УДК 621.396.946:004.056

# МАТЕМАТИЧНА МОДЕЛЬ ПОПЕРЕДЖЕННЯ ПРО КІБЕРЗАГРОЗИ У МОБІЛЬНИХ МЕРЕЖАХ 5G

Бадєєв В.О., Коляденко Ю.Ю., Москалець М.В.
e-mail: valerii.badieiev@nure.ua, yuliia.koliadenko@nure.ua, mykola.moskalets@nure.ua
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна

A model for early warning of cyber threats in 5G networks using Markov processes has been developed. Through simulation modeling in the MATLAB environment, a time diagram of vulnerability detection requests has been obtained. Changes in state probabilities have also been obtained. Thus, knowing the intensity of flows, it is possible to model and predict the processes of incoming vulnerability detection requests in real time.

Безпека телекомунікаційних мереж, у яких канал передачі може використовуватися одночасно багатьма користувачами, є особливо важливою проблемою. У безпроводових міських мережах ця проблема ускладнюється тим, що канал зв'язку є загальнодоступним. Іншими словами, інформація, яка передається в таких мережах, може бути легко перехоплена зловмисниками. Це може призвести до крадіжки персональних даних, фінансових збитків або навіть до порушення безпеки критичної інфраструктури. Безпека інформації є важливим фактором, який визначає надійність 5G [1].

Основною загрозою безпеці таких систем є уразливості, особливо в програмних компонентах. Пошук уразливостей у програмних компонентах є складним і трудомістким завданням, яким займаються здійснюють великі компанії та дослідницькі центри. Інформацію про уразливості можна знайти у загальнодоступних джерелах, таких як Open Source Vulnerability Database, Common Vulnerabilities and Exposures та Natioal Vulnerability Database [1].

Результати попереднього аналізу процесів виявлення та усунення вразливостей свідчать про те, що їх можна представити як систему масового обслуговування (СМО) з необмеженою довжиною черги. Параметри цієї системи можна визначити на основі статистичних даних про виявлення та усунення вразливостей таким чином [1]:

-кількість каналів обслуговування $n$ залежить від кількості організацій або груп розробників, які відповідають за усунення вразливостей конкретного програмного продукту 5G. У найпростішому випадку може бути достатньо одного каналу обслуговування;

- інтенсивність надходження заявок $\lambda$, яка відповідає інтенсивності виявлення вразливостей в програмному продукті 5G можна оцінити на основі кількості вразливостей, опублікованих за аналізований проміжок часу (тиждень, місяць, рік). Ця оцінка може бути отримана на основі аналізу бази даних вразливостей CVE (первинної бази);

- інтенсивність обслуговування заявок $\mu$, яка відповідає інтенсивності усунення вразливостей (випуску оновлень, що виправляють уразливості), може бути оцінена з використанням інформації з бюлетенів безпеки, що публікуються компаніями-виробниками програмного продукту 5G, а також баз вразливостей NVD та OSVDB (вторинні бази);

- час обслуговування $T_{обсл}$ окремих уразливостей в програмному продукті 5G, який також називають «кількістю днів ризику» [2,5], визначається як середній період між появою та усуненням цих уразливостей;

- імовірність того, що заявка на усунення вразливості буде оброблена $Q$, теоретично дорівнює одиниці. Однак на практиці існують випадки, коли деякі вразливості окремих програмних компонентів не усуваються;

- імовірність відмови $P_{відм}$ вразливості - це ймовірність того, що вразливість не буде усунена;

- середня кількість заявок в СМО $z_{ср}$ відображає середню кількість вразливостей, які існують в мережі на даний момент часу та для яких ще не випущено програмне оновлення. Цей показник є одним з найважливіших, адже він визначає число потенційних можливостей для атаки на інфокомунікаційну мережу.

- за середньою кількістю заявок в черзі $r_{ср}$ можна судити про те, скільки вразливостей потребують випуску оновлення;

- середній час очікування заявки в черзі $t_{оч.ср}$ показує, скільки в середньому потрібно часу для усунення вразливості з моменту її виявлення;

- середня кількість зайнятих каналів $k_{ср}$ свідчить про те, скільки робочих груп в середньому зайняті виправленням вразливостей. Цей показник дає уявлення про те, наскільки активно ведеться робота з виправлення вразливостей.

