Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
Завідуюча кафедри кібербезпеки
та захисту інформації
_____ Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Використання цифрових водяних знаків, як додаткового елементу в захисті інформаційних ресурсів компанії»

Виконавець: студентка IV курсу, групи КБ-42

_____ **Олександра КЛИМЕНКО**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник	Юрій ЩЕБЛАНІН.	

Нормоконтроль	Сергій ДАКОВ	

Київ 2022

Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідуюча кафедри кібербезпеки
та захисту інформації
_____ Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** **Клименко Олександрі Богданівній**
(група) (прізвище ім'я по батькові)

Тема дипломної роботи Використання цифрових водяних знаків, як додаткового елементу в захисті інформаційних ресурсів компанії

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Інформаційні ресурси компанії, системи захисту інформації, цифрові водяні знаки, технології використання цифрових водяних знаків в системах захисту інформації

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно розглянути поняття цифрового водяного знаку, дослідити особливості захисту інформації на підприємстві, проаналізувати роль ЦВЗ у захисті інформаційних ресурсів компанії а також реалізувати алгоритм вбудування водяного знаку в цифровий об'єкт

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблений алгоритм внесення цифрових водяних знаків в контент задля додаткового захисту інформаційних ресурсів компанії

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Олександра КЛИМЕНКО (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021– 22.11.2021	*виконано*
2	Аналіз літератури	23.11.2021 – 09.12.2021	*виконано*
3	Обґрунтування вибору рішення	07.12.2022 - 23.12.2022	*виконано*
4	Концепція хмарних обчислень	24.12.2022- 08.01.2022	*виконано*
5	Аналіз проблем інформаційної безпеки в хмарних технологіях	09.01.2022 – 29.01.2022	*виконано*
6	Дослідження вразливостей та загроз	30.01.2022-03.03.2022	*виконано*
7	Розробка рекомендацій щодо вибору хмарної послуги і методу захисту даних, що використовуються в хмарних сервісах	04.03.2022 – 17.04.2022	*виконано*
8	Оформлення пояснювальної записки	18.04.2022 – 29.05.2022	*виконано*
9	Підготовка до захисту дипломної роботи	01.06.2022 – 13.06.2022	*виконано*

Завдання видав _____ (підпис) Юрій ЩЕБЛАНІН (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Олександра КЛИМЕНКО (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Використання цифрових водяних знаків, як додаткового елементу в захисті інформаційних ресурсів компанії» складається зі вступу, основної частини, що містить 3 розділи, списку літератури, джерел та висновку. Загальний обсяг роботи – 42 сторінки. Робота містить 7 рисунків. Список використаних джерел включає 22 джерела.

Об'єкт дослідження – захист інформаційних ресурсів компанії за допомогою цифрових водяних знаків.

Предмет дослідження – цифрові водяні знаки.

Метод дослідження – обробка інформації щодо цифрових водяних знаків і використання її на практиці.

Результати отриманих у дипломній роботі досліджень можуть бути використані спеціалістами із захисту інформації та при подальшому проведенні науково-дослідницьких робіт.

Напрямки подальших досліджень: створення подібних моделей захисту інформаційних ресурсів компанії з використанням цифрового водяного знаку, як додаткового елементу.

Ключові слова: цифрові водяні знаки, захист інформаційних ресурсів компанії.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ЦВЗ	–	Цифровий водяний знак
POS	–	Point of sales
ІВ	–	Інтелектуальна власність
СІБ	–	Система інформаційної безпеки
DRM	–	Digital rights management
PIL	–	Python Image Library
QR-код	–	Quick Response код
ПЗ	–	Програмне забезпечення
BDF	–	Bitmap Distribution Format
IPR	–	Intellectual Property Rights

ЗМІСТ

ВСТУП

Актуальність даної роботи визначається тим, що у наші часи, захист особистих даних це дуже важлива проблема. Загрози, що властиві веб-простору, безпосередньо впливають на підприємства України. У тому числі загрози викрадення інформації, підробки даних, зловмисного комерційного використання, тощо. Цифровий водяний знак у такому сенсі виступає одним з елементів ефективного захисту інформаційних ресурсів, який потребує дослідження.

Тому метою роботи є розробка алгоритму внесення цифрових водяних знаків в контент задля додаткового захисту інформаційних ресурсів компанії.

Для досягнення цієї мети було необхідно вирішити такі завдання:

- Розглянути поняття ЦВЗ, систему ЦВЗ;
- Дослідити особливості захисту інформації на підприємстві;
- Проаналізувати роль ЦВЗ у захисті інформації підприємства;
- Реалізувати алгоритм використання ЦВЗ у цифровий об’єкт.

Практичне значення роботи полягає у аналізі цифрових водяних знаків для інформаційної безпеки компанії та практичній реалізації алгоритму цифрових водяних знаків.

Об’єктом дослідження в даній роботі є захист інформаційних ресурсів компанії за допомогою цифрових водяних знаків.

Предметом дослідження в даній роботі є цифрові водяні знаки.

Методи дослідження

- обробка інформації щодо цифрових водяних знаків;
- аналіз документів, статей, нормативно-правової бази щодо захисту інформації на підприємстві;
- використання отриманих знань на практиці для реалізації алгоритму використання ЦВЗ для захисту інформаційних ресурсів компанії.

РОЗДІЛ 1
ЦИФРОВИЙ ВОДЯНИЙ ЗНАК

1.1 Поняття цифрового водяного знаку

Цифровий водяний знак - це різновид цифрової мітки, приховано вбудованої в дані цифрового зображення. Він використовується для визначення права власності на такий файл, щоб уникнути небажаного розповсюдження, особливо через Інтернет [1]. Ключові сфери застосування ЦВЗ наведено на рис. 1.1.

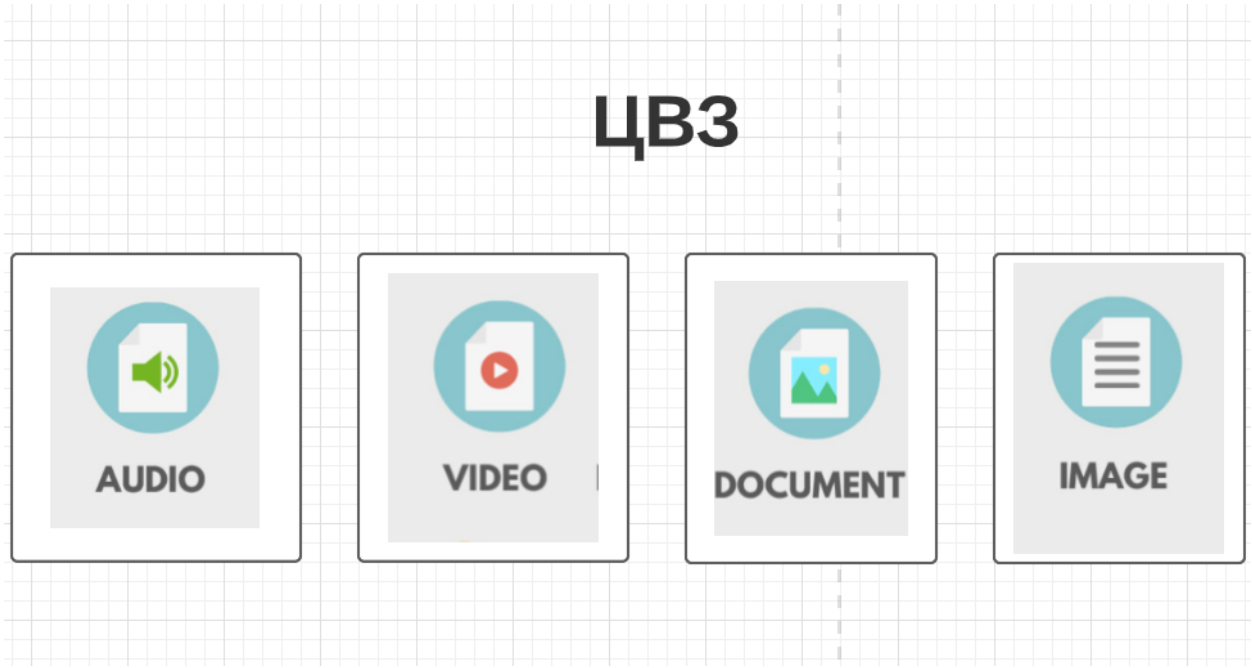

Рисунок 1.1 – Ключові сфери застосування ЦВЗ.

