7. *Беллман Р., Кук Л.Л.* Дифференциально-разностные уравнения / Р. Беллман, Л.Л. Кук. — М. : Мир, 1967. — 548 с.

8. *Хейл Дж.* Теория функционально-дифференциальных уравнений / Дж. Хейл. — М. : Мир, 1984. — 425 с.

9. *Akhmet M.U., Alzabut J., Zafer A.* Perron's theorem for linear impulsive differential equations with distributed delay // Journal of Computational and Applied Mathematics — 2006. — 193. — P. 204–218.

10. *Егорова Н.Е.* Дифференциальный анализ развития малых предприятий, использующих кредитно-инвестиционный ресурс / Егорова Н.Е., Хачатрян С.Р., Маренный М.А. // Аудит и финансовый анализ. — 2000. — № 4 — С. 444-458.

УДК 004.042

Ігнатова Ю. В., к.е.н., ст. викладач
кафедри економіко-математичного моделювання,
Бєгун А. В., к.е.н., проф.,
професор кафедри інформаційного менеджменту,
Київський національний економічний університет імені Вадима Гетьмана

МОДЕЛЮВАННЯ ПРОАКТИВНОГО ВИЗНАЧЕННЯ DDoS-атаки

АНОТАЦІЯ. У статті запропоновано представити роботу інформаційного вузла, який атакується великою кількістю зовнішніх запитів, у вигляді стохастичної моделі масового обслуговування. Запропонована модель та визначені на її основі системні характеристики (ймовірність простою. ймовірність скоєння атаки. середні кількості легальних і нелегальних запитів) дозволяють кількісно оцінити рівень інформаційної безпеки досліджуваного об'єкта.

КЛЮЧОВІ СЛОВА: інформаційна безпека, DDoS-атака, модель масового обслуговування, пуассонівський вхідний потік запитів.

АННОТАЦИЯ. В статье представлена работа информационного узла, атакуемого большим числом внешних запросов, в виде стохастической модели массового обслуживания. Предложенная модель и определенные на ее основе системные характеристики (вероятность простоя, вероятность совершения атаки, среднее число легальных и нелегальных запросов) позволяют количественно оценить уровень информационной безопасности исследуемого объекта.

КЛЮЧЕВЫЕ СЛОВА: информационная безопасность, DDoS-атака, модель массового обслуживания, пуассоновский входной поток требований.

ABSTRACT. Article describes a system which is attacked by a large number of external requests. The proposed stochastic queuing model helps to identify basic system characteristics of the functioning node (the probability of committing the attacks, the average numbers of legal and illegal requests) and quantify the level of information security of the object.

KEY WORDS: information security, DDoS-attack, queuing model, Poisson input flow requirements.

Вступ. Важливою умовою існування бізнесу є достатньо високий рівень інформаційної безпеки компаній, який передбачає захист інформації від випадкових і навмисних нападів, здатних нанести збитки як користувачам, так і власникам інформації. Сучасні методи оброблення, передачі та накопичення інформації сприяли появі нових і розвитку існуючих загроз, які пов'язані із втратами інформації, її перекручуванням та розкриттям. Вочевидь збитки від порушення рівня інформаційної безпеки можуть призвести до великих фінансових втрат і навіть до повного закриття компанії.

Аналіз останніх публікацій з проблеми дослідження загроз інформаційній безпеці бізнесу [1–3, 6–7] дозволяє стверджувати, що в умовах кризи компанії повинні орієнтуватися на обслуговування семи найбільш небезпечних загроз: витоку інформації, інформаційних атак, DDoS-атак, цільових атак і промислового шпигунства, крадіжок у банків та їх клієнтів, внутрішніх крадіжок і шкідництва, зменшення бюджету на інформаційну безпеку. Серед цих загроз слід відзначити найбільш небезпечні — DDoS-атаки: за останній рік їх чисельність подвоїлася, а половина з них була мультивекторною. До того ж кількість DDoS-атак зі швидкістю 100 ГБ у секунду зросла на 200 %, а їх тривалість збільшилась на 28 % [6].

Лідером серед країн за кількістю DDoS-атак є США як одна із провідних країн з розвитку і впровадження сучасних інформаційних

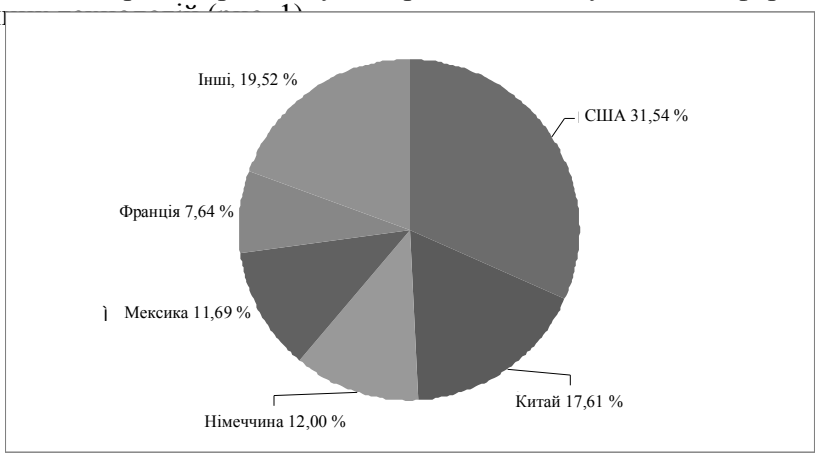

Рис. 1. Країни, що найбільше потерпають від DDoS-атак

Джерело: Сформовано на основі [6].

