У таблиці наведено приблизний рівень точності виявлення вразливостей для різних підходів.

Великі мовні моделі можуть охоплювати широкий спектр уразливостей без жорсткої прив'язки до заздалегідь визначених правил. Завдяки потужним когнітивним здібностям вони краще розуміють семантику коду і можуть надавати пояснення (chain-of-thought) щодо своїх висновків. LLM добре працюють на помірних за розміром фрагментах коду і мають потенціал навчатися на нових патернах атак.

У великих чи складних кодових базах їх точність може знижуватися, зростає ризик «галюцинацій» та хибних спрацьовувань. Деякі тонкі багатофункціональні уразливості LLM досі виявляють ненадійно. Крім того, результати залежать від якості запиту/контексту, а моделі можуть генерувати помилкові або неповні пояснення, що потребує верифікації людиною.

Підходи на основі LLM мають низку переваг у аналізі безпеки коду веб-додатків: висока гнучкість у розумінні контексту, можливість обробляти складні умови та різні мови програмування, а також здатність до природномовного пояснення ризиків. Водночас вони потребують значних обчислювальних ресурсів і можуть давати помилкові результати при погано підібраному prompt. Також показано, що спеціальне донавчання LLM додатково покращує результати виявлення. Таким чином, LLM можуть доповнювати традиційні rule-based та ML-підходи, проте не замінюють їх цілком.

1. OWASP Foundation. Direct Dynamic Code Evaluation – Eval Injection. OWASP. 2024. URL: https://owasp.org/www-community/attacks/Direct_Dynamic_Code_Evaluation_Eval%20Injection (дата звернення: 12.05.2025).
2. Mozilla Developer Network (MDN). Cross-site scripting (XSS). 2024. URL: https://developer.mozilla.org/en-US/docs/Glossary/Cross-site_scripting (дата звернення: 12.05.2025).
3. Tamberg K., Bahsi H. Harnessing Large Language Models for Software Vulnerability Detection: A Comprehensive Benchmarking Study. arXiv. 2024. URL: https://arxiv.org/abs/2405.15614 (дата звернення: 12.05.2025).
4. Ding Y., Fu Y., Ibrahim O., Sitawarin C., Chen X., Alomair B., Wagner D., Ray B., Chen Y. Vulnerability Detection with Code Language Models: How Far Are We? arXiv. 2024. URL: https://arxiv.org/abs/2403.18624 (дата звернення: 12.05.2025).

Можливості та обмеження OSINT у боротьбі з дезінформацією

УДК 004.56.5(043.2)
Олександр Цубера[1] Олександра Чорна[2]
Західноукраїнський національний університет,
fcitcyber25@zoom.wunu.edu.ua

У сучасному інформаційному суспільстві стрімке поширення дезінформації становить суттєву загрозу як для окремих осіб, так і для національної безпеки загалом. Одним із ключових інструментів боротьби з цим явищем є OSINT (Open Source Intelligence) — технологія збору, аналізу та інтерпретації

відкритих джерел інформації. OSINT дає змогу виявляти неправдиві наративи, перевіряти факти, здійснювати атрибуцію джерел та проводити незалежні розслідування, що робить його важливим інструментом у кібербезпеці та журналістиці розслідувань [1]. Метою роботи є аналіз можливостей та обмежень застосування OSINT у виявленні та протидії дезінформації.

На рис.1 подано загальну схему використання OSINT у контексті перевірки достовірності інформації. Вона передбачає багатоступеневу роботу з відкритими джерелами: пошук даних (вебсайти, соціальні мережі, фото, відео), аналіз їхньої автентичності, перевірка часу та місця зйомки, порівняння з іншими відкритими даними.[2]

Рис.1. Схема алгоритму OSINT розслідування

На рис.2 зображено приклад практичного використання OSINT для викриття дезінформації у соціальних мережах. Такий аналіз дозволяє ідентифікувати фейкові акаунти, боти, штучно роздмухані інформаційні кампанії.

