ЗАСТОСУВАННЯ МЕРЕЖ ПЕТРІ В ПРОЦЕСІ ДОСЛІДЖЕННЯ ВПЛИВУ ІНФОРМАЦІЙНИХ ЗАГРОЗ

Мерзлікін В.В.[1], магістр гр. ІПЗм-22, volodymyr.merzlikin.kita@donntu.edu.ua;
Алтухова Т.В.[1], к.т.н., tetiana.altukhova@donntu.edu.ua
[1] Державний вищий навчальний заклад «Донецький національний технічний університет», Луцьк, Україна

На даний час у всій світовій спільноті інформація відіграє досить велику роль, так як забезпечує безпосередню передачу знань, будь-яких подій, описання відчуттів та емоцій та, загалом вважається досить потужною зброєю задля маніпуляції свідомості і подій та відповідними їх можливими наслідками, загальної суспільної думки і формування та впливу на оцінку подій, які відбувалися [1]. З розвитком інформаційно-телекомунікаційних технологій та новітніх методів обробки інформації зараз викликало стрімку реалізацію усіх сучасних можливостей науково-технічного прогресу, глобально-інформаційного і технологічного розвитку в суспільстві. Проте стрімкий розвиток інформатизації призвів до стрімкого виникнення проблем безпосередньо з інформаційною безпекою як в Україні, так і у всьому світі, які, в свою чергу, поділяються на проблеми самого захисту інформації та захисту від інформаційних загроз, тому, враховуючи їх небезпеку, питання їх відвертання та нейтралізації вимагає досить суворих вирішень та відповідних дій, що саме визначило актуальність дослідження впливу інформаційних загроз із застосуванням сучасних інтелектуальних методів моделювання [2].

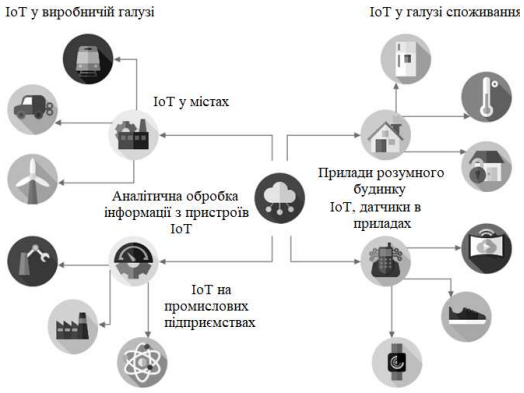

Рисунок 1. Структура IoT [3]

Найбільш вразливою категорією на даний час є Internet of Things (IoT) (рис.1), так як містить досить багато механічних приладів з вбудованими спеціальними датчиками з функціональними можливостями обробки інформації, які, в свою чергу, з кожним роком все біль розвиваються [3]. Однак, у зв'язку з цим, саме порушники безпеки спрямовують свої дії на пошук більш ефективних інструментів та розробку вірусного програмного забезпечення, якому не буде можливості протидіяти сучасні системи захисту. Етапи дослідження кіберзагроз в даній сфері передбачає виконання певних операцій, які наведені на рис. 2 [2]. Тому застосування мереж Петрі для створення імітаційної моделі дослідження впливу кіберзагроз надасть можливість визначити можливі ризики на IoT.

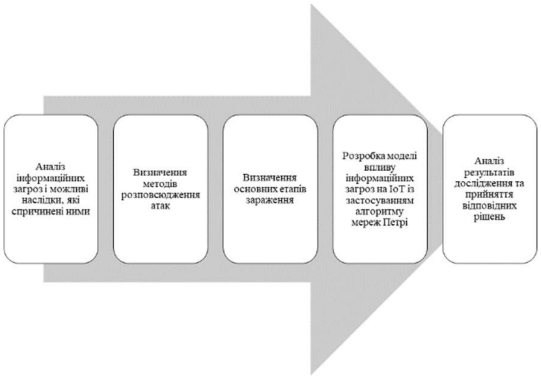

Рисунок 2. Основні кроки проведення дослідження впливу кіберзагроз в сфері IoT

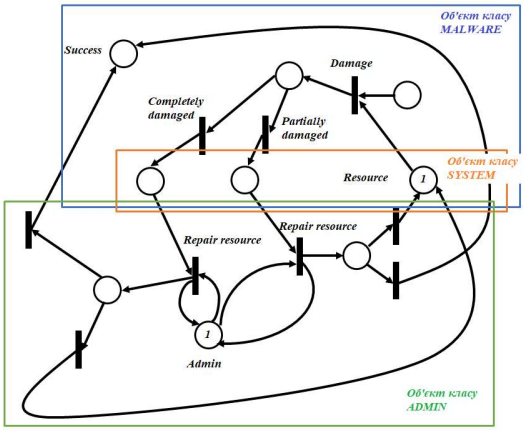

Рисунок 3. Розроблена модель мережі Петрі для дослідження впливу кіберзагроз в сфері IoT

Модель мережі Петрі була побудована для дослідження атаки порушника безпеки із застосуванням небезпечного вірусного програмного застосунку (ВПЗ) на обчислювальний ресурс (рис. 3).