За розташуванням джерела загрози такі атаки підрозділяються на локальні та віддалені. Найпростіший приклад віддаленого споживання ресурсів — атака, яка отримала найменування «SYN-повінь», що являє собою спробу переповнити таблицю напіввідкритих TCP-з'єднань сервера. Така атака щонайменше ускладнює встановлення нових з'єднань з боку легальних користувачів, тобто сервер виглядає як недоступний.

Відповіді на такі пакети «з'їдають» смугу пропускання. Віддалені атаки останнім часом проявляються в особливо небезпечній формі — як скоординовані розподілені атаки, тобто коли на сервер з безлічі різних адрес з максимальною швидкістю спрямовуються цілком легальні запити на з'єднання і/або обслуговування. Зазначимо, що якщо має місце архітектурний прорахунок у вигляді розбалансованості між пропускною здатністю мережі й продуктивністю сервера, то захиститися від розподілених DDoS-атак украй важко.

Постановка задачі. Метою даного дослідження є створення моделі впливу DDoS-атаки на вузол інформаційної системи і отримання системних характеристик процесу впливу атаки на стан рівня інформаційної безпеки компанії. Проілюструємо умовний приклад віддаленої DDoS-атаки на основі стохастичної моделі масового обслуговування з пуассонівським вхідним потоком запитів з метою визначення найуразливіших місць вузла та визначення шляхів попередження загрози.

Розглянемо систему, що складається з одного вузла, який має k каналів обробки інформації, в черзі на обслуговування до яких може надходити n найпростіших запитів: з параметром λ_1, якщо на канал обслуговування надходить безпечний запит; з параметром λ_0, якщо на канал обслуговування надходить нелегальний запит — флуд; з параметром λ_0^*, якщо на вільний канал обслуговування надходить флуд, як шпигун-розвідник. Час обслуговування безпечного запиту каналом розподілено за експоненціальним законом з інтенсивністю μ_1. Час обслуговування флуду розподілено за експоненціальним законом з інтенсивністю μ_0, а при надходженні флуду запит, який знаходиться на обслуговуванні, втрачається (залишає систему). Докладніше схему функціонування вузла представлено на рис. 2.

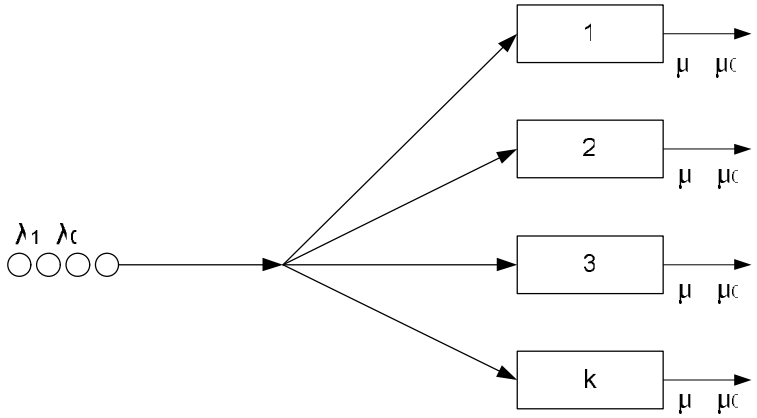

Рис. 2. Схема обробки вузлом легальних та нелегальних запитів

Джерело: Сформовано авторами самостійно

Основна частина. Стохастична модель функціонування вузла, яка представлена системою диференціальних рівнянь, у динаміці (при нескінченно великій черзі) має такий вигляд:

$$P'_{0,0(0,k)}(t) = -\left(\lambda_1 + \lambda_0^*\right)P_{0,0(0,k)}(t) + \mu_1 P_{0,0(1,k-1)}(t) + \mu_0 Q_{0,1(0,k-1)}(t)$$

$$\vdots$$

$$P'_{0,0(m,k-m)}(t) = -\left(\lambda_1 + \lambda_0 + \lambda_0^* + m\mu_1\right)P_{0,0(m,k-m)}(t) + \lambda_1 P_{0,0(m-1,k-m+1)}(t) +$$

$$+ (m+1)\mu_1 P_{0,0(m+1,k-m-1)}(t) + \mu_0 Q_{0,1(m,k-m-1)}(t)$$

$$\vdots \quad (1)$$

$$P'_{0,0(k,0)}(t) = -\left(\lambda_1 + \lambda_0 + k\mu_1\right)P_{0,0(k,0)}(t) + \lambda_1 P_{0,0(k-1,1)}(t) +$$

$$+ k\mu_1 P_{1,0(k,0)}(t) + \mu_0 Q_{1,1(k-1,0)}(t)$$

$$\vdots$$

$$P'_{n,0(k,0)}(t) = -\left(\lambda_1 + \lambda_0 + k\mu_1\right)P_{n,0(k,0)}(t) + \lambda_1 P_{n-1,0(k,0)}(t) +$$

$$+ k\mu_1 P_{n+1,0(k,0)}(t) + \mu_0 Q_{n+1,1(k,0)}(t)$$

$$\vdots$$

$$Q'_{0,p(0,k-p)}(t) = -\left(\lambda_1 + \lambda_0^* + p\mu_0\right)Q_{0,p(0,k-p)}(t) + (p+1)\mu_0 Q_{0,p+1(1,k-p-1)}(t) +$$

$$+ \mu_1 Q_{0,p(1,k-p-1)}(t) + \lambda_0 Q_{0,p-1(1,k-p)}(t) + \lambda_0^* Q_{0,p-1(0,k-p+1)}(t)$$

