УДК 519:004.22
Гринченко П.В.[1], Бакурова А.В.[2], Зарицький О.В.[3], Терещенко Е.В.[4], Широкорад Д.В.[5]
1 асп. НУ «Запорізька політехніка»
2 проф. НУ «Запорізька політехніка»
3 проф. Національний університет ім.Т.Шевченка
4 доц. НУ «Запорізька політехніка»
5 докторант НУ «Запорізька політехніка»

ОЦІНКА НАСЛІДКІВ ВРАЗЛИВОСТЕЙ В МЕРЕЖЕВИХ СИСТЕМАХ

Поширення пристроїв, підключених до Інтернету, революціонізувало спосіб взаємодії людей і організацій із технологіями. Однак цей взаємозв’язок також створює значні ризики для безпеки. Шлюзи, які служать основною точкою доступу для мереж, часто стають цілями зловмисників через їх вразливість. Подібним чином обладнання інтернет-провайдера, включаючи брандмауери та комутатори Ethernet, відіграє вирішальну роль у

безпеці мережі та є чутливим до різноманітних експлойтів. Уразливість ланцюга постачання стала критичною проблемою, оскільки вона може порушити цілісність програмного та апаратного забезпечення на багатьох рівнях.

Основні положення методології побудови системи контролю доступу до мережевих систем були розроблені колективом авторів на основі нечіткої математики і представлені в роботах [1], [2].

Аналізуючи конкретні загальні вразливості та ризики (CVE) в межах сформованої методології [2] в даній роботі висвітлено потенційні ризики для мережевої інфраструктури та безпеки даних. На рис.1 представлена структура параметрів системи нечіткого логічного виведення, що побудована для оцінки важкості наслідків вразливостей в мережевій системі. При побудові системи та визначенні її параметрів використовувався стандарт CVSS [3].

Вхідні параметри системи нечіткого логічного виведення моделюються у вигляді лінгвістичних змінних.

Показник ***OAF (Object Access Frequency)*** визначає частоту доступу до об'єкта (Object access frequency, OAF) системними об'єктами. Його значення розраховується за даними систем реєстрації UAM та UEBA як відношення кількості звернень до об’єкта до загальної кількості звернень до всіх об’єктів системи.

Рівень чутливості інформації ***Information Sensitivity Level (ISL)*** відноситься до класифікації інформації на основі її конфіденційності, що часто визначає рівень захисту та засоби контролю, що необхідні для її захисту. ISL визначає, як має здійснюватися доступ до інформації, ділитися та зберігати на основі потенційного впливу неавторизованого доступу. Терми цієї лінгвістичної змінної та відповідні до них функції приналежності мають наступні позначення: *L, z (0.3 0.4); M, PI (0.2 0.3 0.6 0.9); H, s (0.6 0.7).*

Рівень впливу об'єкта **Level of Object Influence (LOI)** стосується ступеня, до якого об’єкт у системі впливає на інші елементи системи. Це може включати вплив даних, апаратного чи програмного забезпечення на безпеку або робочі можливості системи.

Група метрик ***CIA Impact Metrics (Confidentiality, Integrity, Availability)*** дозволяє оцінити потенційний вплив порушень безпеки на конфіденційність, цілісність і доступність системи. Ці показники допомагають зрозуміти потенційну шкоду, яку може зазнати система в разі порушення, і, відповідно, визначити пріоритетність відповідей.

Ця група метрик містить наступні три параметри.

VI (Vulnerability System Integrity) - вимірює вразливість цілісності системи до порушення. Це стосується ризику несанкціонованих змін, пошкодження даних або несанкціонованих модифікацій, які впливають на

правильність і надійність системи. Терми цієї лінгвістичної змінної та відповідні до них значення: *NONE, 0; LOW, 0.5; HIGH; 1.*

VC (Vulnerability System Confidentiality) відноситься до вразливості системи до порушень, які можуть поставити під загрозу конфіденційність конфіденційної інформації. Він оцінює ризик несанкціонованого доступу до конфіденційних даних. Терми цієї лінгвістичної змінної та відповідні до них функції приналежності мають наступні позначення: *N, z (0.2 0.4); L, PI (0.2 0.3 0.6 0.9); H, S (0.6 0.7).*

VA (Vulnerability System Availability) вимірює потенційні загрози для доступності системи, зокрема ризики, які можуть перешкодити авторизованим користувачам отримати доступ до системи або її даних. Це включає атаки на відмову в обслуговуванні або простої системи.

Метрика ***Safety*** вимірює вплив на безпеку людини-актора або учасника, який передбачувано може отримати травму в результаті використання вразливості. Відповідна лінгвістична змінна приймає такі значення: *Negligible, 0; Marginal, 0.5; Critical, 0.75; Catastrophic, 1.* Показник відноситься до групи додаткових і, як правило, не використовується. Але в даній роботі йому надається особливе значення на випадок, коли в мережевій структурі присутні об’єкти зі штучним інтелектом (наприклад, роботи).

Вихідним параметром системи нечіткого логічного виведення (рис.1) є також лінгвістична змінна:

AS (Attack Severity) refers to the measure of the potential damage or impact an attack could have on a system. This metric helps to assess the seriousness of an attack, including the scale of damage and recovery efforts needed. відноситься до міри потенційної шкоди або впливу, який атака може мати на систему. Цей показник допомагає оцінити серйозність атаки, включно з масштабом шкоди та зусиллями, які необхідні для відновлення. Терми вихідної змінної та відповідні до них функції приналежності мають наступні позначення: *Slight, z (0.15 0.3); Minimal, PI (0.1 0.2 0.4 0.5); Significan,; PI (0.3 0.4 0.65 0.7); Major, PI (0.5 0.67 0.85 0.9); Catastrophic, S (0.7 0.92).*

На рис.2 представлена поверхня відгуку системи нечіткого логічного виведення, що дає оцінку важкості наслідків вразливостей.

