# Програмний модуль виявлення аномалій в соціотехнічних системах

УДК 004.056.53

Тарас Паращук[1], Анна Корченко[2],
Марина Коломієць[3]

*Національний авіаційний університет,*

*[1]taras1039@gmail.com,[2]annakor@ukr.net, [3]m.kolomiiets@nau.edu.ua*

На сьогодні більшість систем виявлення вторгнень стають невід'ємною частиною захисту будь-якої соціотехнічної системи, вони використовуються для моніторингу підозрілої активності в системі та виявлення атакуючих дій неавторизованої сторони.

Останні дослідження, які проведені фахівцями в відповідних галузях за останні роки показали, що корпоративні мережі переважної більшості організацій не здатні забезпечити належний захист від існуючих кіберзагроз на рівні персоналу так і системи. Відзначені дві масштабні кібератаки, які потрясли світову спільноту – віруси WannaCry та NotPetya інфікували сотні тисяч комп'ютерів в різних країнах. Також, користувачі зіткнулися і з низкою інших, менш значних атак, що пов'язані з вірусами-вимагачами, DDoS-атаками, викраданням персональних даних.

Активізація таких кібератак ініціює створення спеціальних технічних рішень, засобів та систем протидії, здатних залишатись ефективними при появі нових або модифікованих видів кіберзагроз з невстановленими або нечітко визначеними властивостями. Загалом такі системи направлені на виявлення підозрілої активності чи втручання в мережу для прийняття адекватних заходів щодо запобігання кібератакам. Ці системи, як правило, достатньо дорогі, мають закритий код та вимагають періодичної підтримки висококваліфікованих фахівців для налаштування до умов конкретних підприємств. Достатньо актуальними і необхідними систем виявлення вторгнень є ті, які орієнтовані на виявлення аномальних станів. Основними їх недоліками є, наприклад, надлишок помилкових спрацювань, складність процесу налаштування, тривалий процес навчання та створення відповідного профілю нормального стану системи. Більш ефективними в цьому є експертні підходи, засновані на використанні знань і досвіду фахівців відповідної предметної галузі.

Виходячи з цього, побудова технічних рішень і створення спеціальних засобів, що дозволяють детектувати раніше невідомі кібератаки шляхом контролю поточного стану нечітко визначених параметрів в слабоформалізованому середовищі оточення, заснованих на експертних підходах, є актуальною задачею.

Метою роботи є розробка програмного модуля формування еталонів параметрів для систем виявлення аномалій в соціотехнічних системах.

В запропонованому модулі формування еталонів параметрів за основу вибрано два параметра: кількість одночасних підключень (КОП) та кількість пакетів з однаковою адресою відправника і одержувача (КПОА), це дозволяє

ефективно виявляти аномалії двох основних видів Spoofing IP, ARP-spoofing та на базовому рівні відслідковувати початок процесу DoS/DDoS-атак. Його можна структурно розділити на такі основні алгоритмічні елементи:

1. ServicesSensors – даний клас відповідає за організацію ефективної роботи сенсорів програмної моделі, які орієнтовані на визначення кількості підключених клієнтів та аналізу пакетів, що надходять до системи.
2. ManagerSensors – даний клас відповідає за отримання та первину обробку даних з сенсорів системи відносно двох основних параметрів аналізу КОП і КПОА.
3. ConstantCoordinates – даний клас відповідає за отримання експертних оцінок відносно параметрів КОП і КПОА, що характеризують основні стани системи в залежності від виникнення критичних чи аномальних ситуацій.
4. CurrentCoordinates – даний клас відповідає за процес конвертації та обробки вхідних даних за допомогою математичних методів (метод лінійної апроксисмації локальними максимумами, базові правила роботи з нечіткими множинами).
5. ParameterSensors – даний клас відповідає за отримання налаштувань «сенсорів» та експертних оцінок за допомогою обміну даними з вище описаними класами та методами.

Таким чином, розроблений програмний модуль, який, за рахунок базового алгоритму та низки розроблених процедур (конструювання координатної сітки; ініціалізації величин на основі набору баз даних та модулів; графічного формування параметрів; пошуку спільних точок відповідно базових правил та графічної інтерпретації результату), дозволяє виявляти аномалії в соціотехнічних системах.