$$\vdots$$

$$Q'_{0,p(m,k-m-p)}(t) = -\left(\lambda_1 + \lambda_0 + \lambda_0^* + m\mu_1 + p\mu_0\right)Q_{0,p(m,k-m-p)}(t) +$$
$$+ \lambda_1\mu_0 Q_{0,p(m-1,k-m-p+1)}(t) + (p+1)\mu_0 Q_{0,p+1(m,k-m-p-1)}(t) +$$
$$+ (m+1)\mu_1 Q_{0,p(m+1,k-m-p-1)}(t) + \lambda_0 Q_{0,p-1(m+1,k-m-p)}(t) + \lambda_0 Q_{0,p-1(m,k-m-p-1)}(t)$$
$$\vdots$$
$$Q'_{n,p(k-p,0)}(t) = -\left(\lambda_1 + \lambda_0 + p\mu_0 + (k-p)\mu_1\right)Q_{n,p(k-p,0)}(t) +$$
$$+ \lambda_1 Q_{n-1,p(k-p,0)}(t) + +(p+1)\mu_0 Q_{n+1,p+1(k-p-1,0)}(t) +$$
$$+ (k-p-1)\mu_1 Q_{n+1,p(k-p-1,0)}(t)$$

У моделі (1) нумерація станів функціонування вузла представлена ймовірностями $P_{n,0(k,0)}(t)$, $P_{0,0(m,k-m)}(t)$ та $Q_{n,p(m,k-m-p)}(t)$, де p — кількість можливих надходжень флуду, p = 1, 2, 3, …; k — кількість каналів обслуговування, k = 1, 2, 3, …; m — кількість вільних каналів обслуговування $m = \overline{1,k}$; n — розмір черги безпечних запитів n = 1, 2, 3, … . Причому в тому випадку, якщо на обслуговування до працюючих каналів надходять тільки безпечні запити, то маємо стани $P_{n,0(k,0)}(t)$ або $P_{0,0(m,k-m)}(t)$, а в тому випадку, якщо вузол атакується флудом, — $Q_{n,p(m,k-m-p)}(t)$.

Так, наприклад, стан $Q_{n,p(m,k-m-p)}(t)$ показує, що в момент часу t в черзі знаходиться n безпечних запитів, p — запитів флуду, m — каналів зайнято, $k-m-p$ — каналів є вільними; стан $P_{n,0(k,0)}(t)$ показує, що в системі відсутній флуд, усі k — каналів є зайнятими безпечними запитами, а вільні канали відсутні.

Для конкретного розміру черги модель (1) може бути представлена таким чином. Наприклад, візьмемо розмір черги n = 4, кількість каналів обслуговування k = 4. Тоді стохастична модель (1) у стаціонарному режимі роботи, тобто незалежно від часу t, може бути подана у вигляді

$$\begin{aligned}
&(\lambda_1 + \lambda_0^*)P_{0,0(0,4)} = \mu_1 P_{0,0(1,3)} + \mu_0 Q_{0,1(0,3)}\\
&\left(\lambda_1 + \lambda_0 + \lambda_0^* + \mu_1\right)P_{0,0(1,3)} = \lambda_1 P_{0,0(0,4)} + 2\mu_1 P_{0,0(2,2)} + \mu_0 Q_{0,1(1,2)}\\
&\left(\lambda_1 + \lambda_0 + \lambda_0^* + 2\mu_1\right)P_{0,0(2,2)} = \lambda_1 P_{0,0(1,3)} + 3\mu_1 P_{0,0(3,1)} + \mu_0 Q_{0,1(2,1)}\\
&\left(\lambda_1 + \lambda_0 + \lambda_0^* + 3\mu_1\right)P_{0,0(3,1)} = \lambda_1 P_{0,0(2,2)} + 4\mu_1 P_{0,0(4,0)} + \mu_0 Q_{0,1(3,0)}\\
&\left(\lambda_1 + \lambda_0 + 4\mu_1\right)P_{0,0(4,0)} = \lambda_1 P_{0,0(3,1)} + 4\mu_1 P_{1,0(4,0)} + \mu_0 Q_{1,1(3,0)}\\
&\left(\lambda_1 + \lambda_0 + 4\mu_1\right)P_{1,0(4,0)} = \lambda_1 P_{0,0(4,0)}(t) + 4\mu_1 P_{2,0(4,0)} + \mu_0 Q_{2,1(3,0)}
\end{aligned} \qquad (2)$$