Розглянуту вище систему масового обслуговування можна представити у вигляді системи станів, де кожному стану буде відповідати певна кількість виявлених вразливостей, присутніх в системі [2], для яких ще немає рекомендації або програмного оновлення для їх усунення. Такі вразливості будемо називати активними. Подібні процеси ефективно описуються марковськими ланцюгами.

Марковські ланцюги мають порівняно мало інженерних застосувань, тому що досить рідко на практиці моменти можливих переходів системи з одного стану в інший заздалегідь відомі та зафіксовані. Набагато частіше переходи з одного стану в інший можуть відбуватися не в фіксовані моменти часу, а в випадкові.

Вважатимемо, що система змінює свій стан під впливом випадкових подій. Ці події відбуваються незалежно одна від одної і слідують пуассонівському закону. Пуассонівський потік не має післядії. Це означає, що ймовірність настання події в майбутньому не залежить від того, що

відбувалося в минулому. Знаючи поточний стан системи $s_i$ в момент $t$ ми можемо прогнозувати її майбутню поведінку, не враховуючи, як вона опинилася в цьому стані. Це значно спрощує аналіз поведінки систем, що описуються пуассонівськими потоками [3].

Вважатимемо, що система в початковий момент перебувала в стані $s_0$ (немає заявки). За допомогою імітаційного моделювання в середовищі Matlab отримано часову діаграму надходження заявок на виявлення вразливостей (рис.1). Таким чином, знаючи інтенсивність потоків можна в реальному масштабі часу моделювати процеси надходження заявок на виявлення вразливостей. На рис. 2. показана зміна ймовірвостей станів: $P_0(t)$ -це ймовірність, що система знаходиться у стані $s_0$ (немає заявки), $P_1(t)$ - це ймовірність, що система знаходиться у стані $s_1$ (надійшла заявка).

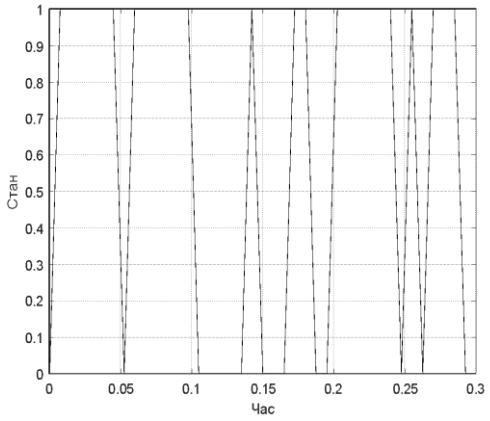


Рисунок 1 – Часова діаграма надходження заявок на виявлення вразливостей

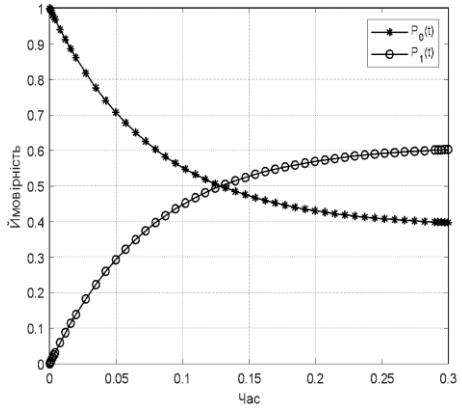


Рисунок 2 – Зміна ймовірвостей станів: $s_0$ - немає заявки, $s_1$ - надійшла заявка

Розроблено модель виявлення та усунення вразливостей у мережах зв'язку 5G на основі апарату марківських процесів. За допомогою даної моделі, знаючи інтенсивності потоків, можна в реальному масштабі часу моделювати процеси надходження заявок на виявлення вразливостей.

Список використаних джерел:

1.Nick McKeown. Openflow: enabling innovation in campus networks/ Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, Jonathan Turner// ACM SIGCOMM Computer Communication Review, 38[2]. - 2008. – 69–74.

2. Koliadenko, Y., Moskalets, M., Badieiev, V., Savchenko, R. Method Radio Resource Allocation in Cognitive Radio Network. Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham.