УДК 004.65 **doi: 10.26906/SUNZ.2018.2.077**

Н.В. Лукова-Чуйко, А.П. Мусієнко, М.О. Коваль

Київський національний університет імені Тараса Шевченка, Київ

ВИКОРИСТАННЯ МЕРЕЖ ПЕТРІ ДЛЯ ПОБУДОВИ МОДЕЛІ ВИЯВЛЕННЯ ЗОВНІШНІХ ВПЛИВІВ НА ІНФОРМАЦІЙНУ СИСТЕМУ

В роботі показано, що інформаційна система має, як правило, складну динамічну структуру, тому можливе використанням мереж Петрі з метою створення моделей виявлення та блокування зовнішніх впливів (DDoS-атак). Дані моделі засновані на описі структури інформаційної системи, на яку здійснюється вплив даною атакою, та процесів зміни станів цієї системи. Створені моделі виявлення та блокування DDoS-атак, які описують за допомогою мереж Петрі процес аналізу вхідного трафіку на предмет наявності даного типу атак, процес виявлення джерел шкідливого трафіку та їх подальшого блокування, що надає можливість для створення відповідних алгоритмів. Побудовані моделі дозволяють підвищити рівень функціональної стійкості інформаційних систем. Під функціональною стійкістю інформаційної системи розуміється властивість системи перебувати в стані працездатності, тобто виконувати необхідні функції протягом заданого інтервалу часу або наробітки в умовах відмов складових частин через зовнішні і внутрішні фактори.

Ключові слова: *функціональна стійкість, інформаційна система, мережі Петрі, DDoS-атака.*

Вступ

Під інформаційною системою будемо розуміти систему передачі даних спеціального призначення для передачі комп'ютерного, голосового та відеотрафіку. Усі інші вимоги, що висуваються до інформаційної системи – продуктивність, надійність, сумісність, керованість, живучість, тощо – пов'язані з якістю передачі даних [1, 2]. Дана мережа належить до класу складних організаційних систем і побудована на основі технологій корпоративних обчислювальних мереж. Інформаційна мережа складається з вузлів комутації і ліній зв'язку між ними. У сучасних умовах на інформаційні системи впливають зовнішні фактори (активний або пасивний вплив зовнішнього середовища). В роботі в ролі зовнішніх факторів розуміються DDoS-атаки. За обставин зростання вартості втраченої інформації при сучасному збільшенні інформаційних потоків між філіями підприємства, в умовах обмеженого фінансування і низького рівня захищеності комутаційного устаткування, актуальною є задача побудови функціонально стійкої інформаційної мережі [3-7].

Взаємодія подій в інформаційній системі має, як правило, складну динамічну структуру [8-10]. При цьому глобальні ситуації в системі формуються за допомогою локальних операцій, що називаються умовами реалізації подій. Умова може мати таку ємність: умова не виконана (ємність дорівнює 0), умова виконана (ємність дорівнює 1), умова виконана з n-кратним запасом (ємність дорівнює n, де n – ціле додатне число). Певні поєднання умов дозволяють реалізовуватися деякій події (передумови подій), а реалізація подій змінює деякі умови (післяумови подій), тобто події взаємодіють з умовами, а умови з подіями. Тому для вирішення вказаного завдання достатньо представити інформаційну систему як структуру.

Мета роботи побудувати моделі виявлення та блокування зовнішніх впливів (DDoS-атак), які описують за допомогою мереж Петрі процес аналізу вхідного трафіку на предмет наявності даного типу атак, процес виявлення джерел шкідливого трафіку та їх подальшого блокування, що надає можливість для створення відповідних алгоритмів.

Основна частина. Першим кроком для побудови моделей функціонування інформаційних систем з використанням мереж Петрі є абстрагування від конкретних фізичних та функціональних особливостей її компонентів [11]. Сукупність дій, що виникає як реалізації подій при функціонуванні інформаційної системи, утворюють процес, що породжується цією системою.

В мережах Петрі умови та події представлені абстрактними символами з двох алфавітів, що не перетинаються [12]. Процес зміни станів інформаційної системи, що описаний мережею Петрі, представлений на рис. 1. Умови-місця та події-переходи пов'язані відношенням безпосередньої залежності (безпосереднім причинно-наслідковим зв'язком), що зображується за допомогою дуг, які ведуть з місць в переходи, а з переходів в місця. Місця, з яких ведуть дуги на даний перехід, називаються його вхідними місцями. Місця, на які ведуть дуги з даного переходу, називаються його вихідними місцями.

