УДК 004.056.53

М.П. Комар, канд. техн. наук, М.С. Лущак, В.М. Огар, І.П. Харкавців, Р.І. Яворський
Тернопільський національний економічний університет, Україна

ІНТЕЛЕКТУАЛЬНІ МЕТОДИ ВИЯВЛЕННЯ ВТОРГНЕНЬ У КОМП'ЮТЕРНІ СИСТЕМИ

M.P. Komar, Ph.D, M.S. Lushchak, V.M. Ohar, I.P. Kharkavtsiv, R.I. Yavorskyi

INTELLIGENT INTRUSION DETECTION METHODS IN COMPUTER SYSTEMS

У зв’язку з постійно наростаючим використанням комп’ютерів у різних сферах науки, техніки, технологій, бізнесу, а також життя людей, інформаційні телекомунікаційні мережі на їх основі піддаються різного роду загрозам. Крім того, користувач не може бути впевнений у захищеності важливої інформації, оскільки кіберзлочинці продовжують масово удосконалювати і розробляти методи та засоби організації кібератак (зловмисний код, мережеві вторгнення і т.д.) [0, 2]. Останнім часом найбільш помітною тенденцією стало поступове стирання рамок і розмивання традиційних кордонів між різними типами загроз і видами шкідливої діяльності [0].

Сучасні комерційні системи виявлення вторгнень не забезпечують належний рівень захисту комп’ютерних систем, їх методи мають ряд недоліків. Так, найточніший на сьогодні метод, що ґрунтується на сигнатурному аналізі, добре функціонує при виявленні вже відомих вторгнень, але абсолютно не придатний для виявлення нових, раніше невідомих. А як показує практика, саме нові, раніше невідомі, вторгнення є причиною глобальних інформаційних катастроф і призводять до величезних фінансових і моральних збитків. Для захисту комп’ютерних систем від невідомих вторгнень розроблено немало евристичних методів. Але вони характеризуються високим рівнем помилок першого і другого роду (ймовірність пропуску атак та ймовірність помилкових спрацювань), що ускладнює застосування евристичних методів. Додатковим недоліком існуючих засобів на їх базі є висока обчислювальна складність. Така ситуація стимулює подальші дослідження, одним із перспективних напрямків яких є застосування методів штучного інтелекту для виявлення вторгнень в комп’ютерні системи.

Разом з тим, відомі підходи характеризуються наявністю недоліків, таких як складність створення або вибору необхідних детекторів вторгнень, громіздкість процедури адаптації до невідомих вторгнень, здатність коректно працювати тільки на невеликих наборах даних, значна обчислювальна складність, особливо в режимі реального часу, а також можливість відключення під час атаки.

Таким чином, розроблення ефективних методів захисту від вторгнень в комп’ютерні системи є надзвичайно актуальним і вимагає нових підходів у цій сфері, дозволить розробити систему захисту від вторгнень, яка характеризуватиметься здатністю до самонавчання та адаптації з метою забезпечення високого рівня безпеки.

Література

1. Kaspersky Security Bulletin [Електронний ресурс] – Режим доступу: https://cdn.securelist.ru/files/2017/12/KSB_Review-of-2017_final_RU.pdf.

2. Дорош В.І. Глибокі нейронні мережі як перспективний напрям виявлення атак в сучасних телекомунікаційних мережах / В.І. Дорош, П.Ю. Якобчук, Едгарс Вейсс, А.В. Фаранович // Збірник тез доповідей міжнар. наук.-техн. конф. молодих учених та студентів «Актуальні задачі сучасних технологій», Тернопіль : ТНТУ, 16–17 листопада, 2017. – С. 205-206.