Розуміння вразливостей системи та того, як вони взаємодіють із ключовими умовами безпеки, має важливе значення для захисту інформації та захисту від кібератак. Були досліджені поширені вразливості системи, пов’язані з такими важливими поняттями, як керування паролями, керування доступом і безпека мережі тощо.

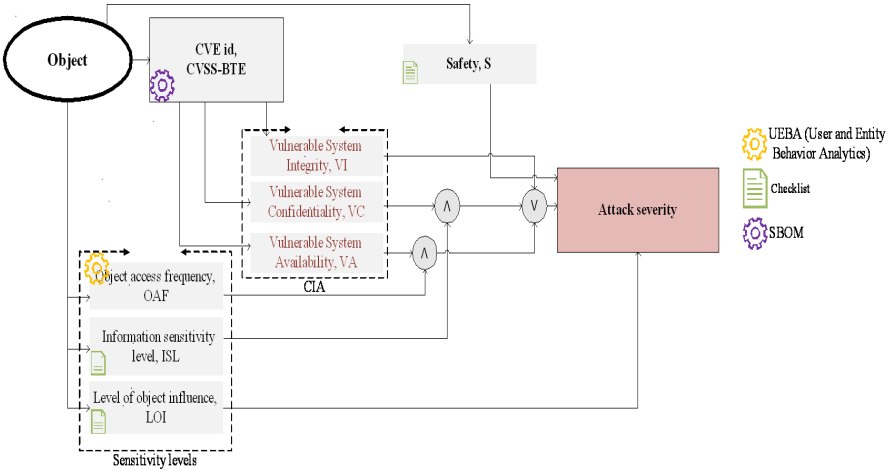

Рисунок 1 – Структура системи нечіткого логічного виведення для оцінки важкості наслідків вразливостей в мережевій системі

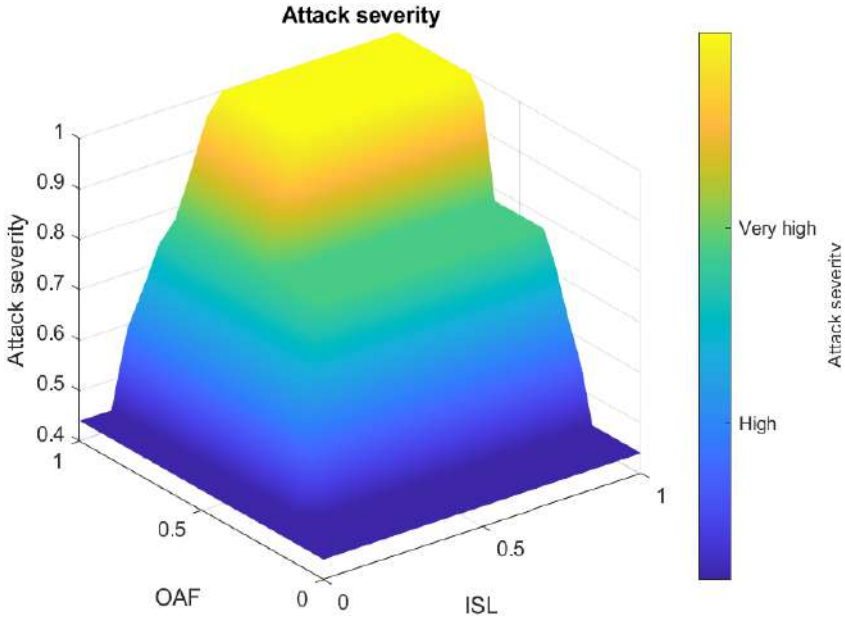

Рисунок 2 – Поверхня відгуку для оцінки важкості наслідків вразливостей (реалізація в пакеті Matlab)

Науковою новизною даної роботи є математична модель оцінки важкості наслідків вразливостей мережевої структури, яка враховує наявність в системі ШІ, та її реалізація в пакеті Matlab.

Розглянуті в цій статті CVE підкреслюють нагальну потребу організацій у впровадженні ефективних механізмів захисту. Визначаючи пріоритетність регулярних оновлень, застосовуючи надійні методи безпеки та проводячи постійні оцінки, можна значно зменшити ризики, що пов'язані з цими вразливими місцями,. У міру розвитку технологій підтримка проактивного підходу до кібербезпеки є важливою для захисту мереж і даних.

Подальший план досліджень передбачає розробку сценаріїв потенційних дій вразливостей в певних системах та стратегій захисту для зменшення ризиків.

Дослідження виконувалось за підтримки проекту "TELEMETRY" в рамках програми Horizon Europe.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A Framework Addressing Challenges in Cybersecurity Testing of IoT Ecosystems and Components / Steve Taylor, Martin Jaatun, Alan McGibney, Robert Seidl, Pavlo Hrynchenko, Dmytro Prosvirin, Rosella Mancilla // Proceedings of the 9th International Conference on Internet of Things, Big Data and Security, Angers – France, April 28 - 30, 20243. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58, 2021.

2. Fuzzy logic-based methodology for building access control systems based on fuzzy logic / Vasyl Lytvyn, Anna Bakurova, Oleh Zaritskyi, Anatoliy Gritskevich, Pavlo Hrynchenko, Elina Tereschenko and Dmytro Shyrokorad // Proceedings of the Modern Data Science Technologies Workshop (MoDaST 2024) Lviv, Ukraine, May 31 - June 1, 2024. – ceur-ws.org/Vol-3723/paper7.pdf

3. Common Vulnerability Scoring System: Specification Document https://www.first.org/cvss/specification-document