Дзьордзь Андрій Ярославович,
магістр спеціальності 125 "Кібербезпека"
Західноукраїнський національний університет

Науковий керівник:
Комар Мирослав Петрович
доктор технічних наук, доцент,
завідувач кафедри інформаційно-обчислювальних систем і управління,
Західноукраїнський національний університет

Підвищення ефективності системи виявлення вторгнень за рахунок апаратної реалізації її компонентів

Аналіз відомих випадків кіберзлочинності, яка, як і раніше наносить компаніям величезні фінансові збитки показав, що зростають як самі витрати компаній, так і час на усунення наслідків комп'ютерних атак. Протягом останніх років кожна друга організація піддалася нападу.

Аналіз відомих підходів до створення систем забезпечення інформаційної безпеки з метою виявлення та класифікації комп'ютерних атак, показав перспективність використання методів штучного інтелекту. Проте, у більшості випадків вони характеризуються прямолінійним підходом і використанням обмеженого набору методів, зокрема, використовується один тип нейронних мереж без їх спеціалізації. При цьому не застосовуються методи зменшення обчислювальної складності, забезпечення надійності самої системи інформаційної безпеки.

Для побудови системи інформаційної безпеки вибрано підхід, що базується інтеграції нейронних мереж та штучних імунних систем. Механізм еволюції нейромережевих імунних детекторів дозволить підвищити достовірність виявлення комп'ютерних атак.

Для підвищення надійності системи інформаційної безпеки запропоновано реалізацію детекторів атак здійснювати на програмованих логічних інтегральних схемах та ввести підсистему прийняття рішень на основі правил нечіткого висновку Мамдані [1].

Узагальнена схема підвищення ефективності системи захисту від комп'ютерних атак показана на рис. 1.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ross T.J. Fuzzy Logic with Engineering Applications. T.J.Ross. McGraw-Hill Inc.(USA), 1995. 600 p.

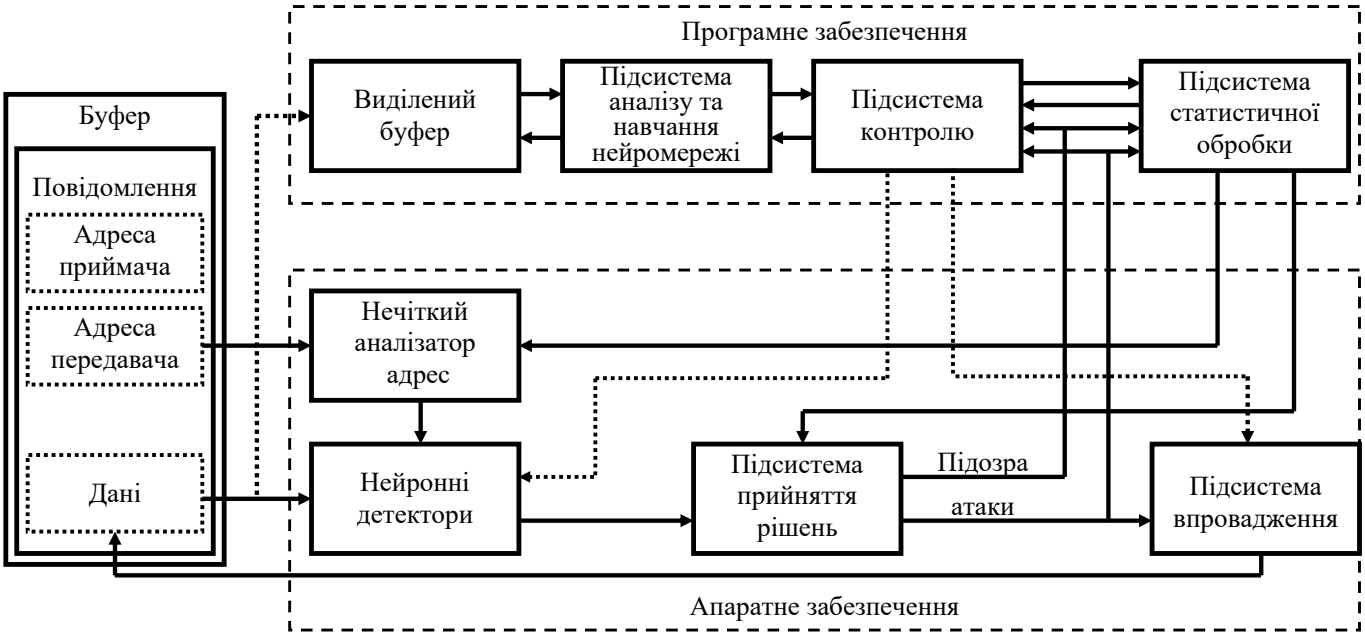

Рис. 1. Узагальнена схема підвищення ефективності системи захисту від комп'ютерних атак

Ця схема складається з двох частин. Перша реалізується апаратно й працює постійно в режимі реального часу. Вона складається з нечітких адресних аналізаторів, набору нейронних детекторів та підсистеми прийняття і реалізації рішень. Друга – реалізована програмним забезпеченням і представлена виділеним комп'ютером, який використовується для аналізу поточних атак та створення відповідних засобів захисту. У цій частині, відповідно до раніше визначених функцій, можна визначити підсистеми для аналізу та навчання нейронних мереж, здійснення керування та статистичної обробки даних кібернападу. Ця частина також включає виділений буфер, де для його детального аналізу записано підозрілий код. Крім того, резидентне програмне забезпечення другої частини відстежує буферні коди, щоб розглядати їх лише як дані. Будь-які інструкції, які входять до коду, містяться в спеціальному буфері, і не можуть бути виконані.

Застосування апарату нечіткої логіки при створенні апаратно-програмного засобу для здійснення виявлення атак для кожного окремого клієнта та врахування поточних параметрів самої системи дозволить забезпечити стійкість криптосистеми до кібератак в режимі реального часу.