$$(\lambda_1+\lambda_0+4\mu_1)P_{2,0(4,0)} = +\lambda_1 P_{1,0(4,0)} + 4\mu_1 P_{3,0(4,0)} + \mu_0 Q_{3,1(3,0)}$$
$$(\lambda_1+\lambda_0+4\mu_1)P_{3,0(4,0)} = \lambda_1 P_{2,0(4,0)} + 4\mu_1 P_{4,0(4,0)} + \mu_0 Q_{4,1(3,0)}$$
$$(\lambda_0+4\mu_1)P_{4,0(4,0)} = \lambda_1 P_{3,0(4,0)}$$
$$(\lambda_1+\lambda_0^*+\mu_0)Q_{0,1(0,3)} = \lambda_0 P_{0,0(1,3)} + 2\mu_0 Q_{0,2(0,2)} + \mu_1 Q_{0,1(1,2)} + \lambda_0^* P_{0,0(0,4)}$$
$$(\lambda_1+\lambda_0^*+2\mu_0)Q_{0,2(0,2)} = \lambda_0 Q_{0,1(1,2)} + 3\mu_0 Q_{0,3(0,1)} + \mu_1 Q_{0,2(1,1)} + \lambda_0^* Q_{0,1(0,3)}$$
$$(\lambda_1+\lambda_0^*+3\mu_0)Q_{0,3(0,1)} = \lambda_0 Q_{0,2(1,1)} + 4\mu_0 Q_{0,4(0,0)} + \mu_1 Q_{0,3(1,0)} + \lambda_0^* Q_{0,2(0,2)}$$
$$(\lambda_1+4\mu_0)Q_{0,4(0,0)} = \lambda_0 Q_{0,3(1,0)} + \lambda_0^* Q_{0,3(0,1)}$$
$$(\lambda_1+\lambda_0+\mu_0+3\mu_1)Q_{1,1(3,0)} = \lambda_1 Q_{0,1(3,0)} + 2\mu_0 Q_{2,2(2,0)} +$$
$$+ 3\mu_1 Q_{2,1(3,0)} + \lambda_0 P_{1,0(4,0)}$$
$$(\lambda_1+\lambda_0+\mu_0+3\mu_1)Q_{2,1(3,0)} = \lambda_1 Q_{1,1(3,0)} + 2\mu_0 Q_{3,2(2,0)} +$$
$$+ 3\mu_1 Q_{3,1(3,0)} + \lambda_0 P_{2,0(4,0)}$$
$$(\lambda_1+\lambda_0+\mu_0+3\mu_1)Q_{3,1(3,0)} = \lambda_1 Q_{2,1(3,0)} + 2\mu_0 Q_{4,2(2,0)} +$$
$$+ 3\mu_1 Q_{4,1(3,0)} + \lambda_0 P_{3,0(4,0)}$$
$$(\lambda_0+\mu_0+3\mu_1)Q_{4,1(3,0)} = \lambda_1 Q_{3,1(3,0)} + \lambda_0 P_{4,0(4,0)}$$
$$(\lambda_1+\lambda_0+2\mu_0+2\mu_1)Q_{1,2(2,0)} = \lambda_1 Q_{0,2(2,0)} + 3\mu_0 Q_{2,3(1,0)} +$$
$$+ 2\mu_1 Q_{2,2(2,0)} + \lambda_0 Q_{1,1(3,0)}$$
$$(\lambda_1+\lambda_0+3\mu_0+\mu_1)Q_{1,3(1,0)} = \lambda_1 Q_{0,3(1,0)} + 4\mu_0 Q_{2,4(0,0)} +$$
$$+ \mu_1 Q_{2,3(1,0)} + \lambda_0 Q_{1,2(2,0)}$$
$$(\lambda_1+4\mu_0)Q_{1,4(0,0)} = \lambda_1 Q_{0,4(0,0)} + \lambda_0 Q_{1,3(1,0)}$$
$$(\lambda_1+\lambda_0+2\mu_0+2\mu_1)Q_{2,2(2,0)} = \lambda_1 Q_{1,2(2,0)} + 2\mu_1 Q_{3,2(2,0)} +$$
$$+ 3\mu_0 Q_{3,3(1,0)} + \lambda_0 Q_{2,1(3,0)}$$
$$(\lambda_1+\lambda_0+3\mu_0+\mu_1)Q_{2,3(1,0)} = \lambda_1 Q_{1,3(1,0)} + \mu_1 Q_{3,3(1,0)} +$$
$$+ 4\mu_0 Q_{3,4(0,0)} + \lambda_0 Q_{2,2(2,0)}$$
$$(\lambda_1+4\mu_0)Q_{2,4(0,0)} = \lambda_1 Q_{1,4(0,0)} + \lambda_0 Q_{2,3(1,0)}$$
$$(\lambda\ +\lambda_0+2\mu_0+2\mu_1)Q_{3,2(2,0)} = \lambda_1 Q_{2,2(2,0)} + 2\mu_1 Q_{4,2(2,0)} +$$
$$+ 3\mu_0 Q_{4,3(1,0)} + \lambda_0 Q_{3,1(3,0)}$$

$$
\begin{aligned}
&(\lambda_1+\lambda_0+3\mu_0+\mu_1)Q_{3,3(1,0)}=\lambda_1 Q_{2,3(1,0)}+\mu_1 Q_{4,3(1,0)}+\\
&+4\mu_0 Q_{4,4(0,0)}+\lambda_0 Q_{3,2(2,0)}\\
&(\lambda_1+4\mu_0)Q_{3,4(0,0)}=\lambda_1 Q_{2,4(0,0)}+\lambda_0 Q_{3,3(1,0)}\\
&(\lambda_0+2\mu_0+2\mu_1)Q_{4,2(2,0)}=\lambda_1 Q_{3,2(2,0)}+\lambda_0 Q_{4,1(3,0)}\\
&(\lambda_0+3\mu_0+\mu_1)Q_{4,3(1,0)}=\lambda_1 Q_{3,3(1,0)}+\lambda_0 Q_{4,2(2,0)}\\
&4\mu_0 Q_{4,4(0,0)}=\lambda_1 Q_{3,4(0,0)}+\lambda_0 Q_{4,3(1,0)}\\
&(\lambda_1+\lambda_0+\lambda_0^*+\mu_0+\mu_1)Q_{0,1(1,2)}=\lambda_1 Q_{0,1(0,3)}+2\mu_1 Q_{0,1(2,1)}+\\
&+2\mu_0 Q_{0,2(1,1)}+\lambda_0 P_{0,0(2,2)}+\lambda_0^* P_{0,0(1,3)}\\
&(\lambda_1+\lambda_0+\lambda_0^*+\mu_0+2\mu_1)Q_{0,1(2,1)}=\lambda_1 Q_{0,1(1,2)}+3\mu_1 Q_{0,1(3,0)}+\\
&+2\mu_0 Q_{0,2(2,0)}+\lambda_0 P_{0,0(3,1)}+\lambda_0^* P_{0,0(2,2)}\\
&(\lambda_1+\lambda_0+\lambda_0^*+2\mu_0+\mu_1)Q_{0,2(1,1)}=\lambda_1 Q_{0,2(0,2)}+2\mu_1 Q_{0,2(2,0)}+\\
&+3\mu_0 Q_{0,3(1,0)}+\lambda_0 Q_{0,1(2,1)}+\lambda_0^* Q_{0,1(1,2)}\\
&(\lambda_1+\lambda_0+\mu_0+3\mu_1)Q_{0,1(3,0)}=\lambda_1 Q_{0,1(2,1)}+3\mu_1 Q_{1,1(3,0)}+\\
&+2\mu_0 Q_{1,2(2,0)}+\lambda_0 P_{0,0(4,0)}+\lambda_0^* P_{0,0(3,1)}\\
&(\lambda_1+\lambda_0+2\mu_0+2\mu_1)Q_{0,2(2,0)}=\lambda_1 Q_{0,2(1,1)}+2\mu_1 Q_{1,2(2,0)}+\\
&+3\mu_0 Q_{1,3(1,0)}+\lambda_0 Q_{0,1(3,0)}+\lambda_0^* Q_{0,1(2,1)}\\
&(\lambda_1+\lambda_0+3\mu_0+\mu_1)Q_{0,3(1,0)}=\lambda_1 Q_{0,3(0,1)}+\mu_1 Q_{1,3(1,0)}+\\
&+4\mu_0 Q_{1,4(0,0)}+\lambda_0 Q_{0,2(2,0)}+\lambda_0^* Q_{0,2(1,1)}
\end{aligned}
\qquad (2)
$$

