УДК 004.056

ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ МОЖАЄВ

доктор технічних наук, професор,
професор кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ

ЮРІЙ ПЕТРОВИЧ ГОРЕЛОВ,

кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ІМУННИХ АЛГОРИТМІВ У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

У зв'язку з безпрецедентно швидким розвитком комп'ютерних і телекомунікаційних технологій та переходом до інформаційного суспільства проблема забезпечення кібербезпеки і побудови інформаційно-безпечних розподілених обчислювальних систем стала однією з найбільш актуальних.

Традиційні методи виявлення вторгнень, що застосовуються сьогодні, не здатні забезпечити надійний захист комп'ютерних систем від проникнення комп'ютерних вірусів, несанкціонованого доступу, вторгнень і ін. Методи штучного інтелекту дозволяють створити принципово нові алгоритми виявлення шкідливих програм та значно підвищити рівень захищеності комп'ютерних систем шляхом реалізації систем виявлення вторгнень (СВВ), які розглядаються як один з базових елементів системи захисту інформаційної системи.

Під СВВ розуміються програмні та програмно-апаратні технічні засоби, що реалізують функції автоматизованого виявлення в інформаційних системах дій, спрямованих на навмисний несанкціонований доступ до інформації, а також спеціальних впливів на інформацію з метою її добування, знищення, перекручення або блокування. Виділяються два типи СВВ: системи виявлення

вторгнень рівня мережі (Network Intrusion Detection System, NIDS) і системи виявлення вторгнень рівня вузла (Host-based Intrusion Detection System, HIDS).

Основне завдання СВВ - аналіз зібраних даних з метою виявлення вторгнень. Для її вирішення використовуються одночасно сигнатурні і евристичні методи. Спосіб пізнання сигнатури полягає в описі атаки у вигляді сигнатури і пошуку даної сигнатури в контрольованому просторі (мережевий трафік, журналі реєстрації і т.д.). Як сигнатура атаки може виступати шаблон дій або рядок символів, що характеризують аномальну активність в інформаційній системі. Незважаючи на ефективність сигнатурного методу, існує проблема створення такої сигнатури, яка б описувала всі можливі модифікації атаки. Для вирішення цієї проблеми застосовуються евристичні методи. Дані методи допомагають виявляти відхилення від нормального функціонування автоматизованої системи, використовуючи еталонну модель функціонування. Спочатку визначається типові значення для таких параметрів, як завантаженість ЦПУ, активність роботи диска, частота входу користувачів в систему і інші. Потім при виникненні значних відхилень від цих значень система сигналізує про загрозливу ситуацію.

Перспективними для розробки алгоритмічного забезпечення систем захисту інформації, що мають вищезгадані властивості, є методи, засновані на принципах роботи нейронної мережі, імітаційного моделювання та імунної системи. Використання останнього методу в СВВ є одним з найбільш перспективних, оскільки сам принцип роботи імунної системи і властивості, якими вона характеризується, максимально орієнтовані на вирішення завдання виявлення інцидентів інформаційної безпеки. Штучна імунна система (ШІС) будується, як правило, тільки на двох центральних поняттях: антиген - антитіло. Як антигени виступають системні виклики або мережеві пакети. При первинній зустрічі імунної системи з антигеном він вивчається, і на підставі складеного шаблону виробляються антитіла, які знищують, блокують або пропускають антиген.

Одним з можливих варіантів створення системи, заснованої на принципах роботи імунної системи людини, є реалізація алгоритму негативного відбору. Для пояснення того, як імунна система "бореться" проти чужорідних антигенів, використовується теорія клональної селекції. Коли антиген проникає в живий організм, він починає розмножуватися і вражати своїми токсинами клітини організму. Ті клітини, які здатні розпізнавати чужорідний антиген, розмножуються способом, пропорційно ступеня їх розпізнавання: чим краще розпізнавання антигену, тим більша кількість потомства (клонів) буде створене. Протягом процесу репродукції клітини окремі клітини піддаються мутації, яка дозволяє їм мати більш високу відповідність (афінність) до антигену, що розпізнається. Навчання в імунній системі забезпечується збільшенням відносного розміру популяції і афінності тих лімфоцитів, які довели свою цінність при розпізнаванні представленого антигену. Основними імунними механізмами при розробці алгоритму є обробка певної множини антитіл з набору клітин пам'яті, видалення антитіл з низькою афінностю, дозрівання афінності та повторний відбір клонів пропорційно їх афінності до антигенів.

ШІС з клональною селекцією дозволяють виявити навмисні зміни в даних, що контролюються. Таким чином, застосування ШІС як евристичного блоку систем превентивного захисту інформації дозволяє ефективно вирішувати завдання виявлення аномалій в діях користувачів систем та мережевого трафіку.

У доповіді розглядаються деякі особливості реалізації алгоритму клональної селекції з використанням процедури мутації, побудови детекторів та антигенів, а також розрахунку афінності антитіл.