В мережі, зображеній на рис. 1 показані стани інформаційної системи, що мають місце в процесі її функціонування. Місця p_1 та p_2 являються вхідними для переходу t_1, а місця p_3 та p_4 – вихідними. В даному випадку подія-перехід t_1 безпосередньо залежить від місць-умов p_1 та p_2, а місця p_3 та p_4 безпосередньо залежать від t_1.

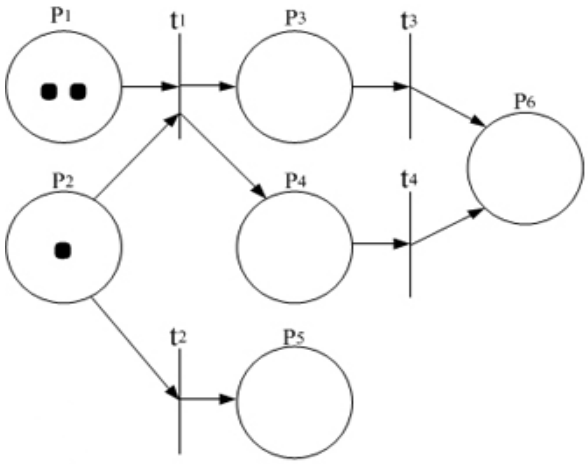

Рис. 1. Процес зміни станів інформаційної системи, що описаний мережею Петрі

В цій же мережі місце p_2 є вхідним одночасно для двох переходів t_1 та t_2, місце p_6 є вихідним одночасно для двох переходів t_3 та t_4.

Перейдемо до побудови моделі виявлення та класифікації DDoS-атак, що представлена на рис. 2.

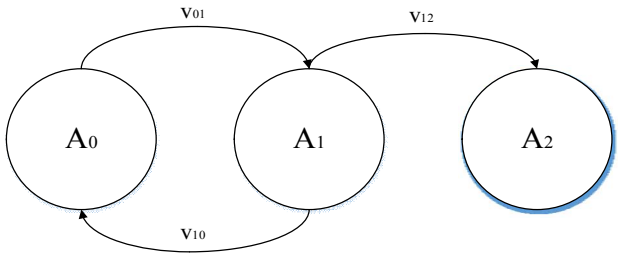

Рис. 2. Графова модель виявлення та класифікації зовнішніх впливів (DDoS-атак) на інформаційну систему

Стан A_0 – обмін пакетами з користувачами, нормальне функціонування інформаційної системи.

Стан A_1 – фіксація перевищень граничного рівня завантаженості каналу зв'язку інформаційної системи.

Стан A_2 – вивід повідомлення про наявність DDoS-атаки та її типу, запуск процесу виявлення джерел шкідливого трафіку.

Перехід v_{01} – перевищення граничного рівня завантаженості каналу зв'язку інформаційної системи або наявність одного піку трафіку.

Перехід v_{10} – перевищення граничного рівня завантаженості каналу зв'язку було менше, ніж три секунди, або не надійшов другий пік трафіку.

Перехід v_{12} – перевищення граничного рівня завантаженості каналу зв'язку було три секунди та більше, або надійшов другий пік трафіку.

Розглянута вище графова модель виявлення та класифікації DDoS-атак віддзеркалює принцип аналізу вхідного трафіку на предмет наявності даного класу атак, але не відображає деталей цього процесу. Тому перейдемо до розгляду детальної моделі виявлення DDoS-атак, що представлена мережею Петрі, зображеною на рис. 3.