Розглянемо особливості стаціонарного режиму функціонування системи (2) докладніше. Введемо такі позначення:

$$\rho_0=\frac{\lambda_0}{\mu_0},\rho_0^*=\frac{\lambda_0^*}{\mu_0},\rho_1=\frac{\lambda_1}{\mu_1}.$$

Використовуючи [4], визначимо ймовірності станів $P_{0,0(m,k-m)}$ та $P_{n,0(k,0)}$ із системи з точністю до $P_{0,0(0,k)}$. З першого рівняння системи (2) маємо $\lambda_1 P_{0,0(0,4)}=\mu_1 P_{0,0(1,3)}\Rightarrow P_{0,0(1,3)}=\rho_1 P_{0,0(0,4)}$. З другого рівняння системи (2) отримаємо $\lambda_1 P_{0,0(1,3)}=2\mu_1 P_{0,0(2,2)}\Rightarrow$

$\Rightarrow P_{0,0(2,2)} = \frac{\rho_1}{2} P_{0,0(1,3)} = \frac{\rho_1^2}{2!} P_{0,0(0,4)}$. Третє рівняння системи (2) надає $\lambda_1 P_{0,0(2,2)} = 3\mu_1 P_{0,0(3,1)} \Rightarrow_1 P_{0,0(3,1)} = \frac{\rho_1}{3} P_{0,0(2,2)}(t) = \frac{\rho_1^2}{3!} P_{0,0(0,4)}$. Тоді стан функціонування вузла під час обробки тільки легальних запитів за відсутності черги $P_{0,0(m,k-m)}$ визначатиметься як $P_{0,0(m,k-m)} = \frac{\rho_1^m}{m!} P_{0,0(0,k)}$.

Аналогічно із системи (1) отримаємо

$\lambda_1 P_{0,0(k,0)} = k\mu_1 P_{1,0(k,0)} \Rightarrow P_{1,0(k,0)} = \frac{\rho_1}{k} P_{0,0(k,0)} = \frac{\rho_1}{k} \cdot \frac{\rho_1^k}{k!} P_{0,0(0,k)} = \frac{\rho_1^{k+1}}{k \cdot k!} P_{0,0(0,k)}$

або $\lambda_1 P_{1,0(k,0)} = k\mu_1 P_{2,0(k,0)} \Rightarrow \quad P_{2,0(k,0)} = \frac{\rho_1}{k} P_{1,0(k,0)} = \frac{\rho_1}{k} \cdot \frac{\rho_1^{k+1}}{k \cdot k!} P_{0,0(0,k)} =$

$= \frac{\rho_1^{k+2}}{k^2 \cdot k!} P_{0,0(0,k)}$. Тоді стан функціонування вузла під час обробки тільки легальних запитів за наявності черги $P_{n,0(k,0)}$ буде мати вигляд $P_{n,0(k,0)} = \frac{\rho_1^n}{k^n} \cdot \frac{\rho_1^k}{k!} P_{0,0(0,k)}$.

Визначимо ймовірності станів системи $Q_{n,p(k-p,0)}$ з точністю до $P_{0,0(0,k)}$, використовуючи властивість збереження потоку [4]. З першого рівняння системи (2) одержимо $\lambda_0 P_{0,0(0,4)} = \mu_0 Q_{0,1(0,3)} \Rightarrow Q_{0,1(0,3)} = \rho_0 P_{0,0(0,4)}$.

Аналогічно можна отримати вираз

$\lambda_0 Q_{0,1(0,3)} = 2\mu_0 Q_{0,2(0,2)} \Rightarrow Q_{0,2(0,2)} = \frac{\rho_0^*}{2} Q_{0,1(0,3)} = \frac{\rho_0^{*2}}{2!} P_{0,0(0,4)}$. Тоді стан функціонування вузла під час обробки тільки нелегальних запитів $Q_{0,p(0,k-p)}$ визначатиметься як $Q_{0,p(0,k-p)} = \frac{\rho_0^{*p}}{p!} P_{0,0(0,k)}$.