Невидимі ЦВЗ вбудовуються в цифрові носії інформації в такий спосіб, що користувачеві має труднощі при виявленні вбудованої мітки, якщо він не знайомий із її форматом. Наприклад, при вибудувані водяного знаку, якщо нам потрібно нанести його на цифрове зображення, то ця процедура може бути зроблена за допомогою зміни яскравості певних точок [2]. Якщо модифікація яскравості незначна, то під час перегляду малюнка людина, швидше за все, не помітить слідів

штучного перетворення. Особливо добре ця техніка працює у випадку, коли водяний знак наноситься на неоднорідні області.

Головною сферою застосування для цифрових водяних знаків на даний момент використання їх в системах захисту від копіювання, які прагнуть запобігти або утримати від несанкціонованого копіювання цифрових даних [3]. Стеганографія застосовує ЦВЗ, коли сторони обмінюються секретними повідомленнями, впровадженими у цифровий сигнал. Використовується як засіб захисту документів з фотографіями - паспортів, посвідчень водія, кредитних карток з фотографіями. Коментарі до цифрових фотографій із описовою інформацією — ще один приклад невидимих ЦВЗ. Хоча деякі формати цифрових даних можуть також нести додаткову інформацію, звану метадані, ЦВЗ відрізняються тим, що інформація "зашита" прямо в сигнал [4]. Об'єкти мультимедіа в цьому випадку будуть контейнерами (носіями) даних. Основна перевага полягає в наявності умовної залежності між подією заміни об'єкта ідентифікації та наявності елемента захисту – прихованого водяного знака. Підміна об'єкта ідентифікації призведе до висновку про підробку документа. Цифрові водяні знаки отримали свою назву від старого поняття водяних знаків на папері (гроші, документи).

Цифрові водяні знаки на будь-яких носіях вважаються галуззю стеганографії, і її головна мета — забезпечити захист авторських прав на інтелектуальну власність та запобігання незаконному копіювання та розповсюдження, як показано на рис. 1.2.

Застосування методів цифрових водяних знаків включають: захист від копіювання, захист авторських прав, відстеження джерела, автоматичний моніторинг і відстеження авторських матеріалів в Інтернеті, програми для відбитків пальців та розширення вмісту. І стеганографія, і цифрові водяні знаки використовують стеганографічні методи для вбудовування даних; отже, стеганографія прагне до непомітності для органів чуття, а цифрові водяні знаки намагаються контролювати надійність як головний пріоритет. Оскільки цифрова копія даних така ж, як і оригінал, цифровий водяний знак вважається інструментом пасивного захисту. Він позначає дані, але не погіршує їх і не контролює доступ до даних.

Рисунок 1.2 – Ключові параметри для Стеганографії та ЦВЗ.

Опис життєвого циклу ЦВЗ:

Спочатку впроваджується у сигнал S у довіреному середовищі водяні знаки за допомогою функції E. Результатом являється сигнал SE. Далі цей новий сигнал розповсюджується через мережу, під час поширення може здійснитися атака. У такому випадку сигнал стає SEA. Водяні знаки можуть бути знищені або пошкоджені. Далі функція виявлення намагається знайти водяні знаки, а функція декодер розшифрувати повідомлення. Можливо це намагається зробити зловмисник [5].

Опис життєвого циклу зображений на рис. 1.3.

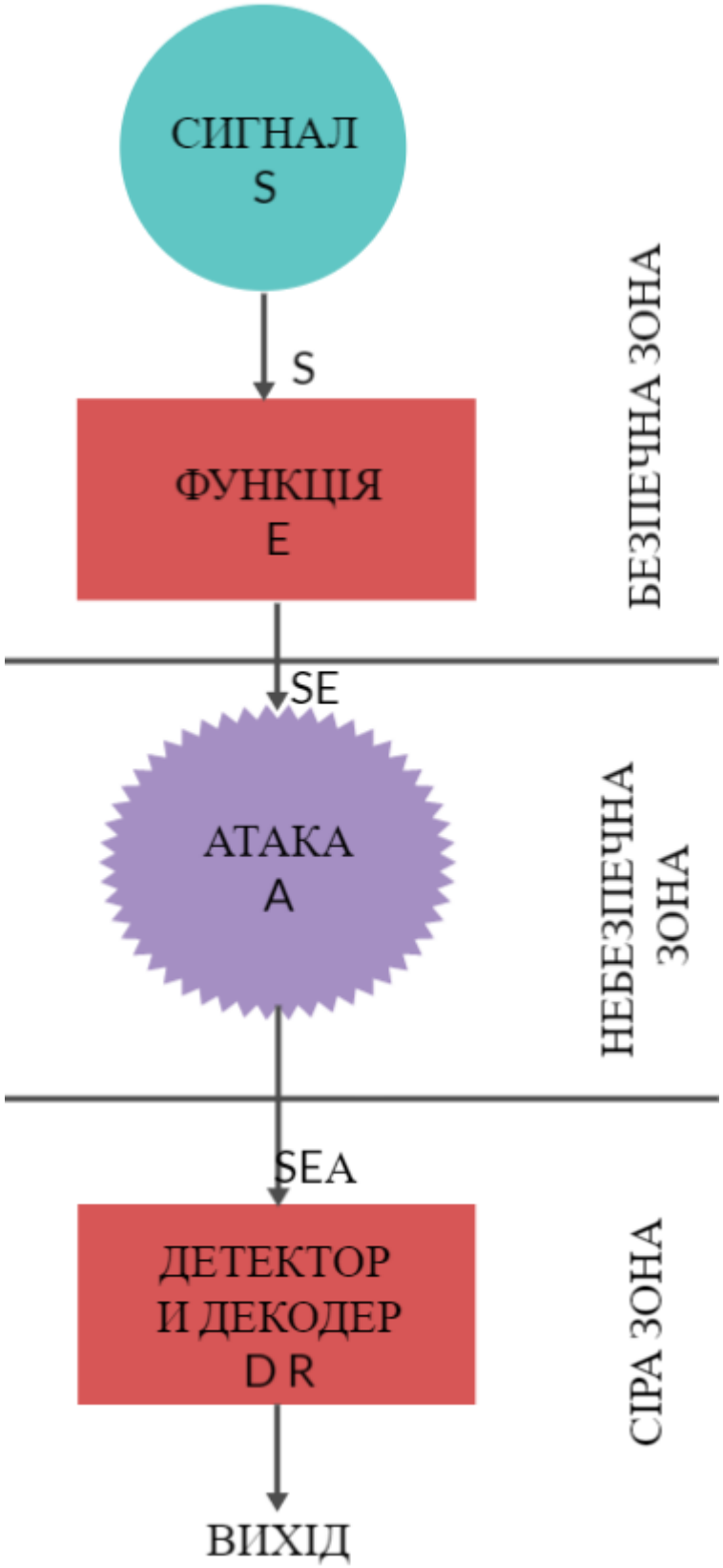

Рисунок 1.3 - Життєвий цикл ЦВЗ.

На основі надійності схеми водяних знаків поділяються на три основні категорії:

• Robust: схеми водяних знаків розроблені таким чином, водяний знак протистоїть маніпулюванню сигналом хоста (так званим атакам) та зазвичай використовуються для захисту прав інтелектуальної власності (IPR)

Програми. Очевидно, що жодна схема водяних знаків не витримує всіх типів модифікацій. Таким чином, стійкість відноситься до підмножини всіх можливих атак і до певної міри сигналу хоста деградація.

• Fragile: у схемах крихких водяних знаків водяні знаки розроблені так, щоб бути вразливими для всіх атак, тобто вони стають невиявленими навіть при незначній зміні даних хоста.

• Semi-fragile: цей клас схем водяних знаків забезпечує вибіркову стійкість до певного набору атак, які вважаються допустимим, у той час як уразливим для інших. Майже всі надійні водяні знаки насправді напівтендітні, але вибіркова надійність не вимога, що накладається розробником системи, а те, що не можна уникнути.

1.2 Системи цифрових водяних знаків

Системи ЦВЗ є одним із напрямів комп'ютерної стеганографії. Система вбудовує в фізичний об'єкт приховану інформацію, яка підтверджує оригінальність об'єкту. Такий об'єкт називається контейнером. Система ЦВЗ є частиною стеганосистеми, відповідно.

Контейнери бувають як заповнені, так і незаповнені, а також, контейнер – як правило, цифровий носій інформації, що має аналогове походження(аудіо-відео файли, статичні зображення).

