Програмний модуль виявлення аномалій в комп'ютерних мережах

УДК 004.056.53

Тарас Паращук[1] , Анна Корченко[2]

Національний авіаційний університет, [1]taras1039@gmail.com,[2]annakor@ukr.net

Широке використання засобів захисту для фільтрування джерел трафіку у комп'ютерних мережах, а також захист від несанкціонованого підключення та доступу не може буде забезпечений на належному рівні з урахуванням усіх можливих шляхів обходу програмних засобів. В роботі запропоновано програмний модуль для виявлення аномалій поведінки мережевого трафіку, заснованого на нечіткій логіці.

Виявлення аномалій є важливою складовою при попередженні атак в комп'ютерних мережах. Тому необхідно чітко визначити причини та фактори появи їх у системі. Саме тому розробка програмного модуля з посиленою концентрацією на питаннях ресурсної ємності та швидкодії процесів виявлення аномалій системи дозволить ефективно визначити в якому стані перебуває комп'ютерна мережа.

Метою є розробка програмного модуля формування еталонів параметрів для систем виявлення аномалій в комп'ютерних мережах.

Новизною є розроблений програмний модуль формування еталонів параметрів для систем виявлення аномалій в комп'ютерних мережах для попередження DOS/DDOS атак, за рахунок використання еталонів параметрів, таких як кількість одночасних підключень (КОП) та кількість пакетів з однаковою адресою (КПОА), що дало можливість виявляти аномалії пов'язані з спуфінг-атаками.

Розроблений модуль орієнтований на виявлення DDoS-атак на сервер і спуфінгу. При цьому для описання цих аномалій зазвичай використовуються такі параметри при аналізі поточного стану системи:

- кількість одночасних підключень до сервера;
- швидкість обробки запитів від клієнтів;
- затримка між запитами від одного користувача,
- кількість пакетів з однаковою адресою відправника і одержувача.

В даному програмному модулі формування еталонів параметрів для систем виявлення аномалій за основу вибрано параметри КОП та КПОА, це дозволяє ефективно виявляти аномалії двох основних видів Spoofing IP, ARP-spoofing та на базовому рівні відслідковувати початок процесу DoS/DDoS-атак. Розглянемо структурну схему програмного модуля виявлення аномалій (рис. 1), де:

БДК – база даних кіберзагроз;

БДП – база даних правил;

БДЕ – база даних еталонів;

МФПЗ – модуль формування поточних значень системи;

МАРН – модуль α-рівней номіналізації;

МІТ – модуль ідентифікуючих термів;

МРА – модуль рівня аномалій;

МВ – модуль візуалізації.

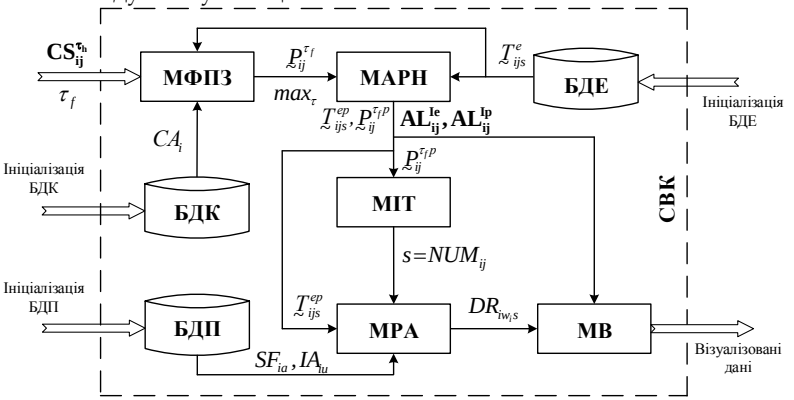

Рис.1. Структурна схема програмного модуля виявлення аномалій

Оскільки на даний момент захист від мережевих атак та аномалій є важливим питанням при розгляді корпоративних та державних структур, тому в даній роботі було розглянуто програмний засіб для виявлення аномалій в комп'ютерних системах. Основна задача якого протидіяти на мережевому рівні аномаліям, які пов'язані наприклад з DoS/DDoS та Spoofing атаками.

Науковий керівник – к.т.н., доцент, Корченко А.О.