УДК 004.056.5:004.421.6

ІНТЕЛЕКТУАЛЬНА СИСТЕМА МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОМИСЛОВОГО ІНТЕРНЕТУ РЕЧЕЙ

Воронський А.В.[1)], **Дементьєв Р.В.**[2)], **Шабат Т.З.**[3)], **Ядчишин О.В.**[4)]
Західноукраїнський національний університет
[1)]магістрант; [2)]студент;[3)]аспірант;[4)]аспірант;

І. Постановка проблеми

Сучасний етап розвитку промислового виробництва пов'язані з масовим використанням інформаційних технологій та кіберфізичних систем, масштабної автоматизацією бізнес-процесів, поширенням технологій штучного інтелекту. Ключові позиції в 4-й промисловій революції, що народжується починає займати промисловий Інтернет речей (Industrial Internet of Things, IIoT). Промисловий Інтернет речей є системою об'єднаних комп'ютерних мереж та підключених до них промислових(виробничих) об'єктів із вбудованими датчиками та програмним забезпеченням (ПЗ) для збору та обміну даними, з можливістю віддаленого контролю та управління в автоматизованому режимі, без участі людини [1,2].

ІІ. Мета роботи

Метою дослідження є розробка інтелектуальної системи моніторингу інформаційної безпеки промислового інтернету речей.

ІІІ. Розробка моделей мовного пакету

Вирішення задачі моніторингу інформаційної безпеки систем IIoT ускладнюється наявністю і використанням різних мережевих протоколів та технологій, проте в цілому в процесі моніторингу ІБ вирішуються такі загальні базові завдання, як: перехоплення мережевого трафіку, його аналіз, прийняття рішення про наявність та клас атаки (або її відсутності), протоколювання, оповіщення.

Для вирішення кола завдань, що розглядається, в роботі пропонується багаторівнева схема інтелектуального аналізу даних трафіку, де на нижніх двох рівнях використовується розподілена дворівнева штучна імунна система (ШІС), на верхньому – система класифікації стану мережевого трафіку IIoT. Розглянемо докладніше функціонування пропонованої ШІС. В першу чергу, ця система повинна отримувати вхідні дані про мережний трафік. Для цього вони мають бути перехоплені або отримані від мережевого обладнання,потім необхідно виділити аналізовані параметри (ознаки) та навести їх до певного виду (нормалізація) [3].

ШІС має у своєму розпорядженні безліч агентів нижнього рівня, розподілених попід мережах, що містять детектори (штучні лімфоцити),що функціонують за принципом «свій/чужий», що виявляють атаки, у тому числі невідомі та класифікуючі відомі.

Дворівнева ШІС також містить агенти верхнього (другого) рівня, які реалізують обчислення на основі принципів теорії небезпеки у вигляді алгоритмів дендритних клітин (ДК), що агрегують дані про атаки від підконтрольних агентів нижнього рівня, що аналізують рівень небезпеки. UML-діаграма класів дворівневої системи представлена на рисунку 1.

Таким чином, розглянута дворівнева ШІС, згідно з рисунком 1 містить два види агентів: першого та другого рівнів,які використовують методи класів «лімфоцит» та «дендритна клітина»відповідно. Агенти першого рівня, використовуючи метод аналізу класу«лімфоцит», готують дані для агентів другого рівня, який реалізує метод аналізу класу дендритних клітин.

Штучна імунна система (ШІС) імітує роботу природної імунної системи людини, призначеної для її захисту від зовнішніх та внутрішніх, відомих та невідомих загроз. При найбільш класичному варіанті побудови ШІС реалізується класифікація за принципом"свій чужий". У такому випадку будується безліч детекторів, кожен з яких містить деякий вектор-рядок, що є реальним або передбачуваним зразком атаки.

Такий рядок може складатися безпосередньо з мережних параметрів з'єднань, що відповідають атакам або аномаліям, або генеруватися випадковим чином, але при забезпеченні її унікальності та гарантії її суттєвої відмінності від даних, що відповідають нормальному мережевому відношенню.

ШІС аналізує дані у форматі деякої послідовності значень. Це може бути послідовність певних подій або набір параметрів, що характеризують одну подію, але у будь-якому випадку дані повинні бути представлені у вигляді вектора-рядка, який також визначається точкою в простір параметрів. Аналіз полягає у визначенні схожості векторів аналізованих даних та еталонних векторів детекторів

«чужого». Якщо вектори досить близькі, вважається, що аналізований екземпляр даних відповідає деякій аномалії.