Вбудування прихованої інформації в контейнер у рамках стеганосистеми відбувається за допомогою стеганокодера, відповідно, вибудування – за допомогою стеганодекодера.

Основною різницею стеганографії та використання систем ЦВЗ від криптографії є те, що криптографія приховує інформацію через операції шифрування, тому, як правило, наперед відомо, що криптограма містить

зашифровану таємну інформацію, а ЦВЗ, в свою чергу, має в собі задачу приховувати таємну інформацію.

Має місце поєднання методів стеганографії з криптографією для підвищення захищеності інформації.

1.3 Роль ЦВЗ у захисті інформації

Нижче описано деякі існуючі області застосування разом із довідковими технологіями, а також представлені тематичні дослідження, висвітлюючи деякі з найбільш поширених реальних сценаріїв. Більшість наведених прикладів стосується водяних знаків цифрових зображень, але загалом вони застосовні до інших носіїв, таких як аудіо- або відеопотоки [6].

- Захист авторських прав

Першою сферою застосування водяних знаків є захист авторських прав на цифрові носії. У цифровому світі практично будь-хто може дублювати цифрові дані чи маніпулювати ними без втрати якості. Це призвело до небачених раніше проблем із порушенням авторських прав. Цифровий водяний знак забезпечує додатковий рівень безпеки в ланцюжку захисту вмісту, щоб запобігти несанкціонованому використанню дублювання вмісту шляхом вбудовування водяних знаків, які визначити оригінальний медіа та дозволене використання вмісту. У такому випадку пристрої зчитують водяний знак під час відтворення або копіювання вмісту. Якщо водяний знак вказує на те, що використання є несанкціонованим, відтворення або копіювання заборонено (можливі й інші дії, наприклад, звук вимкнено), і може відображатися пояснювальне повідомлення. Ефективний захист вмісту допомагає власникам вмісту захищати розважальний аудіо-, кіно- та відео-контент, повідомляти про право власності та права на використання свого вмісту, захистити його від поширених загроз піратства, зокрема записування з відеокамери, обміну файлами однорангового доступу, копіювання, перетворення форматів, кодування та інші форми повторної обробки.

- Ідентифікація вмісту та керування ним

Цифровий водяний знак забезпечує ефективну ідентифікацію вмісту, надаючи унікальний цифровий ідентифікатор для всіх форм медіа-контенту таким чином, щоб він зберігався разом із вмістом, де б він не переміщувався. Цифрові водяні знаки легко вбудовуються в контент, не заважаючи споживачу насолоджуватися ним. Він непомітний для людей, але легко виявляється і розуміється комп'ютерами, мережами та широким спектром поширених цифрових пристроїв. Водяний знак може містити таку інформацію, як от особу власника, спосіб його використання або будь-що інше, що власник хоче передати. Він також може ініціювати заздалегідь визначені дії, зокрема посилання на веб-сайти або інші споживчі враження.

- Фільтрація контенту

Ініціювання дій та блокування Дані, що містяться в цифровому водяному знакі, можуть швидко корелювати з іншим вмістом або діями. З одного боку, після ідентифікації водяного знаку може бути запущена конкретна дія або навіть частина вмісту, що забезпечує інтерактивність клієнта. Наприклад, під час перегляду сцени у фільмі може викликатися певний заклик до дії (наприклад, «Натисніть червону кнопку на пульті, щоб дізнатися більше»). Аналогічно може бути ініційована конкретна та цільова реклама. Замість того, щоб рекламний ролик з'являвся регулярно, рекламний ролик може запускатися відповідно до того, який контент переглядається, і в певний час у вмісті. З іншого боку, цифрові водяні знаки можуть використовуватися для блокування певного вмісту. Після розпізнавання та ідентифікації конкретної ситуації вміст може бути заблоковано. Такі програми можуть виявитися надзвичайно корисними для Інтернету, наприклад, блокувати завантаження на веб-сайт захищених авторським правом фрагментів аудіо чи відео. Крім того, щоб забезпечити безпеку дітей та запобігти потраплянню дітей у вміст для дорослих, батьки можуть встановити спеціальні правила, які попереджають, обмежують або повністю блокують перегляд такого вмісту [7].

- Онлайновий вміст

У корпоративному світі зображення, документи та відео швидко поширюються електронною поштою та у всесвітній мережі. У випадку великих брендів, наприклад, відділи маркетингу повинні ретельно керувати випуском

матеріалів для запуску продуктів і гарантувати, що їхні канали продажів правильно використовують правильні зображення в потрібний час. Доступні служби пошуку в Інтернеті, які постійно сканують Інтернет у пошуках унікального вмісту з водяними знаками. Потім формуються звіти, які повідомляють власника про те, де був знайдений їхній вміст, що дозволяє йому вжити необхідних заходів. Після того, як вміст знайдено, стає доступним широкий спектр автоматизованих дій або повідомлень, починаючи з класичного «Цей вміст доступний для ліцензування». до більш лякаючих «Цей вміст захищено авторським правом; будь ласка, негайно видаліть його». Е. Безпека документів та зображень Унікальний цифровий водяний знак можна легко вставити в кожну копію конфіденційного документа під час його створення та розповсюдження. Дані, що містяться у водяному знаку, можуть включати, хто є одержувачами кожної копії, щоб будь-яка інформація, яка ненавмисно або навмисно просочилась легко відстежується до джерела. Крім того, компанії можуть використовувати мережеві детектори та фільтри електронної пошти для перевірки цифрових водяних знаків у документах та зображеннях, надаючи сповіщення про спробу завантаження в Інтернет або пересилання електронної пошти за межі компанії. Аналогічно, детектори водяних знаків можуть бути включені в різні принтери, сканери та інші пристрої для перевірки наявності водяних знаків у конфіденційних документах, які хтось намагається скопіювати. У цьому випадку водяний знак може викликати дію, наприклад а не копіюйте та не скануйте.

- Мобільний досвід і водяні знаки

Водяні знаки можна легко вставляти в будь-який медіа контент, включаючи журнали, газети, упаковку, плакати, брошури тощо. І, на відміну від 2D штрих-кодів або QR-кодів, які використовуються в деяких мобільних кампаніях, цифрові водяні знаки непомітні для людей і не займають дорогоцінного місця на друкованих матеріалах, що робить технологію набагато «дружнішою до бренду». Цифровий ідентифікатор у водяному знаку можна зіставити з URL-адресою у серверній базі даних, яка потім повертається на телефон споживача.

1.4 Переваги ЦВЗ

- Забезпечення захисту від викрадання оригіналів зображень.

Важлива перевага для компаній, що розроблюють цифрові статичні зображення. Кожна підробка наносить компанії фінансових, репутаційних збитків, що в свою чергу призводить до підвищення ризиків.

- Розширення кола аудиторії та впливу компанії.

До розширення призводить стандартний процес так званого «сарафанного радіо», завдяки якому з кожною новою людиною, що побачить ЦВЗ, збільшується вірогідність розширення аудиторії компанії. Це знайомить нових людей із брендом, який представляє водяний знак, і може залучити нових клієнтів. Це велика перевага, яка навіть не пов’язана з кібербезпекою.

- Зображення можуть містити компоненти відстеження, які надають компанії можливість знати, де були розміщені копії файлу.

Компанія має можливість спостерігати за цими копіями, бачити, чи використовуються вони в комерційних цілях, та, за потреби, вдаватися до певних заходів, щодо фінансових та репутаційних ризиків.

- Розповсюджений метод захисту.

Існує велика кількість підлаштованих під цифровий водяний знак систем, підлаштоване під даний тип захисту нормативно-правове поле. Існує велика кількість готових рішень та варіантів використання, що має велику перевагу для викристання даного методу для захисту інформаційних ресурсів.

- Велика кількість типів об'єктів з можливістю вбудування ЦВЗ.

Починаючи з найпоширеніших варіантів використання, а саме: аудіо, відео файли та статичні цифрові зображення, закінчуючи повноцінними фізичними продуктакми, упаковками, тощо. Це дає змогу захищати абсолютно всі свої продукти за допомогою даного методу.

- Сумісність із криптографією.

Задля підвищення безпеки інформації, стеганографічний метод вбудови Цифрового водяного знаку у цифровий об'єкт може бути поєднано із

криптографічними методами захисту інформації. Стеганографія та криптографія виконують схожі задачі різними шляхами, але можуть бути вільно поєднані, якщо мова йде, наприклад, про цифрові об'єкти із аналоговою природою.

