3. ISO/IEC 27005:2018. Information technology - Security techniques - Information security risk management. Geneva: International Organization for Standardization, 2018. 87 p.
4. MITRE ATT&CK: Design and Philosophy. MITRE Corporation Technical Report. Bedford, MA, 2020. 57 p.

Система нечіткого логічного виводу вразливостей та загроз інформаційної безпеки

УДК 004.056

Володимир Джулій[1], Денис Вишневський[2]

Хмельницький національний університет,
[1]dzhuliivm@khmnu.edu.ua, [2]vushnya5495@gmail.com

Аналіз проведеного дослідження поточного стану в області інформаційної безпеки показує, що темпи розвитку інформаційних та комп'ютерних технологій значно випереджають процес створення програмно-апаратного забезпечення в області інформаційної безпеки. Пріоритетними, в даній ситуації, є задача аналізу, класифікації, виявлення діючих механізмів та засобів проведення атак і загроз інформаційній безпеці системи, які можуть призвести до отримання несанкціонованого доступу до конфіденційних даних, порушення функціонування інформаційної системи, визначення заходів протидії атакам та загрозам, оцінка заданої шкоди, розробка нормативно-правової бази, механізмів захисту та критеріїв інформаційної безпеки системи протидії.

Актуальною залишається задача проектування та розробки методу, системи прогнозування, виявлення вразливостей, загроз безпеки інформації. Як інструмент для досягнення поставленої задачі пропонується використовувати нечітку інформаційно-аналітичну систему прогнозування вразливостей та загроз інформаційної безпеки, що надає функціональні можливості, які представленні на рис. 1.

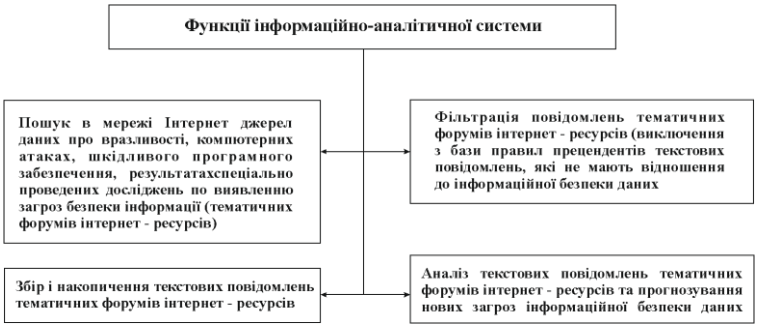

Рис.1. Функції інформаційно-аналітичної системи аналізу потоку повідомлень тематичних інтернет-форумів

Список тематичних джерел форумів містить адреси інтернет- ресурсів, на яких розміщуються текстові публікації про шкідливе програмне забезпечення, вразливості та комп'ютерні атаки [1].

На початковому етапі роботи інформаційно-аналітичної системи список формується експертним шляхом, із загальної кількості форумів тематичних інтернет – ресурсів виділяються ті, тематика яких дозволяє інтернет - інформацію віднести до хакерських (інформація містить результати спеціалізованих досліджень з виявлення вразливостей та загроз інформаційної безпеки конфіденційних даних, повідомлення про комп'ютерні атаки, вразливості, шкідливе програмне забезпечення). Автоматизоване виявлення нових форумів тематичних інтернет-ресурсів, в даній ситуації, можливо, шляхом проведення аналізу різноманітних форумів інтернет-ресурсів, з використанням запропонованих критеріїв відбору текстових повідомлень, що належать до заданої предметної області, для якої проводиться аналіз з використання онтології [2]. Для реалізації фізичної системи, потрібно реалізувати в матеріальні сутності всі елементи логічного представлення.

Для фізичного представлення моделі використовується діаграма UML розгортання, відображається загальна топологія та конфігурація інформаційно-обчислювальної системи, а також розподіл за окремими вузлами компонентів. Вузлами діаграми інформаційно-обчислювальної системи є персональний комп'ютер користувача, сервер адміністратора.

Покращення якості прогнозування виникнення вразливостей та загроз безпеки інформації з використанням систем логічного нечіткого виводу може сприяти збільшення кількості вхідних змінних, використанню більш точних нечітких правил продукцій, також велике значення має визначення функцій приналежності вихідних та вхідних параметрів системи логічного нечіткого виводу, необхідно враховувати статистичні показники потоку текстових повідомлень форумів тематичних інтернет-ресурсів.

1. Ленков С.В**.** Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів / С.В. Лєнков, В.М. Джулій, А.М. Берназ, І.В. Муляр, І.В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2023. – Вип. №78. – С. 123-134.
2. Ленков С.В. Метод протидії поширенню та виявлення шкідливої інформації в соціальних мережах/ С.В. Ленков, В.М. Джулій, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №77. – С. 103-117.

Структура мережі розподілу квантово-захищених ключів у мережах магістральної топології

УДК 004.056

Володимир Джулій[1], Максим Вовкович[2]

Хмельницький національний університет, [1]dzhuliivm@khmnu.edu.ua, [2]maksym.vovkovyhc@gmail.com