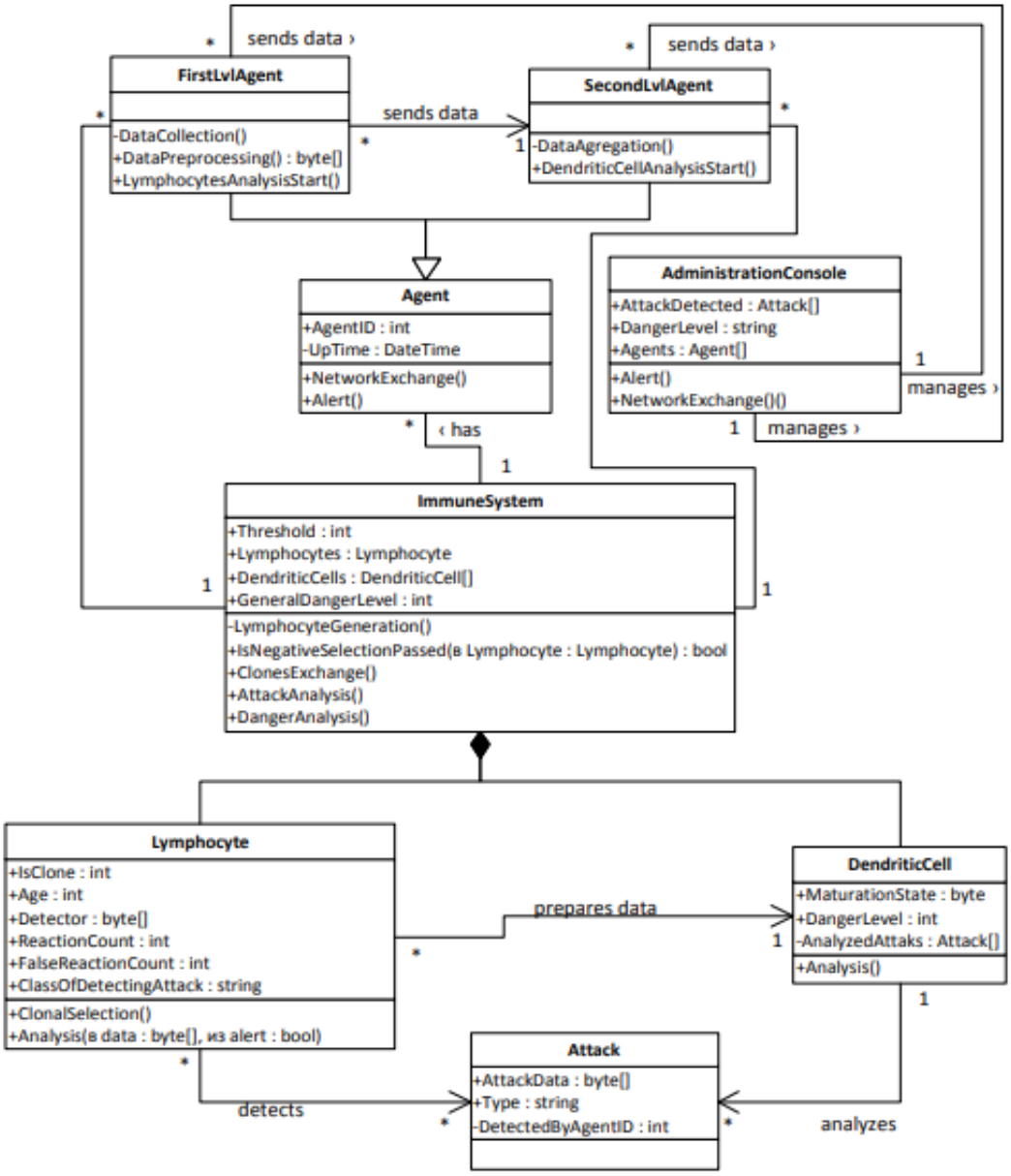

Рисунок 1–Діаграма класів ШІС

При побудові ШІС, що функціонує за принципом «небезпечно/безпечно»детектори імітують роботу так званих дендритних клітин,аналізують наявність або відсутність сигналів небезпеки, безпеки та сигналів про наявність патогенів (PAMP – Pathogen Associated Molecular Pattern).Результатом аналізу є висновок про небезпеку чи безпеку виявленого патогену та активації процесів його нейтралізації або вироблення до нього толерантності відповідно.

Висновок

Для вирішення задачі моніторингу інформаційної безпеки мереж промислового Інтернету речей запропоновано застосування багаторівневого інтелектуального аналізу даних мережевого трафіку, де на нижніх двох рівнях працює розподілена дворівнева штучна імунна система, на верхньому – система класифікації подій.

Список використаних джерел

1. Andrews, Paul S., Drennan, Judy A. An Introduction to Artificial Immune Systems. Springer, 2003. ISBN: 978-1852336634.
2. Corne, David, Timmis, Jon. Artificial Immune Systems: A New Computational Intelligence Approach. Springer, 2003. ISBN: 978-1852336825.
3. Leandro Nunes, Von Zuben, Fernando J. Immunocomputing: Principles and Applications. CRC Press, 2002. ISBN: 978-1584884172.