***Нестеренко О.В**., к.т.н., доц.*
Провідний науковий співробітник
***Нетесін І.Є**., к.ф.-м.н.*
Провідний науковий співробітник
Державне підприємство «Український науковий центр розвитку інформаційних технологій», м. Київ, Україна

ГРАФОВІ МОДЕЛІ КІБЕРБЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Незважаючи на те, що Інтернет речей (*Internet of Things*, IoT) знаходиться тільки на початку свого розвитку, але вже доводиться казати, що це нововведення додає серйозних проблем, пов'язаних з кібербезпекою. Керування пристроями за допомогою міжмашинної взаємодії несе великі загрози не лише для даних, з чим ми звикли мати справу в традиційних інформаційних системах, а й для функціонування підприємств, працездатності критичних інфраструктур і навіть для життя людини.

В даному аспекті нестача досліджень взаємозалежності складових безпекового середовища IoT, досліджень на відповідність умовам, що склалися та можливість адаптації до змін, що відбуваються, виступають тією проблемою, яка потребує розгляду. Досі залишаються невирішеними питання, що полягають у теоретичному вивченні та розкритті підходів до опису взаємодії загроз і різних властивостей інформаційних одиниць (об'єктів) для вибору засобів захисту, які необхідні для розв'язання задач забезпечення безпеки. Перспективним вважається представлення моделей у вигляді графів [1], але й цей підхід потребує подальшого розвитку.

У загальному випадку побудова моделі має за мету необхідність захисту від впливу загроз усім властивостям захищеності, насамперед від загроз, наслідком реалізації яких може бути неприпустимо високий чи високий рівень шкоди, оскільки такі загрози мають комплексний, тобто одночасний вплив на декілька властивостей захищеності. Такі загрози прийнято називати найбільш суттєвими (найбільш небезпечними, найбільш імовірними) загрозами. Виявлення найбільш суттєвих загроз та високого рівня шкоди, нанесеної ресурсу, є основою для визначення в подальшому потрібних засобів захисту, а отже визначення складу потрібних контрзаходів для забезпечення припустимої захищеності, необхідних для захисту засобів, підсистем, механізмів та функцій захисту, тобто дає змогу будувати відповідні моделі систем захисту.

В центрі будь-якої системи моделей знаходиться певна класифікація, яка описує поняття предметної області. Насамперед необхідно розглянути класифікацію загроз та нештатних ситуацій, що можуть виникнути відносно системи IoT. Для аналізу загроз необхідним є визначення можливих каналів та видів загроз, що можуть бути реалізовані відносно системи, а також аналіз основних джерел їх походження.

Одним з найнебезпечніших напрямів атаки, на які варто звернути увагу, є DDoS-атака. Також атака може бути реалізованою віддалено по Інтернету до обладнання IoT, яке має уразливості у безпеці своїх паролів, проблеми з шифруванням даних і з дозволом доступу. Машини, які передають інформацію в незашифрованому виді, можуть зберігати пароль мережі Wi - Fi, до якої вони приєднані. Також IoT-пристрої, які не мають належного захисту, піддаються атакам з метою зараження шкідливим кодом для створення ботнету.

Самі датчики як частини системи IoT є найуразливішими для зловмисників при спробах отримання доступу до основної мережі підприємства. В залежності від розташування датчиків, їх призначення (функціональності), виду з'єднань можна застосувати таку класифікацію уразливості датчиків, на які спрямовані загрози: стек мережевих протоколів (з тих, що використовуються в IoT), радіо-протоколи, засади роботи мікроконтролерів, інжиніринг прошивок та скомпільованих програм, web-уразливості. Враховуючи цю класифікацію, напрямки забезпечення кібербезпеки для IoT зводяться до трьох спрямувань: Hardware security, Software security та Radio security.

