УДК 681.14

ІНФОРМАЦІЙНА СИСТЕМА ПРОГНОЗУВАННЯ ТА ВИЯВЛЕННЯ РІВНЯ ЗАГРОЗ ДЛЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Міщенко М. В. студ. гр. МПІн-181
Науковий керівник: **Трунова О.В.**, к.пед.н., доцент
Національний університет «Чернігівська політехніка»

У сучасному світі питання кібербезпеки набуло досить високої актуальності, адже питома вага інформації, що знаходиться у електронному вигляді зростає з кожним днем, гостро ставлячи питання про її захист.

На даний момент існує ряд інформаційних систем, метою яких є виявлення та запобігання мережевим атакам та аномаліям трафіку, проте більшість з них працює в реальному часі, та надає інформацію про загрозу або вживає необхідних дій за фактом настання цієї загрози. Тому було прийнято рішення про створення інформаційної системи яка б окрім виявлення загроз мала б можливість надавати прогнози щодо майбутнього рівня загроз для досліджуваної мережі. Основним джерелом загроз, який буде аналізувати система, що проектується, є мережевий трафік, який надходить до корпоративної комп'ютерної мережі із глобальної мережі Інтернет. Таким чином, у якості вхідних даних для побудови прогнозу рівня загроз для корпоративної мережі, будемо використовувати набір кількісних та якісних параметрів трафіку, що проходить через мережу за одиницю часу.

Для збору таких даних буде використано програмний мережевий екран PfSense, що побудований на базі ядра FreeBSD та може бути встановленим на вузол, що фізично знаходиться одразу перед роутером. Основною перевагою даного рішення є наявність відкритого API, розробленого для роботи з PfSense – FauxAPI [1], що забезпечує доступ до даних трафіку, що проходить через мережевий екран.

У якості бази даних будемо використовувати InfluxDB, яка призначена для зберігання великих обсягів однотипних даних, зокрема і часових рядів [2]. InfluxDB буде встановлена на окремий сервер, що знаходиться за межами корпоративної комп'ютерної мережі, таким чином забезпечивши ізольованість даних та функціонування незалежно від внутрішніх збоїв мережі.

Програмний модуль збору та аналізу даних буде включати в себе модуль комунікації з FauxAPI для отримання даних трафіку з мережевого екрану корпоративної комп'ютерної мережі, модуль для збереження зібраних часових рядів до бази даних та модуль аналізу та виведення прогнозів відповідно до зібраних часових рядів. Програмна частина буде написана на мові програмування Python. Даний модуль також ізольований від досліджуваної мережі, що дозволяє йому функціонувати незалежно від внутрішніх збоїв мережі.

Архітектура розробленої системи, зображена на рисунку 1.

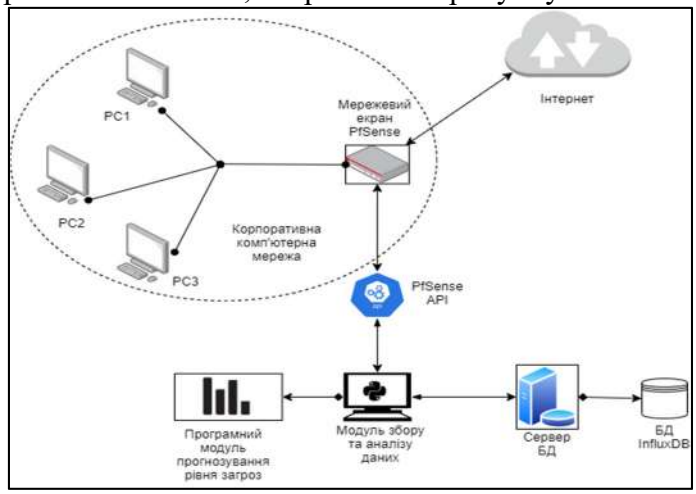

Рисунок 1 – Загальна архітектура системи

Розглядаючи комп'ютерну мережу як складну динамічну систему, процеси в якій протікають нелінійно, можемо зробити припущення про можливість застосування Теорії Хаосу для раннього виявлення нормального (хаотичного) та підозрілого (нехаотичного) перебігу процесів у корпоративній комп'ютерній мережі.