Дослідження впливу інформаційних загроз за отриманою моделлю (рис.3) забезпечувалося на трьох етапах: по-перше, проводилася імітація дії порушника із застосуванням вірусу, по-друге, імітація дій користувача під час та після кібератаки, по-третє, безпосереднє інфікування обчислювального ресурсу вірусним застосунком. За результатами проведення дослідження на всіх трьох етапах було сформовано графічне представлення часового ураження обчислювального пристрою (ОП) (рис. 4).

За отриманими результатами можна зробити висновки, що у разі підвищення можливості відкриття небезпечного вірусного додатку буде найменший час ураження шкідливим ВПЗ обчислювального пристрою, тобто від 0 до 20% час вразливості більш тривалий, зі збільшенням від 25% він зменшується. Таким чином, якщо до 50% можливості завантаження шкідливого програмного забезпечення на комп'ютер надається шанс залишити його неушкодженим, проте після перевищення цієї межі порушник безпеки, здійснивши кібератаку за допомогою вірусу, досягне своєї мети щодо порушення конфіденційності, цілісності та доступності інформації.

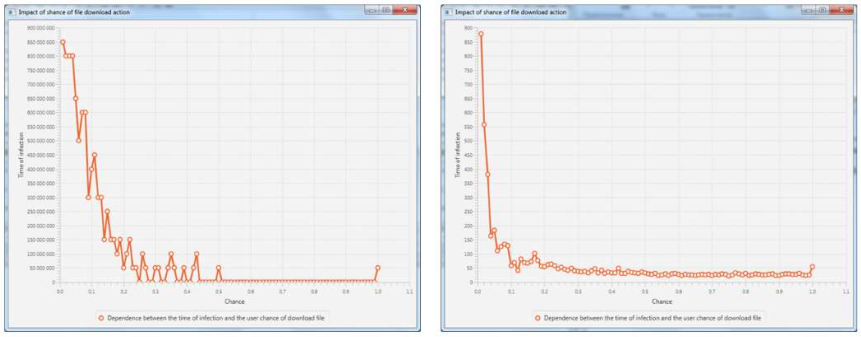

Рисунок 4. Результати дослідження впливу шкідливого вірусного додатку на стан комп'ютера під час його ураження

Література

1. Пархоменко-Куцевіл О.І. Проблеми забезпечення інформаційної безпеки під час здійснення військових операцій та бойових дій. Публічне управління у сфері державної безпеки та охорони громадського порядку, Випуск 28, 2022. – С. 177-188.

2. Живко З.Б., Живко, М.О. Інформаційні загрози: суть і проблеми. Тези доповідей ІІ міжнародної НПК «Безпека та захист інформації в інформаційних системах», 29-30 квітня 2009 року. – Харків: Харківський національний економічний університет. – С. 116-118.

3. Огородников Д.В, Стеценко І.В. Безпека Інтернет речей. Всеукраїнська науково-практична конференція молодих вчених та студентів «Інформаційні системи та технології управління» (ІСТУ-2018) – Київ: НТУУ «КПІ ім. Ігоря Сікорського», 29-30 листопада 2018 р. – С. 113-115.

4. Зайцев Д.А. Математичні моделі дискретних систем: Навчальний посібник / Одеса: ОНАЗ ім. О.С. Попова, 2004. – 40 с.

5. Zaitsev D.A., Shmeleva T.R. Simulating Telecommunication Systems with CPN Tools: Students' book / Odessa: ONAT, 2006. – 60 p.

Анотація

В статті виконано розробку імітаційної моделі дослідження впливу шкідливого вірусного програмного забезпечення на обчислювальний пристрій із застосуванням мереж Петрі та виявлено, що стан пристрою та його можливість ураження залежить від підвищеного шансу відкриття небезпечного вірусного додатку, так як час ураження ним буде зменшуватися.

Ключові слова: інформаційна безпека, Internet of Things, вірусне програмне забезпечення, час ураження, мережі Петрі.

Abstract

The article develops a simulation model for studying the impact of malicious virus software on a computing device using Petri nets and reveals that the state of the device and its possibility of being affected depends on the increased chance of opening a dangerous virus application, as the time of its damage will decrease.

Keywords: information security, Internet of Things, virus software, time of damage, Petri nets.