УДК 004.89

ВИЯВЛЕННЯ АНОМАЛІЙ НА ОСНОВІ ШТУЧНИХ ІМУННИХ СИСТЕМ

Комар М.П.[1)], Тімовський М.В.[2)], Глинський І.І.[3)]
Тернопільський національний економічний університет
[1)] к.т.н.; [2,3)] магістранти

Застосування штучних імунних систем (ШІС) на сьогоднішній день включає наступні області: системи комп'ютерної безпеки, виявлення аномалій і несправностей, багатоагентні системи, моделі самоорганізації, моделі колективного інтелекту та ін.

Останнім часом відбулося злиття комп'ютерних мереж, інформаційних і телекомунікаційних технологій, що дозволило утворити сучасні інформаційні телекомунікаційні мережі (ІТМ), які є складною розподіленою системою, що характеризується наявністю множини взаємодіючих ресурсів, системних та прикладних інформаційних і телекомунікаційних процесів. У таких умовах важливою науково-технічною задачею є забезпечення цілісності, достовірності та конфіденційності інформації. ІТМ піддаються різного роду загрозам, і користувач не може бути впевнений у захищеності важливої інформації, оскільки кіберзлочинці продовжують удосконалювати і розробляти методи і засоби організації мережевих атак. Основним недоліком більшості сучасних комерційних систем виявлення атак (СВА) є неможливість виявлення невідомих атак, оскільки вони використовують на базовому рівні сигнатурний і статистичний методи. В рамках академічних розробок створені десятки СВА, які базуються на евристичних методах. Проте, в комерційних системах вони майже не використовуються, оскільки мають ряд обмежень, пов'язаних з вимогами верифікованості, стійкості, складності обчислювальних алгоритмів і високою ймовірністю помилкових спрацювань. Ситуація, що склалася, стимулює пошук і розробку нових підходів, спрямованих на підвищення достовірності виявлення невідомих атак на ІТМ.

Розглянемо інтеграцію методів ШІС і штучних нейронних мереж (ШНМ) для виявлення аномалій мережевого трафіку. В якості імунного детектора використовується нейронна мережа [0]. Побудова системи здійснюється на основі базових принципів і механізмів біологічної імунної системи, а також на типовій схемі ШІС [2]. Імунні детектори генеруються по випадковому алгоритму, що дає можливість створення великої кількості різноманітних за своєю структурою детекторів. Потім, детектори проходять стадію навчання, де вони набувають здатності коректно реагувати на чужорідні об'єкти або явища. Для того, щоб детектори не генерували помилкові спрацьовування, вони ретельно відбираються. Ті з них, які не навчилися коректно класифікувати об'єкти – знищуються. Відібрані детектори допускаються до виконання функцій по виявленню аномалій. Кожному детектору надається час життя, впродовж якого він може існувати. Якщо впродовж цього часу детектор не виявляє аномалій, то він знищується, а на його місце створюється новий детектор. Якщо детектор виявив аномалію, то відбувається інформування про виявлену аномалію і її знищення. Детектор, що виявив аномалію, трансформується в детектор імунної пам'яті [1].

Розглянемо використання ШІС в технічній діагностиці. Система діагностування повинна забезпечувати мінімальну кількість помилкових спрацьовувань. Тут доцільним є комплексний підхід до діагностування, де для вирішення кожної з задач використовується окремий метод. Наприклад, при рішенні задачі виявлення порушень в роботі технічної системи набагато важливіше в першу чергу визначити чи має місце порушення взагалі, а вже потім шукати його причини і тип. В цьому випадку найбільш підходить метод негативного відбору [3], оскільки задача визначення «свій-чужий» може бути легко трансформована в задачу виявлення аномалії.

Отже, ШІС моделює основні процеси біологічної імунної системи, а також їх взаємодію. Відмінність полягає в способі представлення інформації і структурі імунного детектора. Запропоновані підходи дозволяють виявляти аномалії в параметрах мережевого трафіку та в роботі технічних систем.

Список використаних джерел

1. Комар М.П. Методы искусственных иммунных систем и нейронных сетей для обнаружения компьютерных атак / М.П. Комар // Інформаційна безпека. – 2011. – №1(5). – С. 154–160.
2. Hofmeyr S. Immunity by design: An artificial immune system / S. Hofmeyr, S. Forrest // Gecco. – 1999. – Vol. 2. – P. 1289–1296.
3. Dasgupta D. An anomaly detection algorithm inspired by the immune system / Dasgupta D., Forrest S. // Artificial Immune System and Their Applications, Springer-Verlag, 1999. – P. 262–277.