Для виявлення хаотичності скористаємося підходом з обчислення експоненти Ляпунова λ, що для потоку динамічної системи $F^t(x_0) = x_t$, визначається наступним чином:

$$\lambda(x) = \lim_{t\to\infty} \frac{1}{t} * \ln\|d_x F^t\| \quad (1)$$

В загальному випадку, позитивне значення експоненти вказує на хаотичну поведінку потоку, нульове – на незмінність поведінки, а негативний – на наявність нехаотичної поведінки.

У якості потоку даних системи будемо використовувати значення вхідного трафіку, а саме кількість отриманих пакетів за одиницю часу. Увесь трафік буде розділений на дві вибірки: старий та новий трафік. Після розподілу трафіку, здійснимо прогноз нових значень, базуючись на вибірці старого трафіку. Обчислюючи помилки Δx_k для кожного з передбачень за формулою (1), будемо визначати поведінку їх зміни за допомогою експоненти Ляпунова $\Delta x_0 = x_k - x_k^n$, де x_k^n – передбачене значення x_k.

Якщо значення експоненти буде додатнім, тобто зміна помилки відбувається хаотично. Трафік є нестабільним, що є властиво для корпоративної комп'ютерної мережі, процеси в якій протікають нелінійно. При нульовому значенні експоненти, зміна помилки передбачення, а отже й зміна трафіку відсутня. Якщо експонента набуває від'ємних значення, зміна помилки передбачення не є хаотичною. Трафік стабілізувався, можна зробити висновок, що така зміна може бути викликана DDoS-подібною атакою.

Для опрацювання результатів роботи алгоритму було оброблено два типи трафіку: звичайний трафік та SYN і UDP flood (див. рис. 1.2-1.5).

