Міністерство освіти і науки України

Державний вищий навчальний заклад
«Донецький національний технічний університет»

Кафедра автоматики і телекомунікацій

Донецький науковий центр НАН України і МОН України

«ТАК»

Телекомунікації, автоматизація, комп'ютерно-інтегровані та інформаційні технології

Збірка доповідей Всеукраїнської науково-практичної конференції молодих учених
(Дрогобич, 12 грудня 2024 р.)

Дрогобич
ДВНЗ «ДонНТУ»
2024

УДК 621.39+681+004
Т 15

Т 15 **«ТАК»**: телекомунікації, автоматика, комп'ютерно-інтегровані технології: зб. доповідей Всеукр. наук.-практ. конф. молодих вчених, 12 грудня 2024 р. / ДВНЗ «ДонНТУ; відп. ред. Г.В. Ступак. – Дрогобич: ДВНЗ «ДонНТУ», 2024. – 215 с.

До збірника увійшли матеріали доповідей, представлених на Всеукраїнській науково-практичній конференції молодих учених «ТАК»: телекомунікації, автоматика, комп'ютерно-інтегровані технології. Конференція проводилася кафедрой автоматики та телекомунікацій (АТ) ДВНЗ «Донецький національний технічний університет».

У збірнику представлені результати досліджень та розробок молодих вчених із технічних вузів та наукових закладів України.

Збірник призначений для викладачів, аспірантів і студентів вищих технічних навчальних закладів, а також фахівців з телекомунікацій, автоматизації, інформаційних та комп'ютерно-інтегрованих технологій, електротехніки та електромеханіки.

УДК 621.39+681+004

МОДЕЛЮВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВИЯВЛЕННЯ ЗАГРОЗ

Квітковський І.О., магістр гр. ІПЗм-23,
ivan.kvitkovsky@donntu.edu.ua;
Алтухова Т.В., канд. техн. наук, tetiana.altukhova@donntu.edu.ua
Державний вищий навчальний заклад «Донецький національний технічний університет», Дрогобич, Україна

На сьогоднішній день стан питання забезпечення інформаційної безпеки (ІБ) в Україні та у всьому світі є першочерговим з огляду на те, що з кожним роком спостерігається підвищення проявів порушення безпеки їх критичної інфраструктури та наявності загроз в інформаційному середовищі, тим самим відображаючи всі можливі вразливості для здійснення кібератак [1].

Зараз практично всі підприємства, будь-які установи та організації країн мають свою певну інформаційну систему (ІС), в якій передбачено взаємозв'язок різноманітних методів, засобів та співробітників, формуючи при цьому єдину локальну обчислювальну мережу (ЄЛОМ). В ЄЛОМ забезпечується основний процес отримання, зберігання, обробки і видачі інформації на підприємствах, організаціях та установах. Однак збільшення потоку даних в ній та розширення кола завдань інформаційних систем викликає появу проблеми підвищення частоти здійснення кібератак на ІС та розширення вразливостей інформаційних ресурсів. Причиною виникнення даної проблеми є [2]:

- збільшення кількості завдань, що розв'язуються в інформаційній системі;
- розвиток методів та засобів обробки інформації та порушення інформаційної безпеки;
- збільшення об'єму інформації, яку необхідно обробити;
- розширення функціональних можливостей ЄЛОМ шляхом ускладнення програмно-апаратних компонентів, і, як наслідок, збільшення ймовірності появи вразливостей та помилок в системі [2].

Окрім цього проблема виникає через конкурентність підприємств за отримання доходу, їх стан на ринку за умови ефективного і коректного функціонування інформаційної системи, цілісності інформаційних ресурсів та рівня захисту конфіденційної інформації від несанкціонованого доступу зловмисників як з зовнішнього середовища, так і внутрішнього середовища підприємства. Сучасні процеси забезпечення інформаційної безпеки мають тісний взаємозв'язок із виконанням моніторингу існуючих систем та мереж, в яких відбувається передача інформації і даних [3]. Окрім того, з кожним роком зростають вимоги до систем інформаційної безпеки, що повинні забезпечувати не тільки пасивний захист, наприклад, виконання блокування

несанкціонованого доступу в інформаційній мережі з зовнішнього середовища, а й забезпечувати активний захист, до якого відноситься виявлення кібератак, аналіз причин появи загроз та автоматичне їх усування [4]. Таким чином, проблема забезпечення захисту інформації повинна вивчатися та вирішуватися з точки зору застосування найсучасніших методів і засобів моделювання та новітніх алгоритмів виявлення загроз і автоматизованого прийняття рішень щодо запобігання кібератакам.

Сам процес реалізації загроз порушником ІБ є кібератака на функціональні можливості інформаційної системи задля отримання доступу до конфіденційних даних, тому їх виявлення є першочерговим завданням, яке забезпечить здійснення блокування порушень ІС та знизить можливості витоку інформації і появи інших негативних наслідків вторгнення зловмисника до системи.

