	75
Висновок	80
ЗАГАЛЬНІ ВИСНОВКИ.....	81
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	83

ПЕРЕЛІК СКОРОЧЕНЬ

E2EE	End-to-end encryption
AES	Advanced Encryption Standard
DES	Data Encryption Standard
TLS	Transport Layer Security
IPSec	Internet Protocol Security
WPA2	Wi-Fi Protected Access
RSA	Rivest-Shamir-Adleman
GDPR	General Data Protection Regulation
CCPA	California Consumer Privacy Act
CPRA	California Privacy Rights Act
PII	Personal Identifiable Information
OCR	Optical Character Recognition
IDE	Integrated Development Environment
PDF	Portable Document Format
API	Application Programming Interface
DLP	Data Loss Prevention
TP	True Positive
FP	False Positive
FN	False Negative
TN	True Negative

ШІ	штучний інтелект
ЄС	Європейський Союз
США	Сполучені Штати Америки

ВСТУП

У сучасному світі стрімкого розвитку цифрових технологій та глобалізації інтернету передача відеоданих набула особливого значення в багатьох сферах, таких як дистанційна робота, онлайн-навчання та розваги. Відеодані стали одним із ключових засобів комунікації та обміну інформацією. Однак, разом зі зростанням обсягів відеоданих зростає і необхідність забезпечення приватності та безпеки під час їхньої передачі.

Потреба в захисті приватності під час відео-комунікацій стала також особливо актуальною в умовах військових конфліктів і нестабільної політичної ситуації, як, наприклад, в Україні. Віддалене навчання, робота, а також обмін важливою інформацією через відеодані потребують впровадження сучасних засобів захисту, які можуть гарантувати безпеку даних від стороннього втручання або витоку приватної інформації.

Окремої уваги потребують ризики витоку приватної інформації через текстові дані, що потрапляють у відео (наприклад, написи на екрані, документи у кадрі, повідомлення, що з'являються на пристроях). Такі витoki часто недооцінюються, однак вони можуть містити приватні дані. Це підкреслює необхідність удосконалених сучасних методів виявлення та захисту текстової інформації у відеоданих.

Актуальність. Потреба забезпечення безпеки та приватності при передачі відеоданих значно зросла через активний перехід до дистанційної роботи та онлайн-навчання. Це сприяло збільшенню кількості кібератак та витоків приватної інформації, оскільки передача відеоданих стала важливою складовою щоденних робочих та навчальних процесів.

Безпека відео-комунікацій є важливим фактором для підтримання приватності, особливо під час використання платформ для відео-конференцій і стримінгу, таких як Zoom, Microsoft Teams та Google Meet. Проблеми, пов'язані з порушенням приватності, загострили необхідність у впровадженні більш надійних систем захисту даних.

Мета роботи: підвищення безпеки користувача при передачі відеоданих шляхом розпізнавання та захисту текстових приватних даних на кадрах відео в режимі реального часу.

Предмет дослідження: методи виявлення та захисту приватних атрибутів користувача під час передачі відеоданих.

Об'єкт дослідження: процес безпечної передачі відеоданих.

Методи дослідження: аналітичний огляд сучасних рішень, літератури та законодавчих аспектів, удосконалення методу виявлення та захисту приватних відеоданих, експериментальна оцінка удосконаленого методу виявлення та захисту приватних відеоданих.

Наукова новизна роботи: удосконалено метод виявлення приватної інформації у відеоданих. На відміну від існуючих підходів, що фокусуються переважно на обличчях та інших приватних візуальних об'єктах, запропонований метод базується на динамічному розпізнаванні та семантичному аналізі текстових атрибутів, присутніх на відео кадрах (на документах, екранах, записах) у режимі реального часу, що дозволяє підвищити точність виявлення приватних даних. Також набув подальшого розвитку алгоритм адаптивного маскування відеокadrів, що забезпечує баланс між швидкістю обробки кадрів, рівнем безпеки та мінімізацією втрати корисної візуальної інформації при передачі даних, що є критичним для систем відеоконференцзв'язку.

Практичний результат роботи: розроблено програмний прототип захисту відеоданих, що в автоматичному режимі визначає та приховує приватні текстові дані, що може бути інтегровано в існуючі платформи для дистанційної роботи та навчання. В рамках стартап-проєкту обґрунтовано комерційний потенціал розробки шляхом проведення аналізу ринку та розробки бізнес-моделі впровадження запропонованого методу, що підтверджує економічну доцільність його використання.

Для досягнення мети дослідження було поставлено та вирішено наступні задачі:

1. Проаналізовано сучасний стан забезпечення приватності користувачів при передачі відеоданих.
2. Проведено дослідження проблеми законодавчого регулювання приватності даних користувачів.
3. Досліджено методи виявлення та захисту приватних даних користувачів.
4. Розроблено удосконалений метод для захисту приватності користувачів при передачі відеоданих.
5. Проведено оцінку запропонованого удосконаленого методу для захисту приватності користувачів при передачі відеоданих.
6. Розроблено стартап проєкт удосконаленого методу для захисту приватності користувачів при передачі відеоданих.

РОЗДІЛ 1

СУЧАСНІ МЕТОДИ ЗАБЕЗПЕЧЕННЯ ПРИВАТНОСТІ ПРИ ПЕРЕДАЧІ ВІДЕОДАНИХ

1.1 Основи захисту приватності відеоданих

Спосіб життя мільйонів людей у всьому світі кардинально змінила пандемія COVID-19, адже роботодавці, влада та працівники були змушені адаптуватися до нової реальності, де дистанційна робота та онлайн-навчання швидко набирали оберти. Багатьом довелося різко та поспіхом перетворювати фізичні офіси та політики роботи на віддалені, аби працівники мали змогу працювати в безпеці з дому. Такі організації та компанії не були готові до раптового переходу за досить короткий період часу. На той момент лише 38% підприємств мали готові політики кібербезпеки [3].

Із розвитком цифрових технологій більшість аспектів життя суспільства перемістилися в Інтернет: від онлайн-покупок і спілкування до онлайн-бізнесу та, на жаль, злочинності [4]. Тож перехід до дистанційної роботи та онлайн-навчання лише збільшив кількість атак (рис. 1.1) та ризиків для витоку приватної інформації [1].

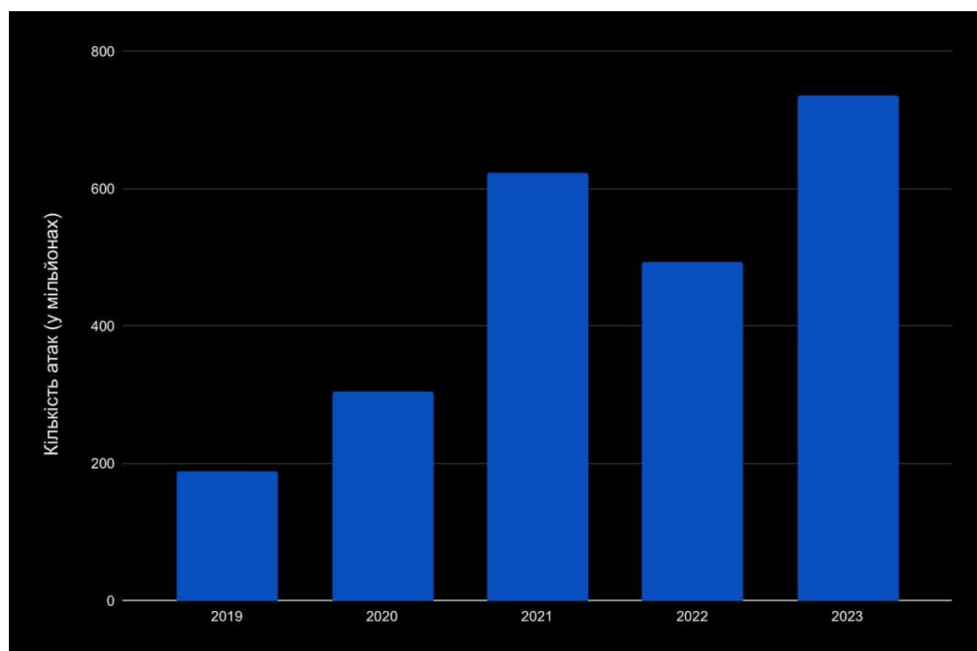


Рисунок 1.1 Кількість кібератак за 2019-2023 роки [1]

Відео складається з безперервного потоку зображень, тобто кадрів. Передача конфіденційних даних незахищеними каналами зв'язку, наприклад, мережею Інтернет, є надзвичайно актуальним питанням сьогодення. Безпека мультимедійної інформації є важливою, оскільки вона може містити важливі дані. Шифрування вважається одним із найбільш надійних способів захисту персональної інформації.

Шифрування – це процес перетворення інформації або даних у код для запобігання несанкціонованому доступу. Його основною метою є захист конфіденційності даних, забезпечення їхньої цілісності та автентичності під час зберігання чи передачі [5].

В свою чергу шифрування відео – це процес перетворення читабельних даних у нечитабельну форму для захисту їхнього вмісту від несанкціонованого доступу під час зберігання або передачі. Воно гарантує, що лише авторизовані користувачі можуть відтворювати відео. Шифрування є критичним для забезпечення приватності в таких сферах, як відеоконференції, стримінгові сервіси та системи відеоспостереження.

Існують різні методи шифрування, щоб захистити інформацію. Загалом їх можна поділити на симетричні та асиметричні (рис. 1.2) [9]. Симетричне шифрування використовує один і той самий ключ, щоб шифрувати та дешифрувати дані. Асиметричний метод використовує два окремих ключі: один для шифрування, а інший для дешифрування. В наступному розділі детальніше розглянуто різні методи шифрування.

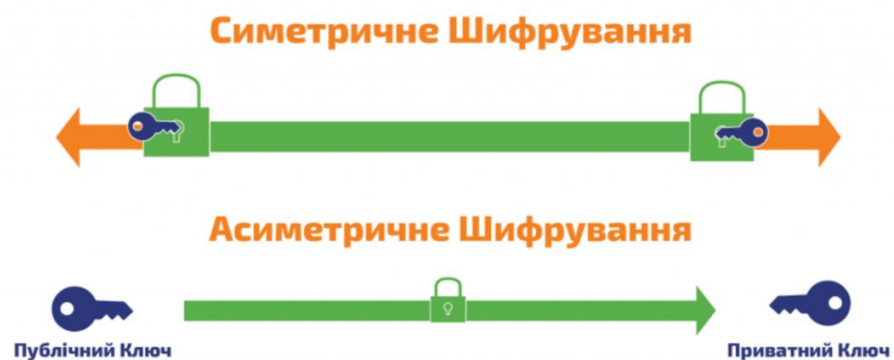


Рисунок 1.2 Типи шифрування для захисту інформації та даних [9]

1.2 Методи шифрування відеоданих

Алгоритм Advanced Encryption Standard (AES) – це сучасний симетричний блочний алгоритм шифрування, який забезпечує високий рівень безпеки та ефективності. Його було розроблено для заміни застарілого алгоритму Data Encryption Standard (DES), що використовувався у криптографії з 1977 року та почав втрачати стійкість через малий розмір ключа та обчислювальні можливості сучасних атак [6].

AES використовує фіксований розмір блоку даних – 128 біт. Залежно від розміру ключа, блоки даних шифруються у 10, 12 або 14 раундів по 128 біт. Алгоритм має високу швидкість шифрування на програмному та апаратному рівні, структурну простоту та ефективність, надійний захист проти сучасних атак, включаючи криптоаналіз. Використовується у багатьох сучасних протоколах безпеки, таких як TLS, IPSec, WPA2, а також у шифруванні баз даних і файлових систем.

У алгоритму AES високий рівень безпеки та гнучкості, проте він складний у реалізації, має обмеження для великих ключів та високі вимоги до ресурсів. Тож AES є потужним і широко використовуваним алгоритмом для захисту даних, забезпечуючи надійність і ефективність при шифруванні великих обсягів інформації.

Rivest-Shamir-Adleman (RSA) – це один із найвідоміших асиметричних алгоритмів шифрування, названий на честь своїх винахідників Рональда Райвеста, Аді Шаміра і Леонарда Адлемана, який використовується для захисту даних через публічний і приватний ключі. Розроблений у 1977 році, він став основою для криптографії з відкритим ключем, яка широко застосовується в цифрових підписах, шифруванні та аутентифікації [7].

RSA базується на використанні двох різних ключів. Відкритий ключ використовується для шифрування даних, а закритий для розшифрування. Алгоритм заснований на математичній складності факторизації великих чисел. Завдяки цьому RSA забезпечує високий рівень безпеки для передачі

конфіденційної інформації. Широко використовується для шифрування електронної пошти, створення цифрових підписів та захисту веб-сайтів.

Алгоритм RSA надійний та має широке застосування, але також низьку продуктивність та необхідність великих ключів. Попри недоліки, RSA залишається популярним завдяки своїй гнучкості та ефективності у комбінації з симетричними алгоритмами шифрування.

Наскрізне шифрування (End-to-End Encryption, E2EE) – це тип шифрування, який гарантує, що дані залишаються зашифрованими від відправника до одержувача. Шифрування відбувається на пристрої відправника, і тільки одержувач може їх розшифрувати за допомогою відповідного ключа. Це запобігає доступу до інформації з боку третьої сторінки, зокрема провайдерів чи серверів [8].

Наскрізне шифрування активно використовується в системах для забезпечення конфіденційності даних. Використовується в захищених месенджерах (WhatsApp, Signal), платформах для відеоконференцій (Zoom), системах електронної пошти (ProtonMail), а також сервісах для зберігання файлів (Mega).

E2EE є важливим інструментом для забезпечення конфіденційності та безпеки даних, особливо в умовах зростаючих загроз в кіберпросторі.

Хаотичний метод шифрування – це метод, який використовує принципи теорії хаосу для шифрування даних. Відмінною рисою цього методу є те, що шифрування базується на нелінійних динамічних системах, які генерують складні і непередбачувані ключі для шифрування. Завдяки цьому, навіть якщо зломисник спробує здійснити атаки на алгоритм, завдяки хаотичним властивостям шифрування, таких атак можна уникнути [2].

Хаотичне шифрування активно використовується для захисту зображень, де хаотичні алгоритми дозволяють створити ключі шифрування, які змінюються динамічно, ускладнюючи їх розшифровку. Це дозволяє створювати криптографічні схеми, які важко зламати навіть за допомогою сучасних методів криптоаналізу.

Хаотичний метод також використовується для шифрування відео, де важливі дані (наприклад, зображення та аудіо) шифруються з використанням складних функцій хаосу для запобігання несанкціонованому доступу, адже має високу стійкість до атак, ефективність для зображень і відеоданих та просту реалізацію, проте його недоліками є складність у відновленні ключів, необхідність точних обчислень та відсутність стандартизації.

Гомоморфне шифрування – це метод шифрування, що дозволяє виконувати обчислення над зашифрованими даними без їх розшифрування. Це унікальна властивість, яка забезпечує безпеку даних протягом усього процесу обробки. Головна ідея полягає в тому, що результат обчислень над зашифрованими даними після розшифрування буде відповідати результату обчислень, проведених над початковими даними [10, 11].

Гомоморфне шифрування використовується в хмарних обчисленнях. Користувач може передати зашифровані дані до хмари, де обчислення виконуються без доступу до початкової інформації. Наприклад, це використовується для забезпечення приватності в обробці медичних записів або фінансових даних. Також використовується в аналізі великих даних, де організації можуть обмінюватися зашифрованими даними і виконувати обчислення над ними без компрометації приватності. У системах електронного голосування використання гомоморфного шифрування дозволяє проводити підрахунок голосів, які залишаються зашифрованими до моменту завершення виборів.

Гомоморфне шифрування є перспективною технологією, яка забезпечує високий рівень конфіденційності та гнучкість для обчислень над зашифрованими даними. Хоча воно має значні обмеження через обчислювальну складність та великі обсяги даних, його застосування у хмарних обчисленнях, аналізі великих даних та електронному голосуванні має великий потенціал.

Попри ефективність криптографічних методів у забезпеченні конфіденційності, шифрування саме по собі не гарантує повного захисту

приватності користувачів. Тому доцільно розглянути технології анонімізації відеоданих як додатковий рівень безпеки.

1.3 Технології анонімізації відеоданих

Захист приватних даних у відео є однією з ключових проблем сучасних технологій аналізу та обробки мультимедійної інформації. В умовах стрімкого розвитку відеоаналітики та її інтеграції в різні сфери, виникає необхідність захисту ідентифікуючих даних, зокрема облич, номерних знаків та інших приватних атрибутів.

Анонімізація – це процес, що дозволяє видалити або змінити чутливу інформацію з метою захисту приватності користувачів або суб'єктів даних. Вона особливо важлива в контексті обробки відео та зображень, де потрібно забезпечити приватність без порушення функціональності даних [12].

Основні методи анонімізації, що застосовуються в контексті відео та зображень: пікселізація, розмиття, заміна частини зображення, додавання шуму та модифікація з використанням штучного інтелекту (ШІ) [13].

Пікселізація – це один із найпоширеніших методів анонімізації, при якому окремі приватні області зображення або відео замінюються мозаїчним ефектом, що утворюється шляхом поділу зображення на великі пікселі (однорідні блоки). Це робить вибрані області нерозбірливими для людського ока, при цьому загальний контекст і структура зображення залишаються зрозумілими [14].

Пікселізація є простим і ефективним методом анонімізації, який широко використовується у різних галузях для захисту приватності. Вона забезпечує базовий рівень приватності, зберігаючи функціональність відео та зображень. Проте для підвищення безпеки та унеможливлення зворотного аналізу пікселізацію слід комбінувати з іншими методами захисту.