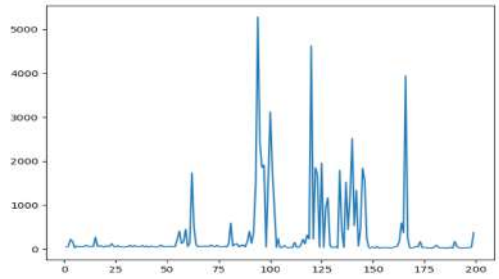

Рисунок 1.2 – Звичайний трафік

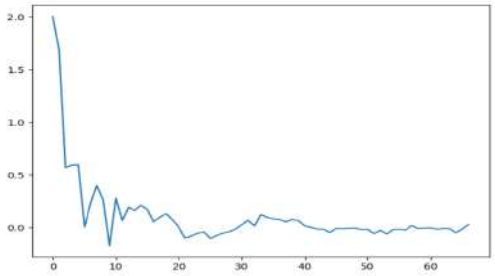

Рисунок 1.3 – Значення експоненти Ляпунова для нормального трафіку

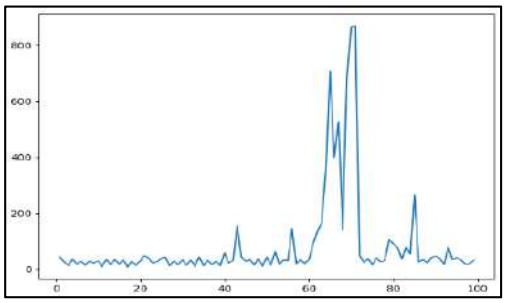

Рисунок 1.4 – SYN та UDP flood

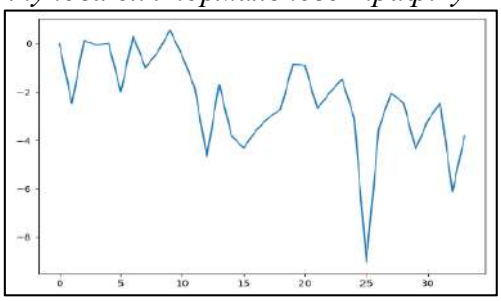

Рисунок 1.5 – Значення експоненти Ляпунова для SYN та UDP flood

Отже, даний метод дозволяє виявити атаки на ранньому етапі, що впливають на рівень мережевого трафіку, викликаючи різкий хаотичний зріст його показників. До таких атак можна віднести DDoS атаки, flooding та brute force атаки. Недоліком даного методу є неможливість його застосування для дальніх горизонтів прогнозування, оскільки відповідно до Теорії Хаосу, динаміка системи значною мірою залежить від початкових умов, що робить довгострокове прогнозування неможливим [3].

В результаті роботи було створено інформаційну систему, метою якої є виявлення та прогнозування рівня загроз для комп'ютерної мережі. Створена система є масштабованою та може бути вдосконалена шляхом накопичення великих об'ємів даних про реальний трафік та застосування нейромережевих методів для виявлення та прогнозування атак та рівня загроз.

Список використаних джерел

1. FauxAPI - v1.3 [Електронний ресурс] – Режим доступу до ресурсу: https://github.com/ndejong/pfsense_fauxapi.
2. What infrastructure and application monitoring can solve for you [Електронний ресурс] – Режим доступу до ресурсу: https://www.influxdata.com/customers/infrastructure-and-application-monitoring/.
3. Мартінзон О.С., Грабар О.І. Теорія хаосу. [Електронний ресурс] – Режим доступу: https://conf.ztu.edu.ua/wp-content/uploads/2017/06/139-2.pdf (дата звернення 13.03.2020 р.). – Назва з екрана.

УДК 681.14

МОДЕЛЮВАННЯ МУЛЬТИАГЕНТНОЇ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

Тарасов О.Є. студ. гр. ПІ-161
Науковий керівник: **Трунова О.В.**, к.пед.н., доцент
Національний університет «Чернігівська політехніка»

Стрімке зростання обчислювальних можливостей комп'ютерів водночас з їх здешевленням призвів до масового впровадження різноманітних програмних систем (ПС) у всіх сферах людської діяльності. Не є виключенням і корпоративні мережі (КМ) – структури, головним призначенням яких є забезпечення ефективності, ергономічності та захищеності роботи і внутрішніх процесів певного підприємства або організації. Якість КМ безпосередньо впливає на ефективність роботи підприємств та організацій, а одним із показників якості КМ є їх захищеність [4]. На сьогодні захист КМ і даних, що в них зберігаються – одна з найбільш критичних задач, з якою стикаються спеціалісти в області інформаційної безпеки, тому дослідження методів для вирішення задач контролю безпеки (КБ) є досить перспективним напрямком.

Метою роботи є дослідження можливості використання мультиагентних систем для вирішення задач контролю безпеки корпоративної мережі та моделювання такої системи.

На сьогодні однією з найбільш перспективних галузей для проведення досліджень є галузь штучного інтелекту (ШІ). Вже існують декілька прикладів успішного використання методів ШІ для вирішення задач КБ. Серед них можна виділити мультиагентні системи (МАС) [3].

Такий підхід має велику кількість переваг: компоненти типової КМ розподілені по декількох вузлах, тому агенти МАС будуть теж функціонувати на різних вузлах, що забезпечить економію обчислювальних ресурсів; використання МАС дозволить легко адаптуватися до змін в мережевій архітектурі; за рахунок створення нових агентів забезпечується гнучкість рішення та висока масштабованість; у зв'язку з розподіленою роботою агентів підвищується відмовостійкість системи: її важче атакувати та вивести з ладу, ніж системи з єдиним сервером захисту; не дивлячись на роздільність окремих агентів, управління всією системою корпоративної безпеки (СКБ) може проводитись централізовано.

СКБ, що побудована по принципу МАС, має у своєму складі декілька класів агентів. Класи агентів та їх цілі представлені в таблиці 1.