Відповідним чином знайдено ймовірності $Q_{n,p(0,0)}$, $Q_{0,p(m,k-m-p)}$, $Q_{n,p(k-p,0)}$ з точністю до $P_{0,0(0,k)}$, а саме: $Q_{n,p(0,0)} = \rho_1^n \cdot \frac{\rho_0^k}{k!} P_{0,0(0,k)}$; $Q_{0,p(m,k-m-p)} = \frac{\rho_1^m}{m!} \cdot \frac{\rho_0^{*p}}{p!} P_{0,0(0,k)}$ та $Q_{n,p(k-p,0)} = \frac{\rho_1^n}{(k-p)^n} \cdot \frac{\rho_1^{k-p}}{(k-p)!} \cdot \frac{\rho_0^p}{p!} P_{0,0(0,k)}$.

Оскільки сума всіх несумісних станів системи, що утворюють повну групу подій, дорівнює одиниці, то, використовуючи умову нормування, знайдемо $P_{0,0(0,k)}$:

$$P_{0,0(0,k)}+\sum_{m=1}^{k}P_{0,0(m,k-m)}+\sum_{n=1}^{\infty}P_{n,0(k,0)}+\sum_{p=1}^{k}Q_{0,p(0,k-p)}+\sum_{m=1}^{k}\sum_{p=1}^{k}Q_{0,p(m,k-m-p)}+$$
$$+\sum_{p=1}^{k-1}\sum_{n=1}^{\infty}Q_{n,p(k-p,0)}+\sum_{n=1}^{\infty}Q_{n,p(0,0)}=1 \qquad (3)$$

Підставимо в (3) знайдені ймовірності:

$$P_{0,0(0,k)}+\sum_{m=1}^{k}\frac{\rho_1^m}{m!}P_{0,0(0,k)}+\frac{\rho_1^k}{k!}\sum_{n=1}^{\infty}\frac{\rho_1^n}{k^n}P_{0,0(0,k)}+\sum_{p=1}^{k}\frac{\rho_0^{*p}}{p!}P_{0,0(0,k)}+$$
$$+\sum_{m=1}^{k}\sum_{p=1}^{k}\frac{\rho_1^m}{m!}\cdot\frac{\rho_0^{*p}}{p!}P_{0,0(0,k)}+\sum_{p=1}^{k-1}\sum_{n=1}^{\infty}\frac{\rho_1^n}{(k-p)^n}\cdot\frac{\rho_1^{k-p}}{(k-p)!}\cdot\frac{\rho_0^p}{p!}P_{0,0(0,k)}+ \qquad (4)$$
$$+\frac{\rho_0^k}{k!}\sum_{n=1}^{\infty}\rho_1^n P_{0,0(0,k)}=1;$$

$$P_{0,0(0,k)}(1+\sum_{m=1}^{k}\frac{\rho_1^m}{m!}+\frac{\rho_1^k}{k!}\sum_{n=1}^{\infty}\frac{\rho_1^n}{k^n}+\sum_{p=1}^{k}\frac{\rho_0^{*p}}{p!}+\sum_{m=1}^{k}\sum_{p=1}^{k}\frac{\rho_1^m}{m!}\cdot\frac{\rho_0^{*p}}{p!}+$$
$$+\sum_{p=1}^{k-1}\sum_{n=1}^{\infty}\frac{\rho_1^n}{(k-p)^n}\cdot\frac{\rho_1^{k-p}}{(k-p)!}\cdot\frac{\rho_0^p}{p!}+\frac{\rho_0^k}{k!}\sum_{n=1}^{\infty}\rho_1^n)=1. \qquad (5)$$

Так як $1+\rho+\frac{\rho^2}{2!}+\frac{\rho^3}{3!}+\frac{\rho^4}{4!}+\cdots+\frac{\rho^k}{k!}\approx e^{\rho}$ та

$\frac{\rho}{k}+\frac{\rho^2}{k^2}+\frac{\rho^3}{k^3}+\frac{\rho^4}{k^4}+\cdots+\frac{\rho^{m-1}}{k^{m1}}+\cdots=\frac{\frac{\rho}{k}}{1-\frac{\rho}{k}}=\frac{\rho}{k-\rho}$, тоді для великих значень *n*, *k* формула (5) набуде вигляду:

$$P_{0,0(0,k)}\left(1+e^{\rho_1}-1+\frac{\rho_1^k}{k!}\cdot\frac{\rho_1}{k-\rho_1}+e^{\rho_0^*}-1+(e^{\rho_1}-1)(e^{\rho_0^*}-1)+\right.$$
$$\left.+(e^{\rho_0}-1)\sum_{p=1}^{k-1}\sum_{n=1}^{\infty}\frac{\rho_1^{n+k-p}}{(k-p)^n(k-p)!}+\frac{\rho_0^k}{k!}\cdot\frac{\rho_1}{1-\rho_1}\right)=1, \qquad (6)$$

або

$$P_{0,0(0,k)} = \frac{1}{e^{\rho_1} + \frac{\rho_1^k}{k!}\cdot\frac{\rho_1}{k-\rho_1} + e^{\rho_0^*} - 1 + (e^{\rho_1}-1)(e^{\rho_0^*}-1) + (e^{\rho_0}-1)} \times$$
$$\times \frac{1}{\sum_{p=1}^{k-1}\sum_{n=1}^{\infty}\frac{\rho_1^{n+k-p}}{(k-p)^n(k-p)!} + \frac{\rho_0^k}{k!}\cdot\frac{\rho_1}{1-\rho_1}}. \qquad (7)$$