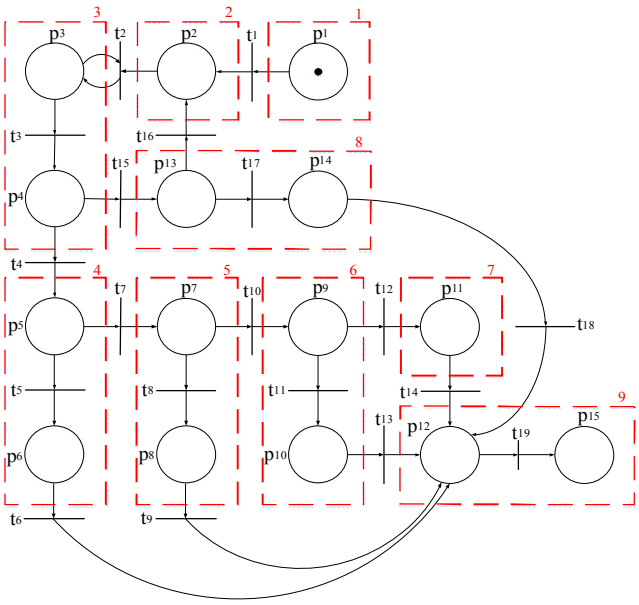

Рис. 3. Модель виявлення та класифікації DDoS-атак

На початку аналізу вхідного трафіку на предмет наявності DDoS-атаки токен знаходиться у місці p_1. Після спрацювання переходу t_1 токен переміщується у місце p_2, і починається обмін пакетами з користувачами інформаційної системи. Далі спрацьовує перехід t_2, токен переміщується в місце p_3, і виконується перевірка рівня завантаженості каналу зв'язку. Якщо перевищення граничного рівня завантаженості не зафіксовано, спрацьовує перехід t_2, і токен залишається в місці p_3. Таким чином, при відсутності перевищення граничного рівня завантаженості токен знаходиться в місці p_3. Якщо фіксується перевищення впродовж однієї секунди, то спрацьовує перехід t_3, і токен переміщується в місце p_4. На даному кроці знову перевіряється завантаженість каналу зв'язку. Якщо вона не перевищує граничний рівень протягом однієї секунди, то спрацьовує перехід t_{15}, і токен переміщується в місце p_{13}. Якщо протягом наступної секунди перевищення не було зафіксовано, то спрацьовує перехід t_{16}, і токен переходить у місце p_2. Якщо перевищення зафіксовано, спрацює перехід t_{17}, токен перейде до місця p_{14}, що призведе до виводу повідомлення про наявність повільної DDoS-атаки. Після чого спрацює перехід t_{18}, токен перейде до місця p_{12}. Якщо при знаходженні токена в місці p_4, спрацює перехід t_4, токен опиниться в місці p_5, та буде перевірено чи мають вхідні сегменти порт призначення 80 (протокол HTTP). Якщо так, то спрацює перехід t_5, буде виведено повідомлення про наявність HTTP-флуда,

після чого спрацює перехід t_6, і токен перейде до місця p_{12}. Якщо ні, то спрацює перехід t_7, токен перейде до місця p_7, і буде перевірено чи протоколом транспортного рівня вхідних сегментів є ICMP. Якщо так, то спрацює перехід t_8, токен перейде до місця p_8, і буде виведено повідомлення про наявність ICMP-флуда, після чого спрацює перехід t_9, та токен опиниться в місці p_{12}. Якщо ні, то спрацює перехід t_{10}, токен перейде до місця p_9, і буде перевірено чи протоколом транспортного рівня вхідних сегментів є UDP. Якщо так, то спрацює перехід t_{11}, токен перейде до місця p_{10}, і буде виведено повідомлення про наявність UDP-флуда, після чого спрацює перехід t_{13}, і токен опиниться в місці p_{12}. Якщо ні, то спрацює перехід t_{12}, токен перейде до місця p_{11}, та буде виведено повідомлення про наявність SYN-флуду. Після чого спрацює перехід t_{14}, і токен переходить до місця p_{12}. Після потрапляння токена у місце p_{12} запускається механізм виявлення джерел шкідливого трафіку, після чого виконується перехід t_{19} та завершення механізму виявлення та класифікації DDoS-атак.

Для опису взаємозв'язків місць та переходів даної мережі Петрі розглянемо її функцію інцидентності:

$$\Phi(p,t) = \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}. \quad (1)$$

Для аналізу динаміки можливих змін розмітки представленої мережі Петрі розглянемо її граф досяжності, що приведений на рис. 4.