1.5 Недоліки ЦВЗ

- Непрозорий водяний знак візуально накладається поверх основного цифрового зображення, відповідно до параметрів ЦВЗ, він може завадити перегляду фактичного об’єкту. Дана проблема вирішується налаштуванням прозорості, вмісту та розміру ЦВЗ. Але при будь-яких параметрах ЦВЗ все ще може спотворити певні деталі зображення.
- За допомогою існуючого на сьогодні програмного забезпечення для цифрових зображень зловмисник може видалити водяний знак, та почати розповсюджувати зображення. Для недосвідчених користувачів зображення буде здаватися абсолютно стандартним, але володар зможе довести факт викрадення при співставленні поширюваного фото і оригіналу.
- Існують складнощі при захисті авторських прав.

ЦВЗ як такий – перевірений часом метод, що використовується кожною компанією, яка захищає свої авторські права. Але, при цьому, сам по собі ЦВЗ не надає пасивного захисту зображення. Він надає можливість ідентифікації власника та доказу власності постфактум, коли вже відбулося викрадення, спотворення, копіювання, тощо [8].

- Постійний аналіз ринку

Створити та вбудувати ЦВЗ – це одна задача, а практичне використання його – зовсім інша. Для того, щоб краще розуміти ситуацію на ринку, та бути впевненим у тому, що продукт компанії не використовується третіми особами для завдання економічних та репутаційних збитків, потрібно періодично перевіряти галузь ринку на наявність компаній, що використовують матеріали, захищені ЦВЗ.

- Для створення та вбудовування водяного знаку потрібен час.

Як правило, компанії при розробці продукту, послуги чи медіа ресурсів, формують точний графік та дати виходу на ринок. Відповідно, система ЦВЗ, яка вбудовує ЦВЗ у зображення повинна працювати швидко, не віднімаючи часу.

Найбільший недолік загальних алгоритмів водяних знаків на практиці

полягає в тому, що вони спотворюють вихідне зображення, ховаючи певні деталі. У конфіденційних програмах, наприклад, військових чи медичних, оригінальне зображення потрібно після вилучення водяного знаку. Ця вимога призвела до ще однієї категорії схем ЦВЗ: реверсивних схем ЦВЗ. У даному типі схеми водяний знак можна повністю видалити. після того, як відбудеться вилучення ЦВЗ, вихідне зображення буде повністю відповідати оригінальному.

Також слід зазначити, що маючи зображення, що містить ЦВЗ, зловмисник може спробувати скопіювати сам ЦВЗ для того, щоб завдати атаки на компанію, наприклад, через підставну людину підмінивши зображення компанії на своє перед відправкою зображення до клієнта, партнера, на ринок, тощо. Даний тип атаки більш складний для попередження та захисту від нього.

Але компанія також має рішення. Наприклад, якщо зловмисник копіює ЦВЗ, він, як правило накладає його на зображення вручну, а компанія використовує для цього алгоритм, що вбудовує та вибудовує ЦВЗ із зображень. Відповідно до цього, компанії залишиться лише вставити зображення в свою програму, та продемонструвати клієнтові докази підробки, отримані при аналізі.

1.6 Цифрові об’єкти, які підлягають захисту ЦВЗ

Будь-який документ, який містить конфіденційні дані, які вам потрібно контролювати або обмежувати доступ, є хорошим кандидатом на водяні знаки. Поширені типи даних, які ви повинні думати про водяні знаки, включають:

- Інтелектуальна власність (ІВ)
- Виробничі плани
- Специфікації та дизайн продукції
- Фінансові документи

- Документи M&A
- Документи з персоналу (HR).
- Інформація про охорону здоров'я
- Юридичні договори
- Регульовані дані (PII, PHI, CUI, FCI тощо)
- Секретна інформація

Водяні знаки цифрової безпеки можна динамічно застосовувати до таких поширених типів файлів:

- Документи Microsoft Office: (.txt, .csv, .doc, .docx, .xls, .xlsx, .ppt, .pptx)
- Зображення: (png, .jpg, .jpeg, .tif, .tiff, .bmp)
- Файли CAD (dgn, .dwf, .dwfx, .dwg, .dwt, .dxf, .ifc, .iges, .plt, .stl, .cff2)
- PDF документи
- Тощо

1.7 Існуючі атаки на системи ЦВЗ

ЦВЗ, як і будь-яка система захисту інформації має певний перелік відомих атак, які повинні розглядатися при використанні даного методу захисту.

Наразі можна навести такі приклади атак на ЦВЗ:

- Скремблювання;
- Спотворення;
- Копіювання;
- Неоднозначності;
- Аналізу чутливості;
- Градієнтного спуску.

Атакою скремблювання є така атака, що шифрує джерело даних перед наданням його до детектора ЦВЗ, і розшифровує після. Є два основних типи даної атаки: перестановка або псевдовипадкове скремлювання.

Непоганим прикладом атак типу скремблювання можна визначити мозаїчну атаку. Процес даної атаки модна описати наступним чином: це розбір зображення на невеликі прямокутники, які наступним кроком формують таблицю, схожу на вхідне зображення, але прямокутники, сформовані на першому кроці розгортаються у певному порядку. Таким чином зображення пройде будь-який скан у веб додатках з перевірки цифрових зображень.

Атаки типу спотворення бувають тимчасовими, геометричними або спрямованими на видалення шумів.

Атаки синхронізації. Атака спрямована на приховання сигналу маючого в собі інформацію водяного знаку, наприклад спотворення водяного знаку за рахунок затримки відео та аудіо каналів сигналів. Але є і більш складні методи даного типу атак. Наприклад, нелінійні спотворення зображень, вибіркові, випадкові видалення стовпців та(або) рядків у зображеннях, відео, аудіо-фрагментах тощо.

Атаки, що спрямовані на видалення шумів, створені для видалення ЦВЗ, які можна описати, як статичний шум. Порушник може використовувати для видалення даного типу ЦВЗ так звані лінійні фільтри.

Атака копіювання ЦВЗ дуже проста і спрямована на перехоплення та повторне використання ЦВЗ. Протидією може слугувати, наприклад, створення для ЦВЗ криптографічного підпису.

Атаки аналізу чутливості навпаки працюють над видаленням ЦВЗ з конкретного цифрового об’єкту, безпосередньо працюючи із аналізом області детектування, та пошуком найкоротшого шляху змін для обходження детектування.

Висновки за розділом 1

Як і будь-який інший метод, ЦВЗ містить в собі як переваги, так і недоліки, та використовується лише в обмеженому колі задач, маючи при цьому велику кількість відомих методів атак.

Попри всі недоліки, даний метод захисту є безальтернативним у відкритому інформаційному полі, є багатофункціональним і доволі ефективним. Наразі його

сфера використання та популярність тільки зростає, і все частіше Українські компанії прибігають до використання Цифрового водяного знаку не тільки для захисту зображень, а і для захисту продукції, упаковки товару, тощо.

Хоча цифрові водяні знаки можуть бути виявлені зловмисником при спробі несанкціонованих дій із власністю компанії, при їх використанні компанія має набагато менше як фінансових, так і репутаційних ризиків, що в свою чергу є найважливішою проблемою будь-якої компанії при взаємодії з відкритим інформаційним простором.

РОЗДІЛ 2
ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ КОМПАНІЇ

2.1 Види інформації на підприємстві

Законом України «Про інформацію» від 02.10.1992 року за режимом обмеження доступу інформація поділяється на відкриту та інформацію з обмеженим доступом.

Стаття 30 закону «Про інформацію» передбачає поділ інформації з обмеженим доступом на таємну інформацію, службову та конфіденційну інформацію [9].

Конфіденційна інформація – це інформація, яка є у володінні, користуванні та(або) розпорядженні окремих фізичних та(або) юридичних осіб, що передбачає поширення цієї інформації за їх бажанням [10].

Інформація, розпорядниками якої є фізичні та(або) юридичні особи, що класифікується як: професійна, комерційна, банківська, ділова, виробнича та(або) інша, та(або) є предметом інтересів наступних категорій: професійний, комерційний, банківський, діловий, виробничій та(або) інших категорій, що не порушує жодної з передбачених чинним законодавством України таємниць, має режим доступу встановлений відповідно до певних категорій її розпорядниками. До цього також відноситься належність інформації до категорії конфіденційної, та формування, розробка, впровадження систем та методів її захисту [11].

