УДК: 004.056:004.415.2:004.75

Грабовий В. А., здобувач вищої освіти,
Штовба С. Д., д-р техн. наук, професор,
професор кафедри інформаційних технологій,
Донецький національний університет імені Василя Стуса

ЗМЕНШЕННЯ РИЗИКІВ УРАЖЕННЯ ШКІДЛИВИМИ ПРОГРАМАМИ В ХМАРНОМУ СЕРЕДОВИЩІ AWS

Анотація. У дослідженні розглянуто методи зменшення ризиків ураження шкідливими програмами в хмарному середовищі AWS за допомогою технологій машинного навчання та автоматизації. Запропоновані підходи сприяють підвищенню загального рівня кібербезпеки.

Ключові слова: AWS, кіберзахист, шкідливе програмне забезпечення, машинне навчання, автоматизація.

Вступ. У сучасних умовах глобальної цифровізації технології хмарних обчислень стають невід'ємною частиною роботи підприємств різних галузей. Використання хмарних сервісів, зокрема Amazon Web Services (AWS), забезпечує масштабованість та гнучкість бізнес-процесів, проте їх використання також підвищує ризик ураження шкідливими програмами. Основною метою цього дослідження є розробка нових підходів до зменшення ризиків ураження шкідливими програмами в хмарному середовищі AWS за допомогою технологій машинного навчання та автоматизації.

Актуальність. Використання AWS є популярним серед підприємств завдяки гнучкості та масштабованості, які вони забезпечують. Однак зростаючий рівень кібератак, зокрема шкідливих програм (малваре), створює значні виклики для безпеки таких середовищ. Шкідливе програмне забезпечення може проникати в хмарні системи через різні вразливості, як-от помилки конфігурації, фішингові атаки або експлуатація вразливостей програмного забезпечення. Особливо важливим є те, що атаки можуть бути спрямовані як на викрадення даних, так і на порушення роботи інфраструктури. Тому підприємства, які використовують AWS, потребують нових підходів до захисту, що базуються на проактивних методах виявлення та швидкої автоматизованої реакції на загрози. Вразливості AWS можуть бути використані зловмисниками для доступу до критично важливої інформації, що підкреслює необхідність створення ефективних моделей захисту.

Згідно зі звітами з кібербезпеки, частота атак на хмарні середовища постійно зростає, що вимагає вдосконалення наявних методів захисту. AWS пропонує потужні засоби для забезпечення безпеки, як-от Amazon GuardDuty, Amazon Inspector, та AWS Shield, проте їх застосування має бути поєднане з правильною конфігурацією та дотриманням найкращих практик. Основні проблеми виникають через людський фактор, неправильне налаштування безпекових політик або недостатню увагу до процесів моніторингу.

До того ж важливим аспектом є інтеграція технологій машинного навчання для автоматизованого виявлення загроз. Використання інструментів на основі штучного інтелекту дає змогу ефективніше виявляти аномалії в поведінці систем

та реагувати на них у режимі реального часу. Такий підхід дає змогу підприємствам мінімізувати ризики ураження шкідливими програмами та забезпечити безперервність бізнес-процесів, що є критичним у сучасних умовах.

Наявні дослідження показують, що використання хмарних технологій без належного рівня безпеки може призвести до значних фінансових втрат і пошкодження репутації. Тому актуальність цього дослідження полягає у розробці нових підходів до зменшення ризиків ураження шкідливими програмами за допомогою автоматизованих систем моніторингу та захисту. Це допоможе підприємствам не лише ефективно протидіяти сучасним кіберзагрозам, але й підвищити загальний рівень безпеки їх хмарної інфраструктури.

Висновки. Застосування технологій машинного навчання та автоматизації процесів виявлення загроз є ефективним підходом для зменшення ризиків ураження шкідливими програмами в хмарному середовищі AWS. Запропонований підхід дає змогу не лише виявляти вже відомі загрози, але й прогнозувати нові, що підвищує загальний рівень кібербезпеки хмарної інфраструктури.

Список використаних джерел

1. Бондар Н. О., Колтун Ю. М. Захист персональних даних користувачів з використанням хмарних сервісів AWS. 2023. URL: https://repository.kpi.kharkov.ua/items/2bad4b42-0e74-4af7-b365-c27d5839017e (дата звернення: 20.10.2024).

2. Пономаренко В. Ю. Дослідження методів забезпечення мережної безпеки в хмарній інфраструктурі. 2024. URL: https://openarchive.nure.ua/entities/publication/cdb3349f-8ac4-40e7-ac3d-04745f164ab2 (дата звернення: 20.10.2024).

3. Щерба М. О. Дослідження методів забезпечення інформаційної безпеки у хмарному середовищі. 2023. URL: https://openarchive.nure.ua/entities/publication/a3625c7e-2444-4b7f-8cdd-43dfc213b350 (дата звернення: 20.10.2024).