трафіку не завжди свідчить про наявність атаки. Однак, наявність даних про рівень аномальності дозволяє прийняти завчасні попереджувальні заходи та дозволяє удосконалити процес виявлення невідомих або сильно видозмінених (модифікованих) атак. Тому, в процесі функціонування ІТМ критичної інфраструктури, пропонується побудувати систему виявлення атак з дворівневою архітектурою, а саме: на першому рівні визначати рівень аномальності трафіку ІТМ, а на другому здійснювати класифікацію атаки з використанням даних про рівень аномальності трафіку.

Задача класифікації модифікованої атаки може бути вирішена з використанням методів штучного інтелекту. Використання сигнатурних методів аналізу в даному випадку вважається малоефективним. Так, в умовах неповної (неточної) інформації про можливу атаку обґрунтованим є використання нечітких систем логічного виводу. Для налаштування та адаптації параметрів таких систем застосовуються підходи, які можуть бути основані на використанні інтелектуальних систем, з використанням математичного апарату нейронних мереж, генетичних алгоритмів, тощо. Використання нейронних мереж дозволяє обрати початкові параметри для налаштування нечітких систем логічного виводу, а також адаптувати їх в процесі функціонування ІТМ. В якості однієї з вхідних величин нейро-нечіткої системи для класифікації атак пропонується використати величину, що отримана на першому етапі аналізу трафіку - $K \in [0,1]$ та характеризує рівень аномальності трафіку. Вихідна величина функціонально визначається залежністю:

$$C_a = f(K, N_1, ..., N_A), \left(a = \overline{1, A}\right) \quad (1)$$

В якості інших вхідних параметрів обрано параметри трафіку з відповідною ознакою a $\left(a = \overline{1, A}\right)$.

УДК004.77

О.С. Трикоз , студент гр.501-ТК
Г.В. Головко, к.т.н., доцент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ ТА БЕЗПЕКА В ІНФОРМАЦІЙНИХ СИСТЕМАХ

«Комп'ютер, як засіб вирішення проблем, сам опинився однією великою проблемою»

На даний час, в Україні, у зв'язку зі входженням у світовий інформаційний простір, швидкими темпами впроваджуються новітні досягнення комп'ютерних і телекомунікаційних технологій. Створюються локальні і регіональні обчислювальні мережі, великі території охоплені

мережами сотового зв'язку, факсиміальний зв'язок став доступний для широкого кола користувачів. Системи телекомунікацій активно впроваджуються у фінансові, промислові, і соціальні сфери. У зв'язку з цим різко зріс інтерес широкого кола користувачів до проблем захисту інформації. Захист інформації - це сукупність організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації. Нормативно-правове забезпечення організації і проведення заходів щодо захисту інформації являє собою сукупність законів, нормативних актів і правил, що регламентують як загальну організацію робіт, так і створення, функціонування конкретних систем захисту інформації. Стає актуальною розробка основи системи забезпечення безпеки інформації - базового закону, що регламентує відношення і розмежування сфери повноважень всіх учасників інформаційних відношень, а також визначальні державні органи, що забезпечують інформаційну безпеку і засоби контролю з боку держави за розмежуванням доступу до інформації

Від початку створення і до цього часу, а це налічує майже 54 роки, мережа інтернет зазнала величезних змін, вона постійно модернізується, покращуються принципи роботи та алгоритми побудови самої системи. Безумовно все це тільки буде розвиватися і в майбутньому. Вже на сьогодні інформаційна система об’єднує в собі мільярди пристроїв за допомогою величезної кількості маршрутизаторів та канальних з’єднань. Особливістю цієї «екосистеми» вважається не її ідеальність, а її здатність легко адаптуватися до проблем, відмовами у системі, помилкам при передачі, втратам даних та багатьох інших непередбачуваних проблем. Втрата, перехоплення та змінення даних, що передаються мережею – глобальна проблема сучасності, яка потребує постійного контролю та вдосконалення методів запобігання цьому явищу.

Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи задач: захист інформації від несанкціонованого доступу (НСД) та захист інформації від витоку технічними каналами. Під НСД звичайно розуміється доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали побічних електромагнітних випромінювань та наводок, акустичні канали, оптичні канали та ін.

Найбільш ефективним захистом від НСД є шифрування та дешифрування даних криптографічним методом, що передаються транспортним каналом. Принцип даного захисту полягає в зашифровуванні даних на початковому пристрою, передача їх по фізичному каналу, та розшифровування на кінцевому пристрою. При такому підході зловмисники, в деякій мірі, можуть перехопити дані, але

змінити їх – ні. Існують симетричні та асиметричні методи шифрування. Принцип обох відрізняється в підході створення ключа безпеки, його передачі та алгоритмом розшифрування.

Оскільки в захисті інформаційної системи зацікавлений не лише виробник систем передачі (маршрутизатори та супутнє обладнання, захищені платформи управління), який у свою чергу створює, адаптує, модернізує існуючі алгоритми захисту у своє обладнання; не лише структура, що організовує цю інфосистему, яка звісно ж на своєму рівні забезпечує захист даних, починаючи з не значних DDOS-атак і закінчуючи розгалуженою системою побудови та аналізу поведінки мережі, створенням ізольованих мереж (VPN тунелі), контролю та відсіювання злоякісного трафіку, що може спричинити НСД до конфіденційної інформації; а звісно ж, основним об'єктом – є людина, яка і створює увесь цей загальний об'єм інформації!

Тому в першу чергу, безпека в інформаційній системі залежить тільки від нас самих, адже кожна дія в мережі, кожне переглядання, скачування, розповсюджування інформації не відбувається безслідно і робити це з розумом та розумінням про те, що нехтування забезпеченням власної безпеки хоча б на рівні антивірусного забезпечення, може спричинити до не приємних наслідків. Так, деякою мірою втраті даних можна завдячити корпораціям, які на своєму рівні забезпечують алгоритми захисту в мережах, які працюють хоча б з якою інформацією, яка потребує шифрування, але в той же час, вдосконалюються і алгоритми обходу систем захисту, і ця боротьба буде відбуватися постійно.

УДК 004.023

D.V. Ievliev, master's degree, 501TN
O. V. Skakalina, Ph.D., associate professor
National University " Yury Kondratyuk Poltava Polytechnic"

APPLIED ASPECT OF SOLVING THE BACKPACK PROBLEM USING A POPULATION-GENETIC ALGORITHM

Approximate algorithms for solving combinatorial optimization problems turn out to be indispensable in situations where obtaining an exact solution requires excessive time costs. Evolutionary algorithms (EA) originate in the works of L. Fogel, A. Owens and M. Walsh, J. Holland, where it was proposed to model the process of biological evolution in order to synthesize structures that are effective in a sense and create artificial intelligence (AI) systems.

A.G. Ivakhnenko and L.A. Rastrigin independently proposed methods of random search, where the ideas of evolution were also used. A characteristic feature of EA is the imitation of the process of evolutionary adaptation of a