До таємної інформації відносять інформацію, яка в собі має відомості, що можуть та(або) становлять будь-яку з таємниць, що передбачені чинним законодавством України, розголошення котрої може призвести до задачі шкоди особі, суспільству та державі. Насамперед комерційна таємниця підприємства передбачена статтею 420 Цивільного кодексу України визначається, що до об’єктів інтелектуальної власності відноситься комерційна таємниця. У статті 505 комерційна таємниця трактується як інформація, що є що є секретною, зокрема, ця інформація в цілому, чи в певних її формах є невідомою та не є легкою у доступі для

тих осіб, які зазвичай працюють із відповідним видом інформації, що надає комерційної цінності даній інформації, та надає законної можливості особі розпоряднику даної інформації використати адекватні за існуючими обставинами заходи збереження її секретності.

Також постановою Кабінету Міністрів України 611 «Про перелік відомостей, що не становлять комерційної таємниці» від 09.08.1993 року сформовано перелік відомостей, які не є і не можуть трактуватися як комерційна таємниця, а саме:

- установчі документи, документи, що дозволяють займатися підприємницькою діяльністю та її окремими видами;
- інформація щодо всіх встановлених форм державної звітності;
- дані, необхідні для обчислення та сплати податків та інших обов'язкових платежів;
- відомості про чисельність та склад працюючих, їх заробітну плату в цілому та за професіями та посадами, а також наявність вільних робочих місць;
- документи про сплату податків та обов'язкових платежів;
- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри завданих при цьому збитків;
- документи про платоспроможність;
- відомості щодо участі посадових осіб підприємства у кооперативах, малих підприємствах, об'єднаннях та інших організаціях, що займаються підприємницькою діяльністю, спілках;
- відомості, що відповідно до чинного законодавства підлягають оголошення.

Також, відповідно до чинного законодавства України, керівник підприємства може віднести відомості, що не становлять комерційної таємниці, до конфіденційної інформації [12].

Статтею 60 Закону України «Про банки та банківську діяльність» від 07.12.2000 року впроваджено термін банківської таємниці. Банківська таємниця –

Інформація стосовно діяльності підприємства, та його фінансового стану, яка стала відомою у процесі обслуговування банку, розголошення якої може призвести до завдання шкоди у вигляді матеріальних або моральних збитків.

Зокрема до банківської таємниці можна віднести наступне:

- відомості про стан рахунків клієнтів, зокрема стан кореспондентських рахунків банків у Національному банку України;
- операції, проведені на користь або за дорученням клієнта, здійснені ним угоди;
- фінансово-економічний стан клієнтів;
- системи охорони банку та клієнтів;
- інформація про організаційно-правову структуру юридичної особи клієнта, його керівників, напрямки діяльності;
- відомості щодо комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;
- інформація щодо звітності по окремому банку, за винятком такої, що підлягає опублікуванню;
- коди, що використовуються банками для захисту інформації.

2.2 Методи захисту інформації компанії

Основною проблемою захисту інформації на підприємствах є забезпечення її надійного збереження в межах підприємства.

Цілями будь-яких систем та методів захисту інформації можуть бути деякі окремі пункти, їх комбінації, або все нижче приведене:

- Запобігання втратам, підробці, витоку, розкраданню інформації підприємства;
- Виявлення та запобігання загрозам безпеки підприємства та безпосередньо розпорядника інформації
- Виявлення та запобігання несанкціонованому доступу до інформації, спробам з копіювання, знищення або спотворення інформації підприємства.

Ключем для формування робочої та ефективної системи інформаційної безпеки(СІБ) є системний підхід до розробки методів захисту інформації, що повинен включати в себе наступну базу рішень:

- Аналіз можливих загроз, на базі яких буде розроблено найраціональніші методи із захисту інформації
- Забезпечення безперервного контролю роботи СІБ
- Постійний пошук слабких місць системи

Пророблюючи розробку методів захисту інформаційних ресурсів на підприємстві, першочергово повинно бути впроваджено наступні методи:

- Програмно-технічний
  - Робота над запобіганням витоку інформації за межи підприємства
  - Протидія несанкціонованому доступу
  - Протидія перехопленням інформації
- Організаційний
  - Сертифікація систем захисту інформації на підприємстві
  - Контроль персоналу
  - Розроблення стандартизації методів захисту інформації у межах

2.3 Роль та функція ЦВЗ на підприємстві

Захист інформації завдяки ЦВЗ здійснюється у таких основних напрямах:

- Відстеження взаємодій

Власник даних формує окремий ЦВЗ для кожної копії будь-яких даних, кожний новий ЦВЗ може мати, наприклад, порядковий номер, що буде відрізнятися від попередніх, та наступних. І тоді, якщо з підприємства буде виток даних, буде набагато легше знайти джерело витоку.

- Автентифікація даних

Автентичність даних може бути захищена завдяки цифровому підпису, котрий міститиме в собі зашифроване повідомлення. Підпис підтверджує що із даним об’єктом взаємодіяв саме правовласник, це просто та ефективно. Але такий підпис

має в собі один недолік: це безпосередньо можливість його втрати при експлуатації. На допомогу у вирішенні цієї проблеми приходить вбудування підпису безпосередньо на дані, що будуть захищеними ЦВЗ [13].

- Контроль незаконного копіювання

ЦВЗ, що було вбудовано безпосередньо у дані цифрового об’єкту є найкращім захистом від незаконного копіювання.

- Сумісність різних технологій

Використання ЦВЗ потрібно для деяких систем, щоб застаріла система могла отримати оновлену версію додатків

- Широкомовний контроль

Цей напрям відіграє одну з найважливіших ролей у теле-радіомовленні. Е як пасивний тип контролю мовлення, так і активний тип. Для пасивного типу потребується велика база даних, з якою система буде постійно перевіряти сигнал, у той час, як активний тип контролю потребує менших апаратних ресурсів, і для реалізації такої системи, у сигнал додається ідентифікаційна інформація, а перевірка системою відбувається у окремих областях сигналу [14].

- Ідентифікація власника

На сьогодні це найвідоміша галузь використання ЦВЗ. Один з основних методів позначення авторського права на цифровий контент. ЦВЗ непомітний, але напряму пов’язаний із даними цифрового об’єкту.

- Доказ права власника

Через те, що зловмисник може використовувати водяний знак будь-якої людини, щоб мати можливість отримати нелегально права на певний об’єкт. У такому випадку є простий шлях рішення підтвердження права власності – детектор із обмеженою доступністю. Якщо лише правовласник має детектор, тільки він може зняти без ушкодження файлу ЦВЗ [15].

2.4 Приклади використанні ЦВЗ на підприємстві

На сьогодні сучасна стеганографія має одне з найбільш потрібних у цифровому просторі рішення: вбудування у цифровий контент ЦВЗ. Це основа сьогоднішнього захисту прав на цифровий контент та захисту DRM (Digital rights management) систем.

Прихований маркер, який несе в собі посилання, вбудовується у цифровий об’єкт і є максимально стійким для перетворень його контейнера.

Існують напівкрихкі та крихкі ЦВЗ, які здатні зберігати в собі всю інформацію про спроби передачі та спроби порушення цілісності контейнера.

Прикладами використання цифрових водяних знаків є:

- Серійна упаковка

Використання у виробництві серійних товарів, ЦВЗ, допомагає чітко відслідковувати рух та місцезнаходження товарів, як зменшуючи крадіжки у компанії, так і покращуючи якість та рівень сервісу для користувача.

- Захист бренду

Система покращення протидії підроблення продукції компанії, пришвидшення та полегшення вживання протидій компанії, для того, щоб знизити ризики використання ім’я бренду третіми сторонами [16].

- Комерційний друк

Ефективне розповсюдження інформації про сервіс від компанії до споживача шляхом лише водяного знаку. Також компанія може перетворити друковані матеріали на POS-матеріали(point of sales) в динаміці. Це дозволить об’єднати фізичний контент із цифровим та провести легку інтеграцію користувача у цифровому середовищі у напрямок діяльності підприємства та послуги.

- Переробка сміття

ЦВЗ наразі починає використовуватися для автоматизації, поліпшення та пришвидшення сортування відходів та сміття великих компаній, що безпосередньо пришвидшує розвиток напряму переробки сміття. Цей шлях розвитку ЦВЗ наближає наше фізичне середовище до цифровізації та у майбутньому може дійти до

використання ЦВЗ у багатьох неочікуваних місцях, як, наприклад маркування насіння, м’яса, штучного м’яса тощо [17].