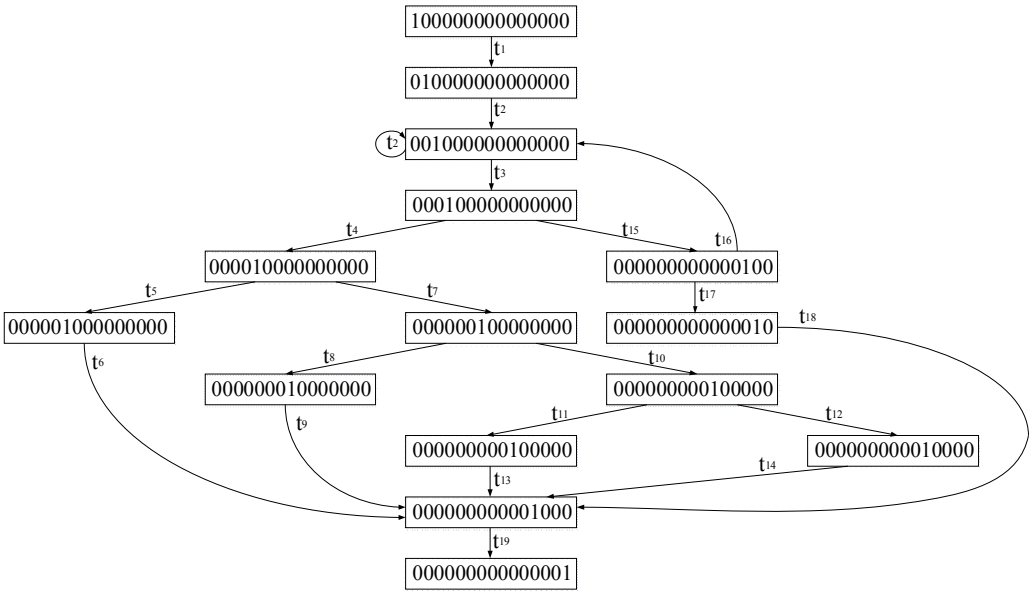

Рис. 4. Граф розміток мережі Петрі, що описує механізм аналізу вхідного трафіку

Сутність даної моделі додатково розкривається функціональною схемою її роботи. Дана схема зображена пунктирною лінією. Блок 1 показує початок аналізу вхідного трафіку на предмет наявності DDoS-атаки. Це початок роботи мережі Петрі. Блок 2 відображає обмін даними з легітимними користувачами мережі. При відсутності атаки постійно спрацьовує перехід t_2, і виконується перевірка завантаженості каналу зв'язку. Якщо вона не перевищує граничний рівень, то робота мережі продовжується в блоці 2, що є показником нормального функціонування ІТМ. В противному випадку в блоці 3 визначається характер перевищення. Якщо воно має суцільний характер протягом інтервалу очікування, виконується перехід до блоку 4, в якому перевіряється наявність на прикладному рівні протоколу HTTP. Якщо даний протокол виявлений, робиться висновок про наявність HTTP-флуду і виконується перехід до блоку 9, де запускається процес блокування атаки. Якщо HTTP не виявлений робиться перехід до блоку 5, в якому перевіряється наявність на транспортному рівні протоколу ICMP. У разі його виявлення робиться висновок про наявність ICMP-флуду і виконується перехід до блоку 9. В противному випадку – перехід до блоку 6, в якому перевіряється наявність на транспортному рівні протоколу UDP. Якщо він виявлений робиться висновок про наявність UDP-флуду і виконується пе-

рехід до блоку 9. В противному випадку робиться перехід до блоку 7, де робиться висновок про наявність SYN-флуду, після чого виконується перехід до блоку 9. Якщо в блоці 3 виявлені піки трафіку, виконується перехід до блоку 8, де робиться висновок про наявність повільної DDoS-атаки, після чого виконується перехід до блоку 9.

Розглянемо графову модель виявлення джерел шкідливого трафіку, що представлена на рис. 5.

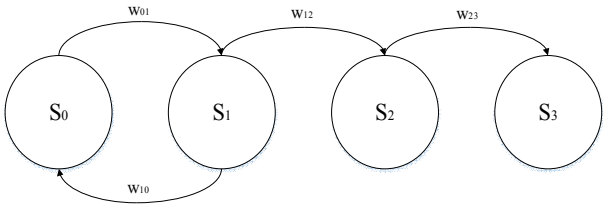

Рис. 5. Графова модель блокування DDoS-атак

Стан S_0 – виділення в базі даних вхідних сегментів, що прибули впродовж трьох секунд від початку атаки.