Розмиття – це технологія, що змінює чіткість зображення і відео, щоб зробити деталі менш розпізнаваними, таким чином приховуючи приватну інформацію. Розмиття часто застосовується для приховування певних

елементів на зображеннях або відео без повної анонімізації. Мета цієї технології приховати приватну інформацію, зберігаючи загальний контекст зображення. Найпоширенішими видами є: Гаусове розмиття (Gaussian blur) та розмиття за допомогою фільтрів [15].

Розмиття є важливим і зручним інструментом для забезпечення приватності візуальних даних, зберігаючи контекст даних. Однак їх використання вимагає ретельного налаштування, щоб знайти баланс між захистом даних і збереженням їхньої корисності, а для повної анонімізації необхідно комбінувати розмиття з іншими методами.

Додавання шуму – це один із ключових методів анонімізації, який використовується для захисту приватності даних. Цей метод дозволяє модифікувати вихідні дані, додаючи випадкові зміни до числових або візуальних атрибутів, тим самим знижуючи ризик ідентифікації приватних елементів. У контексті анонімізації відео та зображень додавання шуму забезпечує приховування ідентифікаційних елементів без втрати загального контексту. Підходи додавання шуму, що використовуються для анонімізації [16]: адитивний шум, мультиплікативний шум та статистичний фон для додавання шуму.

Додавання шуму є ефективним та гнучким інструментом для забезпечення анонімізації візуальних даних, особливо коли потрібно зберегти контекст і базову структуру зображення. Незважаючи на можливу втрату деталей та обмеження в рівні захисту, простота реалізації робить його важливим компонентом систем захисту приватності.

Штучний інтелект у контексті анонімізації зображень та відео включає використання алгоритмів, які імітують людське сприйняття та прийняття рішень для автоматичного захисту приватної інформації. За допомогою ШІ можна автоматизувати процеси, які раніше вимагали ручного втручання, наприклад, автоматично виявляти особисті дані або приватні області та застосовувати до них методи анонімізації.

Штучний інтелект є потужним інструментом для захисту приватних даних на відео та зображеннях. Однак важливо враховувати обчислювальні ресурси та можливі помилки при використанні цієї технології.

Методи анонімізації є важливими інструментами для захисту приватних даних у відео. Вибір між різними підходами залежить від конкретних вимог до безпеки, швидкості обробки та якості відео.

Висновок

У першому розділі було розглянуто сучасні методи забезпечення приватності при передачі відеоданих, що є ключовим аспектом у забезпеченні конфіденційності та безпеки користувачів у цифровому середовищі.

Зокрема, симетричне шифрування, такі як AES, забезпечує високу швидкість і надійність при обробці великих обсягів даних. Натомість асиметричні методи, такі як RSA, гарантують додатковий рівень безпеки, дозволяючи ефективно обмінюватися ключами. Наскрізне шифрування стало стандартом у сучасних відеоплатформах, забезпечуючи конфіденційність навіть у випадках, коли мережі чи сервери скомпрометовані.

Особливу увагу приділено технологіям анонімізації, які активно використовуються для захисту особистої інформації у відеоданих. Методи пікселізації, розмиття та додавання шуму дозволяють приховувати приватні дані без шкоди для функціональності відео. Штучний інтелект відіграє ключову роль у сучасних підходах до анонімізації, автоматизуючи процеси виявлення та приховування приватних елементів.

Загалом, використання зазначених технологій забезпечує комплексний захист відеоданих від потенційних загроз, дозволяючи зберігати конфіденційність та безпеку користувачів у сучасному цифровому середовищі. Однак важливо враховувати обмеження кожного методу, адаптуючи їх до конкретних потреб і сценаріїв застосування.

При розгляді основних питань розділу 1 були використані літературні джерела [1-17].

РОЗДІЛ 2

ЗАКОНОДАВЧІ АСПЕКТИ ЗАХИСТУ ПРИВАТНОСТІ ПРИ ПЕРЕДАЧІ ВІДЕОДАНИХ

2.1 Регуляторна база ЄС

У сучасному світі цифрових технологій захист приватності є одним із найважливіших викликів для регуляторних органів різних країн. Зростання кількості кіберзагроз і постійне збільшення обсягів персональних даних, що передаються через мережі, підкреслюють необхідність розробки чітких і ефективних законодавчих норм. Захист приватності при передачі відеоданих потребує уваги не лише на технічному, але й на юридичному рівні, щоб забезпечити баланс між правами користувачів та інтересами компаній [36].

На міжнародному рівні ключову роль у формуванні стандартів відіграє General Data Protection Regulation (GDPR), який був ухвалений у Європейському Союзі (ЄС) у 2016 році, а повноцінно вступив у силу 25 травня 2018 року. Основна мета GDPR – встановлення єдиного стандарту захисту даних у ЄС та надання суб'єктам персональних даних більшого контролю над їхньою інформацією. Водночас регламент надає бізнесу чіткі вказівки щодо збору, обробки та зберігання персональних даних, включаючи відео [18].

GDPR визначає «персональні дані» як будь-яку інформацію, що стосується ідентифікації фізичної особи («суб'єкта даних»); фізична особа – це особа яку можна ідентифікувати прямо чи опосередковано, зокрема за ідентифікатором, таким як ім'я, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор або за одним чи кількома факторами, характерними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної ідентичності цієї фізичної особи [19].

Впровадження загального регламенту захисту даних у Європейському Союзі має низку переваг, які сприяють не лише захисту прав громадян, але й покращенню бізнес-середовища та посиленню відповідальності компаній за обробку даних. Перевагами впровадження GDPR є уніфікація правил для всіх країн-членів ЄС, підвищення довіри споживачів, покращення інформаційної

безпеки, спрощення бізнес-процесів, вплив на міжнародні регуляції, штрафи як стимул дотримання законодавства (наприклад, у 2019 році Google сплатив 50 млн. євро за порушення принципу прозорості та законності в обробці даних [20]).

Розділ 3 GDPR охоплює права суб'єкта даних, які є фундаментальними для забезпечення прозорості, доступу та контролю громадян над їхніми персональними даними. Ці права надають фізичним особам можливість не лише знати, як їхні дані обробляються, але й контролювати цей процес. Права суб'єктів даних, встановлені GDPR, гарантують прозорість, контроль і відповідальність у процесі обробки персональної інформації. Їх дотримання забезпечує захист приватності громадян ЄС, сприяє довірі до компаній та підтримує високі стандарти обробки даних.

У межах GDPR контролери та процесори відіграють ключову роль у забезпеченні захисту персональних даних. Розділ 4 GDPR детально регулює їхні обов'язки, права, а також вимоги до безпеки й взаємодії. GDPR детально регламентує обов'язки та відповідальність контролерів і процесорів, а також вимоги до безпеки даних. Це дозволяє забезпечити високий рівень захисту персональних даних, сприяючи довірі між громадянами, бізнесом та регуляторами.

Регламент встановлює ключові принципи обробки даних: законність, справедливість і прозорість; обмеження застосування; мінімізація даних; точність даних; обмеження зберігання; цілісність і конфіденційність; підзвітність [21]. Ці принципи однаково застосовуються як до традиційних текстових даних, так і до персональних даних, що можуть бути присутні у відео.

У контексті захисту приватності відеоданих вимоги GDPR мають особливе значення. Відеоконтент часто містить персональні дані у неструктурованій формі, наприклад: написи на екранах, документи, текстові повідомлення, адреси, ідентифікаційні номери чи інші елементи, що дають можливість ідентифікувати особу. Тому компанії, які збирають, зберігають або

обробляють відеодані, повинні впровадити комплекс заходів, спрямованих на захист таких даних та забезпечення відповідності GDPR.

Основні кроки для забезпечення відповідності GDPR в контексті обробки відеоданих [22]:

1. Оцінка поточного стану обробки даних. Аналіз типів відеозаписів, джерел їх отримання та наявності текстових або інших персональних даних у відеопотоці. Визначення ризиків витоку даних через візуальний контент.

2. Розробка політики конфіденційності. Внесення положень щодо обробки відео та зображень, включно з методами виявлення та захисту персональних даних, правилами зберігання та доступу.

3. Призначення відповідальної особи. Особа, відповідальна за захист даних, має здійснювати контроль за процесами обробки відеоданих, зокрема за застосуванням технологій анонімізації, блюру або фільтрації приватних даних.

4. Інвентаризація даних. Виявлення всіх оброблюваних відеоданих, класифікація за рівнем ризику та визначення, які категорії персональних даних містяться у відео (імена, номери документів, обличчя, адреси тощо).

5. Впровадження технічних і організаційних заходів захисту. Використання алгоритмів для розпізнавання та автоматичного приховування персональних даних у відео, шифрування відеофайлів, контроль доступу, безпечне зберігання та передавання даних.

6. Забезпечення права суб'єктів даних. Надання можливості особам отримати доступ до відеоданих, де вони представлені, а також вимагати їх видалення або знеособлення, якщо це не суперечить юридичним обов'язкам.

7. Навчання співробітників. Підготовка персоналу щодо роботи з відеоданими: правила зйомки, обробки, зберігання, а також можливі ризики, пов'язані з появою приватних даних у відео.

8. Реагування на інциденти. Розробка процедури дій у випадку компрометації відеоданих, включно з механізмами швидкого виявлення витоку, повідомлення регулятора та суб'єктів даних.

9. Аудит і моніторинг процесів. Регулярне тестування системи захисту відеоданих, перевірка коректності роботи алгоритмів знеособлення та оновлення політик відповідно до нових загроз.

10. Адаптація договорів з партнерами. Включення вимог щодо безпечної обробки відеоданих у контракти, зокрема з компаніями, що здійснюють зберігання, аналітику або трансляцію відео.

Реалізація цих 10 кроків дозволяє організаціям не лише відповідати вимогам GDPR, а й забезпечити належний рівень захисту персональних даних у відеоконтенті, підвищити довіру користувачів, мінімізувати ризики витоку інформації та сприяти формуванню безпечних практик обробки візуальних даних у цифровому середовищі.

GDPR охоплює будь-яку форму персональних даних, включно з інформацією, що може бути відтворена на зображеннях і у відеозаписах. Це стосується як біометричних характеристик, так і текстової інформації, яка може бути ідентифікатором особи або містити інші персональні дані.

2.2 Регуляторна база США

Система захисту персональних даних у США базується на Каліфорнійському законі про захист приватності споживачів (California Consumer Privacy Act, CCPA), який був прийнятий 2018-го року, проте набув чинності лише у 2020 році та є фундаментальним регулюванням для захисту конфіденційності громадян. CCPA надає права споживачам і зобов'язує бізнес інформувати про способи збору та обробки даних, а також дотримуватись правил безпеки [23].

У 2023 році до CCPA були внесені зміни через прийняття Каліфорнійського закону про права на конфіденційність (California Privacy Rights Act, CPRA). CPRA розширив права споживачів і наклав додаткові обов'язки на бізнес, включаючи введення нових категорій даних, таких як конфіденційні персональні дані, а також зобов'язав призначення відповідальної особи з захисту даних для великих організацій [24].

Ці закони створюють стандарти для обробки даних і слугують орієнтиром для інших штатів у США, а також впливають на міжнародну практику захисту персональної інформації.

Основні положення CCPA [25]:

1. Права споживачів: право знати про те, які персональні дані збираються, як вони використовуються та кому передаються; право на видалення персональних даних, якщо вони більше не потрібні для законної обробки; право заборонити продаж своїх даних третім сторонам; право доступу до персональних даних, які обробляються бізнесом, і відомості про типи даних, що зберігаються, а також способи їх використання.

2. Обов'язки бізнесу: інформувати користувачів про цілі збору даних до початку їх обробки; забезпечувати реалізацію запитів користувачів щодо даних; пропонувати прості механізми для заборони продажу даних, наприклад, кнопку «Do Not Sell My Personal Information» на веб-сайтах.

3. Розширення через CPRA: створення окремої категорії «конфіденційних персональних даних», які вимагають додаткового захисту; призначення відповідального за захист даних для великих організацій.

4. Поширення CCPA: закон застосовується до компаній, які відповідають хоча б одному з наступних критеріїв: річний валовий дохід не менше 50 мільйонів доларів, обробляють дані щонайменше 50 000 споживачів або отримують принаймні 50% доходу від продажу персональних даних.

Американські політики конфіденційності, такі як CCPA і CPRA, мають багато спільного з GDPR, зокрема право на доступ до даних і їх видалення. Однак США надає більше свободи бізнесу, а GDPR акцентує увагу на централізованому регулюванні та високих штрафах за порушення.

CCPA регулює обробку персональних даних і встановлює чіткі межі щодо того, які дані вважаються захищеними, а які залишаються поза його впливом. Розглянемо визначені основні категорії особистої інформації, що підпадають під регулювання, а також винятки, які важливо враховувати [24].

Особиста інформація (Personal Identifiable Information, PII) включає будь-які дані, які дозволяють ідентифікувати особу або пов'язані з нею: ім'я, адреса, електронна адреса – це базові дані, які використовуються для ідентифікації осіб у транзакціях, контрактах або онлайн-профілях; номер соціального страхування – критично важлива інформація для забезпечення конфіденційності та фінансової безпеки; біометрична інформація – відбитки пальців, зображення сітківки або дані розпізнавання обличчя, які активно використовуються в технологіях безпеки; інформація про зайнятість – записи про роботу, включаючи посади, зарплати та звільнення, які можуть впливати на приватність; освітня інформація – дані про оцінки, записи про навчання або сертифікати; історія веб-перегляду – включає дані про активність користувачів в Інтернеті, такі як відвідані веб-сайти, IP-адреси або дані про використання додатків. ССРА не поширюється на загальнодоступна інформацію та інформація про здоров'я.

ССРА охоплює широкий спектр персональних даних, які можуть бути використані для ідентифікації особи та забезпечує баланс між прозорістю, захистом даних і функціональністю для бізнесу.

У 2023 році були внесені суттєві зміни до ССРА через CPRA. Оновлений регламент має значний вплив на бізнес і споживачів, посилюючи захист персональних даних та підвищуючи вимоги до компаній [26, 27]. Ці зміни мають особливе значення у контексті обробки відеоданих, які часто містять як явні, так і приховані текстові персональні дані користувачів.

Основні зміни ССРА, важливі для захисту приватності відеоданих:

1. Розширення прав споживачів. Користувачі отримали ширші можливості контролю над своїми персональними даними, включно з тими, що можуть з'являтися у відео. Це означає доступ до відеозаписів, право вимагати їх видалення або обмеження обробки, якщо відео містить ідентифікаційні фрагменти.

2. Створення категорії «конфіденційних персональних даних». До цієї категорії належать расова чи етнічна приналежність, сексуальна орієнтація,

фінансова інформація, геолокація та інші чутливі дані. У відео такі дані можуть бути присутні неявно, наприклад у вигляді написів на документах, екранних повідомлень, елементів інтерфейсу, логотипів чи маркерів, які розкривають чутливу інформацію.

3. Збільшення відповідальності бізнесу. Компанії несуть підвищену юридичну відповідальність за неналежний захист персональних даних у відео. Це включає технічні заходи щодо виявлення, приховування або знеособлення приватних даних у відеоматеріалах.

4. Підвищення вимог до прозорості. Бізнес повинен чітко інформувати користувачів про те, які відеодані збираються, чи містять вони персональні дані, у яких цілях вони обробляються та як захищаються.

Зміни ССРА посилили захист персональних даних та права споживачів, що надають більше контролю над їхніми особистими відомостями. Введення нових вимог посилює захист приватності, підвищує довіру до компаній і надає більш чіткі правила для ведення бізнесу в межах США. Це особливо важливо для компаній, які працюють із відеоаналітикою, відеоспостереженням, відеохостингом або застосунками, що записують і обробляють відеоконтент.

Основні зміни у ССРА для бізнесу у контексті роботи з відеоданими:

1. Процес очищення даних. Передбачає виявлення та усунення або знеособлення персональних даних у відео, наприклад, анонімізація написів, номерів, документів, адрес та інших чутливих елементів.

2. Оновлення внутрішніх політик та систем. Політики повинні містити окремі положення про роботу з відеоданими: строки зберігання, правила доступу, методи захисту та алгоритми обробки приватної інформації в кадрі.

3. Аудити та оцінка ризиків. Регулярне тестування систем відеообробки, оцінка ризиків витоку приватних даних, перевірка коректності інструментів анонімізації та фільтрації.

4. Контракти з третіми сторонами. Необхідно встановлювати вимоги до підрядників і партнерів, які обробляють відео, включно з гарантіями виявлення та захисту персональних даних у матеріалах.

Зміни, внесені CPRA, значно підвищують стандарти захисту інформації та встановлюють додаткові обов'язки для бізнесу. Бізнеси, що працюють з персональними відеоданими, повинні адаптуватися до нових вимог, оскільки невідповідність може призвести до серйозних юридичних і фінансових наслідків. Важливо впроваджувати стратегії для безпеки даних, регулярні аудити та покращення внутрішніх політик для забезпечення відповідності CCPA та CPRA.

CCPA та CPRA мають важливе значення для захисту персональних даних, включаючи інформацію, яка може бути зафіксована у відео та зображеннях. Однак навколо цих законів виникають численні неточності, які можуть привести до неправильного розуміння вимог щодо приватних даних.

Регуляторна база США розвивається, адаптуючись до викликів цифрової епохи. CCPA та CPRA створюють комплексну систему захисту персональних даних, що поширюється і на відео та зображення, які містять текстові та графічні приватні дані користувачів. У контексті захисту приватності відеоданих ці закони формують чіткі вимоги щодо виявлення, обмеження доступу та анонімізації приватної інформації у відеоконтенті. Це визначає високі стандарти безпеки для будь-яких технологій відеоаналітики, відеозахисту та передачі відеоданих.

2.3 Регуляторна база України

Україна активно розвиває нормативну базу для захисту персональних даних в епоху цифровізації, що є особливо важливим у контексті обробки відеоданих. Закон «Про захист персональних даних» (№2297-VI) забезпечує регулювання обробки даних і конфіденційності. Цей закон спрямований на забезпечення прав суб'єктів даних та сприяє інтеграції України в міжнародний простір захисту даних.