- Цифрові зображення та документи

ЦВЗ може допомагати компанії виявляти неправомірне використання цифрових активів ззовні та безпосередньо співробітниками компанії. Комбінування ЦВЗ з іншими технологіями дозволяє дуже чітко контролювати канали витоку інформації, методи, кінцевих вигодоздобувачів [18].

- Аудіо

Вбудування ЦВЗ у аудіо може дуже допомагати у ідентифікуванні та підтримці метаданих, а у суміші із технологіями по типу блокчейн, можна підтверджувати авторство пісень, точні дати створення аудіо-файлів тощо.

Висновки за розділом 2

В цьому розділі були розглянуті переваги, недоліки ЦВЗ, об’єкти що підлягають захисту цією системою, а також існуючі атаки на системи ЦВЗ.

Попри всі недоліки, даний метод захисту є багатофункціональним і доволі ефективним. Наразі його сфера використання та популярність тільки зростає, і все частіше Українські компанії прибігають до використання Цифрового водяного знаку не тільки для захисту зображень, а і для захисту продукції, упаковки товару, тощо. Це позитивно впливає на захист інформації цих підприємств.

При вбудуванні ЦВЗ компанія має набагато менше як фінансових, так і репутаційних ризиків, що в свою чергу є однією з найважливіших проблем будь-якої компанії при взаємодії з відкритим інформаційним простором.

Підсумовуючи цей розділ, будь-яка компанія має складну структуру безпеки даних, яка будується з безлічі факторів, процесів та документів. Головне завдання на сьогоднішній день будь-якої компанії - домогтися максимальної автоматизації систем безпісності, а також домогтися того, щоб системи безпеки не впливали на бізнес-процеси.

Для компанії ЦВЗ не є першорядним типом захисту даних, проте обов'язковим і необхідним на різних етапах. Підприємство працює з різними типами інформації, і велику кількість моніторингових систем можна просто прибрати або спростити, якщо компанія використовуватиме ЦВЗ для кожної копії документів та цифрових об'єктів. Також за допомогою ЦВЗ можна захищати торгівельну марку компанії. Переробка сміття також полегшується з допомогою ЦВЗ. Це створить пасивний контроль каналів витоків інформації. У публічному ж полі компанія отримає можливість з легкістю контролювати підроблення своєї продукції, захищати свої авторські права та покращувати методи розповсюдження, відстеження безпосередньо цього самого розповсюдження товарів, допомагати клієнтам визначати справжність продукції так само.

РОЗДІЛ 3
ПРАКТИЧНА РЕАЛІЗАЦІЯ АЛГОРИТМУ ЦВЗ ДЛЯ ЗАХИСТУ ТОРГОВЕЛЬНОЇ МАРКИ КОМПАНІЇ

3.1 Критерії до алгоритму ЦВЗ

До алгоритму захисту бренду за допомогою ЦВЗ були визначені такі критерії:

- візуальна схожість оригіналу файлу та стего.

Це виходить з того, що основна ціль використання ЦВЗ- передати інформацію так, щоб приховати факт передачі. Після цього, якщо стего та оригінал візуально не відрізняються, наявність мітки виявити важко. Крім того, зображення все ще можна прочитати, що теж важливо [19].

- висока швидкодія ПЗ.

Швидкодія потрібна для зручності користувача. В середньому, веб-додаток можна назвати швидким та зручним для користувачів, якщо перша відповідь на запит клієнта надається впродовж однієї секунди.

- висока складність вилучення ЦВЗ із файлу.

Стійкість до вилучення потрібна якщо зловмисник дізнався про існування мітки, при зміні формату файлу або зменшенні його розміру. В такому разі мітка може пошкодитись і зображення може ускладнитись шумами. Робастий алгоритм, або мітка, має перешкоджати діям зловмисника.

3.2 Підбір інструментів розробки

Python був обраний в якості мови для розробки ПЗ. Це високорівнева мова програмування зі зручним для розробника синтаксисом. Це універсальна мова з великою кількістю наукових матеріалів у мережі Інтернет, та великою спільнотою. Навіть стандартна бібліотека Python дуже велика. Більшість задач вирішується імпортом саме необхідного інструменту з набору стандартної бібліотеки Python. Але

якщо не вийшло вирішити проблему стандартними засобами, є досить багато сторонніх бібліотек, якими можна скористатися. За допомогою Python можна працювати з віддаленими серверами, великими масивами даних, з зображеннями та графіками [20].

При виборі мови програмування, конкуренцію цій мові становила мова R, але вона націлена більше на наукові розрахунки і обчислення. А Python- мова широкого застосування та профілю в багатьох сферах: консольні утиліти, розрахунки, боти, веб-додатки та багато іншого [21]. Саме через це була обрана саме ця мова програмування- розроблене ПЗ буде придатне для вбудування в різноманітні працюючі системи. Це буде зробити набагато легше, ніж з багатьма іншими мовами програмування, в тому числі з R.

3.3 Розробка алгоритму ЦВЗ

Для розробки алгоритму було обрано таку бібліотеку як PIL. PIL — це бібліотека зображень Python від Фредріка Лунда та учасників. Вона додає можливості обробки зображень до вашого інтерпретатора Python. Ця бібліотека забезпечує широку підтримку форматів файлів, ефективне внутрішнє представлення та досить потужні можливості обробки зображень [22].

Основна бібліотека зображень розроблена для швидкого доступу до даних, що зберігаються в кількох основних форматах пікселів. Він повинен забезпечити міцну основу для загального інструменту обробки зображень.

Серед можливостей пакету:

- читання зображень різних форматів (PNG, JPEG, TIF, GIF і ін.);
- збереження зображень в ці формати; розбір зображень
- на складові (кольорові зображення на канали);
- робота з зображенням, як з двовимірним масивом даних.

Що зручно, дані зображення легко перетворюються в типи даних, з якими працює пакет numpy, і назад. Немає необхідності докладати додаткові зусилля для візуалізації двовимірного масиву даних.

PIL був використований для реалізації всього проекту.

Були використані такі модулі бібліотеки PIL:

- Image

Модуль Image надає клас з такою ж назвою, який використовується для представлення зображення PIL. Модуль також забезпечує ряд заводських функцій, включаючи функції завантаження зображень з файлів і створення нових зображень.

- ImageDraw

Модуль ImageDrawзабезпечує просту 2D-графіку для Imageоб'єктів. Можна використовувати цей модуль для створення нових зображень, коментування або ретушування наявних зображень, а також для створення графіки на льоту для використання в Інтернеті.

- ImageFont

Модуль ImageFontвизначає клас з такою ж назвою. Примірники цього класу зберігають растрові шрифти та використовуються разом із PIL.ImageDraw.ImageDraw.text()методом.

PIL використовує власний формат файлу шрифтів для зберігання растрових шрифтів, обмежений 256 символами. Можливо використовувати pilfont.py із pillow - scripts для перетворення дескрипторів шрифтів BDF та PCF (формати шрифтів вікон X) у цей формат.

Починаючи з версії 1.1.4, PIL можна налаштувати на підтримку шрифтів TrueType і OpenType (а також інших форматів шрифтів, які підтримуються бібліотекою FreeType). Для попередніх версій підтримка TrueType доступна лише як частина пакета imToolkit.

Безпосередньо вбудовування ЦВЗ відбувається тривіальним способом, це дозволяє йому бути швидким і зручним для використання у режимі реального часу.

Алгоритм використання ЦВЗ для захисту торгівельної марки компанії наведено у Додатку А.