Тоді модель відношень множини загроз T і множини об'єктів O можна представити дводольним графом $G_{TO} = (V(T,O), E(T,O))$, у якому множини вершин його долей $T \cup O = V(T,O)$, $T \cup O = V(T,O)$, $T = \{T1, T2, \ldots, T_{|T|}\}$, $O = \{O1, O2, \ldots, O_{|O|}\}$, де $|T|$, $|O|$ -

кількість елементів відповідно множин *T* та *O*,*T* ∩ *O* = Ø та множина ребер *E(T,O)*, в якому ребро $(T_p, O_q) \in E(T,O)$, якщо є загроза *Tp* об'єкту *Oq*. Спрямованість загроз до об'єктів визначається на основі їх описів (класифікації).

У відповідності до відомої моделі безпеки з повним перекриттям [2], яка будується виходячи з положення, що система безпеки повинна мати принаймні один засіб для забезпечення безпеки на кожному можливому шляху дії загрози на об'єкт, в нашій моделі з'являється третій набір, що описує механізми забезпечення безпеки

$M = \{M_1, M_2, \dots, M_r, \dots\}, r = 1, 2, \dots$.

В ідеальному випадку набір механізмів *M* повинен усувати всі ребра (T_p, O_q). На практиці ж M_r виконує функцію "бар'єру", забезпечуючи деяку міру опору спробам реалізації загрози. Включення в модель множини *M* перетворює граф G_{TO} в тридольний граф $G_{TMO} = (V(T,M,O), E(T,M), E(M,O))$.

Побудова графу G_{TMO} є нетривіальною задачею, зважаючи на складність зв'язків графу G_{TO}. Щоб полегшити розв'язання цієї задачі достатньо розшукати на графі G_{TO} компоненти зв'язності, тобто такі його підграфи $G_i = (V_i, E_i)$, що $G_{TO} = \cup Gi$, але $V_i \cap V_j = Ø$ та $E_i \cap Ej = Ø$, *i, j =1,2,…, i ≠ j*, у той час як у будь-якому G_i будь-які вершини *u* та *v* з'єднані простим ланцюгом.

Для знаходження компонент зв'язності можливо застосувати відомі алгоритми. Більшість алгоритмів на графах використовують їх представлення за допомогою матриці суміжності або списків суміжних вершин. У разі представлення графу за допомогою списків суміжних вершин для пошуку компонент зв'язності зазвичай застосовують алгоритми, які базуються на алгоритмах пошуку в глибину та пошуку в ширину, які досліджують граф методом обходу усіх вершини і ребер, використовуючи механізми рекурсії, фарбування вершин або ребер, поняття предків і нащадків, міток часу тощо [3,4].

Тепер послідовно розглядаючи отримані підграфи G_i визначення необхідних механізмів захисту з набору *M* вочевидь значно спрощується.

Але залишається проблема оцінки пріоритетності та вартості реалізації вибраних механізмів захисту. Для цього традиційно відомим є визначення передусім оцінки ризиків, яка випливає з ймовірності здійснення загрози та рівня шкоди (збитків) від порушень по кожному з їх видів.

Таким чином створення графових моделей безпекового середовища IoT для визначення впливів різного типу загроз та захищеності об'єктів свідчить про зручність їх застосування, надаючи ефективний інструмент менеджерам і розробникам засобів захисту. Одночасне застосування елементів класифікації (онтологічних описів) підвищить рівень конкретності моделі та більш чіткого уявлення щодо стану середовища.

ЛІТЕРАТУРА

1. Качинський А.Б. Ієрархія факторів типових сценаріїв реалізації DDos-атак / А.Б. Качинський, В.М. Ткач, А.А. Поденко // Математичне моделювання в економіці, 2017. – №1-2. – С. 17-30, 2018. – №1. – С. 31-48.)

2. Хоффман Л.Дж. Современные методы защиты информации / Л.Дж. Хоффман. Пер. с англ. / М.: Советское радио, 1980. – 264 с.

3. Кормен Т. Алгоритмы. Построение и анализ / Т. Кормен, Ч. Лейзерсон, Р. Ривест, К. Штайн / пер. с англ. – 2-е изд. – Москва–Санкт-Петербург–Киев: Издательский дом «Вильямс», 2013. – 1296 с.

4. Харари Ф. Теория графов / Ф. Харари / пер. с англ. – М: «Мир», 1973. – 302 с.