Отже, визначивши ймовірність простою системи, встановимо, що M_1 — середню кількість легальних запитів, які розташовані в системі — в черзі і в обробці вузлом:

$$M_1 = (\sum_{m=1}^{k} mP_{0,0(m,k-m)} + \sum_{n=1}^{\infty}(n+k)P_{n,0(k,0)} + \sum_{m=1}^{k}\sum_{p=1}^{k} mQ_{0,p(m,k-m-p)} +$$
$$+ \sum_{p=1}^{k}\sum_{n=1}^{\infty} nQ_{n,p(0,0)} + \sum_{p=1}^{k-1}\sum_{n=1}^{\infty}(n+k-p)Q_{n,p(k-p,0)})P_{0,0(0,k)}; \qquad (8)$$

або

$$M_1 = (\sum_{m=1}^{k} m\frac{\rho_1^m}{m!} + \frac{\rho_1^k}{k!}\sum_{n=1}^{\infty}(n+k)\frac{\rho_1^n}{k^n} + \sum_{m=1}^{k}\sum_{p=1}^{k} m\frac{\rho_1^m}{m!}\cdot\frac{\rho_0^{*p}}{p!} + \frac{\rho_0^k}{k!}\sum_{n=1}^{\infty} n\rho_1^n +$$
$$+ \sum_{p=1}^{k-1}\sum_{n=1}^{\infty}(n+k-p)\frac{\rho_1^n}{(k-p)^n}\cdot\frac{\rho_1^{k-p}}{(k-p)!}\cdot\frac{\rho_0^p}{p!})P_{0,0(0,k)}, \qquad (9)$$

так як $\sum_{m=1}^{k} m\frac{\rho_1^m}{m!} = \rho_1 e^{\rho_1}$;

$$\sum_{n=1}^{\infty} n\frac{\rho_1^n}{k^n} = \frac{\rho_1}{k}\sum_{n=1}^{\infty} n\left(\frac{\rho_1}{k}\right)^{n-1} = \frac{\rho_1}{k}\left(\sum_{n=1}^{\infty}\left(\frac{\rho_1}{k}\right)^n\right)' = \frac{\rho_1}{k}\left(\frac{\rho_1}{k-\rho_1}\right)' = \frac{\rho_1}{(k-\rho_1)^2};$$

$$\sum_{n=1}^{\infty} n\rho_1^n = \rho_1\sum_{n=1}^{\infty} n\rho_1^{n-1} = \rho_1\left(\sum_{n=1}^{\infty}\rho_1^n\right)' = \rho_1\left(\frac{\rho_1}{1-\rho_1}\right)' = \frac{\rho_1}{(1-\rho_1)^2},$$ тоді формула (9) перетворюється на:

$$M_1 = (\rho_1 e^{\rho_1} + \frac{\rho_1^{k+1}}{k!(k-\rho_1)^2} + \frac{\rho_1^{k+1}}{(k-1)!(k-\rho_1)} + \rho_1 e^{\rho_1}(e^{\rho_0^*} - 1) + \\ + \frac{\rho_0^k}{k!}\frac{\rho_1}{(1-\rho_1)^2} + \sum_{p=1}^{k-1}\sum_{n=1}^{\infty}(n+k-p)\frac{\rho_1^n}{(k-p)^n}\cdot\frac{\rho_1^{k-p}}{(k-p)!}\cdot\frac{\rho_0^p}{p!})P_{0,0(0,k)}. \quad (10)$$

Аналогічно, M_2 — середня кількість нелегальних запитів, які розташовані в системі, визначається, як

$$M_2 = \sum_{p=1}^{k} pQ_{0,p(0,k-p)} + \sum_{m=1}^{k}\sum_{p=1}^{k} pQ_{0,p(m,k-m-p)} + \\ + \sum_{p=1}^{k-1}\sum_{n=1}^{\infty} pQ_{n,p(k-p,0)} + \sum_{n=1}^{\infty} kQ_{n,p(0,0)};$$

$$M_2 = (\sum_{p=1}^{k} p\frac{\rho_0^{*p}}{p!} + \sum_{m=1}^{k}\sum_{p=1}^{k} p\frac{\rho_1^m}{m!}\cdot\frac{\rho_0^{*p}}{p!} + \\ + \sum_{p=1}^{k-1}\sum_{n=1}^{\infty} p\frac{\rho_1^n}{(k-p)^n}\cdot\frac{\rho_1^{k-p}}{(k-p)!}\cdot\frac{\rho_0^p}{p!} + \frac{k\rho_0^k}{k!}\sum_{n=1}^{\infty}\rho_1^n)P_{0,0(0,k)};$$

$$M_2 = (\rho_0^* e^{\rho_0^*} + \rho_0^* e^{\rho_0^*}(e^{\rho_0^*} - 1) + \sum_{p=1}^{k-1}\sum_{n=1}^{\infty} p\frac{\rho_1^n}{(k-p)^n} \times \\ \times \frac{\rho_1^{k-p}}{(k-p)!}\cdot\frac{\rho_0^p}{p!} + \frac{k\rho_0^k\rho_1}{(k-1)!(1-\rho_1)})P_{0,0(0,k)}. \quad (11)$$

Зазначені характеристики дозволяють оцінити рівень інформаційних загроз підприємства, адже на основі моделі (1) можна прогнозувати виникнення небажаних подій у вигляді ймовірностей $Q_{0,p(0,k-p)}$, $Q_{n,p(0,0)}$, $Q_{0,p(m,k-m-p)}$, $Q_{n,p(k-p,0)}$.

Для знаходження конкретних характеристик вузла оброблення встановимо такі початкові умови: нехай інтенсивність надходження безпечних запитів становить 5 шт./год, надходження флуду на працюючий канал — 6 шт./год, надходження флуду на непрацюючий канал — 6 шт./год. Інтенсивність обслуговування безпечних запитів складає 20 шт./год, небезпечних — 10 шт./год, тоді $\lambda_1 = 5$, $\lambda_0 = 6$, $\lambda_0^* = 6$, $\mu_1 = 20$, $\mu_0 = 10$.

