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.

Таблиця 1 - Класи та цілі агентів мультиагентної системи

Агент	Ціль
Агент аналізу (АА)	Провести аналіз середовища, виявити вразливості та повідомити про них агента налаштування. Дочекатись усунення проблеми.
Агент налаштування (АН)	Усунути вразливість та підтвердити її відсутність.
Агент захисту (АЗ)	Забезпечити обчислення коефіцієнтів відхилень (КВ) окремих компонентів КМ та всього середовища в цілому. Виявити підозрілі дії.
Агент протидії (АП)	Усунути процес здійснення несанкціонованих дій, їх джерело та наслідки.
Агент навчання (АН)	Зібрати, обробити та поширити данні про вразливості для навчання інших агентів.

Загальний вигляд модельованої МАС та зв’язки між агентами представлені на рисунку 1.

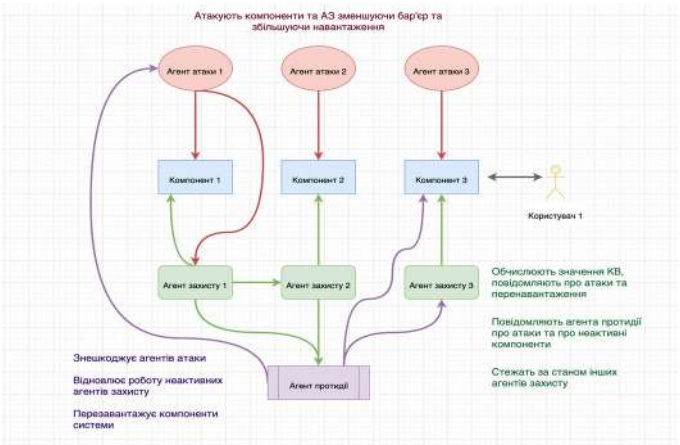

Рисунок 1 – Загальний вигляд МАС

Для моделювання МАС були використані спрощені варіанти агентів та компонентів КМ. В аналізі залучені агенти захисту, агенти протидії, а також агенти, що моделюють поведінку звичайного користувача, зловмисника і компонента – агент-користувач, агент-зловмисник і агент-компонент відповідно [1].

Найбільш цікавим для детального розгляду є агент захисту (АЗ), оскільки ціллю його роботи є виявлення загроз у реальному часі (див. рис. 2). Робота даного агента базується на визначенні коефіцієнта відхилення (*КВ*) відповідного компонента КМ [1].

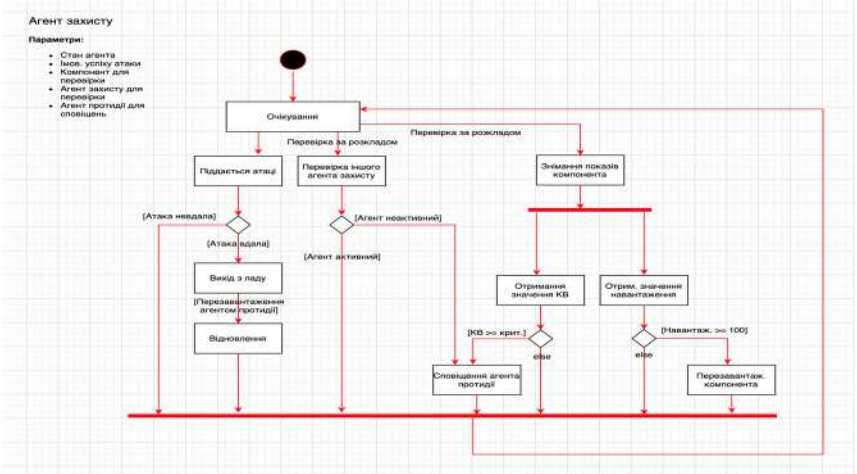

Рисунок 2 – Діаграма станів агента захисту

Алгоритм обчислення КВ залежить від специфіки роботи конкретного компонента КМ. Для модельованої системи обчислення *КВ* відбувається на основі навантаження на компоненти КМ.

Підхід обчислення КВ полягає в аналізі величини кута між двома прямими. Для цього АЗ знімає *N*-показань навантаження. Обчислення кута відбувається для кожного *N*-знімання. Зняті показання утворюють 3 точки: $(x_1, y_1), (x_2, y_2), (x_3, y_3)$, де x_1 – час першого знімання, y_1 – його значення, x_2 – середній час *N*-знімань, y_2 – середнє значення *N*-знімань, x_3 – час останнього знімання, y_3 – відповідне значення. Для отриманих трьох точок будуються дві прямі, кожна з яких описується рівнянням (за точкою та кутовим коефіцієнтом). Перша пряма проходить через першу та другу точки, друга – через другу та третю. За кутовим коефіцієнтам обчислюється тангенс кута між прямими, а через нього і сам кут:

$$KB = arctan(\frac{k_2 - k_1}{1 + k_1 \times k_2}), \qquad \text{де } k_1 = \frac{y_2 - y_1}{x_2 - x_1}, k2 = \frac{y_3 - y_2}{x_3 - x_2}.$$

Адаптивність даного підходу полягає в роботі на підставі *N*-останніх знімань значень.

При перевищенні *КВ* певного порогу агент захисту повідомляє агента протидії про виявлену підозрілу активність. Окрім цього, незалежно від значення КВ, агент захисту повідомляє агента протидії про критичне значення навантаження на компонент (дорівнює 100).

Додатково кожен АЗ є «ревізором» іншого АЗ і з деякою періодичністю перевіряє його працездатність. Якщо АЗ знаходиться у непрацездатному стані, про це також повідомляється агент протидії.

Реалізація змодельованої мультиагентної системи захисту корпоративної мережі на одній з високорівневих мов програмування дозволить кількісно оцінити *КВ* та визначити вразливі місця системи, виявити умови, які сприяють агентам-зловмисникам в успішному проведенні атак.

У якості вдосконалення системи можна запропонувати розробку нових агентів захисту з іншими підходами до визначення *КВ*, наприклад, на основі аналізу SQL-запитів до бази даних КМ.

Список використаних джерел

1. Петров С. А. Исследование и разработка методов и средств создания эталонов для оценки защищённости корпоративных программных систем: дис. … канд. техн. наук. Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Национальный исследовательский университет «МЭИ», Москва, 2014.
2. Теория и практика UML. Диаграмма состояний [Електронний ресурс]. – 2009 – Режим доступу: https://it-gost.ru/articles/view_articles/97 (дата звернення: 02.04.20). - Назва з екрана
3. Многоагентная система [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Многоагентная_система (дата звернення: 02.04.20). - Назва з екрана
4. Корпоративная сеть [Електронний ресурс]. – Режим доступу: https://www.stekspb.ru/autsorsing-it-infrastruktury/it-glossary/corporate-network/ (дата звернення: 02.04.20). - Назва з екрана