УДК 004.738.5:338.46(075)

Пістунов Ігор Миколайович
д.т.н., професор,
професор кафедри економічної кібернетики та інформаційних технологій
Державний вищий навчальний заклад
«Національний гірничий університет»
м. Дніпропетровськ

РОЗРАХУНОК ПОЧАТКУ КІБЕРАТАКИ

Підприємства, які ведуть свою діяльність із застосуванням прийомів електронної комерції мають достатньо високий рівень ризику. Їх діяльність можна описати стохастичною V-моделлю [1].

Одну із найбільших загроз діяльності такого підприємства є кібератака.

Кібератакою називається ситуація, коли кількість звернень з Інтернету до інформаційної системи (ІС), що обслуговує запити клієнтів через Інтернет, різко зростає [2]. При цьому, сервер ІС починає працювати все повільніше, намагаючись задовольнити усі запити, доки не припиняє роботу.

Визначити початковий момент кібератаки дуже важливо, оскільки це дозволить зменшити втрати на компенсацію її наслідків.

Знайдемо критерій початку кібератаки за статистичними розрахунками.

Для цього розіб’ємо весь період роботи інформаційної системи, що обслуговує зовнішні запити електронної комерції, на рівні проміжки часу. Ними можуть бути: година, доба, тиждень, але в умовах роботи через Інтернет, краще встановити ці проміжки не більше ΔT = 20-30 хв.

Далі потрібно налагодити постійний контроль над кількістю вхідних запитів.

Після визначення кількості запитів у кожному проміжку не менше 40, потрібно розрахувати середню кількість звернень M_x.

Скористаємося гіпотезою, що потік подій частіше за все характеризується експоненційним законом розподілу [3]. Він характеризується функцією

розподілу виду $$F(x)=\int_0^x l\cdot e^{-lx}dx=1-e^{-lx},\ \text{ïðè}\ x\ge 0,\ F(x)=0,\text{ïðè}\ x<0 \qquad (1)$$

Математичне сподівання дорівнює $$M_x=\int_0^\infty l\,xe^{-lx}dx=\frac{1}{l}\quad . \qquad (2)$$

Медіана може бути знайдена як $$M_e=-\mathrm{Ln}0.5/\lambda\approx 0.69/\lambda. \qquad (3)$$

Звідкіля, $$\left.\begin{array}{l} l=\dfrac{1}{\mathrm{M_x}},\\ l=-\dfrac{Ln0.5}{Me}\end{array}\right\} \qquad (4)$$

Вираз (5) дозволяє знайти зв'язок між медіаною і середнім

$$Me=-\frac{M_x}{Ln0.5}. \qquad (5)$$

Задамо довірчу ймовірність β, яка визначить допустимий рівень ймовірності попадання кількості вхідних звернень в інтервал [*Me; K*], де *K* – реальне число звернень на проміжку ΔT. Очевидно, що ймовірність попадання на цей інтервал має складати половину довірчої ймовірності

$$\frac{b}{2}\ge P(\mathrm{Me}<\mathrm{x}<\mathrm{K})=\mathrm{EXP}(-l\,\mathrm{Me})-\mathrm{EXP}(-l\,\mathrm{K}). \qquad (6)$$

Підставимио значення λ з (4) в (6)

$$\frac{b}{2}\ge \mathrm{EXP}(-\frac{\mathrm{Me}}{\mathrm{M_x}})-\mathrm{EXP}(-\frac{\mathrm{K}}{\mathrm{M_x}}), \qquad (7)$$

А медіану, в свою чергу виразимо через середнє

$$\frac{b}{2}\ge \mathrm{EXP}(\frac{\mathrm{M_\div}}{\mathrm{M_x}\mathrm{Ln}0.5})-\mathrm{EXP}(-\frac{\mathrm{K}}{\mathrm{M_x}}). \qquad (8)$$

Приведемо вираз до виду

$$b\ge 2\cdot\mathrm{EXP}(\frac{1}{\mathrm{Ln}0.5})-\mathrm{EXP}(-\frac{\mathrm{K}}{\mathrm{M_x}})=0{,}47258018-2\cdot\mathrm{EXP}(-\frac{\mathrm{K}}{\mathrm{M_x}}). \qquad (9)$$

Знайдемо тепер допустиме перевищення кількості вхідних викликів інформаційної системи над середним їх значенням $\frac{b-0{,}47258018}{2}\ge -\mathrm{EXP}(-\frac{\mathrm{K}}{\mathrm{M_x}})$

звідкіля $$\mathrm{M_x}\cdot\mathrm{Ln}\left(\frac{b-0{,}47258018}{2}\right)\ge \mathrm{K} \qquad (10)$$

Отже, якщо кількість звертань до ІС K перевищить значення виразу з правої частини (10), можна вважати, що кібератака вже почалася.

Розуміючи, що вираз $\frac{K}{M_x}$ є перевищенням середнього у відносних одиницях, зробимо розрахунок відповідності деяких популярних значень довірчої ймовірності до міри перевищення кількості вхідних викликів над середнім. Результати розрахунків представлені у табл. 1.

Таблиця 1

Розрахунок відповідності значення довірчої ймовірності та міри перевищення кількості вхідних викликів на їх середнім значенням

b	$\frac{K}{M_x}$
0,6	2,753415
0,75	1,975370
0,8	1,809659
0,85	1,667544
0,9	1,543136
0,95	1,432506
0,98	1,371564
0,99	1,352048
0,999	1,334803
0,9999	1,333095

З табл. 1 можна зробити висновок, що в разі перевищення тільки у півтора рази, можна зі ймовірністю більше 0,9 вважати, що кібератака вже почалася.

Список використаних джерел**:**

1. Пістунов І.М. Стохастична V-модель управління підприємством з високим рівнем природного ризику/ Економіка: проблеми теорії та практики/ І..М. Пістунов - Вип.. 189, том.У.- Д.: ДНУ: 2004. - С.1530-1535.
2. Пістунов І.М. Безпека електронної комерції: навч. Посібник/ І..М. Пістунов – Дніпропетровськ: Національний гірничий університет, 2011. – 125 с
3. Пістунов І.М. Теорія ймовірності та математична статистика для економістів. З елементами електронних таблиць: Навч. Посібник/ І.М.Пістунов, Н.В.Лобова – Дніпропетровськ: Національний гірничий університет, 2005.– 110 с.

.