УДК 004.056

Шаров Вячеслав Александрович, аспирант, Нижневартовский государственный университет, г. Нижневартовск

МАТЕМАТИЧЕСКИЕ МОДЕЛИ, ЧИСЛЕННО - АНАЛИТИЧЕСКИЕ МЕТОДЫ ДЛЯ ОПТИМИЗАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ПОГЛОЩАЮЩИХ ЦЕПЕЙ МАРКОВА

Аннотация. В данной работе рассматриваются математические модели, численно-аналитические методы и программные решения, используемые для оптимизации систем защиты информации на основе поглощающих цепей Маркова. Описаны ключевые свойства таких цепей, включая матрицу переходов, фундаментальную матрицу и вероятности поглощения. Разработаны численные алгоритмы для анализа вероятности успешного взлома и времени до критических состояний. Программная реализация предложенной модели продемонстрирована на языке Python.

Annotation. This paper discusses mathematical models, numerical analytical methods and software solutions used to optimize information security systems based on absorbing Markov chains. Key properties of such circuits are described, including the transition matrix, fundamental matrix, and absorption probabilities. Numerical algorithms have been developed to analyze the probability of successful hacking and the time to critical conditions. The software implementation of the proposed model is demonstrated in Python.

Ключевые слова: поглощающие цепи Маркова, цепи Маркова, кибербезопасность, кибератаки, математические методы.

Keywords: absorbing Markov chains, Markov chains, cybersecurity, cyberattacks, mathematical methods.

ВВЕДЕНИЕ

Развитие технологий привело к появлению новых методов кибератак. Данная проблема требует более структурированного и формализованного подхода для решения вопроса оптимизации систем защиты информации.

Одним из таких подходов является применение математических моделей, основанных на теории цепей Маркова, позволяющих анализировать вероятностные процессы в системах защиты информации.

Поглощающие цепи Маркова описывают системы имеющие конечные состояния. Модели, построенные на основе поглощающих цепей Маркова позволяют предсказать вероятность успешности кибератаки, или, наоборот, отказоустойчивость системы защиты. Так же модель может помочь оценить среднее время до наступления критического состояния.

Цепи Маркова – это стохастические процессы, в которых вероятность перехода в следующее состояние зависит только от текущего состояния и не зависит от предшествующих состояний. Если существует хотя бы одно состояние S_i, для которого вероятность перехода в него из самого себя равна $1(P_{ii}=1)$, а из остальных состояний оно достижимо, то цепь является поглощающей. К основным характеристикам поглощающих цепей Маркова относят:

- Матрицу переходов P, состоящую из вероятностей переходов между состояниями
- Поглощающие состояния
- Фундаментальную матрицу $N=(I-Q)^{-1}$, где Q – подматрица переходов, описывающая переходы между непоглощающими состояниями.

Системы защиты информации можно представить в виде цепей Маркова, где состояния соответствуют различным уровням безопасности системы как, например, «нормальная работа»/«подозрительная активность»/«взлом». Переходы между состояниями моделируют события (атаки, сбои, защитные меры), где поглощающие состояния это – «атака отражена»/«система успешно атакована».

Для численного анализа поглощающих цепей Маркова можно использовать Python и библиотеку NumPy, которая позволяет работать с

матрицами и решать системы линейных уравнений. Рассмотрим модель атаки на сервер, где возможны следующие состояния:

1. S_0 – нормальная работа (начальное состояние).
2. S_1 – первая попытка взлома.
3. S_2 – усиление атаки.
4. S_3 – сервер взломан (поглощающее состояние).
5. S_4 – атака отражена (поглощающее состояние).

Матрица переходов для такой модели будет выглядеть следующим образом (Рисунок 1)

$$P = \begin{bmatrix} 0.7 & 0.3 & 0 & 0 & 0 \\ 0 & 0.6 & 0.4 & 0 & 0 \\ 0 & 0 & 0.5 & 0.5 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Рисунок 1 Матрица переходов

Далее потребуется написать код для вычисления фундаментальной матрицы и вероятностей поглощения:

```
import numpy as np
# Матрица переходов (P)
P = np.array([
    [0.7, 0.3, 0,   0,   0],
    [0,   0.6, 0.4, 0,   0],
    [0,   0,   0.5, 0.5, 0],
    [0,   0,   0,   1,   0],
    [0,   0,   0,   0,   1]
])
# Выделяем матрицу Q (непоглощающие состояния)
Q = P[:3, :3]
```

```
# Вычисляем фундаментальную матрицу N = (I - Q)^(-1)
I = np.eye(Q.shape[0])
N = np.linalg.inv(I - Q)
# Выводим фундаментальную матрицу
print("Фундаментальная матрица N:")
print(N)
# Вычисляем вероятности поглощения B = N * R
R = P[:3, 3:]  # Переходы из непоглощающих состояний в поглощающие
B = np.dot(N, R)
print("\nВероятности поглощения:")
print(B)
```

Фундаментальная матрица N показывает, сколько шагов в среднем система будет находиться в каждом состоянии перед поглощением.

Матрица B показывает вероятность того, что система в итоге перейдёт либо в состояние "сервер взломан", либо в состояние "атака отражена".

Стоит обратить внимание на то, что состояния S_3 и S_4 являются поглощающими. Таким образом, с помощью фундаментальной матрицы N можно определить среднее время, за которое система перейдет в одно из поглощающих состояний, и вероятность успешности атаки.

Говоря о вероятности поглощения, мы говорим о R матрице, которая описывает вероятность перехода из непоглощающих состояний в поглощающие. Так можно определить вектор вероятностей поглощения B

$$B=NR$$

Это позволяет вычислить, с какой вероятностью в конечном счете окажется система в каждом из поглощающих состояний.

В заключении можно сказать, что при грамотном подходе к анализу матрицы переходов и вероятности поглощения можно:

- Выявить слабые места – состояния с высокой вероятностью перехода во «взлом».
- Моделировать защитные меры – например, добавление механизмов блокировки для уменьшения вероятности перехода в уязвимые состояния.
- Оценить эффективность стратегий – сравнивая различные сценарии.

Список литературы

1. Гнеденко Б. В. Курс теории вероятностей. — М.: Наука, 1988. — 528 с.
2. Кемени Дж., Снелл Дж. Классические цепи Маркова. — М.: Мир, 1972. — 360 с.
3. Феллер В. Введение в теорию вероятностей и её приложения. Том 1. — М.: Мир, 1967. — 528 с.
4. Климов Г. П. Марковские процессы и их применение. — М.: Физматлит, 2007. — 312 с.
5. Stallings W. Cryptography and Network Security: Principles and Practice. — 7th ed. — Pearson, 2017. — 800 p.
6. Ross S. M. Introduction to Probability Models. — 12th ed. — Academic Press, 2019. — 828 p.