Стан S_1 – сортування виділених сегментів по вихідному програмному порту.

Стан S_2 – визначення програмного порта, з якого прибула найбільша кількість сегментів.

Стан S_3 – запуск процесу блокування шкідливого трафіку.

Перехід w_{01} – знайдені сегменти, що прибули впродовж трьох секунд від початку атаки.

Перехід w_{10} – сегменти, що прибули впродовж трьох секунд від початку атаки, не знайдені.

Перехід w_{12} – сортування сегментів по вихідному програмному порту завершено, перехід до визначення порта, з якого прибула найбільша кількість сегментів.

Перехід w_{23} – порт, з якого прибула найбільша кількість сегментів, визначений, перехід до блокування шкідливого трафіку.

Розглянута вище графова модель виявлення джерел шкідливого трафіку не відображає деталей цього процесу. Тому перейдемо до розгляду детальної моделі виявлення DDoS-атак, що представлена мережею Петрі, зображеною на рис. 6.

При запуску механізму блокування DDoS-атаки токен знаходиться в місці p_1, спрацьовує перехід t_1, і токен опиняється в місці p_2, де перевіряється тип атаки. Після цього спрацьовує перехід t_2, токен переходить в місце p_3, і виконується підключення до бази даних. Далі якщо спрацьовує перехід t_3, токен переміщується в місце p_4, що означає наявність повільної DDoS-атаки. Якщо має місце флуд, то спрацьовує перехід t_4, і токен переходить до місця p_5. Після цього токен шляхом спрацювання переходу t_5 або t_6 потрапляє до місця p_6, в якому визначається джерело шкідливого трафіку (зовнішнє або внутрішнє). Якщо джерело внутрішнє, то спрацьовує перехід t_7, і токен переходить до місця p_7, де виконується сортування вихідних IP-адрес джерел шкідливого трафіку за кількістю пакетів від більшого до меншого.

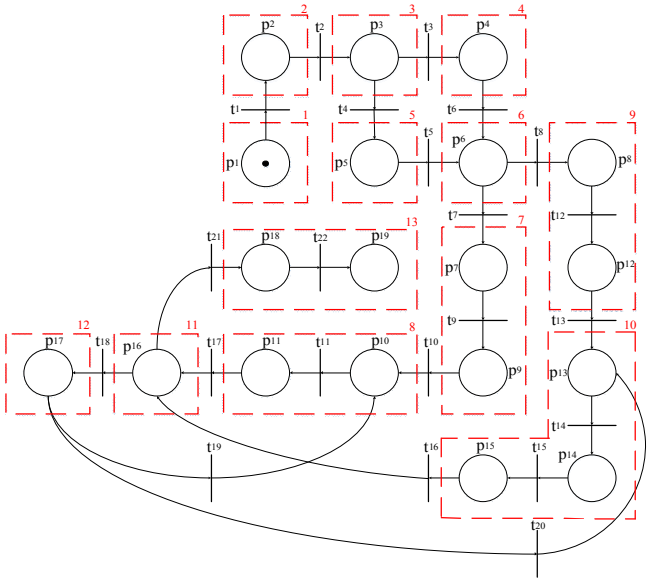

Рис. 6. Модель блокування DDoS-атак

Після цього спрацьовує перехід t_9, і токен опиняється в місці p_9, де виконується запис відсортованого списку у відповідну таблицю бази даних. Далі спрацьовує перехід t_{10}, токен потрапляє в місце p_{10}, де виконується відключення порта комутатора, з якого надходять пакети з IP-адреси, першої в списку. Після цього спрацьовує перехід t_{11}, токен потрапляє в місце p_{11}, де виконується видалення зі списку IP-адрес першої. Якщо джерело зовнішнє, спрацьовує перехід t_8, токен потрапляє в місце p_8, де виконується обробка зчитаної з бази даних інформації, а саме сортування вихідних програмних портів джерел шкідливого трафіку за кількістю сегментів від більшого до меншого. Далі спрацьовує перехід t_{12}, токен потрапляє в місце p_{12}, де виконується запис відсортованого списку у відповідну таблицю бази даних. Після цього спрацьовує перехід t_{13}, токен потрапляє в місце p_{13}, де виконується відправлення сегментів-відповідей на перший в списку порт по резервному каналу зв'язку. Далі спрацьовує перехід t_{14}, токен потрапляє в місце p_{14}, де виконується підміна вихідної IP-адреси вихідних пакетів сервера адресою програмного шлюзу. Після цього спрацьовує перехід t_{15}, токен потрапляє в місце p_{15}, і виконується видалення першого в списку порта. Далі внаслідок спрацювання переходу t_{15} або t_{16} токен потрапляє в місце p_{16}, де перевіряється завантаженість каналу зв'язку. Якщо вона перевищує граничну, то спрацьовує перехід t_{18}, токен потрапляє в місце p_{17}, де перевіряється джерело атаки. В залежності від типу атаки спрацьовує або перехід t_{19}, або t_{20}, токен потрапляє або в місце p_{10}, або в p_{13} відповідно. Якщо завантаженість менше граничної, спрацьовує перехід t_{21}, і токен переходить в місце p_{18}, в якому