Основні положення Закону України «Про захист персональних даних», що мають відношення до відеоданих [28]:

Стаття 1. Сфера дії Закону: поширюється на правові відносини, пов'язані з обробкою та захистом персональних даних. Якщо відео містить персональні дані і обробляється не для особистих цілей, воно підпадає під дію закону.

Стаття 2. Визначення термінів: «персональні дані» – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована; «суб'єкт персональних даних» – фізична особа, персональні дані якої обробляються.

У контексті відео до персональних даних можуть належати: обличчя та біометричні дані, текст на документах, екранах пристроїв або бейджах, адреси, номери телефонів, державні номерні знаки або інші текстові об'єкти у відео, що дозволяють встановити особу.

Стаття 5. Об'єкти захисту: персональні дані, які: можуть бути конфіденційними, якщо це передбачено законом або визначено суб'єктом даних; не належать до конфіденційних, якщо стосуються осіб, які виконують державні або публічні функції; відкриті для доступу, якщо це передбачено законами, наприклад, щодо антикорупційних декларацій.

Для відео це означає, що навіть побічне відображення приватної інформації в кадрі зобов'язує систему забезпечувати належний рівень захисту.

Стаття 6. Загальні вимоги до обробки персональних даних: мета обробки – дані, як і відеодані можуть оброблятися лише за згодою суб'єкта або в інших передбачених законом випадках; пропорційність – обробка має бути обмежена конкретною, законною метою; точність – дані повинні бути актуальними та точними; конфіденційність – захист, як даних, так і відеоданих від несанкціонованого доступу.

Стаття 7. Особливі вимоги до обробки персональних даних: встановлює обмеження на обробку конфіденційних персональних даних та відео, що розкривають расове чи етнічне походження, політичні, релігійні переконання, або даних, пов'язаних зі здоров'ям чи статевим життям. Обробка таких даних дозволяється лише за певних умов, зокрема за згодою суб'єкта, для захисту

життєво важливих інтересів, у законній професійній діяльності або для судового захисту прав.

Стаття 8. Права суб'єкта персональних даних: отримувати інформацію про свої персональні дані та мету їх обробки; вимагати виправлення, видалення або блокування даних у разі їх незаконної обробки.

Тож, особа має право вимагати видалення відео чи окремих елементів, якщо в кадр випадково потрапили її персональні дані.

Статті 10-14. Використання персональних даних; підстави для обробки персональних даних; збирання персональних даних; накопичення та зберігання персональних даних; поширення персональних даних: охоплюють обробку, захист, інформування, збирання, накопичення, зберігання і передачу даних третім особам, що здійснюється за згодою суб'єкта персональних даних або відповідно до закону.

Перераховані дії з відеоданими допускається лише за згодою суб'єкта або у випадках, передбачених законом.

Стаття 15. Видалення або знищення персональних даних: підстави для видалення: закінчення строку зберігання; припинення правовідносин; вказівки Уповноваженого чи рішення суду; спеціальні випадки, коли дані, зібрані з порушенням закону або під час контррозвідувальної діяльності, видаляються відповідно до законодавства.

Якщо відео містить приватні дані, зібрані без законних підстав, воно має бути видалене або анонімізоване так, щоб персональні дані неможливо було відновити.

Стаття 24. Забезпечення захисту персональних даних: забезпечення захисту даних від втрати, знищення, незаконної обробки; призначення структурного підрозділу чи відповідальної особи, яка організовує захист даних.

У випадку відеоданих такими заходами є: шифрування відеофайлів; обмеження доступу до відео; анонімізація приватних даних у кадрі; аудит систем відеоаналітики.

Стаття 28. Відповідальність за порушення законодавства про захист персональних даних: будь-яке порушення законодавства у сфері захисту персональних даних карається відповідно до чинного законодавства, включно з адміністративними та судовими санкціями.

У контексті відеоданих ця норма має ключове значення, оскільки будь-яка система, що фіксує або обробляє відео чи зображення з текстовими ідентифікаційними елементами, несе ризики правопорушення у разі неналежного захисту таких відомостей.

Стаття 29. Міжнародне співробітництво та передача персональних даних: передача персональних даних або відео з персональними даними іноземним суб'єктам дозволяється за умови відповідності міжнародним стандартам, зокрема GDPR.

Стаття 30. Прикінцеві положення: закон набрав чинності з 1 січня 2011 року. У період воєнного стану допускається передача персональних даних за спрощеною процедурою для надання медичної допомоги.

Закон України «Про захист персональних даних» забезпечує комплексний підхід до регулювання питань захисту конфіденційної приватної інформації. Він встановлює чіткі вимоги до суб'єктів, які працюють із персональними даними, та забезпечує права фізичних осіб на захист їхньої приватності. Його виконання є важливим для дотримання етичних норм і міжнародних стандартів. Ці положення створюють фундамент для забезпечення прав громадян у сфері персональних даних, водночас сприяючи прозорості у діяльності державних органів і приватних структур.

Багато українських банків запровадили політики захисту персональних даних, що відповідають як національному законодавству, так і міжнародним стандартам. Наприклад, банки використовують двофакторну аутентифікацію, шифрування транзакцій та сертифікацію за ISO 27001.

Українські технологічні компанії також активно адаптують свої політики до вимог міжнародних стандартів, таких як GDPR, забезпечуючи додаткову прозорість для клієнтів із ЄС.

Закон «Про захист персональних даних» прямо стосується задачі захисту приватності відеоданих, оскільки у відео можуть міститися персональні текстові дані, доступ до яких може призвести до порушення прав суб'єкта. Вибрані статті українського законодавства формують чітку правову необхідність розробки та впровадження технологій захисту відеоданих. Таким чином, нормативно-правове поле України повністю підтримує та обґрунтовує актуальність дослідження, а саме удосконалення методу виявлення та захисту приватних даних у відео, здатного автоматично захищати приватність користувачів шляхом виявлення та анонімізації текстових персональних даних у відео.

2.4 Порівняння підходів до законодавчого регулювання

З метою порівняння розглянемо три основні нормативні акти у сфері захисту персональних даних (табл. 2.1): GDPR (ЄС); CCPA (США) та Закон України «Про захист персональних даних» [29, 30, 31].

Таблиця 2.1 Порівняння законодавчих норм

Країна	ЄС	США	Україна
Законодавча норма	GDPR	CCPA	Закон «Про захист персональних даних»
Сфера дії	Усі компанії, які обробляють дані громадян ЄС	Компанії з річним валовим доходом не менше 50 мільйонів доларів, обробляють дані щонайменше 50 000 споживачів	Усі суб'єкти, які обробляють персональні дані на території України
Права суб'єктів даних	Право на доступ, виправлення, видалення, обмеження обробки, перенесення даних	Доступ до даних, право відмови від продажу, видалення	Доступ до даних, виправлення, видалення, обмеження обробки

Продовження таблиці 2.1 Порівняння законодавчих норм

Підстава для обробки	Згода, виконання договору, законний інтерес, захист життєвих інтересів	Згода або бізнес-потреби	Згода, законні підстави, виконання зобов'язань
Штрафи за порушення	До 20 млн євро або 4% річного доходу компанії	До \$7,500 за порушення або \$2,500 за ненавмисне шкоду	Адміністративні санкції, рішення суду
Прозорість обробки	Високий рівень, зобов'язання інформувати про мету та використання даних	Вимога політик конфіденційності для споживачів	Обов'язок повідомлення суб'єктів про обробку даних
Міжнародна передача даних	Дозволяється лише до країн із належним рівнем захисту	Немає чітких обмежень, окрім внутрішніх гарантій	Дозволена за згодою суб'єкта чи при забезпеченні належного захисту
Особливості конфіденційності приватних даних	Спеціальні обмеження на обробку даних про здоров'я, релігію тощо	Особливі вимоги до медичних і фінансових даних	Визначено окремо обробку конфіденційних приватних даних

Українське законодавство у сфері захисту персональних даних значною мірою відповідає міжнародним стандартам, зокрема вимогам GDPR. Водночас, ССРА має свою унікальність, спрямовану на регулювання персональних даних переважно з точки зору прав споживачів і обмеженого бізнесу. Для України актуальним є подальше вдосконалення механізмів відповідності європейським стандартам, включаючи посилення контролю за виконанням норм і інтеграцію сучасних технічних заходів захисту приватної інформації [35, 36].

Забезпечення прав суб'єктів даних, прозорість обробки, санкції за порушення та механізми міжнародної передачі даних – основні аспекти, які потребують покращення в Україні для забезпечення належного рівня безпеки в умовах цифровізації.

Висновок

У другому розділі було детально розглянуто регуляторну базу захисту персональних даних у різних країнах, включаючи Україну, Європейський Союз та США. Аналіз основних нормативних актів, таких як GDPR, CCPA і Закон України «Про захист персональних даних», дозволяє зробити кілька важливих висновків.

Усі розглянуті нормативи містять спільні принципи: законність, прозорість, цілісність, конфіденційність, а також підзвітність суб'єктів обробки даних. Хоча вони різняться у формулюваннях, їхня правова природа відображає загальну тенденцію для забезпечення максимального контролю суб'єкта над його персональними даними та мінімізації ризиків їх ідентифікації, витоку чи неправомірної обробки.

З погляду дослідження захисту приватності відеоданих, включно з виявленням та приховуванням приватної інформації на зображеннях і у відеопотоці, правове поле створює чіткі вимоги щодо того, які дані слід вважати персональними та які обов'язки покладаються на власників даних. Особливо релевантними є положення, що стосуються: обмеження доступу до персональних даних, видалення персональних даних, відповідальності за порушення законодавства, міжнародної передачі даних та відповідності міжнародним стандартам.

Задачі захисту приватності у відеоданих, зокрема автоматизоване виявлення та приховування текстових елементів, що містять персональну інформацію, безпосередньо впливають із загальних вимог GDPR щодо мінімізації обсягу персональних даних, забезпечення їхнього належного захисту та недопущення несанкціонованого розкриття.

Реалізація механізмів розпізнавання та маскування чутливої текстової приватної інформації на візуальних даних є одним із практичних інструментів дотримання GDPR, оскільки дозволяє контролювати доступ до персональної інформації в мультимедійних потоках, що сьогодні становлять значну частину цифрового контенту.

Таким чином, правові вимоги визначають широку категорію даних, які можуть потрапити у відео та підлягають захисту. До них належать: персональні дані, що з'являються у кадрі та непрямі ідентифікатори, які можуть бути розпізнані і пов'язані з конкретною особою.

Порівняння правових вимог із технічними викликами демонструє, що захист приватності відеоданих перестає бути не обов'язковим технічним завданням, а стає вимогою законодавчих норм і умовою юридичної відповідальності суб'єктів обробки.

Нормативно-правова база прямо визначає актуальність і необхідність технічних рішень, спрямованих на захист приватності інформації у відеоданих, а також формує вимоги щодо обов'язковості впровадження таких рішень у практику обробки відео. Застосування методів автоматизованої анонімізації відео не лише знижує юридичні ризики, але й забезпечує захист прав осіб, приватність яких може бути порушена через технологічні можливості аналізу та розпізнавання відео.

При розгляді основних питань розділу 2 були використані літературні джерела [18-31, 35, 36].

РОЗДІЛ 3

МЕТОДИ ВИЯВЛЕННЯ ТА ЗАХИСТУ ПРИВАТНИХ ДАНИХ

3.1 Категорії приватних даних

Аналіз приватних даних має ключове значення для забезпечення захисту інформації, яку користувачі вважають приватною. Вивчення ставлення до захисту приватності дозволяє зрозуміти ризики витоку чутливої інформації, розробити ефективні заходи захисту, а також інтегрувати принципи приватності у сучасні технології, включаючи системи штучного інтелекту.

Стаття «Towards a Visual Privacy Advisor: Understanding and Predicting Privacy Risks in Images» [32] присвячена вивченню відношення користувачів до конфіденційності приватних даних у цифрових зображеннях. Основна увага приділяється класифікації даних, оцінці їхньої приватності та прогнозуванню ризиків, пов'язаних із використанням таких даних у мережі.

Автори використовували опитування для збору даних, вивчення відповідей користувачів та побудови метрик оцінки ризиків конфіденційності. Ключові метрики включають рівень сприйняття приватних даних, частоту використання певної інформації в мережі та рівень довіри до цифрових платформ (табл. 3.1).

Таблиця 3.1 Основні атрибути конфіденційності приватних відеоданих

Категорія	Визначення	Приклад
Медичні дані	Інформація про фізичне або психічне здоров'я людини	Медична історія, діагнози, рецепти
Дані документів	Інформація, пов'язана з офіційними документами особи	Ідентифікаційні номери, паспорт, водійське посвідчення
Фінансові дані	Дані, що розкривають фінансовий стан або банківські операції	Номер кредитної картки, реквізити рахунків
Біометричні дані	Дані, що стосуються фізіологічних характеристик для ідентифікації особи	Відбитки пальців, фото обличчя

Продовження таблиці 3.1 Основні атрибути конфіденційності приватних відеоданих

Особисті дані	Інформація, що ідентифікує фізичну особу	Ім'я, номер телефону, електронна адреса
Локаційні дані	Інформація про місце перебування або маршрут особи	Геолокація, GPS-координати
Соціальні дані	Відомості про взаємозв'язки або соціальний статус особи	Інформація про друзів, членів сім'ї, соціальний статус
Онлайн-активність	Дані про дії особи в Інтернеті, включаючи відвідувані сайти та пошукові запити	URL-адреси, історія пошуку

Цей аналіз демонструє різний рівень важливості категорій приватних даних для користувачів, зокрема медичні дані сприймають, як найбільш конфіденційні; дані документів мають високий рівень конфіденційності через ризики ідентифікації; фінансові дані трохи поступаються медичним і документам, але все ж є критичними; біометричні дані знаходяться в середині списку, оскільки використовуються для ідентифікації; особисті дані менш конфіденційні порівняно з іншими категоріями, хоча залишаються важливими; локаційні дані є важливими, але в багатьох профілях оцінюються як менш критичні; соціальні дані і онлайн-активність показали найнижчу конфіденційність у більшості користувачів.

3.2 Технології для розпізнавання тексту на зображеннях

У підрозділі вище визначено, які саме типи інформації вважаються конфіденційними приватними даними відповідно до законодавства, міжнародних стандартів та результатів опитувань. Категоризація створює основу для подальших технічних рішень. У даному підрозділі розглядаються інструменти, за допомогою яких можна технічно виявляти ці категорії у відеокадрах.

Технології розпізнавання тексту на зображеннях мають критичне значення в забезпеченні приватності даних користувачів. З поширенням цифрових платформ виникає необхідність ефективно виявляти приватну інформацію з зображень, які містять текстові дані, для запобігання витоку або несанкціонованому доступу до приватних даних.

Основна роль таких технологій полягає у швидкому та точному виявленні приватних даних, таких як фінансові, особисті чи медичні атрибути. Вони слугують першим етапом для подальшої анонімізації текстів у зображеннях, забезпечуючи захист даних під час передачі відеоданих.

Технологія OCR (Optical Character Recognition, Оптичне розпізнавання тексту) – це автоматизоване перетворення зображень рукописного, машинописного або друкованого тексту у цифровий формат, що відтворює текстову інформацію у вигляді послідовності символів, придатних для подальшого редагування та обробки у текстових редакторах. Оптичне розпізнавання тексту дозволяє редагувати текст, здійснювати пошук слова або фрази, зберігати його в компактнішій формі, аналізувати інформацію, а також застосовувати до тексту електронний переклад та форматування. Оптичне розпізнавання тексту є досліджуваною проблемою в галузях розпізнавання образів, штучного інтелекту і комп'ютерного зору.

Основні етапи OCR [33]:

1. Отримання зображення – сканування або знімок.
2. Попередня обробка – видалення шумів, покращення контрасту.
3. Виділення текстових блоків – визначення зон з текстом.
4. Розпізнавання символів – кожен символ аналізується за шаблоном або за допомогою нейронної мережі.
5. Післяобробка – корекція помилок, форматування.

Сучасні інструменти для розпізнавання тексту забезпечують високу точність і швидкість аналізу текстових даних на зображеннях. Одним із провідних рішень є Google ML Kit Text Recognition [34], який підтримує

багатомовне розпізнавання тексту з використанням сучасних моделей машинного навчання.

ML Kit здатен розпізнавати текст кількома мовами, включаючи друкований текст і написаний від руки, що підвищує універсальність технології. Працює локально на пристрої, що гарантує вищий рівень приватності і знижує ризики витоку даних. Використовується для аналізу тексту в реальному часі та інтегрується у мобільні додатки.

У контексті захисту приватних даних на зображеннях та відео Google ML Kit Text Recognition доцільно використати для розпізнавання текстової інформації у кадрі та подальшої класифікації, як приватної або публічної за допомогою регулярних виразів та словників. При цьому важливо враховувати якість вхідних зображень та наявні обмеження в налаштуваннях. Застосування технології розпізнавання тексту Google ML Kit підвищує ефективність і точність виявлення та обробки приватної інформації. Її інтеграція підвищує рівень приватності користувачів та мінімізує ризики витоку інформації, оскільки обробка даних здійснюється безпосередньо на пристрої.

3.3 Аналіз суміжних робіт з захисту приватних даних

Підрозділ 3.2 описує технологічну основу, його можливості, особливості роботи, обмеження та придатність до обробки відеоданих у реальному часі. Це дає розуміння того, які інструменти можуть бути використані в практичних рішеннях для захисту приватної інформації. Підрозділ 3.3 переходить від окремих технологій до аналізу комплексних систем, що вже реалізують виявлення та анонімізацію даних.

Сучасні дослідження у сфері захисту приватності користувачів зосереджені переважно на задачах автоматичної де-ідентифікації обличчя на зображеннях і відео або на ручному приховуванні приватної інформації за допомогою відеоредакторів. Однак такі підходи зазвичай не охоплюють текстові елементи, що можуть містити персональні дані (ім'я, адресу, номер документа тощо).

У цьому підрозділі розглянуто сучасні комерційні та наукові рішення, які реалізують задачі виявлення чутливих даних у відео та зображеннях для анонімізації. Метою аналізу є співставлення властивостей і архітектур цих рішень для розробки удосконаленого методу виявлення та захисту приватних відеоданих. Вибрані аналоги представляють як промислові продукти, так і наукові підходи, що дозволяє всебічно оцінити сильні сторони та обмеження різних архітектур.

Google Cloud Data Loss Prevention Application Programming Interface (DLP API) – це хмарний сервіс для виявлення, класифікації та редагування приватної інформації у структурованих і неструктурованих даних. DLP API може аналізувати зображення, PDF-файли, текстові поля тощо, використовуючи набір вбудованих детекторів `infoTypes` для виявлення типів чутливих даних (наприклад, email, телефон, IP-адреса). Результатом роботи є анонімізоване зображення, де знайдені фрагменти замінено непрозорими прямокутниками або масками [37].

Хмарна модель Google DLP забезпечує широкий спектр можливостей, у тому числі підтримку власних регулярних виразів, словників, кастомних моделей і логування змін. Проте такий підхід потребує відправлення даних на сервер, що створює ризик розкриття приватної інформації під час передачі та не дозволяє використовувати DLP у системах із вимогами до локальної обробки. Також сервіс орієнтований на обробку статичних зображень, а не на потоки відео у реальному часі.

Veritone Redact – комерційне рішення для автоматичної та ручної анонімізації відео з можливістю виявлення облич, голосів та об'єктів. Система орієнтована на потреби правоохоронних органів, юридичних структур та органів державної влади. Veritone використовує комбінацію детекції об'єктів (включаючи OCR) та автоматичного трекінгу, що дозволяє застосовувати однакову трансформацію до об'єкта протягом усього відео. Користувач може вручну перевірити або відкоригувати результати у графічному інтерфейсі перед експортом готового відео [38].

Система демонструє високий рівень точності в сценаріях post-processing, тобто після запису відео. Проте Veritone не підтримує обробку в реальному часі, оскільки працює у хмарному середовищі або на серверних інстанціях.

Стаття «SecurePose: Automated Face Blurring and Human Movement Kinematics Extraction from Videos Recorded in Clinical Settings» [39] описує дослідницький підхід, орієнтований на клінічні відеозаписи, який поєднує розмиття облич для приватності та оцінку положення тіла для подальшого аналізу рухів людини. Таким чином, система виконує дві задачі одночасно: зберігає анонімність суб'єкта, але водночас дозволяє зберегти корисні ознаки для медичного чи поведінкового аналізу.

Основна ідея SecurePose – баланс між приватністю і корисністю даних, система не просто приховує обличчя, а робить це так, щоб не втратити значущі для аналізу дані.

Стаття «Preserving privacy by de-identifying face images» [40] присвячена методам де-ідентифікації облич, у якій аналізується ефективність різних підходів – пікселізація, Gaussian blur, blackout, заміна синтезованими зображеннями. Дослідження порівнює рівень приватності (наскільки метод заважає ідентифікувати людину) і рівень корисності (наскільки залишаються доступними поведінкові або емоційні характеристики).

Порівняння розглянутих в цьому підрозділі робіт наведено в таблиці 3.2:

Таблиця 3.2 Порівняння суміжних робіт

Назва	Google Cloud DLP API	Veritone Redact	SecurePose	De-identifying face images
Тип даних	Зображення, PDF-файли	Відео	Відео	Зображення
Об'єкти анонімізації	Текст, об'єкти	Обличчя, об'єкти	Обличчя	Обличчя
Місце обробки	Хмара	Хмара	Локально	Локально
Режим обробки	Післяобробка	Післяобробка	У реальному часі	Післяобробка
Приватність	Середня	Середня	Висока	Висока

Аналіз показав, що більшість існуючих рішень реалізують хмарну обробку та орієнтовані переважно на обличчя або візуальні об'єкти, а не на текстові елементи. На основі аналізу суміжних робіт та законодавчих норм пропонується удосконалення методу виявлення та захисту приватних відеоданих шляхом автоматичного розпізнавання та анонімізації текстової приватної інформації локально на пристрої користувача та в режимі реального часу. Запропонований підхід сприятиме підвищенню рівня безпеки та забезпечуватиме анонімізацію приватних відеоданих у режимі реального часу, що є особливо важливим у сучасних умовах цифровізації.

Висновок

У третьому розділі було проведено аналіз сучасних підходів до виявлення та захисту приватних даних у відеоданих. Було досліджено класифікацію приватних атрибутів, розглянуто технологію розпізнавання тексту на зображеннях і відео та проаналізовано суміжні роботи.

Результати показали, що категоризація приватних даних, таких як медичні, фінансові, соціальні, біометричні та інші атрибути, дозволяє ефективніше визначати ступінь їхньої чутливості та пріоритизувати заходи захисту. Було сформовано список основних атрибутів, які вимагають особливої уваги при обробці відеоданих.

Як технологію розпізнавання тексту на зображеннях, було розглянуто Google ML Kit Text Recognition, яка є одним із найбільш адаптованих рішень для мобільних додатків. Завдяки локальній обробці даних ML Kit забезпечує високий рівень приватності та здатний працювати у режимі реального часу, як з друкованим текстом, так і написаним від руки. Впровадження цієї технології є критично важливим для автоматичного виявлення приватних атрибутів у відео перед їх анонімізацією.

У результаті аналізу сучасних наукових та комерційних рішень у сфері анонімізації відео та зображень встановлено, що більшість із них орієнтовані на виявлення та приховування візуальних об'єктів, або на хмарну постобробку

зображень та відео. Такі рішення, як Google Cloud DLP API та Veritone Redact, демонструють високу точність і гнучкість у роботі з даними, однак залежать від віддалених серверів і не гарантують повної приватності користувача. Наукові підходи, представлені в роботах SecurePose та Preserving privacy by de-identifying face images, фокусуються на оптимізації балансу між приватністю й аналітичною корисністю даних, проте переважно обмежуються сферою обробки облич або тілесних ознак.

На відміну від розглянутих аналогів, запропонований удосконалений метод захисту приватності користувача передбачає локальне виявлення та анонімізацію текстових елементів на відео в реальному часі, поєднуючи технології оптичного розпізнавання тексту, лексичний аналіз за словниками та фільтрацію регулярними виразами. Такий підхід усуває необхідність передавання даних до зовнішніх серверів та підвищує рівень захисту приватної інформації користувача.

Таким чином, проведений аналіз суміжних рішень підтвердив актуальність і наукову новизну розробленого методу, а саме поєднання обробки в реальному часі, автономності та фокусування на текстових персональних даних створюючи новий рівень безпеки відео-комунікацій у цифровому середовищі. Розділ демонструє важливість інтеграції сучасних технологій у системи захисту приватних даних. Подальші дослідження мають бути зосереджені на оптимізації алгоритмів виявлення приватних даних, підвищенні точності розпізнавання тексту та розробці багатофункціональних рішень, що відповідають зростаючим вимогам приватності у цифровому середовищі.

При розгляді основних питань розділу 3 були використані літературні джерела [32-36, 39, 40].

РОЗДІЛ 4

РОЗРОБКА УДОСКОНАЛЕНОГО МЕТОДУ ДЛЯ ЗАХИСТУ ПРИВАТНИХ ДАНИХ КОРИСТУВАЧА ПРИ ПЕРЕДАЧІ ВІДЕОДАНИХ

4.1 Опис удосконаленого методу для захисту приватності користувача при передачі відеоданих

Сучасні підходи до захисту приватності користувачів у відео здебільшого зосереджені на забезпеченні безпечної передачі відеоданих, проте вони приділяють менше уваги процесам анонімізації окремих елементів відео, які можуть містити персональні дані. Це створює певні прогалини у комплексному захисті інформації, оскільки навіть при безпечній передачі відеопотоку можуть залишатися фрагменти, що дозволяють ідентифікувати конкретну особу.

У рамках проведеного дослідження було проаналізовано чинні законодавства щодо захисту персональних даних у різних юрисдикціях, зокрема в Україні, країнах Європейського Союзу та Сполучених Штатах Америки. Додатково були опрацьовані наукові статті та результати опитувань, які висвітлюють пріоритетність окремих категорій персональних даних з точки зору їх важливості та чутливості для користувачів. На основі цього аналізу була сформована та детально проаналізована таблиця, що класифікує персональні дані за їх критеріями важливості та необхідністю захисту на відео в режимі реального часу.

План роботи удосконаленого методу для захисту приватності користувача (дивись рис. 4.1):

1. Отримання відео з камери смартфона.
2. Знаходження тексту на відео.
3. Аналіз тексту на відео відповідно до таблиці з класифікацією персональних даних.
4. Анонімізація тексту на відео відповідно до координат тексту на відео.
5. Виведення анонімізованого відео на екрані смартфона.



Рисунок 4.1 План роботи удосконаленого методу захисту приватності користувача

Таблиця з класифікацією та аналізом персональних даних, у поєднанні з технологією розпізнавання тексту Google ML Kit, стали основою для розробки удосконаленого методу для захисту приватності користувача під час передачі відеоданих у реальному часі. Запропонований додаток на основі удосконаленого методу виявлення та захисту приватності відеоданих має автоматично виявляти та анонімізувати чутливі елементи відеоконтенту, забезпечуючи високий рівень приватності. Таким чином, поєднання правових та технічних аспектів створює комплексний підхід до забезпечення приватності у сучасних відео-комунікаційних системах.

4.2 Особливості реалізації удосконаленого методу для захисту приватності користувача при передачі відеоданих

Розробка удосконаленого методу захисту приватності користувача виконана з використанням офіційного середовища розробки Android Studio та мови програмування Kotlin. Такий вибір забезпечує повну інтеграцію з

екосистемою Android, високу продуктивність, а також легку підтримку сучасних бібліотек і технологій для обробки зображень та відео в реальному часі.

Android Studio – це офіційне інтегроване середовище розробки (Integrated Development Environment, IDE) для платформи Android. Середовище забезпечує розробника повним набором інструментів для створення, налагодження та оптимізації мобільних додатків. Використання Android Studio також надало можливість легко інтегрувати сторонні бібліотеки, зокрема Google ML Kit для розпізнавання тексту на відео в режимі реального часу [41].

Kotlin – це сучасна, статично типізована мова програмування, яка є рекомендованою для розробки Android-додатків. Вона забезпечує кращу безпеку коду та меншу ймовірність помилок порівняно з Java. Вона є більш лаконічною та виразною, що скорочує обсяг коду і прискорює процес розробки та підтримки застосунку на основі удосконаленого методу виявлення та захисту приватності відеоданих. Вона має повну сумісність з Java (Kotlin-код може використовувати Java-бібліотеки), що дозволяє легко інтегрувати існуючі Android-фреймворки та інструменти [42].

Розглянемо фізичну модель удосконаленого методу захисту приватності користувача при передачі відеоданих:

Архітектурні блоки:

- Camera Input (CI) – камера смартфона. Дає відеопотік кадрів F_t .
- Preprocessor (P) – масштабування, поворот кадру, перетворення форматів, підготовка для OCR.
- OCR Module (O) – Google ML Kit Text Recognition – перетворює кадр F_t в набір текстових елементів $E_t = \{e_{t1}, \dots, e_{tn}\}$ з координатами і текстом.
- Sensitive Detector (S) – набір правил: регулярні вирази та словники. Повертає категорії чутливості для кожного елемента.
- Anonymizer (A) – приймає координати для анонімізації та накладає маску/блюр.

Формула для опису потоку даних (4.1):

$$F_t \xrightarrow{P} F'_t \xrightarrow{O} E_t = \{(s_i, b_i, c_i)\} \xrightarrow{S} \{(s_i, b_i, C_i, \text{score}_i)\} \xrightarrow{A} F''_t, \quad (4.1)$$

де F_t – початковий кадр у часі t , P – преобробка (орієнтація, масштаб), F'_t – оброблений кадр у часі t , E_t – набір текстових елементів, O – розпізнавання тексту для кожного елемента e_i : текст – s_i , прямокутник з координатами – b_i , впевненість – c_i , S – детектор чутливої інформації, C_i – знайдені категорії приватної інформації, score_i – оцінка впевненості, A – анонімізація: на виході анонімізований кадр F''_t .

Формула (4.1) описує повний цикл обробки одного кадру відео. Вхідний кадр F_t спочатку проходить попередню обробку (P), потім OCR-розпізнавання (O), після чого виконується семантична перевірка на приватні дані (S), і, анонімізація (A), у результаті чого отримуємо захищений кадр F''_t .

Ця модель формалізує роботу системи локального захисту приватності при передачі відеоданих, тобто алгоритм переходу від необробленого кадру до анонімізованого з урахуванням виявленого тексту та його категорій.

Розглянемо математичну модель удосконаленого методу виявлення та захисту приватності відеоданих:

Позначення:

- Кадри: $F_t, t \in \mathbb{N}$ – послідовність відеокадрів (потік). Індекс t змінюється в межах натуральних чисел.
- OCR оператор $O: F \mapsto \{e_i\}$. Для елемента e : $e = (s, b, c)$, де s – текст (string), b – прямокутник з координатами (bounding box), $c \in [0,1]$ – впевненість OCR. Оператор O описує процес розпізнавання тексту (OCR), який перетворює вхідний кадр F у множину текстових елементів $\{e_i\}$, де кожен елемент містить розпізнаний текст s , його координати b та рівень впевненості c .
- Sensitive detector $S: s \mapsto C$, де C – множина знайдених категорій (може бути порожньою). Оператор S позначає систему виявлення приватних даних, яка для кожного рядка s повертає множину категорій C , що

описують тип знайденої інформації. S складається з двох підоператорів: regex-based R та dictionary-based D : $S(s) = R(s) \cup D(s)$. Розпізнавання чутливого тексту реалізується через об'єднання двох підсистем: $R(s)$ – результат пошуку за регулярними виразами; $D(s)$ – результат пошуку у словниках ключових термінів. Таким чином, повна множина знайдених категорій – це об'єднання обох методів.

- Anonymizer оператор $A: (F, \{b_i\}) \mapsto F'$ – накладення блюру/маски у зонах b_i . Оператор A описує процес анонімізації кадру. На вхід він отримує вихідний кадр F та множину областей $\{b_i\}$, які містять чутливу інформацію, а на виході повертає новий кадр F' , у якому ці області були анонімізовані.

Виявлення приватної інформації для кадру F_t :

- OCR отримує множину елементів (дивись 4.2):

$$E_t = O(F_t) = \{e_{t1}, \dots, e_{tn_t}\}, e_{ti} = (s_{ti}, b_{ti}, c_{ti}), \quad (4.2)$$

Після застосування OCR до кадру F_t отримуємо множину розпізнаних текстових елементів E_t , де кожен елемент e_{ti} містить текст s_{ti} , координати b_{ti} та рівень впевненості c_{ti} . Кількість знайдених елементів у кадрі дорівнює n_t .

- Для кожного елемента застосовується детектор (дивись 4.3):

$$C_{ti} = S(s_{ti}) = R(s_{ti}) \cup D(s_{ti}), \quad (4.3)$$

Для кожного розпізнаного тексту s_{ti} виконується перевірка приватності за допомогою оператора S . Результатом є множина категорій C_{ti} , до яких може належати даний текст.

Позначимо бінарну змінну p (4.4):

$$p_{ti} = \begin{cases} 1, & \text{якщо } C_{ti} \neq \emptyset \\ 0, & \text{якщо } C_{ti} = \emptyset \end{cases} \quad (4.4)$$

Бінарна змінна p_{ti} вказує, чи містить текстовий елемент e_{ti} приватну інформацію. Якщо множина знайдених категорій C_{ti} не порожня – тобто хоча б один тип приватної інформації виявлено – тоді $p_{ti} = 1$; інакше $p_{ti} = 0$.

- Множина зон для анонімізації у кадрі (4.5):

$$B_t = \{b_{ti} \mid p_{ti} = 1\}, \quad (4.5)$$

Множина B_t містить координати всіх областей у кадрі, які потрібно анонімізувати. Вона формується із координат тих елементів, для яких було виявлено приватність ($p_{ti} = 1$).

Анонімізація і вихідний кадр (дивись 4.6):

$$F'_t = A(F_t, B_t), \quad (4.6)$$

Анонімізований кадр F'_t отримується шляхом застосування оператора A до вихідного кадру F_t та множини областей B_t , які потрібно замаскувати. Таким чином, на виході отримуємо відеокادر без видимих приватних даних.

Тип анонімізації задаємо як функцію $a(b; \theta)$. Тобто (дивись 4.7):

$$A(F, B) = F \odot \bigcup_{b \in B} a(b; \theta), \quad (4.7)$$

де $\odot$ – застосування поелементної операції на множині пікселів у боксах B , θ – параметри анонімізації (інтенсивність блюру).

Функція $A(F, B)$ (4.7) описує процес накладення анонімізації. Для кожного прямокутника $b \in B$ виконується функція $a(b; \theta)$, яка створює локальну маску анонімізації. Після цього всі маски об'єднуються, формуючи глобальну карту анонімізації, яка застосовується до кадру F за допомогою поелементної операції $\odot$.

Результат анонімізації кадру F дорівнює початковому кадру, до якого застосовано операцію накладання $\odot$ із сукупністю всіх масок анонімізації, згенерованих для кожної області b із набору B , відповідно до параметрів θ .

