

УДК 004.492.3

А.Р. Бориславський

Тернопільський національний економічний університет, Україна

ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В ОС ANDROID НА ОСНОВІ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ

A.R. Boryslavskyi

DETECTION MALWARE ON ANDROID BASED ON INTELLIGENT ON TECHNOLOGIES

З року в рік операційна система Android збільшує свою популярність. Ще в червні 2013 року компанія Google Inc. оголосила, що має понад 1 мільярд активних користувачів Android щомісяця. А станом на 2018 рік Android мав найбільшу встановлену базу з усіх операційних систем загального призначення.

Програми для Android, що розширюють функціональність пристроїв, написані в основному мовою програмування Java за допомогою набору програм для розробки програмного забезпечення Android (SDK). Офіційний магазин, Google Play Store, є основним магазином додатків, встановлених на пристроях Android, які відповідають вимогам сумісності Google. Google Play Store дозволяє користувачам переглядати, завантажувати та оновлювати програми.

Android має великий вибір сторонніх програм, які користувачі можуть придбати, завантаживши та встановивши файл APK програми, або завантаживши їх за допомогою програми магазину додатків, яка дозволяє користувачам встановлювати, оновлювати та видаляти програми зі своїх пристроїв. Таке розмаїття програм Android і магазинів додатків робить проблеми безпеки дуже нагальними.

Google Inc. розробила вбудовану систему безпеки, яка базується на впровадженні «пісочниці» для запуску програми та відображає всі необхідні дозволи для встановленого додатка. Так, наприклад, додатку погоди може знадобитися ввімкнути збереження даних або підключення до Інтернету, але не потрібно читати SMS-повідомлення або отримувати доступ до особистих даних. Переглянувши дозволи, користувач може встановити або відмовитися від програми. Реалізація «пісочниці» та системи дозволів зменшує вплив вразливостей, але не виключає їх повністю.

Як результат, загрози безпеці для Android зростають експоненціально. Так, компанія Trend Micro повідомила, що кількість загроз зловмисних програм Android зросла до 25000 зразків [1]. Інша антивірусна компанія, Лабораторія Касперського, виявила 35000 зловмисних зразків за весь 2018 рік [2]. Кіберзлочинці заражають мобільні пристрої з наступною метою: а) викрадення грошей з рахунків користувачів; б) викрадення інформації про власників пристроїв, включаючи усі дзвінки, листування, паролі до соціальних мереж тощо. Загальновідомо, що сучасним антивірусам властиві кілька недоліків. Найважливішими з них є невміння методів на основі сигнатур виявляти невідомі шкідливі програми та недосконалість евристичних методів, що застосовуються. На підставі вищевикладеного сформульовано мету роботи – підвищення ефективності виявлення шкідливих програм в ОС Android шляхом розробки моделей і алгоритмів на основі інтелектуальних технологій.

Література

1. Trend Micro Електронний ресурс] – Режим доступу : <http://www.trendmicro.eu/index.html>.
2. Kaspersky Lab Електронний ресурс] – Режим доступу : <http://www.kaspersky.com>.