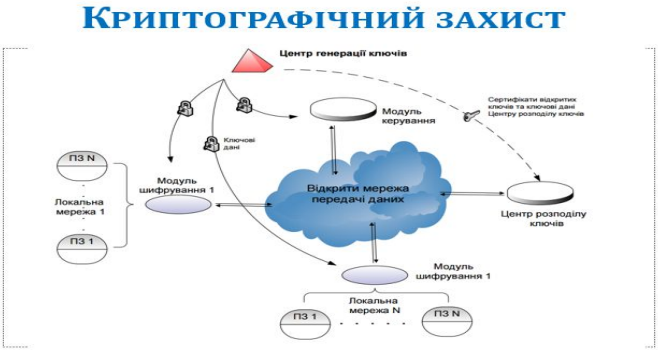
дешифрування, і його знання не дає можливості визначити секретний ключ. Єдиним недоліком моделі є необхідність адміністративної роботи – ключі (і відкриті, і закриті) треба десь зберігати і час від часу оновлювати. Сьогодні існує достатня кількість криптографічних алгоритмів. Найбільш поширеними з них є стандарт шифрування даних DES (Data Encryption Standart) та алгоритм RSA, названий за першими літерами прізвищ розробників (Rivest, Shamir, Adleman), розроблені у 1970-х роках. Обидва алгоритми є державними стандартами США. DES є симетричним алгоритмом, а RSA – асиметричним. Ступінь захищеності під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується.



Отже, розвиток криптосистем і підвищення надійності цифрових підписів створює необхідні передумови для заміни паперового документообігу електронним і переходу до здійснення електронних операцій. [1]

Література

1. https://sites.google.com/site/zahistlokalnoiemerezi/zahist/kriptograficnij-zahist.

УДК 621.391

Ю.М. Здоренко, к.т.н.,
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»,
М.С. Здоренко

СИСТЕМА ВИЯВЛЕННЯ МОДИФІКОВАНИХ АТАК В ІНФОРМАЦІЙНО- ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Пріоритетним напрямком кібернетичного захисту сучасних інформаційно-телекомунікаційних мереж (ІТМ) критичної інфраструктури є використання систем виявлення атак. Аналіз даних про характеристики трафіку такими системами дозволяє здійснювати класифікацію можливої атаки та здійснити заходи щодо її попередження. Поява невідомих або модифікованих атак обмежує та робить неефективним використання систем виявлення на основі сигнатурних методів. Аномальний характер

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