Розглянемо метрики удосконаленого методу захисту приватності користувача:

– Точність та повнота виявлення приватних даних (4.8, 4.9):

Для оцінювання ефективності роботи системи виявлення приватної інформації використовуються стандартні метрики – точність (Precision) (4.8) та повнота (Recall) (4.9).

$$\text{Precision} = \frac{TP}{TP+FP}, \quad (4.8)$$

$$\text{Recall} = \frac{TP}{TP+FN}, \quad (4.9)$$

де TP (True Positive) – кількість елементів, які правильно визначено як приватні (система виявила приватну інформацію там, де вона справді є), FP (False Positive) – кількість помилкових спрацьовувань, коли система виявила приватну інформацію там, де її насправді немає, FN (False Negative) – кількість пропущених випадків, коли приватна інформація присутня, але система її не виявила.

Precision (точність) показує, який відсоток знайдених системою елементів дійсно належать до приватної інформації. Іншими словами, це міра надійності виявлення наскільки часто система має рацію, коли повідомляє про знайдений приватний фрагмент.

Recall (повнота) показує, яку частку від усіх реальних елементів приватних даних система змогла знайти. Це показник чутливості системи наскільки повно вона охоплює усі випадки приватної інформації.

– Комплексна метрика F_1 (4.10):

Для інтегральної оцінки роботи системи використовується F_1 -міра (4.10), яка є гармонійним середнім між Precision і Recall (4.8, 4.9):

$$F_1 = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}, \quad (4.10)$$

Ця метрика відображає збалансованість між точністю та повнотою виявлення. Якщо система має високу точність, але низьку повноту (або навпаки), значення F_1 буде зменшене, тому ця міра стимулює рівновагу між обома показниками.

Для ефективної системи захисту приватної інформації у відеопотоці бажано, щоб значення $F_1 > 0,8$, що свідчить про високу якість виявлення приватних даних у режимі реального часу.

– Пропускна здатність (4.11):

$$T_p \leq \frac{1}{\text{fps}}, \quad (4.11)$$

T_p – час обробки кадру в секундах, fps – частота кадрів відео.

Це часове обмеження для обробки одного кадру. Щоб забезпечити роботу в реальному часі, час обробки одного кадру має бути не більшим за тривалість одного кадру у відеопотоці.

– Миготіння (4.12):

Для уникнення миготіння анонімізованих областей у відеопотоці, коли система може тимчасово «втрачати» або «повертати» об'єкт між кадрами, використовується механізм темпорального згладжування (temporal smoothing).

$$p_{ti}^{\text{smoothed}} = 1(\sum_{j=t-m+1}^t p_{ji} \geq k), \quad (4.12)$$

де p_{ti} – бінарний індикатор виявлення i -го елемента p кадри t , m – розмір ковзного вікна (кількість попередніх кадрів, які враховуються для аналізу стабільності), k – поріг стабільності, мінімальна кількість кадрів, у яких елемент має бути виявлений, щоб вважати його стійким.

Формула (4.12) описує тимчасове згладжування результатів виявлення, щоб уникнути "миготіння" анонімізації. Якщо для певного елемента i впродовж останніх m кадрів виявлення було позитивним принаймні k разів, то в поточному кадри він також вважається приватним. Функція $1(\sum_{j=t-m+1}^t p_{ji} \geq k)$ – це індикатор, який дорівнює 1, якщо умова виконується, і 0 – якщо ні.

Фізична модель представляє процес анонімізації текстових приватних атрибутів на відеокадрах, математична модель – абстрактне відображення через оператори, а метрики – інструмент кількісної оцінки точності, стабільності та продуктивності реалізованої системи. У сукупності ці три рівні забезпечують повний цикл перевірки та оптимізації удосконаленого методу захисту приватності відеоданих користувача.

4.3 Опис реалізації удосконаленого методу для захисту приватності користувача при передачі відеоданих

Для розкриття принципу роботи удосконаленого методу виявлення та захисту приватності відеоданих найбільш доцільно використати блок-схему, оскільки вона наочно демонструє логіку виконання основних етапів обробки відеоданих та анонімізації приватної інформації.

Блок-схема дозволяє послідовно відобразити основні модулі та алгоритми, що реалізовані в програмному коді, та показати, як саме здійснюється захист приватних даних під час обробки відеопотоку в реальному часі. Блок-схема роботи удосконаленого методу для захисту приватності користувача (рис. 4.2):

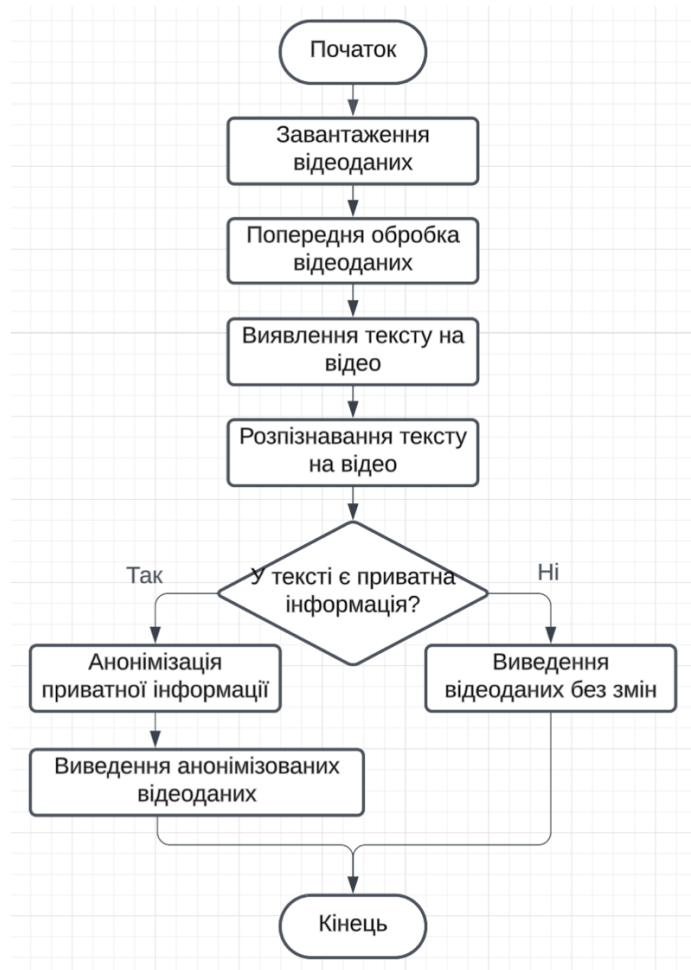


Рисунок 4.2 Блок-схема роботи удосконаленого методу захисту приватності користувача

Розглянемо детально кожен етап, представлений на блок-схемі:

1. Завантаження відеоданих. На першому етапі здійснюється ініціалізація роботи камери смартфона та отримання відеопотоку. Для цього використовується модуль захоплення зображення, який забезпечує доступ до попереднього перегляду камери в режимі реального часу та передає кадри для подальшої обробки.

2. Попередня обробка відеоданих. Після отримання відеокадру виконується попередня обробка, яка включає оптимізацію зображення: корекцію розміру, кольору, формату та повороту кадру для узгодження з вимогами модуля розпізнавання тексту. Метою цього етапу є підвищення точності розпізнавання та покращення продуктивності подальшої обробки.

3. Виявлення тексту на відео. На цьому етапі за допомогою бібліотеки Google ML Kit виконується пошук текстових елементів на зображенні. Алгоритм визначає області кадру, в яких присутні символи чи слова, та формує їх координати у вигляді прямокутних меж.

4. Розпізнавання тексту на відео. Після визначення зон з текстом відбувається процес розпізнавання символів та перетворення їх у машинний текст (OCR, Optical Character Recognition). Результатом цього етапу є ідентифікація тексту, який міститься у виділених областях відеокадру.

5. Перевірка виявленого тексту на наявність приватної інформації. Отриманий текст передається до спеціального модуля аналізу, який здійснює пошук приватних даних відповідно до попередньо сформованих правил. Перевірка виконується за двома механізмами:

- Регулярні вирази – використовується для виявлення чітко формалізованих даних: паспортних номерів, IBAN, номерів телефонів, електронних адрес, IP-адрес, геолокаційних координат тощо;
- Словниковий аналіз – застосовується для пошуку слів або термінів, що можуть містити приватні дані (наприклад: імена людей, медичні терміни, фінансові установи, адреси). Для цього удосконалений метод захисту приватності користувача використовує словники, сформовані на основі реальних категорій приватних даних.

Якщо текст містить ознаки персональної інформації – виконується анонімізація, якщо ні – він виводиться без змін.

6. Анонімізація приватної інформації. У випадку виявлення чутливих даних на текст накладається маска. Анонімізація здійснюється шляхом: накладення ефекту блюру (розмиття), затемнення або часткового приховування текстових областей, застосування зміни кольору, зафарбування або інших візуальних методів приховування. Маскування виконується саме за координатами розпізнаного тексту, що дозволяє приховати лише приватну інформацію без впливу на весь кадр.

7. Виведення відеоданих. На останньому етапі оброблений кадр повертається на екран смартфона. Залежно від результатів перевірки користувач бачить: анонімізоване відео (якщо приватні дані знайдені) або оригінальне відео без змін (якщо чутлива інформація відсутня). Процес виконується безперервно для кожного нового кадру відео, що забезпечує роботу удосконаленого методу виявлення та захисту приватності відеоданих в режимі реального часу.

Висновок

У четвертому розділі було детально описано розробку, архітектуру, математичну формалізацію та реалізацію удосконаленого методу для захисту приватності користувача під час передачі відеоданих. Основна мета полягала у створенні системи, здатної виявляти та анонімізувати приватну текстову інформацію у відеопотоці в режимі реального часу, без необхідності передавання даних у хмару.

Запропонований удосконалений метод захисту приватності користувача поєднує технології оптичного розпізнавання тексту із механізмами виявлення чутливих даних, що базуються на регулярних виразах і словникових базах. Це дозволяє системі розпізнавати текстові приватні дані та виконувати їх автоматичну анонімізацію за допомогою розмиття чи маскування у межах виявлених областей кадру.

Фізична модель представляє процес анонізації текстових приватних атрибутів на відеокадрах, де визначено послідовність модулів: від захоплення кадру камерою до формування анонізованого відеопотоку. Математична модель формалізує ці процеси через оператори O , S , A , що описують розпізнавання, класифікацію та анонізацію даних відповідно. Ключові формули дозволяють математично описати роботу системи, зокрема процес визначення приватності p_{ti} , вибір зон анонізації V_t та накладення масок анонізації $A(F, V)$.

Для оцінювання ефективності удосконаленого методу виявлення та захисту приватності відеоданих визначено низку метрик якості: Precision (точність) та Recall (повнота) – для оцінки точності і повноти виявлення приватних елементів; F_1 -міра – як збалансований показник ефективності; T_p – для забезпечення обробки відео в реальному часі; темпоральне згладжування – для усунення ефекту миготіння при анонізації.

Удосконалення запропонованого методу захисту приватності користувача полягає не лише в фокусі на розпізнавання та захист приватних текстових даних, що відрізняє його від існуючих рішень, орієнтованих на візуальні об'єкти, але й у повній локальності обробки даних, що усуває ризики витоку приватної інформації через мережу та забезпечує низьку затримку обробки. На відміну від хмарних або серверних рішень, запропонований підхід є автономним, швидким і придатним для широкого використання у мобільних застосунках.

Розроблений додаток на основі цього методу успішно реалізує повний цикл захисту приватності від виявлення до анонізації та забезпечує комфорт, безпеку і контроль користувача над власними даними під час зйомки чи трансляції відео. Таким чином, у розділі обґрунтовано теоретичні основи, математичні моделі, алгоритмічну реалізацію та практичні переваги удосконаленого методу захисту приватних відеоданих користувача.

При розгляді основних питань розділу 4 були використані літературні джерела [41, 42].

РОЗДІЛ 5

ОЦІНКА РОЗРОБЛЕНОГО УДОСКОНАЛЕНОГО МЕТОДУ ДЛЯ ЗАХИСТУ ПРИВАТНИХ ДАНИХ КОРИСТУВАЧА ПРИ ПЕРЕДАЧІ ВІДЕОДАНИХ

5.1 Тестування удосконаленого методу для захисту приватності користувача при передачі відеоданих

Для оцінки ефективності запропонованого удосконаленого методу виявлення та захисту приватності відеоданих було проведено тестування додатку в умовах максимально наближених до реальних сценаріїв використання. Тестування виконувалося на смартфоні Android, із встановленим розробленим додатком, що реалізує локальний пошук та анонімізацію приватної текстової інформації на основі OCR, регулярних виразів та словників.

Метою тестування є оцінка коректності роботи всіх етапів удосконаленого методу захисту приватності користувача та перевірка здатності системи виявляти й анонімізувати приватну текстову інформацію у відеопотоці в режимі реального часу. Тестування проводилося за двома напрямками: функціональне тестування (перевірка правильності виявлення та обробки даних) та продуктивне тестування (перевірка швидкодії, стабільності та використання ресурсів смартфона).

Для оцінки роботи методу були сформовані тестові відеофрагменти, які містять різні типи текстової інформації, класифікованої як приватна:

- номери телефонів;
- номери банківських карток та IBAN;
- електронні адреси;
- IP-адреси.

Тестування проводилося на смартфоні OnePlus 11 з такими характеристиками:

- Android 16;
- процесор Qualcomm Snapdragon 8 Gen 2;

- оперативна пам'ять 16 ГБ;
- вбудована пам'ять 256 ГБ;
- стандартна камера 24 fps.

Вибір цього смартфона зумовлений його високою продуктивністю та достатнім запасом обчислювальних ресурсів для роботи OCR та алгоритмів аналізу в реальному часі.

Для кожного тесту фіксувалися чи було правильно класифіковано текст як приватний або публічний та час обробки одного кадру. Саме тестування відбувалося у декілька етапів (рис. 5.1): знімалося відео, потім було обрано деякі кадри з відео де є приватна інформація та кадри де немає приватної інформації, після чого відбувалося тестування цих кадрів та їх оцінка для подальшого аналізу та висновку.

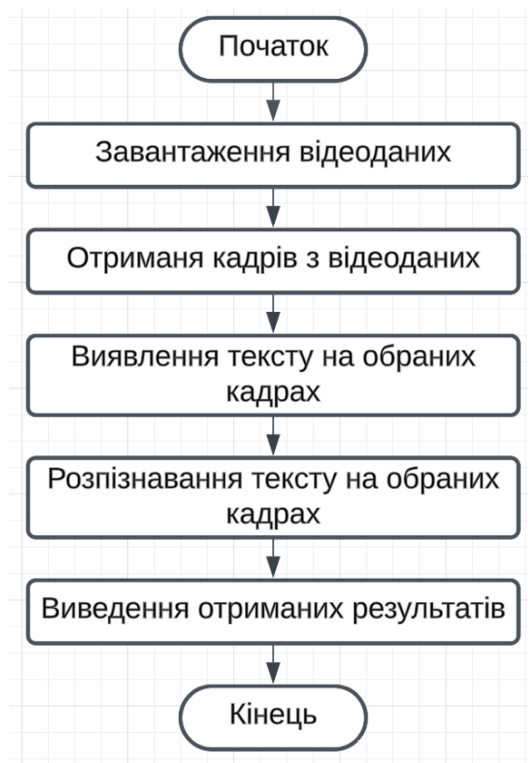


Рисунок 5.1 Блок-схема основних кроків тестування

Тестування проводилися за сценаріями:

- Тест 1 розпізнавання кадрів лише з номерами телефонів (рис. 5.2):

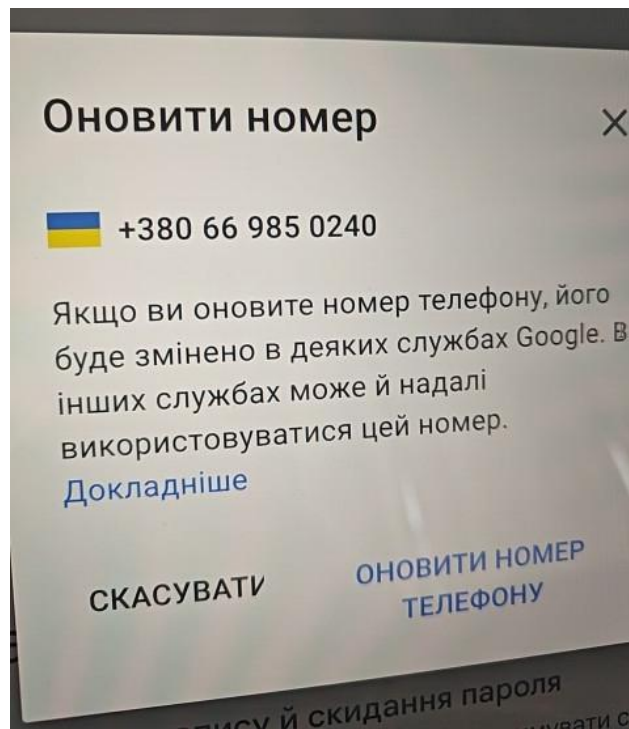


Рисунок 5.2 Приклад кадру з номером телефону

Було знято коротке відео з якого за допомогою розробленої програми було обрано кадри, що містять текстову приватну інформацію, а саме номери телефонів, для тестування удосконаленого методу виявлення та захисту приватності відеоданих. Вибрані кадри покривають всі типові українські номери, що дозволило оцінити стійкість алгоритму до різних форматів структурованих числових даних.

