НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ

ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «КІБЕРБЕЗПЕКА ЕНЕРГЕТИКИ»

Матеріали

31 травня 2023 року

Київ – 2023

УДК [621.3+620.9]::[004[056.53+42+94] + 504.06]
ББК 31
Б-39

Рекомендовано до друку Вченою радою Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України (протокол № 04 від 25 травня 2023 р.)

Б-39 **Кібербезпека енергетики,** науково-практична конференція Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України : матеріали, 31 травня 2023 р. Київ : ІПМЕ ім. Г.Є.Пухова НАН України, 2023. 117 с.

В-39 **Cybersecurity of energy**, scientific-practical conference of the G.E. Pukhov Institute for Modeling in Energy Engineering National Academy of Sciences of Ukraine : materials, May 31, 2023. Kyiv: PIMEE NAS of Ukraine, 2023. 117 p.

Здоренко Юрій Миколайович,
Національний університет «Полтавська політехніка імені Юрія Кондратюка», доцент кафедри компютерних інформаційних технологій та систем, к.т.н.,
zdorenkoviti@gmail.com

Здоренко Марина Сергіївна,
marishkina84@gmail.com

МЕТОД ВИЯВЛЕННЯ 0-DAYАТАК В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТУКТУРИ

Кібернетичний захист інформаційно-комунікаційних мереж (ІКМ) об'єктів критичної інфраструктури, а саме енергетичної галузі є важливою складовою забезпечення безпеки держави. Системи виявлення атак для таких мереж потребують постійного удосконалення. Аналіз потоків даних, що передаються в цих мережах дозволяє здійснювати виявлення можливої атаки та здійснити заходи щодо її попередження на основі наявних відомостей про такі атаки в минулому. Тому поява невідомих або модифікованих атак робить неефективним використання систем виявлення на основі сигнатурних методів. Трафік за номальними характеристиками не завжди свідчить про наявність нової (0-day) атаки. Тому для ІКМ об'єктів критичної інфраструктури, пропонується реалізувати новий метод виявлення атак, який ґрунтується, на використанні даних про рівень аномальності трафіку.

Використання сигнатурних методів аналізу, як було зазначено вважається малоефективним. Тому задачу виявлення нової або модифікованої атаки пропонується вирішувати з використанням підходів на основі штучного інтелекту. В умовах недостатньої (неточної) інформації про можливу атаку обґрунтованим є використання нечітких систем логічного виводу [1].

Для налаштування та адаптації параметрівтаких систем застосовуються підходи, які можуть бути основані на використанні математичного апарату штучних нейронних мереж. Це дозволить обрати початкові параметри для налаштування нечітких систем логічного виводу, а також, у разі потреби, змінювати їх в процесі функціонування ІКМ.

У якості вхідних величин нейро-нечіткої системи для класифікації атак пропонується використати величину, що характеризує рівень аномальності трафіку та дані про кількість вхідних та вихідних пакетів з відповідною ознакою, а саме: IP-адреса відправника та одержувача, порт відправника та одержувача, загальна кількість вхідних (вихідних) пакетів.

Вихідна величина визначається в процесі навчання нейронної мереж із використанням алгоритму оберненого поширення помилки, як функціонально залежна від вхідних величин.

Передбачається, що використання пропонованого методу на основі даних про рівень аномальності значно удосконалить процес виявлення невідомих або модифікованих атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Здоренко Ю. М., Фесьоха В.В. Нейро-нечітка система виявлення вторгнень в інформаційно-телекомунікаційних мережах. *Збірник наукових праць ВІТІ*. 2018. Вип. № 3. С. 83–89.