виводиться повідомлення, що атака заблокована. Далі спрацьовує перехід t_{22}, токен потрапляє в місце p_{19}, і процес блокування завершується.

Для опису взаємозв'язків місць та переходів даної мережі Петрі розглянемо її функцію інцидентності:

$$\Phi(p, t) =$$

$$= \begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}. \quad (2)$$

Для аналізу динаміки можливих змін розмітки представленої мережі Петрі розглянемо її граф досяжності, що приведений на рис. 7.

Сутність даної моделі додатково розкривається функціональною схемою її роботи. Дана схема зображена пунктирною лінією. Блок 1 відображає початок блокування виявленої атаки. В блоці 2 перевіряється тип атаки, після цього в блоці 3 виконується підключення до бази даних, в якій зчитується інформація про вхідний трафік в заданому інтервалі часу. Якщо атака повільна, то виконується перехід до блоку 4, якщо флуд – то до блоку 5. Далі робота мережі переміщується в блок 6, в якому визначається джерело шкідливого трафіку (зовнішнє або внутрішнє). Якщо джерело внутрішнє, то виконується перехід до блоку 7, де виконується обробка зчитаної з БД інформації, а саме сортування вихідних IP-адрес джерел шкідливого трафіку за кількістю пакетів від більшого до меншого, запис відсортованого списку у відповідну таблицю бази даних. Після цього робиться перехід до блоку 8, в якому виконується відключення порту комутатора, з якого надходять пакети з IP-адреси, першої в списку, та видалення зі списку цієї адреси. Якщо джерело зовнішнє, то виконується перехід до блоку 9, де виконується обробка зчитаної з БД інформації, а саме сортування вихідних програмних портів джерел шкідливого трафіку за кількістю сегментів від більшого до меншого, запис відсортованого списку у відповідну таблицю бази даних. Після цього робиться перехід до блоку 10, в якому виконується відправлення сегментів-відповідей на перший в списку порт по резервному каналу зв'язку з підміною вихідної IP-адреси сервера адресою програмного шлюзу, та видалення зі списку вхідних сегментів першого. Після виконання блокування робота мережі переходить до блоку 11, в якому перевіряється завантаженість каналу зв'язку. Якщо вона все ще перевищує граничну, то виконується перехід до блоку 12, в якому перевіряється джерело атаки. В залежності від результату робиться перехід або до блоку 8, або до блоку 10. Якщо перевищення не зафіксовано, то виконується перехід до блоку 13, де виводиться повідомлення, що атака заблокована.

Висновок

Оскільки взаємодія подій в інформаційній системі має, як правило, складну динамічну структуру, тому можливе використанням мереж Петрі з метою створення моделей виявлення та блокування зовнішніх впливів (DDoS-атак). Дані моделі засновані на описі структури інформаційної системи, на яку здійснюється вплив даною атакою, та процесів зміни станів цієї системи.