Результат розпізнавання кадрів лише з номерами телефонів (дивись рис. 5.3):

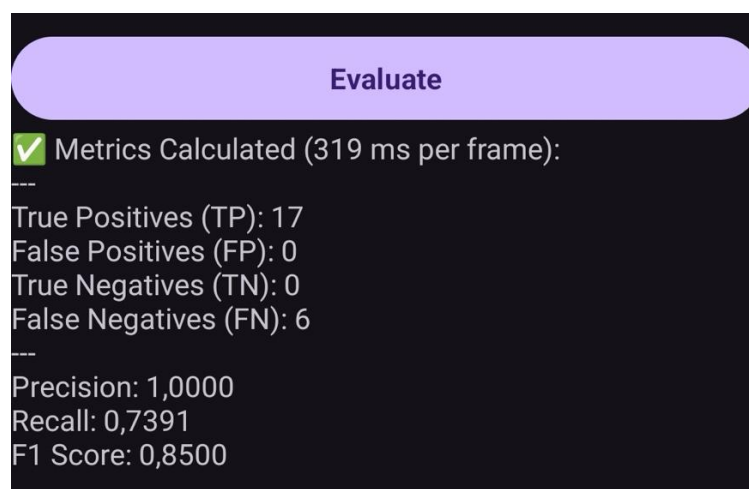


Рисунок 5.3 Отриманий результат тестування 1

Оцінка розпізнавання кадрів лише з номерами телефонів: система виконала розпізнавання та класифікацію приватної інформації з такими показниками: True Positives (TP): 17; False Positives (FP): 0; True Negatives (TN): 0; False Negatives (FN): 6; Precision: 1,0000; Recall: 0,7391; F1 Score: 0,8500; середній час обробки кадру: 319 мс.

Тест 1 показав, що алгоритм дуже точно визначає приватні дані цього типу, тобто не було жодного хибного спрацювання, коли звичайний текст був би розпізнаний як номер телефону. Водночас показник повноти свідчить, що частина номерів (6 випадків із 23) не була виявлена, що зумовлено якістю зображення або низькою контрастністю окремих символів. Загальний показник якості F1 Score = 0,85 підтверджує ефективність методу в реальних умовах.

- Тест 2 розпізнавання кадрів лише з номерами банківських карт та IBAN (рис. 5.4):



Рисунок 5.4 Приклад кадру з номером банківської картки та кадру з IBAN

Було знято коротке відео з якого за допомогою розробленої програми було обрано кадри, що містять текстову приватну інформацію, а саме номери банківських карт та IBAN, для тестування удосконаленого методу виявлення та захисту приватності відеоданих. Тестування дозволило оцінити роботу

методу на довгих структурованих числових послідовностях, де важливими є стабільність OCR та точність регулярних виразів.

Результат розпізнавання кадрів лише з номерами банківських карт та IBAN (дивись рис. 5.5):

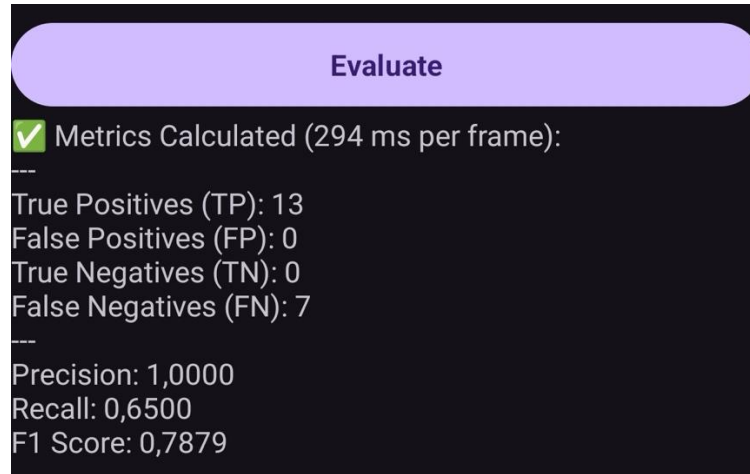


Рисунок 5.5 Отриманий результат тестування 2

Оцінка розпізнавання кадрів лише з номерами банківських карт та IBAN: система виконала розпізнавання та класифікацію приватної інформації з такими показниками: True Positives (TP): 13; False Positives (FP): 0; True Negatives (TN): 0; False Negatives (FN): 7; Precision: 1,0000; Recall: 0,6500; F1 Score: 0,7879; середній час обробки кадру: 294 мс.

Тест 2 показав, що алгоритм не допускає хибних розпізнавань, що є критично важливим для фінансової інформації. Висока точність підтверджує коректність класифікації кожного розпізнаного фрагмента. Однак повнота демонструє, що близько третини банківських номерів не були виявлені, що зумовлено: дрібним шрифтом на окремих кадрах, нерівномірним освітленням та низькою контрастністю символів. Попри це, F1 Score = 0,8 вказує на прийнятну точність для реальних відеосценаріїв.

- Тест 3 розпізнавання кадрів лише з електронною поштою (рис. 5.6):

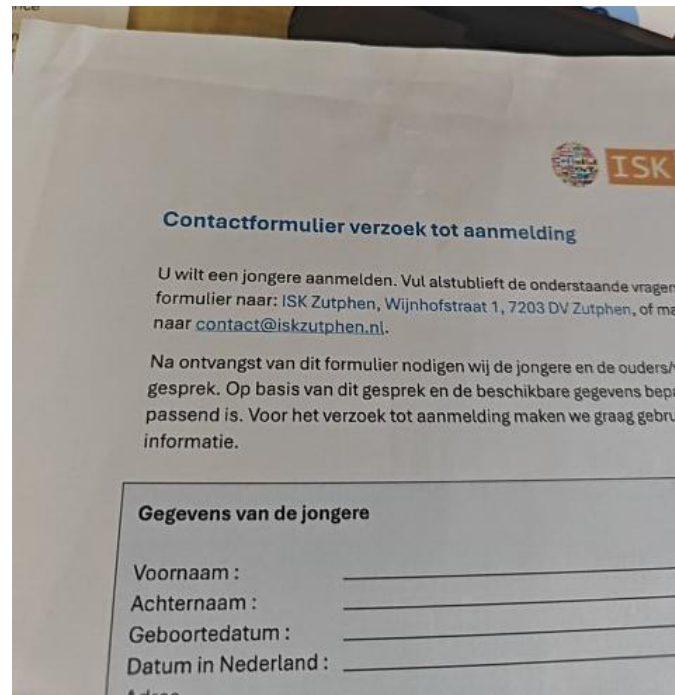


Рисунок 5.6 Приклад кадру з електронною поштою

Було знято коротке відео з якого за допомогою розробленої програми було обрано кадри, що містять текстову приватну інформацію, а саме електронну пошту різних форматів, для тестування удосконаленого методу виявлення та захисту приватності відеоданих.

Результат розпізнавання кадрів лише з електронною поштою (дивись рис. 5.7):

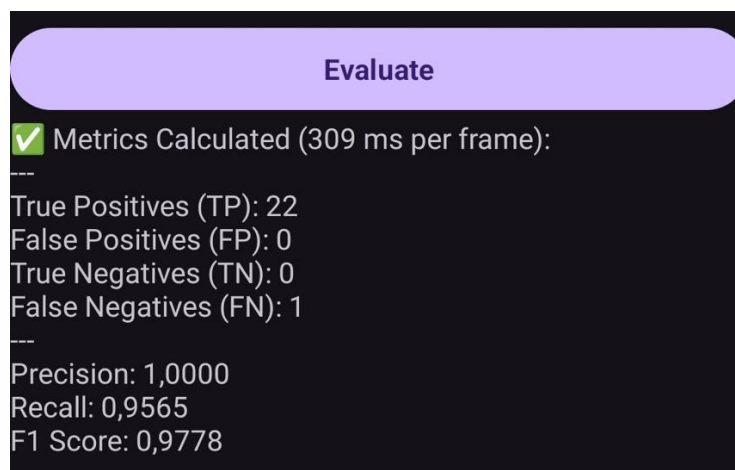


Рисунок 5.7 Отриманий результат тестування 3

Оцінка розпізнавання кадрів лише з електронною поштою: система виконала розпізнавання та класифікацію приватної інформації з такими показниками: True Positives (TP): 22; False Positives (FP): 0; True Negatives (TN):

0; False Negatives (FN): 1; Precision: 1,0000; Recall: 0,9565; F1 Score: 0,9778; середній час обробки кадру: 309 мс.

Електронні адреси виявилися найкраще розпізнаваним типом приватних даних. Precision = 1 і Recall = 0,96 свідчать, що: алгоритм впевнено розрізняє поштові адреси від довільного тексту, регулярні вирази для email працюють максимально стабільно, OCR добре зчитує символи, що типово містяться у поштових адресах. Лише один випадок неправильного розпізнавання був пов'язаний з тим, що електронна адреса частково виходила за межі кадру. F1 Score = 0,98 – найвищий результат серед усіх тестів.

- Тест 4 розпізнавання кадрів лише з IP-адресами (рис. 5.8):

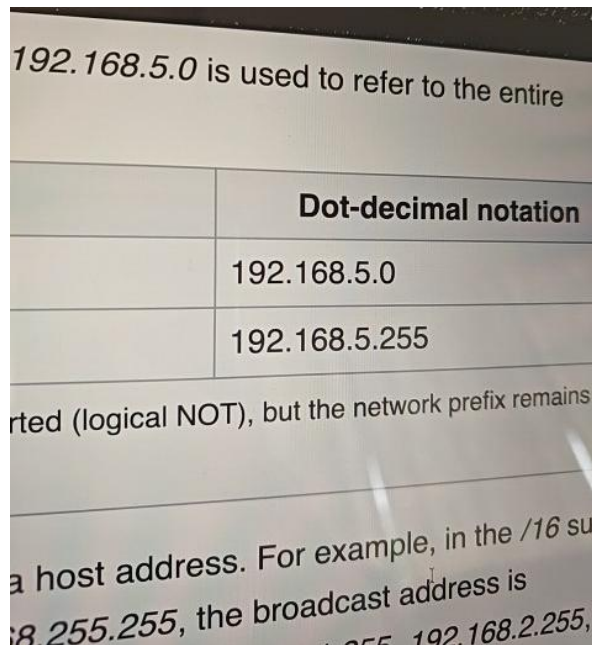


Рисунок 5.8 Приклад кадру з IP-адресою

Було знято коротке відео з якого за допомогою розробленої програми було обрано кадри, що містять текстову приватну інформацію, а саме IP-адреси, для тестування удосконаленого методу виявлення та захисту приватності відеоданих. Такі адреси є короткими та структурованими, тому тест оцінює точність роботи з цифровими послідовностями із крапками як роздільниками.

Результат розпізнавання кадрів лише з IP-адресами (дивись рис. 5.9):

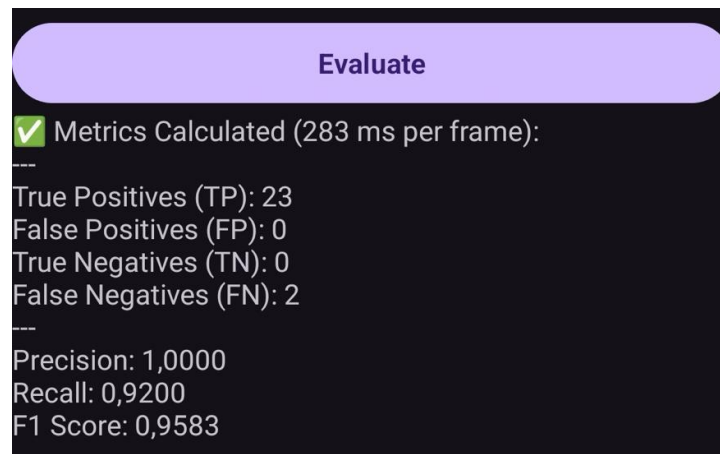


Рисунок 5.9 Отриманий результат тестування 4

Оцінка розпізнавання кадрів лише з IP-адресами: система виконала розпізнавання та класифікацію приватної інформації з такими показниками: True Positives (TP): 23; False Positives (FP): 0; True Negatives (TN): 0; False Negatives (FN): 2; Precision: 1,0000; Recall: 0,9200; F1 Score: 0,9583; середній час обробки кадру: 283 мс.

Алгоритм показав високу ефективність для тесту 4: Recall = 0,92 означає, що майже всі IP-адреси були виявлені правильно. FN = 2 виник через: низьку чіткість зображення в динамічних кадрах, можливе злиття цифр та крапок під час OCR. Максимальна точність підтверджує, що хибних визначень не було. F1 Score = 0,96 демонструє стабільну якість розпізнавання. Найменший час обробки серед усіх тестів (283 мс/кадр) пояснюється простішою структурою даних.

- Тест 5 розпізнавання кадрів лише з публічною інформацією (рис. 5.10):

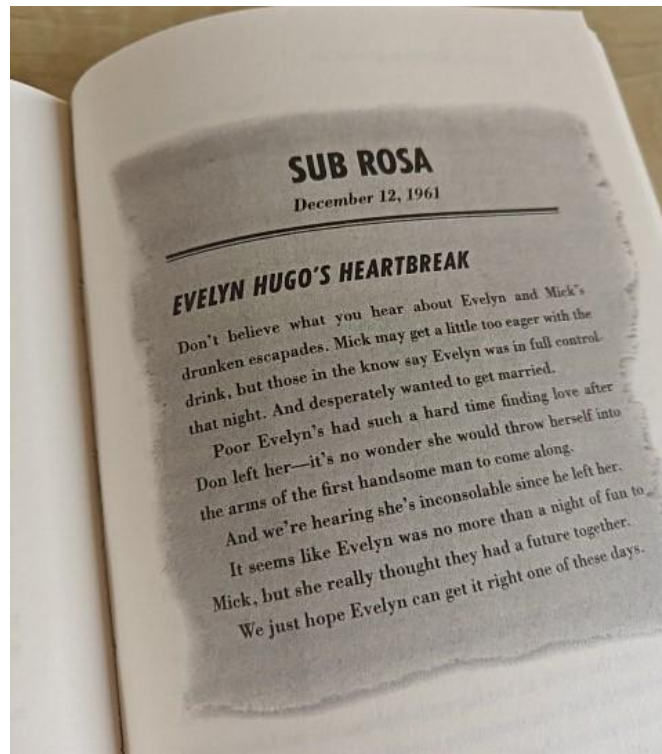


Рисунок 5.10 Приклад кадру з публічною інформацією

Було знято коротке відео з якого за допомогою розробленої програми було обрано кадри з текстовою публічною інформацією для тестування удосконаленого методу виявлення та захисту приватності відеоданих. Цей тест перевіряє стійкість алгоритму до хибно позитивних спрацювань, що є одним із найважливіших аспектів при роботі з анонімізацією.

Результат розпізнавання кадрів лише з публічною інформацією (дивись рис. 5.11):

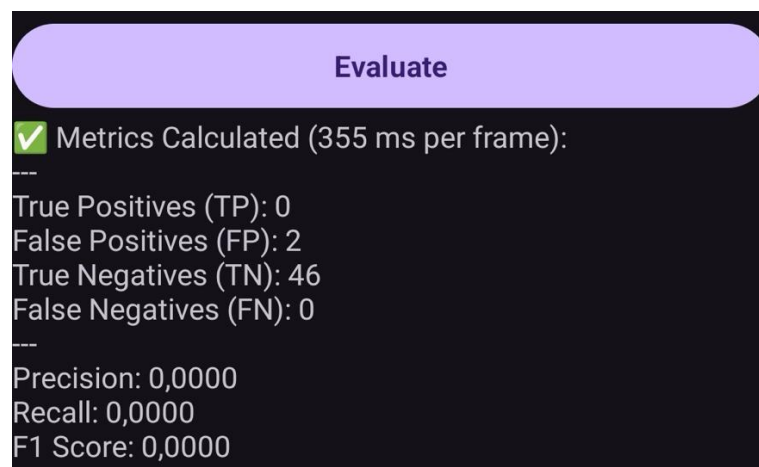


Рисунок 5.11 Отриманий результат тестування 5

Оцінка розпізнавання кадрів лише з публічною інформацією: система виконала розпізнавання та класифікацію приватної інформації з такими

показниками: True Positives (TP): 0; False Positives (FP): 2; True Negatives (TN): 46; False Negatives (FN): 0; Precision: 0,0000; Recall: 0,0000; F1 Score: 0,0000; середній час обробки кадру: 355 мс.

Оскільки тест 5 не містив приватної інформації, очікувані значення TP та FN мали дорівнювати нулю, що відповідає реальним результатам. Єдине, що аналізується – це FP. Було виявлено 2 хибно позитивні спрацювання, що становить лише ~4 % від усіх кадрів. Причини FP: наявність числових послідовностей, схожих на приватну інформацію. У реальних умовах показник FP є важливим, і його зниження потребує подальшого уточнення регулярних виразів та додаткової фільтрації символів. Середній час обробки кадру (355 мс) найбільший серед усіх тестів, що пояснюється великою кількістю довільного тексту на екрані.

- Тест 6 розпізнавання кадрів з приватною та публічною інформацією (рис. 5.12):

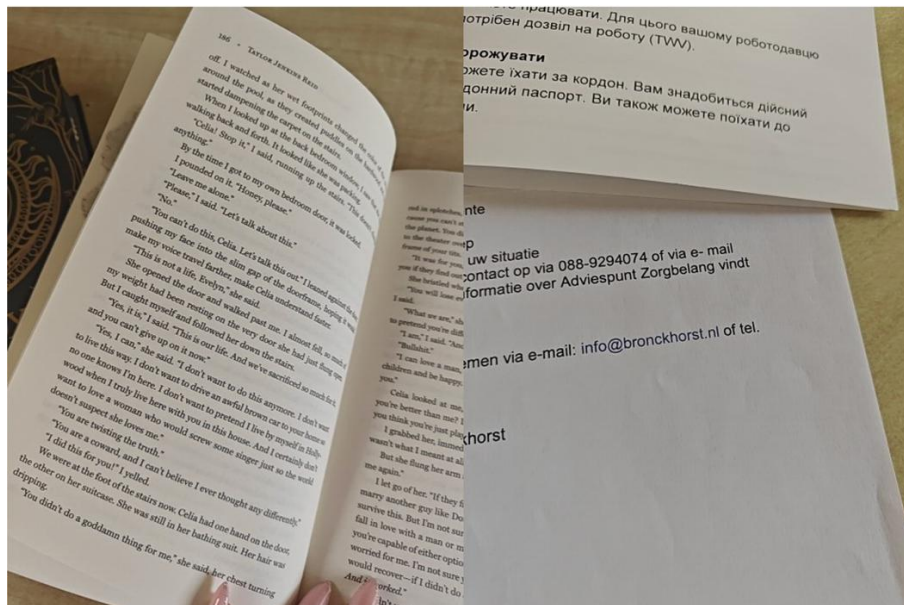


Рисунок 5.12 Приклад кадру з публічною інформацією та кадру з приватною інформацією

Було знято коротке відео з якого за допомогою розробленої програми було обрано кадри з текстовою приватною та публічною інформацією для тестування удосконаленого методу виявлення та захисту приватності відеоданих. Це найскладніший тип тестування, що моделює реальний

відеопотік, оскільки перевіряється здатність алгоритму працювати з фрагментами різної чутливості одночасно.

Результат розпізнавання кадрів з приватною та публічною інформацією (дивись рис. 5.13):

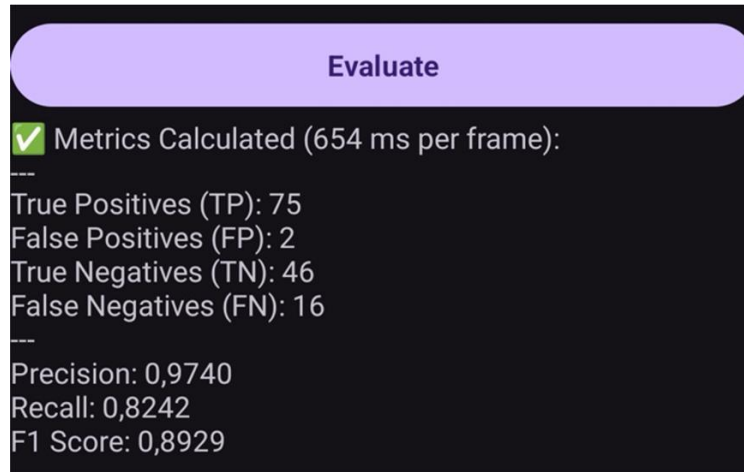


Рисунок 5.13 Загальний результат тестування 6

Оцінка розпізнавання кадрів з приватною та публічною інформацією: система виконала розпізнавання та класифікацію приватної інформації з такими показниками: True Positives (TP): 75; False Positives (FP): 2; True Negatives (TN): 46; False Negatives (FN): 16; Precision: 0,9740; Recall: 0,8242; F1 Score: 0,8929; середній час обробки кадру: 654 мс.

Тест 6 продемонстрував високу ефективність алгоритму в умовах змішаних типів даних: Precision = 0,97 дуже точне відокремлення приватної інформації від публічної, лише 2 хибно позитивних визначення. Recall = 0,82 понад 82% приватних даних було виявлено правильно, інші 16 випадків FN були пов'язані зі складністю сцени та різноманітністю форматів. F1 Score = 0,9 висока загальна якість у найбільш наближених до реальних умовах.

5.2 Аналіз удосконаленого методу для захисту приватності користувача при передачі відеоданих

Аналіз результатів тестування удосконаленого методу виявлення та захисту приватності відеоданих дозволяє комплексно оцінити його ефективність як у розпізнаванні приватної інформації, так і в продуктивності.

Проведені тести охоплювали різні типи текстових даних, що належать до категорії приватних: номери телефонів, банківські реквізити, електронні адреси та IP-адреси. Окремо було досліджено реакцію системи на публічний текст, а також змішані типи інформації, що найточніше моделює реальні сценарії роботи відеопотоку.

Модуль оптичного розпізнавання символів показав високу стійкість до кадрів середньої складності та структурованих даних. Найвищі значення Recall отримано у тестах з електронною поштою та IP-адресами. Це пояснюється тим, що OCR краще обробляє текст середньої довжини з чіткими роздільниками.

Найскладнішим виявився тип даних, пов'язаний з банківськими картами та IBAN. Розпізнавання довгих послідовностей дрібних цифр, особливо за умов слабкого освітлення або низької контрастності, призвело до зменшення Recall. Це вказує на необхідність подальшого підсилення попередньої обробки кадру.

У всіх тестах, що містили приватну інформацію, показник Precision = 1,0000 або близький до цього значення. Це підтверджує правильність побудови регулярних виразів та ефективність словникових моделей, що дозволяють уникнути хибних класифікацій.

Особливе значення має Тест 5 (публічний текст), у якому очікувалися нульові TP. Тут було зафіксовано лише 2 FP (~4 % усіх кадрів), що свідчить про високий рівень стійкості алгоритму до хибних спрацювань. Це важлива характеристика, оскільки у реальному відеопотоці публічна інформація з'являється значно частіше, ніж приватна.

F1 Score є збалансованим показником, який враховує як точність, так і повноту. Найкращі результати отримано у тестах з електронними адресами, IP-адресами та змішаному наборі даних. Це означає, що метод добре підходить для реальних відеосценаріїв, де зустрічаються різні типи приватної інформації.

Час обробки одного кадру варіювався від 283 мс до 654 мс залежно від складності текстового наповнення. Найшвидші результати отримано у тестах

із цифровими структурованими даними (ІР-адреси). Найповільніші у випадках змішаних типів даних, що потребувало одночасного застосування кількох регулярних шаблонів.

Для узагальнення проведено порівняння всіх тестів за такими параметрами: точність класифікації, повнота класифікації, F1 Score та середній час обробки кадру (табл. 5.1).

Таблиця 5.1 Порівняння отриманих тестових даних

Тип даних	TP	FP	TN	FN	Precision	Recall	F1 Score	Час/кадр
Телефонні номери	17	0	0	6	1,0000	0,7391	0,8500	319 мс
Банківські картки та IBAN	13	0	0	7	1,0000	0,6500	0,7879	294 мс
Електронні адреси	22	0	0	1	1,0000	0,9565	0,9778	309 мс
ІР-адреси	23	0	0	2	1,0000	0,9200	0,9583	283 мс
Змішаний текст	75	2	46	16	0,9740	0,8242	0,8929	654 мс

Удосконалений метод захисту приватних даних під час передачі відеопотоку демонструє високу ефективність у розпізнаванні приватної текстової інформації на мобільному пристрої. Алгоритм характеризується: максимальною точністю класифікації у всіх тестах з приватними даними; високою повнотою для більшості типів тексту; стійкістю до хибних розпізнавань.

Найскладнішими для розпізнавання виявилися довгі фінансові реквізити, що потребують додаткового покращення якості OCR. Попри це, загальний F1 Score у змішаному тесті становить 0,9, що підтверджує практичну придатність методу для реального використання в задачах анонімізації відеопотоків.

Висновок

У п'ятому розділі було проведено повне тестування та всебічний аналіз удосконаленого методу захисту приватної інформації на відео. Тестування

охоплювало функціональні характеристики системи (розпізнавання та класифікація приватного тексту) та показники продуктивності (час обробки кадру, стабільність роботи на мобільному пристрої).

На основі результатів тестів підтверджено коректність роботи всіх етапів методу: попередня обробка кадрів забезпечує якісне введення для OCR; модуль оптичного розпізнавання символів демонструє високу точність з більшістю структурованих даних; регулярні вирази та словникові моделі дозволяють максимально точно ідентифікувати приватну текстову інформацію; механізм класифікації стійкий до хибних позитивних спрацювань.

Показник Precision у всіх тестах із приватною інформацією становив 1,0000, що свідчить про відсутність помилкових визначень приватного тексту як публічного. Це є ключовою вимогою систем анонімізації відеопотоків, оскільки хибні спрацювання можуть призводити до втрати важливої контекстної інформації. Показники Recall та F1 Score підтвердили, що метод забезпечує високу повноту виявлення приватних даних. Тест на публічному тексті підтвердив низький рівень хибних позитивних спрацювань, що демонструє високу стійкість алгоритму до неоднозначних випадків та великої кількості несуттєвої інформації у кадрі. Продуктивна частина тестування показала, що найбільше навантаження спостерігалось під час аналізу змішаних відеокадрів, де одночасно присутні кілька типів текстової інформації.

Таким чином, результати тестування та аналізу демонструють, що запропонований удосконалений метод захисту приватності користувача відповідає поставленим вимогам й забезпечує якісний рівень захисту приватних текстових даних у відеопотоці.

РОЗДІЛ 6

РОЗРОБКА СТАРТАП ПРОЄКТУ

6.1 Опис стартап проєкту

Стартап проєкт спрямований на створення додатку, що автоматично розпізнає текстову інформацію у відео та анонімізує конфіденційні приватні дані користувачів для забезпечення приватності. Основна функціональність полягає у виявленні фрагментів тексту, які містять персональні або чутливі дані (ПІБ, адреси, номери банківських карток та паспортів тощо), з подальшою їх анонімізацією. Система орієнтована на автоматизацію процесів попередньої обробки відео перед публікацією у відкритих джерелах або передачею стороннім сторонам. Це дозволяє уникнути витoku приватної інформації, який може стати наслідком людського фактору або недосконалого ручного редагування.

Метою проєкту є оцінка доцільності реалізації додатку, який дозволить у реальному часі:

- виявляти текстові фрагменти за допомогою технології Google ML Kit Text Recognition;
- здійснювати класифікацію виявленого тексту за типами приватності;
- автоматично анонімізувати потенційно небезпечні для приватності елементи;
- забезпечувати повну локальну обробку без передавання відео до хмарних сервісів, що гарантує безпеку персональних даних користувачів.

Проєкт поєднує елементи комп'ютерного зору, обробки природної мови та захисту даних, створюючи рішення, яке може знайти практичне застосування у медіа, журналістиці, бізнесі та соціальних мережах.

Розглянемо загальні характеристики проєкту (табл. 6.1):

Таблиця 6.1 Загальні характеристики проєкту

Показник	Значення
Ціль проєкту	Захист приватних текстових даних при обробці відео/зображень; запобігання витоку конфіденційної приватної інформації; забезпечення відповідності законодавчим нормам
Цільова аудиторія	Маркетингові агенції; розробники мобільних застосунків; відеоредактори; журналісти; блогери; стрімери
Джерела доходів	Підписки (Pro/Business); продаж реклами у застосунку
Унікальні переваги проєкту	Локальна обробка без відправки даних у хмару; швидка робота; легка інтеграція з відеоредакторами
Вигоди для користувачів	Захист приватних даних; підвищення довіри клієнтів; зниження ризиків порушення приватності
Ключові ризики	Низька якість відео, помилкове розпізнавання, конкуренція

Визначення сильних, нейтральних та слабких факторів проєкту (дивись табл. 6.2):

Таблиця 6.2 Сильні, нейтральні та слабкі фактори проєкту

Категорія	Опис
Сильні фактори	Використання готових рішень; відсутність потреби у власних серверах; високий рівень приватності; можливість локальної обробки даних
Нейтральні фактори	Конкуренція з існуючими сервісами; потреба у просуванні та маркетингу; технічні обмеження мобільних пристроїв
Слабкі фактори	Залежність від якості відео; можливі помилки при розпізнаванні тексту

Вхідні дані проєкту:

- Основні дані: відео з текстовою інформацією;
- Платформа для розробки застосунку: Android Studio;
- Мова програмування: Kotlin;
- Тип проєкту: мобільний застосунок;
- Тип доступу: локальний.

Проєкт є технічно здійсненним завдяки використанню готових рішень Google ML Kit Text Recognition для розпізнавання тексту, що не вимагають потужних серверів та локальної обробки, що підвищує швидкість роботи й зменшує витрати на сервери та гарантує збереження приватності користувачів.

6.2 Оцінка стартап проєкту

Мета оцінки стартап проєкту полягає у визначенні економічної доцільності, фінансової ефективності та прибутковості впровадження системи автоматичного розпізнавання і анонімізації тексту у відео. Фінансова оцінка стартап-проєкту дозволяє визначити прибутковість, термін окупності та інвестиційну привабливість проєкту. Основними джерелами доходу є підписки користувачів та рекламні надходження, а прогноз розвитку базується на поступовому збільшенні кількості користувачів протягом трирічного періоду.

Початкові пункти для розрахунку фінансових показників:

1. Користувачі: зростання від 500 до 10 000 (30% – користувачі з підпискою, 70% – безкоштовні користувачі).
2. Підписки: 70% користувачів – Pro (800 грн/міс), 30% користувачів – Business (2000 грн/міс). Середня вартість підписки 1160 грн/міс або 3480 грн/квартал.
3. Реклама: 200 грн/користувач/квартал.

Короткий опис фінансових витрат:

1. Вартість використання: включає плату за ліцензування програмного забезпечення, мобільні платформи, а також витрати на розміщення застосунку в маркетплейсах.

2. Технічні витрати: складається з розробки застосунку, технічної підтримки користувачів, оновлення системи розпізнавання тексту, тестування та усунення помилок.

3. Адміністративні витрати: містять оплату праці за бухгалтерські та юридичні послуги, оренду офісного приміщення та комунальні платежі.

4. Витрати на рекламу/маркетинг: входять цифрова реклама, SEO та контент-маркетинг, SMM (соціальні мережі), PR та партнерські кампанії, програми лояльності та промоакції.

Основні положення фінансової оцінки:

1. Прогноз кількості користувачів протягом 3 років (табл. 6.3);
2. Прогноз доходів від підписок та реклами (табл. 6.4);
3. Прогноз витрат на технічне, маркетингове, адміністративне забезпечення (табл. 6.5);
4. Розрахунок прибутку, податків та грошового потоку (табл. 6.6);
5. Підсумкові фінансові показники проекту (табл. 6.7).

Оцінку проводили з урахуванням таких параметрів:

1. Податкова ставка – 22%;
2. Процентна ставка дисконтування (для NPV) – 10%;
3. Період прогнозування – 3 роки (12 кварталів);
4. Валюта розрахунку – гривня.

На початковому етапі проект орієнтований на 500 користувачів, з поступовим зростанням до 10 000 активних користувачів наприкінці третього року. При цьому близько 30% користувачів користується платною підпискою.

Таблиця 6.3 Прогноз кількості користувачів

Рік	Квартал	Кількість користувачів	Підписники (30%)
1	1 кв	500	150
1	2 кв	800	240
1	3 кв	1 200	360
1	4 кв	2 000	600
2	1 кв	3 000	900
2	2 кв	4 000	1 200

Продовження таблиці 6.3 Прогноз кількості користувачів

2	3 кв	5 500	1 650
2	4 кв	7 000	2 100
3	1 кв	8 000	2 400
3	2 кв	9 000	2 700
3	3 кв	9 500	2 850
3	4 кв	10 000	3 000

Основними джерелами доходу є: підписки Pro (800 грн/міс) і Business (2000 грн/міс), середня ціна підписки становить 3480 грн/квартал та реклама 200 грн з одного користувача на квартал.

Таблиця 6.4 Прогноз доходу проєкту

Кв	Підписки	Реклама	Загальний дохід
1	522 000	70 000	592 000
2	835 200	112 000	947 200
3	1 252 800	168 000	1 420 800
4	2 088 000	280 000	2 368 000
1	3 132 000	420 000	3 552 000
2	4 176 000	560 000	4 736 000
3	5 742 000	770 000	6 512 000
4	7 308 000	980 000	8 288 000
1	8 352 000	1 120 000	9 472 000
2	9 396 000	1 260 000	10 656 000
3	9 918 000	1 330 000	11 248 000
4	10 440 000	1 400 000	11 840 000

Витрати включають усі основні статті, необхідні для забезпечення життєвого циклу проєкту: технічна підтримка, реклама, адміністративні послуги, інші супутні витрати.

Таблиця 6.5 Прогноз витрат проєкту

Кв	Технічне обслуговування	Реклама /маркетинг	Адміністративні витрати	Інші витрати	Загальні витрати
1	400 000	480 000	600 000	200 000	1 680 000
2	400 000	480 000	600 000	200 000	1 680 000
3	400 000	480 000	600 000	200 000	1 680 000

Продовження таблиці 6.5 Прогноз витрат проєкту

4	400 000	480 000	600 000	200 000	1 680 000
1	800 000	640 000	800 000	400 000	2 640 000
2	800 000	640 000	800 000	400 000	2 640 000
3	800 000	640 000	800 000	400 000	2 640 000
4	800 000	640 000	800 000	400 000	2 640 000
1	1 200 000	800 000	1 000 000	400 000	3 400 000
2	1 200 000	800 000	1 000 000	400 000	3 400 000
3	1 200 000	800 000	1 000 000	400 000	3 400 000
4	1 200 000	800 000	1 000 000	400 000	3 400 000

Чистий прибуток – це прибуток від проєкту після вирахування всіх витрат та податків. Він показує фактичний дохід, який залишається у розпорядженні після сплати податків і може бути використаний для реінвестування, виплати дивідендів або покриття поточних потреб.

Грошовий потік – це накопичення чистого прибутку (або збитків) за кожен період діяльності. Грошовий потік дає змогу визначити момент, коли проєкт переходить від збитковості до прибутковості (точку беззбитковості).

Таблиця 6.6 Прогноз прибутку і грошового потоку проєкту

Кв	Доходи	Витрати	Прибуток до податків	Податок 22 %	Чистий прибуток	Грошовий потік
1	592 000	1 680 000	-1 088 000	—	-1 088 000	-1 088 000
2	947 200	1 680 000	-732 800	—	-732 800	-1 820 800
3	1 420 800	1 680 000	-259 200	—	-259 200	-2 080 000
4	2 368 000	1 680 000	688 000	151 360	536 640	-1 543 360
1	3 552 000	2 640 000	912 000	200 640	711 360	-832 000
2	4 736 000	2 640 000	2 096 000	461 120	1 634 880	802 880
3	6 512 000	2 640 000	3 872 000	851 840	3 020 160	3 823 040
4	8 288 000	2 640 000	5 648 000	1 242 560	4 405 440	8 228 480
1	9 472 000	3 400 000	6 072 000	1 335 840	4 736 160	12 964 640
2	10 656 000	3 400 000	7 256 000	1 596 320	5 659 680	18 624 320
3	11 248 000	3 400 000	7 848 000	1 726 560	6 121 440	24 745 760
4	11 840 000	3 400 000	8 440 000	1 856 800	6 583 200	31 328 960

Чиста поточна вартість обчислюється за формулою (6.1):

$$NPV = \sum_{t=0}^n \frac{S_t}{(1+i)^t}, \quad (6.1)$$

де S_t – чистий грошовий потік у період t ; i – процентна ставка дисконтування для одного періоду; n – номер останнього досліджуваного періоду (горизонт інвестиції).

Внутрішня норма прибутку обчислюється за формулою (6.2):

$$\sum_{t=0}^n \frac{S_t}{(1+IRR)^t} = 0, \quad (6.2)$$

де S_t – чистий грошовий потік у період t ; n – номер останнього досліджуваного періоду (горизонт інвестиції).

Таблиця 6.7 Підсумкові фінансові показники проєкту

Показник	Значення
Чистий прибуток за 3 роки	31 328 960 грн
NPV 10%	24 455 631 грн
IRR	48%
Термін окупності	6 кварталів (1,5 роки)

Для представлення розрахованих фінансових показників стартап проєкту нижче наведено графік (дивись рис. 6.1):

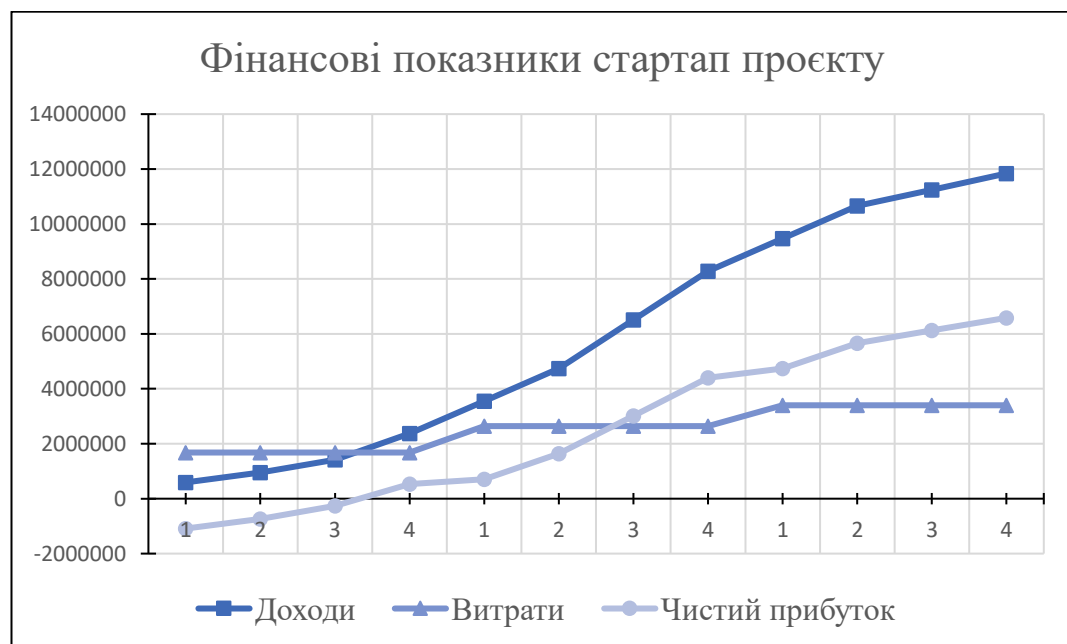


Рисунок 6.1 Фінансові показники стартап проєкту

Результати розрахунку показують, що найбільшу частку витрат складають адміністративні та маркетингові витрати, тоді як технічні витрати та обслуговування мають стабільну тенденцію зростання у міру масштабування. Основним фактором підвищення прибутковості є зростання кількості підписників. Позитивний чистий грошовий потік формується з другого року роботи, що робить проєкт перспективним для подальшого розвитку. Високе значення NPV та IRR свідчить про високу інвестиційну привабливість проєкту, а короткий термін окупності робить його фінансово стійким.

Висновок

У шостому розділі було виконано оцінку фінансової ефективності стартап проєкту, спрямованого на захист приватних текстових даних у відео. Розрахунки показали, що проєкт є економічно доцільним, технічно здійсненним та фінансово рентабельним.

Незважаючи на початкові витрати, уже на другий рік діяльності система забезпечує стабільний позитивний грошовий потік. Показники $NPV = 24\,455\,631$ грн, $IRR = 48\%$ та термін окупності 1,5 роки підтверджують високу рентабельність і можливість подальшого масштабування продукту на міжнародний ринок.

Для оцінки фінансової ефективності проєкту було проведено розрахунки основних показників: доходів, витрат, прибутку, грошового потоку, чистої поточної вартості (NPV) та внутрішньої норми прибутку (IRR). Розрахунки здійснювалися на основі прогнозних даних кількості користувачів (табл. 6.3), доходів (табл. 6.4), витрат (табл. 6.5), прибутку (табл. 6.6) та підсумкових показників (табл. 6.7).

ЗАГАЛЬНІ ВИСНОВКИ

Досліджено актуальні методи забезпечення приватності користувачів при передачі відеоданих, що включає як технічні, так і законодавчі аспекти. Потреба в безпеці відеоінформації, зокрема через зростаючий обсяг онлайн-комунікацій, набуває особливого значення. У дисертації розглянуто основні підходи до захисту конфіденційних приватних даних, застосування різних методів шифрування та анонімізації, а також сучасні технології для виявлення загроз приватності, зокрема за допомогою штучного інтелекту. Та отримано наступні результати:

1. За результатами дослідження показано, що поєднання різних технічних підходів і використання сучасних алгоритмів для шифрування, анонімізації та виявлення загроз приватності дозволяє значно підвищити захист відеоданих. Водночас необхідно враховувати обмеження кожного з методів і оптимізувати їх використання в залежності від конкретних умов і вимог.

2. З точки зору законодавства, інтеграція стандартів GDPR у європейському просторі забезпечує ефективний захист текстових персональних даних, включаючи відеоінформацію, а відповідні норми в США та Україні сприяють розвитку глобальних підходів до захисту приватності. Важливою є також перспектива вдосконалення законодавчих ініціатив, спрямованих на підвищення стандартів захисту відеоданих.

3. Проаналізовано існуючі методи виявлення та захисту приватних даних. Детально досліджено категорії приватної інформації у відео з законодавчої та користувацької точок зору. Узагальнено результати наукових праць, що демонструють потребу у вдосконаленні, адже обробка відео нерідко пов'язана з появою приватних текстових даних, які необхідно ідентифікувати та анонімізувати. Також підтверджено наукову новизну напрямку, оскільки існуючі рішення не забезпечують локальну, автономну обробку даних в режимі реального часу.

4. Під час розробки удосконаленого методу захисту приватних відеоданих було обґрунтовано вибір технічних підходів та архітектури рішення, зокрема

поєднання OCR, словникових фільтрів та регулярних виразів для виявлення текстової інформації у відео. Також було представлено математичну й фізичну модель рішення, що забезпечують автономну обробку без передачі відеоданих на зовнішні сервери. Підкреслено переваги такого методу, серед яких підвищена безпека, мінімізація ризику витоку приватної інформації та можливість масштабування під різні сценарії застосування.

5. Проведено всебічну оцінку ефективності розробленого удосконаленого методу захисту приватності користувача. Тестування додатку в умовах, максимально наближених до реальних, підтвердило коректність роботи всіх етапів: від виявлення текстових даних до їхньої анонімізації. Було враховано два ключові типи перевірки: функціональне тестування та тестування продуктивності. Отримані результати доводять, що метод забезпечує стабільність, точність і достатню швидкодію для застосування на мобільних пристроях.

6. Представлено практичну реалізацію у вигляді стартап-проєкту та оцінено перспективи впровадження розробленого удосконаленого методу виявлення та захисту приватності відеоданих. На основі виконаних досліджень та тестувань сформовано бачення продукту, його потенційну ринкову нішу та ключові переваги в контексті сучасних викликів щодо приватності у відео комунікаціях.

Таким чином, під час дослідження послідовно доведено актуальність проблеми, сформовано науково обґрунтований підхід до її вирішення, розроблено удосконалений метод захисту приватності користувача і підтверджено його ефективність тестуванням.

Результати роботи апробовано на конференціях «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2025 та "Перспективи телекомунікацій" ПТ-2025, що підтверджує релевантність дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Огнівчук Марія. Прогноз кіберзагроз 2024. H-X Technologies. [Електронний ресурс] – URL: <https://www.h-x.technology/ua/blog-ua/cyber-threats-forecast-2024-ua>.
2. KANKONKAR, Jyoti TG; NAIK, Nitesh. Image security using image encryption and image stitching. In: 2017 International Conference on Computing Methodologies and Communication (ICCMC). IEEE, 2017. p. 151-154.
3. PRANGGONO, Bernardi; ARABO, Abdullahi. COVID-19 pandemic cybersecurity issues. Internet Technology Letters, 2021, 4.2: e247.
4. LALLIE, Harjinder Singh, et al. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 2021, 105: 102248.
5. Захист інформації в телекомунікаційних системах: Навчальний посібник (лист МОНУ №1.4/18 – Г – 183 від 02.06.2009 р.) / Г.Ф. Конахович, В.П. Климчук, С.М. Паук, В.Г. Потапов, В.М. Чуприн, О.О. Горбунов. – 380 с.
6. SHAFIQ, Sobia, et al. Video encryption techniques: A review. In: 2019 International Conference on Digitization (ICD). IEEE, 2019. p. 174-177.
7. IMAM, Raza, et al. Systematic and critical review of rsa based public key cryptographic schemes: Past and present status. IEEE access, 2021, 9: 155949-155976.
8. Міжнародна конференція «Передові технології в інформаційно-комунікаційній інженерії» (ATICE'2023). Матеріали конференції/Міжнародний гуманітарний університет, Одеса, 2023: Бондаренко М.О., 2023. – 102 с.
9. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються?. Hostpro Wiki. [Електронний ресурс] – URL: <https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/>.
10. SEN, Jaydip. Homomorphic encryption-theory and application. Theory and practice of cryptography and network security protocols and technologies, 2013, 31.

11. ACAR, Abbas, et al. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (Csur)*, 2018, 51.4: 1-35.
12. Анонімізація і псевдонімізація даних за GDPR: що це означає на практиці. Legal IT group. [Електронний ресурс] – URL: <https://legalitgroup.com/sprava-t-557-20-znachennya-ta-vpliv-na-zahist-danih/>.
13. Exploring AI-based Anonymization of Industrial Image and Video Data in the Context of Feature Preservation | AI Research Paper Details. Your Roadmap to the AI Revolution – AIModels.fyi. [Електронний ресурс] – URL: <https://www.aimodels.fyi/papers/arxiv/exploring-ai-based-anonymization-industrial-image-video>.
14. BINDEMANN, Markus, et al. The effect of image pixelation on unfamiliar-face matching. *Applied Cognitive Psychology*, 2013, 27.6: 707-717.
15. CRETE, Frederique, et al. The blur effect: perception and estimation with a new no-reference perceptual blur metric. In: *Human vision and electronic imaging XII*. SPIE, 2007. p. 196-206.
16. MIVULE, Kato. Utilizing noise addition for data privacy, an overview. *arXiv preprint arXiv:1309.3958*, 2013.
17. TRIESS, Sabrina C.; LEITRITZ, Timo; JAUCH, Christian. Exploring AI-based Anonymization of Industrial Image and Video Data in the Context of Feature Preservation. In: *2024 32nd European Signal Processing Conference (EUSIPCO)*. IEEE, 2024. p. 471-475.
18. Data Privacy Laws Worldwide | Ultimate Overview 2023. Actonic – Unfolding your potential. [Електронний ресурс] – URL: <https://actonic.de/en/data-privacy-laws-worldwide-ultimate-overview-2023/#1680168010723-12077be8-9af6>.
19. General Data Protection Regulation (GDPR) – Legal Text. General Data Protection Regulation (GDPR). [Електронний ресурс] – URL: <https://gdpr-info.eu/>.

20. Лугановська Є. GDPR: 10 порад щодо адаптації бізнесу до його вимог [Електронний ресурс] / Є. Лугановська // eba. – 2019. – URL: <https://eba.com.ua/gdpr-10-porad-shhodo-adaptatsiyi-biznesu-do-jogo-vymog/>.
21. Нужний В. Нові вимоги ЄС до захисту персональних даних з травня 2018 року | Channel4IT.com. Світ IT та кібербезпеки. [Електронний ресурс] – URL: <https://channel4it.com/publications/Nov-vimogi-S-do-zahistu-personalnih-danih-z-travnnya-2018-roku-30154.html>.
22. GDPR: General чи все-таки Global? [Електронний ресурс] // Журнал «Вісник МСФЗ». – 2018. – № 6. – URL: https://msfz.ligazakon.ua/ua/magazine_article/FZ001542.
23. Überarbeitung L. What is CCPA?. Actonic – Unfolding your potential. [Електронний ресурс] – URL: <https://actonic.de/en/knowledge-base/what-is-ccpa/>.
24. Modispacher P. How to comply with CCPA: the ultimate guide for 2023. Actonic – Unfolding your potential. [Електронний ресурс] – URL: <https://actonic.de/en/how-to-comply-with-ccpa-the-ultimate-guide-for-2023/>.
25. Modispacher P. How to comply with the CCPA Right to Know. Actonic – Unfolding your potential. [Електронний ресурс] – URL: <https://actonic.de/en/how-to-comply-with-the-ccpa-right-to-know/>.
26. Modispacher P. Significant changes to CCPA in 2023 – an overview. Actonic – Unfolding your potential. [Електронний ресурс] – URL: <https://actonic.de/en/significant-changes-to-ccpa-in-2023-an-overview/>.
27. Modispacher P. How CCPA changes in 2023 affect your business. Actonic – Unfolding your potential. [Електронний ресурс] – URL: <https://actonic.de/en/how-ccpa-changes-in-2023-affect-your-business/>.
28. Закон України «Про захист персональних даних» [Електронний ресурс] // Законодавство України. – 2019. – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/2297-17>.

29. Averina V. CCPA vs. GDPR: data privacy laws in Europe and the USA. Actonic – Unfolding your potential. [Електронний ресурс] – URL: <https://actonic.de/en/ccpa-vs-gdpr-data-privacy-laws-in-europe-and-the-usa/>.
30. Modispacher P. Data Privacy Laws explained. Actonic – Unfolding your potential. [Електронний ресурс] – URL: <https://actonic.de/en/privacy-policy-comparison/>.
31. Überarbeitung L. What is the difference between de-identification/pseudonymization (CCPA) and anonymization (GDPR)? Actonic – Unfolding your potential. [Електронний ресурс] – URL: <https://actonic.de/en/knowledge-base/what-is-the-difference-between-de-identification-pseudonymization-ccpa-and-anonymization-gdpr/>.
32. OREKONDY, Tribhuvanesh; SCHIELE, Bernt; FRITZ, Mario. Towards a visual privacy advisor: Understanding and predicting privacy risks in images. In: Proceedings of the IEEE international conference on computer vision. 2017. p. 3686-3695.
33. Що таке OCR (оптичне розпізнавання символів)? Переваги, проблеми та випадки використання [Інфографіка]. [Електронний ресурс] – URL: <https://uk.shaip.com/blog/ocr-definition-benefits-challenges-and-use-cases-infographic/>.
34. Text recognition v2 | ML Kit | Google for Developers. Google for Developers. [Електронний ресурс] – URL: <https://developers.google.com/ml-kit/vision/text-recognition/v2>.
35. Солоденко М.А. «РОЗПІЗНАВАННЯ ТА ЗАХИСТ ТЕКСТОВИХ ПРИВАТНИХ АТРИБУТІВ КОРИСТУВАЧІВ МОБІЛЬНИХ ПРИСТРОЇВ В МЕДІАДАНИХ» // XVII науково-технічна конференція студентів та аспірантів «Перспективи розвитку інформаційно-телекомунікаційних технологій та систем» ПРІТС 2025: Збірник тез конференції. К.: КПІ ім. Ігоря Сікорського, 2025. – с. 367.
36. Солоденко М.А., Педан С.І. «ДОСЛІДЖЕННЯ ЗАКОНОДАВЧИХ АСПЕКТІВ ЗАХИСТУ ПРИВАТНОСТІ ПРИ ПЕРЕДАЧІ ВІДЕОДАНИХ» //

XIX Міжнародна науково-технічна конференція "Перспективи телекомунікацій" ПТ-2025: Збірник матеріалів конференції. К.: КПІ ім. Ігоря Сікорського, 2025. – с. 249.

37. Redact sensitive data from images | Sensitive Data Protection | Google Cloud. Google Cloud. [Електронний ресурс] – URL: https://cloud.google.com/sensitive-data-protection/docs/redacting-sensitive-data-images?utm_source=chatgpt.com.

38. Veritone Redact: Quick Start Guide. Support Veritone. [Електронний ресурс] – URL: https://support.veritone.com/s/article/000001464?language=en_US.

39. BAJPAI, Rishabh; ARAVAMUTHAN, Bhooma. SecurePose: Automated Face Blurring and Human Movement Kinematics Extraction from Videos Recorded in Clinical Settings. arXiv preprint arXiv:2402.14143, 2024.

40. NEWTON, Elaine M.; SWEENEY, Latanya; MALIN, Bradley. Preserving privacy by de-identifying face images. IEEE transactions on Knowledge and Data Engineering, 2005, 17.2: 232-243.

41. Download Android Studio & App Tools – Android Developers. Android Developers. [Електронний ресурс] – URL: <https://developer.android.com/studio>.

42. Kotlin and Android | Android Developers. Android Developers. [Електронний ресурс] – URL: <https://developer.android.com/kotlin>.