Інструкції для запису ЦВЗ у файл на мові Python:

```
#Зчитування посилання на файл з клавіатури
infile_path = input("Enter the image file path : ")
```

```
# Константи
INPUT_IMAGE_FILE = infile_path
OUTPUT_IMAGE_FILE = infile_path+".converted.png"
FONT_LOCATION  = 'font file path'
FONT_SIZE = 20
H_SPACING = 70
V_SPACING = 90
FONT_OPACITY = 25
WATERMARK_TEXT = "Watermark text"
# Імпорт основних пакетів із PIL
from PIL import Image, ImageDraw, ImageFont
#Відкриття зображення
im = Image.open(INPUT_IMAGE_FILE)
font = ImageFont.truetype(FONT_LOCATION, FONT_SIZE)
watermark_text = WATERMARK_TEXT
im_width, im_height = im.size # gathering parent image size
#Створення редагованого зображення
drawing = ImageDraw.Draw(im)
text_width, text_height = drawing.textsize(watermark_text, font) # gathering size of the text
# Ініціалізація текстового водяного знака підзображення
im_text = Image.new('RGBA', (text_width, (text_height)), (255, 255, 255, 0)) # creating new transparent sub image for watermark text
drawing = ImageDraw.Draw(im_text)
drawing.text((0,0), watermark_text, fill=(255,255,255, FONT_OPACITY), font=font) # adding the text to the new sub-image
current_width = im_width
current_height = im_height
up_down = +1 # for interesting tiling pattern ( up down position difference )
# Цикл для додаткових водяних знаків
```

```
        #нижній горизонтальний водяний знак повторюється
        while current_width > text_width + H_SPACING:
            new_position = (current_width - text_width) - H_SPACING , current_height + (up_down * (V_SPACING//2))
            im.paste(im_text, new_position, im_text) # pasting the watermark on the parent image
            current_width, current_height = new_position
            # Створення вертикального повтору для кожного горизонтального в нижньому рядку
            repeat_current_width, repeat_current_height = new_position
            while repeat_current_height > text_height + V_SPACING:
                repeat_new_position = repeat_current_width , (repeat_current_height - text_height - V_SPACING)
                im.paste(im_text, repeat_new_position, im_text) # pasting the watermark on the parent image
                repeat_current_width, repeat_current_height = repeat_new_position
            up_down *= -1
        # saving output to outfile
        im.save(OUTPUT_IMAGE_FILE)
```

3.4 Результати використання алгоритму

Результатом роботи та використання розробленого алгоритму використання ЦВЗ в статичне цифрове зображення, маємо оригінальне зображення та зображення із вбудованим в нього Цифровим водяним знаком. Це продемонстровано на першому прикладі на рис. 3.1 та рис. 3.2 відповідно.

Рисунок 3.1 Оригінал зображення

Рисунок 3.2 Зображення з водяним знаком

Тепер проаналізуємо як алгоритм веде себе на іншому зображенні. Це буде проілюстровано на наступному прикладі, рисунки 3.3, 3.4.

Рисунок 3.3 Оригінал зображення

Рисунок 3.4 Зображення з водяним знаком

Можемо побачити, що алгоритм себе поводить однаково на обох прикладах.

Алгоритм виконано за зазначеними в даному розділі технічними вимогами, а також, відповідаючи головним завданням ЦВЗ, реалізуючи складний для видалення ЦВЗ високої прозорості візуально. Алгоритм є універсальним у тому розумінні, що

процес вбудування ЦВЗ буде проходити однаково для будь-якого цифрового статичного зображення у форматі png, що має аналогову природу.

Відповідно, даний алгоритм має в собі можливість глибокого налаштування. При генерації ЦВЗ можуть бути задані непрозорість(від 1 до 100), розмір, зміст ЦВЗ, тощо.

Даний алгоритм має потенціал до поліпшення при розробці для боротьби із основними існуючими на даний момент типами захисту від інформаційних атак. Відповідає вимогам чинного законодавства України, та може бути використаний будь-якою компанією, що зареєструвала торговельну марку на території України.

Висновки за розділом 3

У цьому розділі були досконало розглянуті критерії до алгоритму ЦВЗ. Чітко пояснений підбір інструментів розробки алгоритму, а саме мову програмування Python, а також використані бібліотеки у самій програмі. Були продемонстровані всі етапи розробки програмного забезпечення а також представлені результати виконання програми після реалізації алгоритму.

Результатом розробки алгоритму та його тестування, маємо зображення із вбудованим у нього ЦВЗ, що містить зображення слова «Alex».

Даний тип захисту відносно нескладний у реалізації, що несе дуже велику фінансову вигідність при використанні компанією для захисту інформації. Але при цьому метод захисту не ідеальний, і вже має багато методів атаки на нього.

ВИСНОВКИ

У даній роботі були вирішені всі завдання, які були поставлені для досягнення мети, а саме:

- Розглянути поняття ЦВЗ систему ЦВЗ
- Дослідити особливості захисту інформації на підприємстві
- Проаналізувати роль ЦВЗ у захисті інформації підприємства
- Реалізувати алгоритм використання ЦВЗ у цифровий об’єкт

У першому розділі розглянуто питання ЦВЗ, переваги і недоліки використання ЦВЗ. Було проаналізовано наукову літературу щодо ролі ЦВЗ у захисті інформації та об’єктів які можна захистити за допомогою ЦВЗ. Завершається розділ аналізом атак на системи ЦВЗ.

У другому розділі були розглянуті особливості захисту інформаційних ресурсів компанії. Спочатку були проаналізовані види інформації на підприємстві, а потом методи їх захисту. Далі були розглянуті Функції ЦВЗ на підприємстві та приклади його використання.

У третьому розділі був реалізований алгоритм використання ЦВЗ для захисту торгової марки компанії. Для цього спочатку були виставлені критерії до алгоритму ЦВЗ, потім були підібрані інструменти розробки. Також у третьому розділі чітко розписаний весь алгоритм та показані результати використання алгоритму.

Розроблений алгоритм залишає великий потенціал для подальшої розробки та покращення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Що таке водяний знак : веб-сайт. URL: https://www.watermark-image.com/watermarking.aspx

2. Цифровой водяной знак : стаття. URL: https://ru.wikipedia.org/wiki/Цифровой_водяной_знак#Свойства_цифровых_водяных_знаков

3. Варіанти використання цифрових водяних знаків : веб-сайт. URL: https://www.digimarc.com/blogs/6-digital-watermarking-technology-use-cases

4. Водяной знак для фотографии : веб-сайт. URL: https://compress.ru/article.aspx?id=9686#:~:text=Цифровой%20водяной%20знак%20—%20это%20цифровой,печатного%20водяного%20знака%2C%20он%20невидим.

5. Стеганография : стаття. URL: https://ru.wikipedia.org/wiki/Стеганография#Типы_стеганографических_систем_на_основе_ЦВЗ

6. Дослідження технологій забезпечення захисту авторських прав : веб-сайт. URL: http://www.rusnauka.com/23_ADEN_2015/Informatica/4_198127.doc.htm

7. Pros and Cons of Digital Watermarking : веб-сайт. URL: https://brandongaille.com/12-pros-and-cons-of-digital-watermarking/

8. Іванов В.Г., Любарський М.Г., Карасюк В.В., Ломоносов Ю.В.,Захист авторських прав мультимедійних даних «Юридична академія України імені Ярослава Мудрого», м. Харків

9. Lecture Notes on Cryptography / Goldwasser S., Bellare M. – Cambridge, Massachusetts, 2001.

10. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII Голос України. 13.11.1992.

11. Информация на предприятии: виды и защита : веб-сайт. URL: http://cons.parus.ua/_d.asp?r=01PJEc35cbd398fc87b0cdf7544114928574a

12. Дослідження технологій забезпечення захисту авторських прав : веб-сайт. URL: http://www.rusnauka.com/23_ADEN_2015/Informatica/4_198127.doc.htm

13. Про банки і банківську діяльність: Закон України від 17.12.2000 р. № 2121-III Урядовий кур'єр. 17.01.2001. (№ 48). С. 650

14. Цифровые водяные знаки — новые методы защиты информации : веб-сайт. URL: https://www.itweek.ru/security/article/detail.php?ID=105054

15. invisible watermarks in images : веб-сайт. URL: https://stackoverflow.com/questions/44101/invisible-watermarks-in-images

16. Jordi Nin, Sergio Ricciardi. Digital Watermarking Techniques and Security Issues. - Department of Computer Architecture, Technical University of Catalonia - BarcelonaTECH (UPC)

17. Ways to protect data with digitalsecurity watermarks : веб-сайт. URL: https://www.archtis.com/15-ways-to-protect-data-with-digital-security-watermarks/#:~:text=Why%20Should%20You%20Use%20Watermarks,they%20are%20handling%20sensitive%20information.

18. Цифровий водяний знак : веб-сайт. URL: https://kolosok.lviv.ua/index/cifrovij/uk/vodanoj-cifrovij-vodanij-znak

19. Стаття: Лєнков С.В., Шкуліпа П.А., Прухніцький В.І., Красильников С.Р., Шляхи підвищення захисту авторського права за допомогою використання цифрових водяних знаків. КНУ ім. Тараса Шевченка, Київ.