Створені моделі виявлення та блокування DDoS-атак, які описують за допомогою мереж Петрі процес аналізу вхідного трафіку на предмет наявності

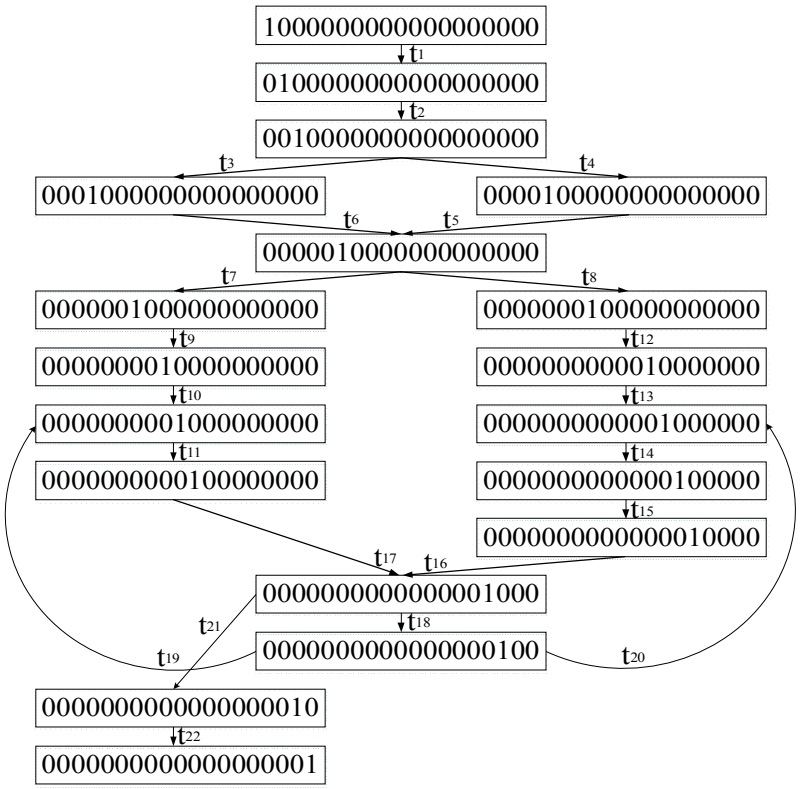

Рис. 7. Граф розміток мережі Петрі, що описує механізм блокування DDoS-атак

даного типу атак, процес виявлення джерел шкідливого трафіку та їх подальшого блокування, що надає можливість для створення відповідних алгоритмів.

Побудовані моделі дозволяють підвищити рівень функціональної стійкості інформаційних систем. Під функціональною стійкістю інформаційної системи розуміється властивість системи перебувати в стані працездатності, тобто виконувати необхідні функції протягом заданого інтервалу часу або наробітки в умовах відмов складових частин через зовнішні і внутрішні фактори.

Список літератури

1. Додонов А.Г. Введение в теорию живучести вычислительных систем / А.Г. Додонов, М.Г. Кузнецова, Е.С. Горбачик; Отв. ред. Гуляев В.А.; АН УССР. Ин-т пробл. регистрации информации. – К.: Наукова думка, 1990. – 184 с.

2. Кравченко Ю.В. Функціональна стійкість – властивість складних технічних систем / Ю.В. Кравченко О.В. Барабаш // Збірник наукових праць. – К.: НАОУ, 2002. – Бюл. № 40. – С. 225-229.

3. Саланда І.П. Математична модель структури розгалуженої інфораційної мережі 5 покоління (5G) на основі випадкових графів / І.П. Саланда, О.В. Барабаш, А.П. Мусієнко, Н.В. Лукова-Чуйко // Наукове періодичне видання «Системи управління, навігації та зв'язку». – Полтава: ПНТУ, 2017. – Вип. 6 (46). – С. 118 – 121.

4. Саланда І.П. Система показників та критеріїв формалізації процесів забезпечення локальної функціональної стійкості розгалужених інформаційних мереж / І.П. Саланда, О.В. Барабаш, А.П. Мусієнко // Наукове періодичне видання «Системи управління, навігації та зв'язку». – Полтава: ПНТУ, 2017. – Вип. 1 (41). – С. 122 – 126.

5. V.A. Mashkov, O.V. Barabash Self-checking and Self-diagnosis of Module Systems on the Principle of Walking Diagnostic Kernel Engineering Simulation. – Amsterdam: OPA, 1998. Vol. 15. pp. 43-51.

7. Барабаш О.В. Методика накопичення діагностичної інформації в системах інтелектуального відеоконтролю / О.В. Барабаш, С.В. Бодров, А.П. Мусієнко Системи управління, навігації та зв'язку. – Полтава: ПНТУ, 2015. – Вип. 1 (33). – С. 118 – 121.