Будь-яке порушення інформаційної системи передбачає декілька етапів, що входять в «життєвий цикл кібератаки», які демонструють основну структуру процесу успішної реалізації загроз в ІС зловмисником (рис.1) [5].

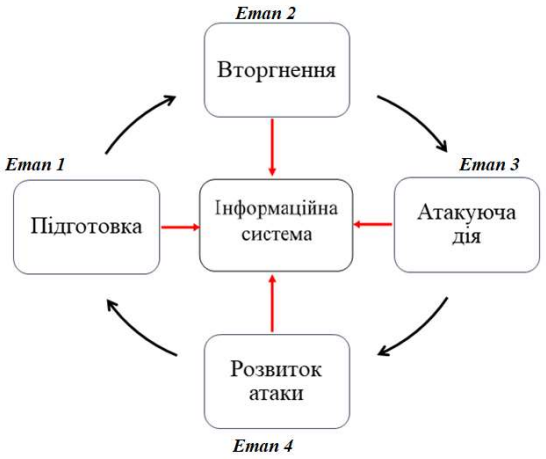

Рисунок 1. Життєвий цикл кібератаки на ІС

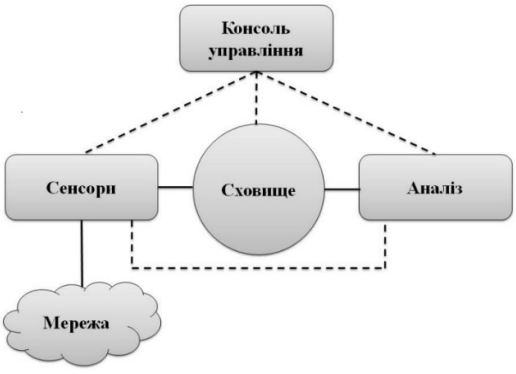

Рисунок 2. Базова структура систем інформаційної безпеки виявлення загроз

З огляду на це, розробка систем інформаційної безпеки виявлення загроз є необхідним засобом захисту інформаційних систем від небезпечної та підозрілої активності в мережі, базова структура якої наведена на рис. 2 [6].

Розробка моделі такої системи здійснювалася із використанням мереж Петрі задля відображення основних процесів виявлення кібератаки на інформаційну систему в залежності від різних факторів впливу та виявлення аномальної поведінки загроз в ній (рис. 3).

Дослідження отриманої моделі здійснювалося у два етапи, а саме моделювання динаміки процесу функціонування моделі мережі Петрі системи інформаційної безпеки виявлення загроз (рис.4) та динаміки її реагування на кібератаки (рис.5). За отриманими результатами дослідження виконана

верифікація та визначена щільність ймовірності часу реагування розробленою системою під час порушення інформаційної системи загрозами (рис. 6).

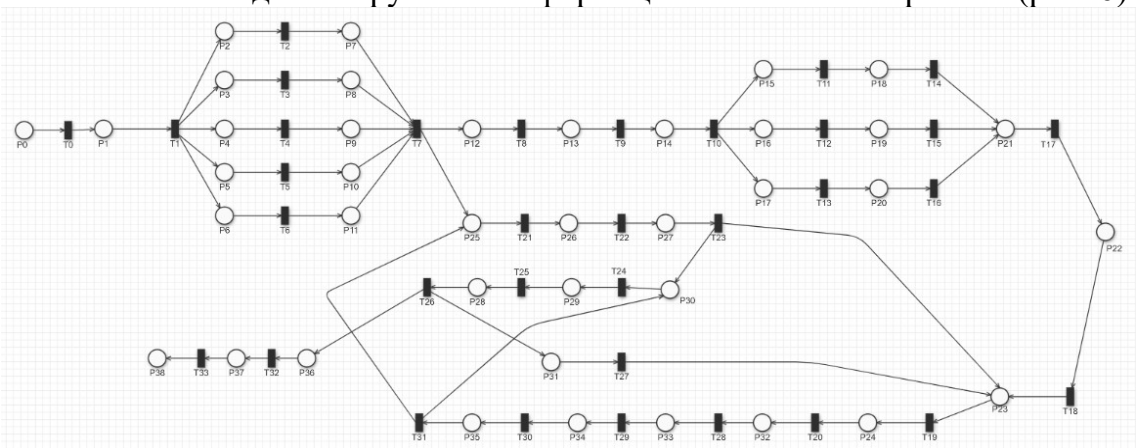

Рисунок 3. Розроблена модель системи інформаційної безпеки виявлення загроз на основі мереж Петрі