20. 100 днів коду: повний навчальний курс Python Pro на 2022 рік : веб-сайт. URL: https://www.udemy.com/course/100-days-of-code/learn/lecture/23154980#overview

21. Чому Python, а не будь-яка інша мова програмування : веб-сайт. URL: https://dvmn.org/encyclopedia/qna/9/pochemu-python-a-ne-ljuboj-drugoj-jazyk-programmirovanija/

22. How to Work With a PDF in Python : веб-сайт. URL: https://realpython.com/courses/pdf-python/

ДОДАТОК А

Алгоритм використання ЦВЗ для захисту торгівельної марки компанії

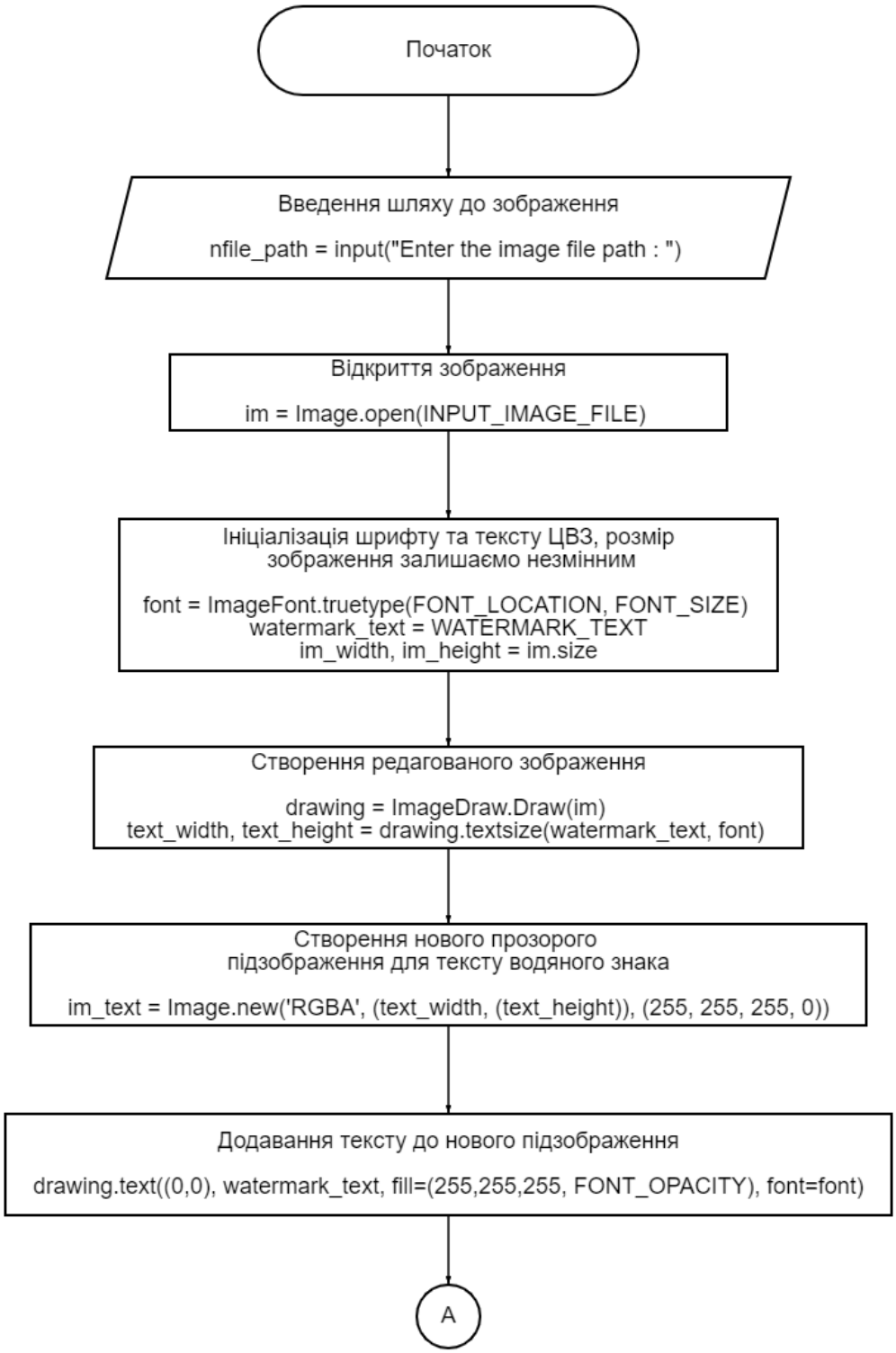

Рисунок А.1.1 – Алгоритм використання ЦВЗ, частина 1

Продовження додатку...

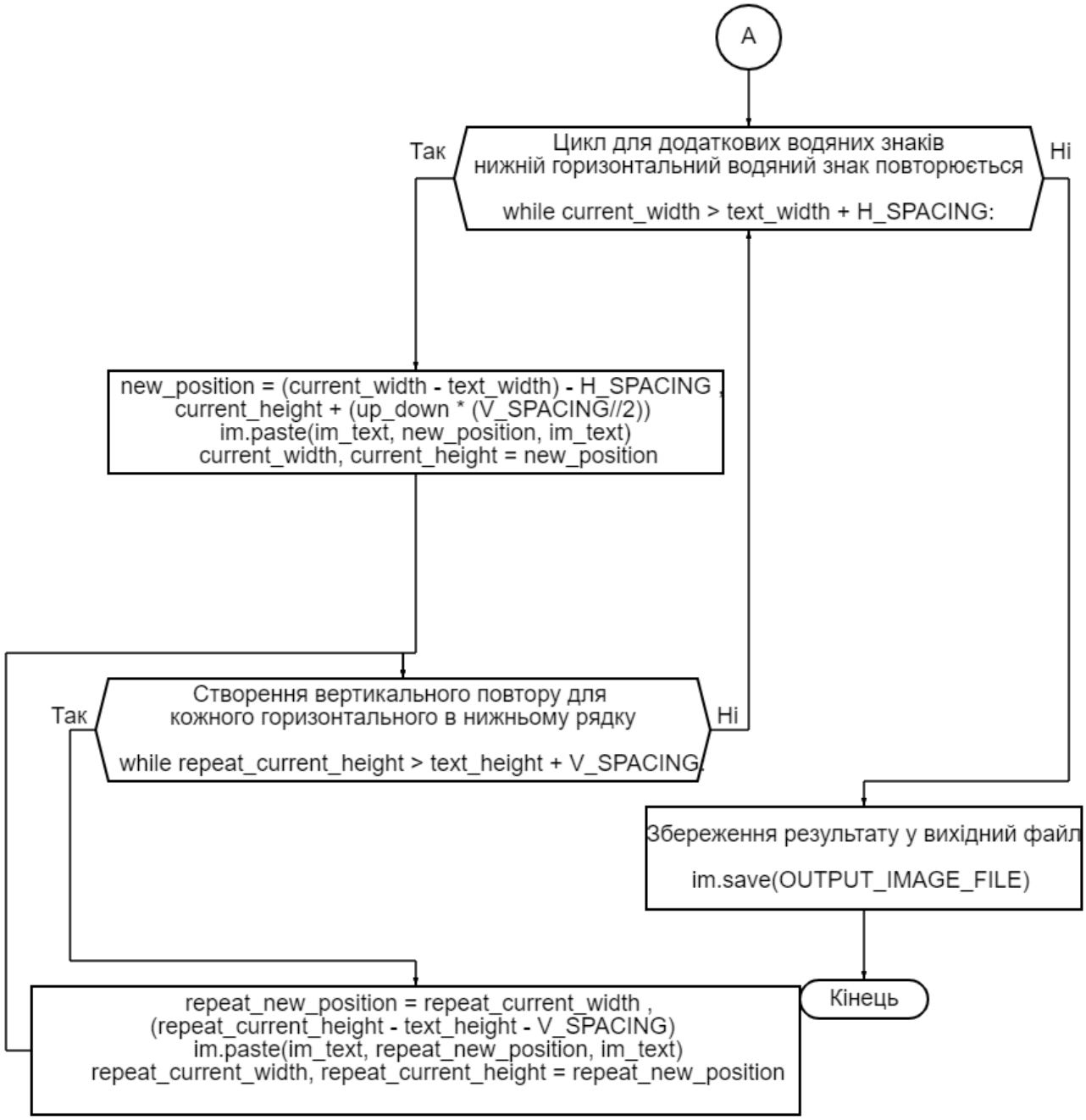

Рисунок А.1.2 – Алгоритм використання ЦВЗ, частина 2