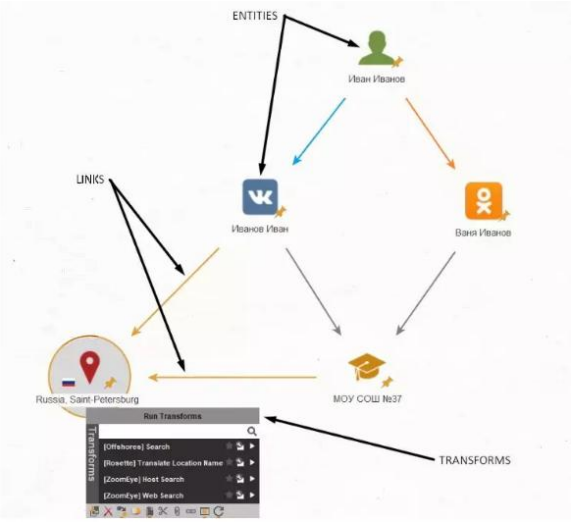

Рис.2. OSINT інструмент Maltego

Попри значні переваги, OSINT має низку обмежень. Зокрема, доступ до деяких джерел може бути обмеженим або піддаватися цензурі, а інтерпретація даних — суб'єктивною. Також існують юридичні та етичні аспекти, пов'язані з обробкою особистої інформації. Проте навіть з цими обмеженнями, OSINT залишається потужним інструментом для протидії інформаційним загрозам.[3]

У роботі було проаналізовано можливості використання OSINT у боротьбі з дезінформацією, визначено основні інструменти та етапи аналізу, а також окреслено головні переваги та обмеження даного підходу.

1. Higgins, A. (2023). Bellingcat and the Rise of Open-Source Investigations. The New York Times. URL: https://www.nytimes.com/bellingcat-osint (дата звернення: 01.04.2025).
2. OSINT Framework. URL: https://osintframework.com/ (дата звернення: 01.04.2025).
3. NATO StratCom COE. Detecting Disinformation: Best OSINT Practices. URL: https://stratcomcoe.org (дата звернення: 01.04.2025).

Розробка алгоритму вбудовування цифрових водяних знаків у відео

УДК 004.056

Ксенія Чабаненко[1], Наталія Кушніренко[2]
Національний університет «Одеська політехніка»,
[1]chabanenkoksenia3@gmail.com, [2]kushnirenko@op.edu.ua

Традиційні методи захисту, такі як криптографія чи контроль доступу, не гарантують збереження авторства або джерела походження після публікації

контенту у відкритих середовищах. У зв'язку з цим цифрові водяні знаки виступають ефективним засобом вирішення задач ідентифікації, верифікації та відстежування цифрових ресурсів. Особливої актуальності набуває розробка таких алгоритмів вбудовування, які забезпечують баланс між високою стійкістю до атак (наприклад, перекодування, фільтрація, стиснення), непомітністю для користувача та достатньою ємністю для передавання службової інформації [1].

У роботі представлено алгоритм вбудовування цифрових водяних знаків у частотну область з використанням дискретного косинусного перетворення. Запропонований підхід передбачає розподіл інформації водяного знака між аудіодоріжкою та кадровими складовими відео. Метою дослідження є створення ефективного алгоритму захисту авторських прав на мультимедійний контент шляхом вбудовування цифрового водяного знака. Реалізований алгоритм забезпечує підвищену стійкість водяного знака до атак і високий рівень непомітності.

Для досягнення зазначеної мети запропонований алгоритм використовує такі елементи:

- вбудовування у частотні коефіцієнти відео- та аудіофрагментів;
- розподіл цифрового водяного знака між аудіодоріжкою та відеокадрами;
- використання ключа для псевдовипадкової вибірки елементів.

Алгоритм використовує дискретне косинусне перетворення (ДКП) для переведення вхідних даних — кадрів та аудіосемплів — у частотну область і вбудовування водяного знака за методом Коха, що ґрунтується на модифікації співвідношення між парою середньочастотних коефіцієнтів [2]. Даний метод вбудовування передбачає розділення вхідного зображення на блоки розміром 8*8 пікселів та застосуванням ДКП до кожного окремого блоку, при цьому вбудовування відбувається з урахуванням того, що один блок придатний для запису одного біта інформації.