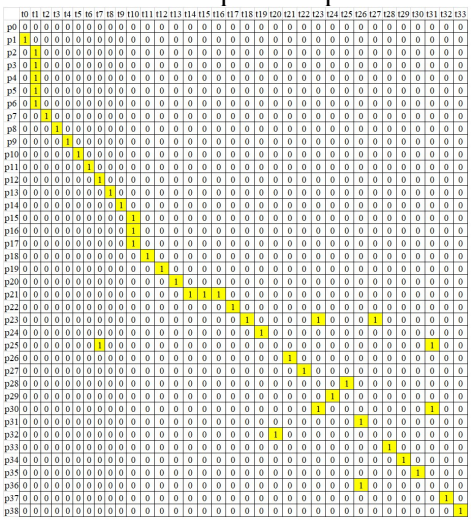

Рисунок 4. Результат дослідження динаміки процесу функціонування побудованої моделі мережі Петрі системи інформаційної безпеки виявлення загроз

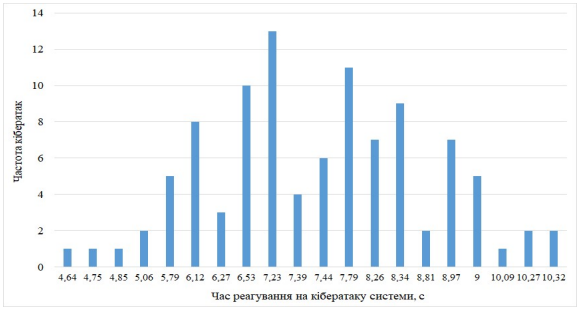

Рисунок 5. Динаміка реагування розробленої системи ІБ виявлення загроз відносно частоти здійснення кібератаки порушниками безпеки

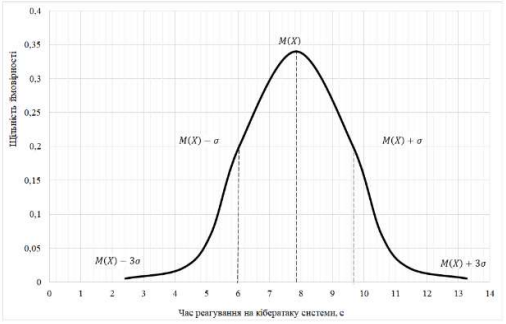

Рисунок 6. Результати визначення щільності ймовірності часу реагування розробленою системою під час порушення інформаційної системи загрозами

Таким чином, отримані результати дослідження показали, по-перше, що отримана модель мережі Петрі володіє такими властивостями, як детермінованість та послідовність, тобто в кожний момент часу мережа буде знаходитися у відповідному стані із існуючих, причому для них можна визначити наявність чи відсутність кіберзагрози з певною ймовірністю. По-друге, виявлено, що середній час реагування розробленою системою під час порушення інформаційної безпеки загрозами знаходиться в межах від 5 до 11 с, що показує ефективність реагування на порушення безпеки загрозами в інформаційній системі.

Література

1. Комаров М. Ю., Гончар С. Ф., Дмітрієва Д. О. Дослідження проблеми кіберживучості об'єктів критичної інформаційної інфраструктури. Ядерна та радіаційна безпека, 1(89), 2021. С. 59-66.

2. Дзьобань О.П., Соснін О.В. Інформаційна безпека: нові виміри загроз, пов'язаних з інформаційно-комунікаційною сферою. Гуманітарний вісник ЗДІА, №60, 2015. – С. 24-34.

3. NVD – Home [електронний ресурс]. Режим доступу: https://nvd.nist.gov/ (дата звернення 04.09.2024).

4. CVE – CVE [електронний ресурс]. Режим доступу: https://cve.mitre.org/ (дата звернення 04.09.2024).

5. Запорожченко М. М. Місце OSINT в життєвому циклі кібератаки /М. М. Запорожченко// Телекомунікаційні та інформаційні технології, №1(78), 2023. – С. 53-60. - DOI: 10.31673/2412-4338.2023.015360

6. Мєшков В. І., Віролайнен В. О. Аналіз сучасних систем виявлення та запобігання вторгнень в інформаційно-телекомунікаційних системах [електронний ресурс]. Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/2fc5d863-fb1a-4334-a33d-ceee718222ff/content (дата звернення 20.10.2024).

Анотація

В статті проаналізовано причини виникнення проблеми інформаційної безпеки та запропоновано модель системи виявлення загроз із застосуванням мереж Петрі. Проведено дослідження динаміки процесу функціонування розробленої моделі та динаміки реагування її на кібератаки.

Ключові слова: інформаційна безпека, модель системи виявлення загроз, мережі Петрі, динаміка процесу функціонування, час реагування.

Abstract

The article analyses the reasons for the emergence of the information security problem and proposes a model of a threat detection system using Petri nets. The dynamics of the functioning of the developed model and the dynamics of its response to cyber attacks are studied.

Keywords: information security, model of a threat detection system, Petri nets, dynamics of the functioning process, time of response.

ЗМІСТ