2. Zoria Y. Massive cyber attack hits Ukrainian e-services. Euromaidan Press. 2024. https://euromaidanpress.com/2024/01/25/massive-cyber-attack-hits-ukrainian-e-services/

3. Reuters. Iberia mess places timely focus on grid resilience. 2025. https://www.reuters.com/breakingviews/iberia-mess-places-timely-focus-grid-resilience-2025-04-30/

Розробка системи для виявлення підозрілих текстових повідомлень

УДК 004.056.55:004.8:681.3

Іван Боцанюк[1], Олена Агаджанян[2]

Національний університет «Одеська політехніка»,
[1]9480582@stud.op.edu.ua, [2]o.v.ahadzhanian@op.edu.ua

Із зростанням кількості фішингових, шахрайських та шкідливих повідомлень, що надсилаються через електронну пошту, виникає потреба у створенні гнучких та ефективних засобів захисту користувачів[1], зокрема в межах особистих або корпоративних систем. Особливої актуальності набуває локальне фільтрування повідомлень без залучення хмарних сервісів, оскільки останні можуть порушувати вимоги до конфіденційності в процесі обробки чутливих персональних або службових даних. Електронна пошта, як один із найпоширеніших каналів цифрового спілкування, становить основну ціль зловмисників, оскільки дозволяє комбінувати соціальні та технічні вектори атаки[2]. Враховуючи це, тема роботи сфокусована саме на електронних листах як на найбільш уразливому, розповсюдженому та структурованому форматі цифрового повідомлення, де доцільно застосовувати багатоетапний аналіз.

Метою роботи стало створення програмного забезпечення для виявлення підозрілих електронних повідомлень, яке функціонує автономно на локальному комп'ютері користувача, використовує виключно бібліотеки з відкритим вихідним кодом і враховує обмеження ресурсів системи. Основною особливістю проєкту є розгортання повноцінної системи фільтрації, що поєднує різні підходи до аналізу: від евристичних методів до машинного навчання у єдиному середовищі, без потреби в зовнішніх обчислювальних або API-сервісах. Такий підхід може бути легко адаптований і до інших типів цифрових повідомлень (наприклад, повідомлень в соціальних мережах), за умови врахування специфіки структури повідомлення, протоколів або вмісту.

Розроблений застосунок включає модулі для аналізу ключових елементів електронного листа: вкладень, текстового вмісту, HTML-коду, заголовків та гіперпосилань. Додатково реалізовано оптичне розпізнавання тексту з зображень та автоматичний переклад тексту на англійську мову для уніфікації вхідних даних перед обробкою. Це дозволяє інтегрувати зображений контент у загальний аналіз тексту, що є важливою частиною сучасних фішингових кампаній. На основі сукупності показників кожного модуля реалізовано систему зваженої оцінки з відповідним нормуванням і логікою пріоритетів: найнебезпечніші ознаки автоматично переміщують повідомлення до категорії «Небезпечні», тоді як менш виразні ознаки оцінюються в сукупності. Глобальна

оцінка формується на основі порогових значень: нижче -50 - «Небезпечні/Спам», від -50 до 50 - «Підозрілі», вище 50 - «Прийнятні».

Текстова частина повідомлень аналізується з використанням донавченої трансформерної моделі DistilBERT, натренованої на корпусі з 18650 повідомлень (61 % безпечних, 39 % - фішинг або спам). Тестування на незалежному наборі з 3021 прикладу показало стабільну ефективність: precision 0.98 і recall 0.98 для безпечних листів, precision 0.96 і recall 0.97 для небажаних. Важливо, що класифікація може виконуватися навіть на бюджетному процесорі (Intel i3 11-го покоління) з використанням лише ~900 МБ оперативної пам'яті, що свідчить про придатність розробленої системи для широкого використання без потреби у високопродуктивному обладнанні.

Під час аналізу було виявлено як переваги, так і обмеження локального підходу. Система здатна ефективно виявляти шаблонні та повторювані атаки, включаючи окремі випадки цільового фішингу. Водночас, локальна природа рішення обмежує його здатність до глибокого аналізу вкладень (наприклад, емуляція виконання, sandboxing), що важливо при виявленні складних загроз, прихованих у, здавалося б, легітимному вмісті (наприклад, шкідливі скрипти у PDF-файлах). Окремо слід зазначити, що повністю автономне функціонування системи унеможливлює доступ до актуалізованих онлайн-баз загроз, без яких суттєво знижується ефективність захисту від нових або модифікованих типів атак.

