УДК 004.89
Кінашович Д.–ст. гр. КСМм-51
Тернопільський національний економічний університет

ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК НА ОСНОВІ НЕЙРОМЕРЕЖЕВИХ ТЕХНОЛОГІЙ

Науковий керівник: викладач Комар М.П.

В даний час відбувається безперервне зростання кількості атак і зловживань у сфері високих технологій. Тому забезпеченню безпеки комп'ютерних систем приділяється все більше і більше уваги. Традиційні методи виявлення атак, такі, як сигнатурний метод або метод виявлення аномалій [1], не дозволяють досягти оптимальних характеристик виявлення атак.

Сьогодні застосовуються різноманітні методи і засоби для захисту від мережевих атак, проте всі вони мають ряд істотних недоліків, і не здатні повною мірою захистити користувача від вторгнень [2]. У зв'язку з цим, для надійного захисту комп'ютерних систем від мережевих вторгнень необхідно розробляти нові методи захисту.

Одним з перспективних напрямів забезпечення безпеки комп'ютерних систем є використання методів штучного інтелекту (ШІ), таких як нейронні мережі, штучні імунні системи, еволюційне програмування і т.д., які вже довели свою ефективність у вирішенні складних задач розпізнавання, класифікації, управління і виявлення. На їх основі вже існують прототипи систем захисту комп'ютерної інформації. Застосування методів ШІ дозволить створити ефективну адаптивну самонавчальну систему виявлення мережевих вторгнень і підвищити рівень захисту комп'ютерних систем від атак хакерів.

Для виявлення мережевих вторгнень необхідно аналізувати вхідний і вихідний мережеві трафіки. Мережевий трафік в задачах виявлення розділяють на два класи: нормальний і аномальний. Нормальний трафік характеризує нормальне, безпечне з'єднання. Аномальний трафік характеризує мережеву атаку. Ми вважаємо, що кожний тип атаки характеризується певним набором характеристик параметрів з'єднання, виділяючи наявність якого можна не тільки виявляти факт, спробу мережевого вторгнення, але і визначити до якого типу це вторгнення відноситься.

Для вирішення завдання виявлення мережевих вторгнень пропонується використовувати штучні нейронні мережі. Вся задача розбивається на ряд підзадач: аналіз мережевого трафіку з метою виявлення набору характеристик для кожного типу атаки; кластеризація даних про з'єднання, що дозволить виявити кореляцію між типами атак і виділити характерні ознаки для кожного типу атаки; розробка структури нейромережевого детектора для аналізу трафіку, виявлення і класифікація мережевого вторгнення; розробка алгоритмів навчання і функціонування нейромережевого детектора для виявлення атак хакерів.

Передбачається, що розробка системи виявлення комп'ютерних атак, заснованої на застосуванні методів нейронних мереж, дозволить істотно підвищити ймовірність виявлення невідомих мережевих вторгнень.

Література

1. Методы обнаружения нарушителя / http://www.ssl.stu.neva.ru/sam.

2. Комар М.П. Использование искусственных иммунных систем и нейронных сетей для обнаружения компьютерных атак / Сборник VI Республиканской научной конференции молодых ученых и студентов "Современные проблемы математики и вычислительной техники", Брест, 26-28 ноября 2009, часть 1, ст. 16-18.