8. Барабаш О.В. Алгоритм самодіагностування технічного стану вузлів комутації інформаційних систем / О.В. Барабаш, Д.М. Обідін, А.П. Мусієнко // Сучасний захист інформації. – К.: № 2 – 2014. – С. 114- 121.

9. Лукова-Чуйко Н.В. Математична модель взаємовідносин загроз та комплексних систем захисту інформації / Н.В. Лукова-Чуйко // Вісник інженерної академії України. – № 3. – 2015 р. – С. 131-135.

10. Лукова-Чуйко Н.В. Метод мінімізації середньої затримки пакетів у віртуальних з'єднаннях мережі підтримки хмарного сервісу / Г.А. Кучук, А.А. Коваленко, Н.В. Лукова-Чуйко // Системи управління, навігації та зв'язку – № 2(42) – 2017. – С. 117 – 120.

11. Лукова-Чуйко Н.В. Метод прихованої передачі даних в інформаційних системах із застосуванням стеганографії / О.В. Барабаш, Н.В. Лукова-Чуйко, А.П. Мусієнко, А.О. Смірнов // Сучасний захист інформації: науково-технічний журнал. – К.: ДУТ, 2017. – № 4. – С. 43 – 49.

12. Котов В.Е. Сети Петри / В.Е. Котов. – М.: Наука. Главная редакция физико-математической литературы, 1984. – 158 с.

13. Лукова-Чуйко Н.В. Ефективність управління ресурсами e-learning в гіперконвергентному середовищі / Н.Г. Кучук, Н.В. Лукова-Чуйко // Системи управління, навігації та зв'язку. – Полтава: ПНТУ, 2018. – Вип. 1 (47). – С. 123 – 126.

Надійшла до редколегії 21.02.2018

Рецензент: д-р техн. наук, проф. О.О. Можаєв, Національний технічний університет «ХПІ», Харків.

ИСПОЛЬЗОВАНИЕ СЕТЕЙ ПЕТРИ ДЛЯ ПОСТРОЕНИЯ МОДЕЛИ ВЫЯВЛЕНИЯ ВНЕШНИХ ВОЗДЕЙСТВИЙ НА ИНФОРМАЦИОННУЮ СИСТЕМУ

Н.В. Лукова-Чуйко, А.П. Мусиенко, М.А. Коваль

В работе показано, что информационная система, имеет, как правило, сложную динамическую структуру, поэтому возможно использованием сетей Петри с целью создания моделей выявления и блокирования внешних воздействий (DDoS-атак). Данные модели основаны на описании структуры информационной системы, на которую оказывается воздействие данной атакой, и процессов изменения состояний этой системы. Созданные модели выявления и блокирования DDoS-атак, которые описывают с помощью сетей Петри процесс анализа входящего трафика на предмет наличия данного типа атак, процесс выявления источников вредоносного трафика и их дальнейшего блокирования, что дает возможность для создания соответствующих алгоритмов. Построенные модели позволяют повысить уровень функциональной устойчивости информационных систем. Под функциональной устойчивостью информационной системы понимается свойство системы находиться в состоянии работоспособности, то есть выполнять необходимые функции в течение заданного интервала времени или наработки в условиях отказов составных частей через внешние и внутренние факторы.

Ключевые слова: *функциональная устойчивость, информационная система, сети Петри, DDoS-атака.*

USE OF PETRI NETWORK FOR CONSTRUCTION FOR EXTERNAL EFFECTS DETECTION ON THE INFORMATION SYSTEM

N.V. Lukova-Chuiko, A.P. Musienko, M.O. Koval

In this paper it is shown that, the information system has, as a rule, a complex dynamic structure, so it is possible to use Petri Networks to create models for detecting and blocking external influences (DDoS attacks). These models are based on the description of the structure of the information system, which is influenced by this attack and processes of changing the states of this system. Models for detecting and blocking DDoS attacks, which describes the process of analyzing incoming traffic for the presence of this type of attack using the Petri Networks, the process of detecting sources of malicious traffic and their subsequent blocking, which provides the ability to create appropriate algorithms are created. The built models allow to increase the level of functional stability of information systems. Under the functional stability of the information system is understood the property of the system to be in a state of efficiency, that is, to perform the necessary functions within the given interval of time or works in the conditions of refusals of component parts through external and internal factors.

Keywords: *functional stability, information system, Petri Networks, DDoS-attack.*