З метою забезпечення балансу між захистом та конфіденційністю, доцільним є впровадження поміркованих компромісів: наприклад, здійснювати аналіз не повного посилання, а лише доменного імені; дозволяти обмежене використання зовнішніх сервісів виключно для тих повідомлень, які попередньо були класифіковані як підозрілі локально. Такий вибір зменшує ризик витоку приватних даних, зберігаючи при цьому можливість використання актуальних джерел у критичних випадках.

Також слід зважати на відставання деяких відкритих рішень (у сфері перекладу чи OCR) у порівнянні з комерційними аналогами. Утім, розвиток відкритих технологій, зокрема за рахунок залучення спільноти та поширення доступних моделей, дозволяє сподіватися на скорочення цього розриву в майбутньому. Противагою відсутності доступу до централізованих сервісів є зростання якості й оптимізації локальних інструментів, що з часом сприятиме підвищенню ефективності автономних систем без компромісу для конфіденційності користувача.

Загалом, створений застосунок демонструє, що використання комплексного аналізу електронної пошти в локальному середовищі є технічно можливим та ефективним навіть у рамках обмежених ресурсів. З огляду на тенденції розвитку відкритих бібліотек, моделей і технологій оптимізації, можна очікувати подальше зменшення розриву між локальними рішеннями та потужними хмарними платформами, що зробить приватні захищені системи дедалі доступнішими для широкого кола користувачів.

1. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report: 4th Quarter 2024. 2024. URL: https://www.apwg.org/trendsreports/ (дата звернення: 25.04.2025)

Altulaihan E., Alismail A., Rahman M. M., Ibrahim A. Email security issues, tools, and techniques used in investigation. *Sustainability*. – 2023. – Vol. 15. – №10612.

Формалізація методики побудови безпечних інформаційних систем екологічного моніторингу

УДК 004.75

Кирило Вадурін[1], Андрій Перекрест[2]
Кременчуцький національний університет імені Михайла Остроградського, [1]kir3337@gmail.com, [2]pksg13@gmail.com

Наразі спостерігаються тенденції до розширення використання датчиків якості повітря в інфраструктурі Smart City для моніторингу екологічної ситуації. Існують платформи для збору та аналізу даних, проте питання безпеки інформаційних систем та формалізації відповідних методик залишаються поза увагою. Актуальність запланованої роботи пов'язана з необхідністю забезпечення безпеки та надійності інформаційних систем екологічного моніторингу в умовах розширення інфраструктури Smart City.

У ході аналізу подібних рішень виявлено, що питання безпеки інформаційних систем екологічного моніторингу, особливо в контексті Smart City, потребують додаткової уваги. Airly [1] пропонує комплексні рішення для моніторингу якості повітря, але питання безпеки даних не є пріоритетними. У той же час, існують дослідження, спрямовані на забезпечення безпеки та енергоефективності аутентифікації в розумних містах за допомогою біометрії та криптографічних методів [2], проте вони не враховують специфіку датчиків якості повітря. Платформи, такі як Kyiv Smart City [3], демонструють можливості моніторингу якості повітря, але потребують удосконалення в частині довгострокової підтримки та інтеграції з іншими міськими системами. Державна система моніторингу довкілля в Україні [4] потребує модернізації та впровадження сучасних технологій для забезпечення ефективного збору та аналізу даних. Таким чином, невирішеними залишаються питання формалізації безпеки, масштабування рішень та інтеграції даних моніторингу з іншими системами Smart City.

Метою роботи є формалізація методики побудови безпечних інформаційних систем екологічного моніторингу на основі розподіленої апаратної інфраструктури датчиків якості повітря та виконавчих пристроїв Smart City, що забезпечить захист даних та надійність функціонування системи.

Основними завданнями, що наразі не вирішені, є розробка конкретних методів формалізації безпеки інформаційних систем екологічного моніторингу, забезпечення захисту даних та надійності розподіленої апаратної інфраструктури датчиків якості повітря, а також вирішення питань масштабування, довгострокової підтримки та інтеграції даних моніторингу з іншими міськими системами.