У більшості випадків, вбудовування цифрових водяних знаків у відео передбачає його представлення у вигляді послідовності зображень (кадрів), в які вбудовується знак [3].

У запропонованому алгоритмі відео розглядається як сукупність паралельних послідовностей: відеокадрів та відповідних фрагментів аудіодоріжки. Для вибірки кадрів, семплів та блоків, до яких вбудовується знак, використовується числовий ключ. Запропонований алгоритм забезпечує високий рівень надійності та стійкості ЦВЗ завдяки розподілу інформації між кадрами та аудіокомпонентами сигналу. Такий підхід дозволяє зменшити ступінь модифікації кожного окремого носія, що підвищує непомітність, порівняно з методами, які використовують виключно кадри в якості вхідних даних.

З метою забезпечення індивідуального та непередбачуваного розподілу водяного знака у відео застосовується генерація псевдовипадкових чисел. Текстовий ключ K використовується для ініціалізації генератора

псевдовипадкових чисел (ГПВЧ), який формує значення за наступною формулою:

$$R = min + (Nmod(max - min + 1)), \quad (1)$$

де *R*– псевдовипадкове число в межах діапазону [min,max], *N* – ціле число, отримане з хешу повідомлення-ключа, а *min, max* – мінімальне та максимальне значення діапазону, в якому генерується число. Отже, процес вбудовування включає наступні етапи:

1) розподіл відео на аудіодоріжку та кадрові складові;
2) ініціалізація генератора псевдовипадкових чисел за текстовим ключем;
3) вибір кадрів/семплів та блоків на основі псевдовипадкової вибірки;
4) перетворення обраних фрагментів у частотну область методом ДКП;
5) вбудовування ЦВЗ за методом Коха у середньочастотні коефіцієнти.

Таким чином, запропонований алгоритм забезпечує підвищену стійкість до атак завдяки розподілу водяного знаку між відео- та аудіоскладовими. Використання псевдовипадкового числа як основи для ключової вибірки забезпечує варіативність і непередбачуваність структури вбудовування. Описаний алгоритм був розроблений з метою реалізації у веб-застосунку для захисту мультимедійних даних. Програмна реалізація здійснюється з використанням сучасних бібліотек для обробки медіаданих, що забезпечують доступ до окремих кадрів відео та аудіофрагментів. Такий підхід дозволяє забезпечити зручність використання та масштабованість рішення в реальних умовах.

1. Мартинюк Г. В., Мелешко Т. В., Бичков В. В. Огляд існуючих задач, які можна вирішувати за допомогою стеганографії. Забезпечення кібербезпеки та захисту інформації: Колективна монографія. Київ: Європейський університет, 2023. с. 159–168.
2. Fridrich, J. Digital image steganography using stochastic modulation / Fridrich J., Goljan M. // Department of Electrical and Computer Engineering; SUNY Binghamton, Binghamton, NY, USA.
3. Шостак Н. В., Безрук В. М., Астраханцев А. А. Вибір переважного алгоритму вбудовування цифрових водяних знаків в відеофайли. Радіоелектроніка, інформатика, управління. 2018. № 3. с. 167-173.

ITSM-рішення як інструмент підвищення ефективності реагування на інциденти інформаційної безпеки

УДК 621.395.7 (043.2)
Максим Чмель[1], Геннадій Шаповалов[2]
Національний університет «Одеська політехніка»,
[1]9480565@stud.op.edu.ua, [2]shapovalov@op.edu.ua

У сучасному цифровому середовищі, де бізнес-процеси нерозривно пов’язані з інформаційними технологіями, стійкість компанії залежить не лише від технічного рівня захисту, а й від здатності організовано й оперативно реагувати на інциденти інформаційної безпеки. Витоки даних, збої в роботі