Нехай кількість каналів обслуговування дорівнюватиме $k = 4$, розмір черги також встановимо рівним у чотири запити. Знайдемо основні системні характеристики функціонування вузла, такі як ймовірність простою, ймовірність атаки нелегальними запитами, середні кількості легальних і нелегальних запитів, що розташовуватимуться в системі.

Використовуючи (7), ймовірність простою вузла $P_{0,0(0,4)} = 0{,}4$, а середня кількість легальних запитів, що розташовуватимуться в системі, становитиме, за (10), $M_1 = 0{,}19$, нелегальних за формулою (11) — $M_2 = 0{,}67$.

Якщо розв'язати систему (2) стандартним алгебраїчним методом, тобто замінюючи останній рядок системи (2) на умову нормування та використовуючи метод оберненої матриці, який розглянуто у [5, с. 214], отримаємо $P_{0,0(0,4)} = 0{,}39$, $M_1 = 0{,}18$ та $M_2 = 0{,}67$. Причому найбільш вірогідними станами системи є $P_{0,0(0,4)} = 0{,}39$, $Q_{0,1(0,3)} = 0{,}28$.

Отже, знайдені системні характеристики дають змогу оцінити ймовірність атаки та найуразливіші місця вузла, і на їх основі визначити рівень інформаційних загроз підприємства.

Висновки. Ключовим питанням визначення інформаційної безпеки підприємства постає питання визначення рівня інформаційних загроз. В якості базової моделі оцінки загроз DDos-атаки пропонується використовувати стохастичну модель масового обслуговування з пуассонівським вхідним потоком та встановленим рівнем черги.

Отримання аналітичних виразів для оцінки показників рівня інформаційних загроз у рамках розглянутої моделі дозволяє визначити системні характеристики функціонування вузла, такі як імовірність простоїв, ймовірності скоєння атаки, найуразливіші місця атаки, середні кількості легальних і нелегальних запитів. Це дозволяє кількісно оцінити рівень інформаційної безпеки досліджуваного об'єкта та вжити відповідних запобіжних заходів — переглянути оперативність обробки запитів вузлом.

Література

1. *Бєгун А.В.* Тенденції розвитку ринку засобів інформаційної безпеки в економіці // Моделювання та інформаційні системи в економіці : зб. наук. праць / А. В. Бєгун. — К. : КНЕУ, 2012. — Вип. 87. — С. 259-265.

2. *Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин. — М. : ДМК Пресс, 2012. — 592 с.

3. Информационная безопасность и защита информации : [учеб. пособие для студ. высш. учеб. заведений] / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под. ред. С. А. Клейменова. — 3-е изд., стереотип. — М. : Академия, 2008. — 336 с.

4. *Клейнрок Л.* Теория массового обслуживания / Л. Клейнрок ; [пер. с англ. И. И. Грушко ; под ред. В. И. Неймана]. — М. : Машиностроение, 1979. — 432 с.

5. *Іващенко Л.В.* Про одну модель управління зернопереробним підприємством з урахуванням системних характеристик / Ю. В. Ігнатова, Л. В. Іващенко // Моделювання та інформаційні системи в економіці : зб. наук. праць. — К. : КНЕУ, 2013. — Вип. 89. — С. 209-218.

6. [Електронний ресурс]. — Режим доступу : http://internetua.com/kolicsestvo-DDoS-atak-za-god-uvelicsilos-pocsti -v-dva-raza

7. [Електронний ресурс]. — Режим доступу : http://www.krdu-mvd.ru/_files/kafedra_ib/52.pdf

УДК 519.865.7

Кисіль Т. М., асистент,
Київський національний економічний університет імені Вадима Гетьмана

КОНЦЕПТУАЛЬНІ МОДЕЛІ ДІАГНОСТИКИ БАНКРУТСТВ ЗАСНОВАНІ НА МЕТОДАХ ШТУЧНОГО ІНТЕЛЕКТУ

АНОТАЦІЯ. В даній статті розглянуто класичні підходи до оцінювання ймовірності банкрутств банківських систем. Проведено моделювання діагностики банкрутств, заснованих на методах штучного інтелекту з використанням алгоритму зворотного поширення помилки багатошарової нейронної системи.

КЛЮЧОВІ СЛОВА: алгоритм зворотного поширення помилки, алгоритм навчання, бази даних, банківська система, банкрутства, діагностика банкрутств, моделі, методи, моделювання, нейроні мережі, показники, прийняття рішень, фінансова криза, фінансовий аналіз.

АННОТАЦИЯ. В данной статье рассмотрены классические подходы к оценке вероятности банкротств банковских систем. Проведено моделирование диагностики банкротств, основанные на методах искусственного интеллекта с использованием алгоритма обратного распространения ошибки многослойной нейронной системы.

КЛЮЧЕВЫЕ СЛОВА: алгоритм обратного распространения ошибки, алгоритм обучения, базы данных, банковская система, банкротства, диагностика банкротств, модели, методы, моделирование, нейронные сети, показатели, принятие решений, финансовый, финансовый анализ.

ABSTRACT. In this article the classical approaches to estimate the probability of bankruptcy banking systems. The simulation diagnostics failures based on the methods of artificial intelligence algorithms using back propagation multilayer neural system.

KEY WORDS: the algorithm of back propagation algorithm training database, banking, bankruptcy, bankruptcy diagnosis, models, methods, modeling, neural networks, performance, decision making, financial crisis, financial analysis.