УДК 004.056.5

КОМПЛЕКСНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ ХМАРНИХ ПЛАТФОРМ ДЛЯ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ТА НЕЙТРАЛІЗАЦІЇ ШКІДЛИВИХ ФАЙЛІВ

Андрій ДЕНЕГА, Валентина ЯЩУК, Андрій ІВАНУСА
Львівський державний університет безпеки життєдіяльності

Анотація. *Досліджено сучасні підходи до аналізу хмарного програмного забезпечення з метою виявлення шкідливих файлів. Розвиток хмарних сервісів та SaaS-рішень значно збільшив обсяг оброблюваних даних, що підвищує ризики компрометації корпоративної інформації. Особливу увагу приділено методам статичного та динамічного аналізу, поведінковій аналітиці та машинному навчанню для класифікації шкідливих об'єктів. Запропоновано інтегративну модель оцінки ризику, яка поєднує технічні, поведінкові та контекстні параметри, що забезпечує підвищену точність та швидкість виявлення загроз у хмарних середовищах.*

Ключові слова: *хмарне програмне забезпечення, шкідливі файли, машинне навчання, аналіз поведінки, кіберзахист.*

Abstract. *Modern approaches to analyzing cloud software for the purpose of detecting malicious files are investigated. The development of cloud services and SaaS solutions has significantly increased the amount of processed data, which increases the risks of compromising corporate information. Particular attention is paid to static and dynamic analysis methods, behavioral analytics, and machine learning for classifying malicious objects. An integrative risk assessment model is proposed that combines technical, behavioral, and contextual parameters, which provides increased accuracy and speed of threat detection in cloud environments.*

Keywords: *cloud software, malicious files, machine learning, behavioral analysis, cyber security.*

Хмарні платформи забезпечують високу масштабованість, гнучкість та доступність, але водночас стають привабливою мішенню для кібератак, включно зі шкідливими файлами, що маскуються під легітимний контент. Основними векторами загроз у хмарних сервісах є виконувані файли (.exe), скрипти (.bat, .ps1), макроси VBA (.docm, .xlsm), PDF-файли з вбудованим JavaScript, архіви з паролем та виконувані об'єкти у контейнерах OLE. Сучасні шкідливі файли часто використовують обфускацію, енкрипцію payload та техніку Living-Off-the-Land (LOLbins) для обходу антивірусних сканерів і sandbox-середовищ.

Сьогодні виділено три ключові напрями виявлення шкідливих файлів у хмарному середовищі. Перший напрям – статичний аналіз, який передбачає перевірку хешів, сигнатур файлів, метаданих та інтеграцію з базами Threat Intelligence. Прикладом такого підходу є виявлення шкідливого

макросу з командою CreateObject("WScript.Shell") та викликом URLDownloadToFile для завантаження payload. Для PDF-файлів застосовується аналіз вбудованого JavaScript та перевірка на відомі уразливості за стандартом CVE. Другий напрям – динамічний аналіз, який здійснюється у sandbox або емуляторі хмарного середовища; під час запуску файлу відстежується його поведінка, включно зі створенням процесів, мережею активністю, маніпуляціями з файловою системою та доступом до критичних ресурсів. Наприклад, це може бути запуск PowerShell-скрипта для завантаження шкідливих DLL-файлів у пам'ять без запису на диск (in-memory attack). Третій напрям – поведенкова аналітика та машинне навчання, що дозволяє класифікувати об'єкти на основі аномальної активності, включаючи нестандартні виклики API, підозрілі комбінації параметрів у скриптах, повторювані мережеві запити та незвичні ланцюжки процесів. Використання алгоритмів класифікації, таких як Random Forest та XGBoost, а також нейронних мереж, дозволяє автоматично виявляти обфусковані та zero-day загрози.

Щодо архітектури обробки файлів у хмарному середовищі, пропонується багаторівнева схема (рис.1).

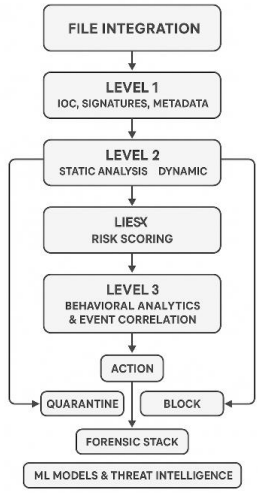

Рисунок 1 – Блок-схема архітектури багаторівневої обробки файлів у хмарному середовищі

На першому рівні здійснюється прийом і первинна перевірка файлу на сигнатури та відомі індикатори компрометації (IOC). Другий рівень забезпечує статичний та динамічний аналіз із застосуванням sandbox і емуляторів операційних систем, де відстежується поведінка файлів та виявля-

ються потенційні атаки in-memory. На третьому рівні інтегруються поведінкові алгоритми та моделі машинного навчання для оцінки аномалій та кореляційного аналізу подій у SIEM. Заключний етап включає автоматичне блокування або поміщення в карантин файлів з високим ризиком, а також збереження логів для подальшого розслідування. Така архітектура дозволяє реалізувати превентивний підхід, знижуючи ймовірність пропуску шкідливих об'єктів у корпоративну хмарну інфраструктуру.

Блок-схема архітектури багаторівневої обробки файлів у хмарному середовищі ілюструє процес проходження інгрестованих файлів первинної перевірки (Level 1 — IOC, сигнатури, метадані), далі розподіляються на статичний і/або динамічний аналіз (Level 2), на основі отриманих індикаторів формується ризик-скор і передається на рівень поведінкової аналітики та кореляції подій (Level 3). За результатами приймається автоматизоване рішення (карантин/блок/сповіщення), а артефакти й логи направляються у форензик-стік та для підживлення ML-моделей і Threat Intelligence.

Отже, для ефективного виявлення шкідливих файлів у хмарних сервісах необхідне комплексне поєднання статичного, динамічного та поведінкового аналізу з використанням алгоритмів машинного навчання. Запропонована багаторівнева архітектура обробки файлів забезпечує точність, швидкість реагування та адаптивність до нових типів загроз, включно із zero-day атаками. Подальші дослідження можуть зосередитися на інтеграції Zero Trust принципів для контролю доступу, оптимізації алгоритмів машинного навчання для реального часу та масштабуванні систем раннього попередження у великих корпоративних хмарних середовищах.

Література

1. Ящук В.І., Івануса А.І., Маслова Н.О., Ткачук Р.Л., Брич Т.Б. Концептуалізація інтегративного використання баз даних вразливостей у контексті системного менеджменту інформаційної безпеки // Вісник Львівського державного університету безпеки життєдіяльності. – 2025. – Т. 31. – С. 59–61

2. Ящук В.І. Simulation Of Investment It Project Management Tasks / В.І. Ящук // Інновінг сучасних трендів в менеджменті безпеки: національна безпека та оборона»: збірник тез доповідей Всеукраїнської науково-практичної конференції м. Львів, 23 травня 2025 року. Львів: ЛДУ БЖД, 2025. 460 с. (С.247-253).

3. Valentina Yashchuk, Andriy Ivanusa, Nataliya Maslova, Rostyslav Tkachuk, Taras Brych INTEGRATION OF VULNERABILITY DATABASES INTO ISMS – A PATH TO ENHANCING CYBER RESILIENCE OF CRITICAL SYSTEMS // Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference. Drohobych: Donetsk National Technical University, 2025. 184 p.60-66.