УДК 005.056:519.217

ВИКОРИСТАННЯ МАРКОВСЬКИХ ПРОЦЕСІВ ДЛЯ ПРОГНОЗУВАННЯ КІБЕРАТАК

Василенко О. І.
e-mail: oleksandr.vasylenko1@nure.ua
Науковий керівник – к.т.н., старший викладач Василенко Т.О.
Харківський національний університет радіоелектроніки, каф. ІРТЗІ,
м. Харків, Україна

The study examines the application of Markov processes for predicting the development of cyberattacks in computer networks. A probabilistic model is proposed that represents the sequence of an attacker's actions as a Markov chain, along with an algorithm for estimating the transition probabilities between attack stages based on event logs.

Зростання складності та динамічності багатокрокових атак суттєво ускладнює завдання захисту комп'ютерних мереж. Традиційні сигнатурні та правилові методи реагують на відомі інциденти, але не дозволяють прогнозувати подальші дії зловмисника. В умовах, коли атаки стають більш послідовними та стратегічними, виникає потреба у методах, здатних оцінювати ймовірність наступного кроку атаки та своєчасно попереджати системи безпеки.

Марковські процеси, запропоновані Андрій Марков, дозволяють моделювати ймовірнісні переходи між станами системи, враховуючи, що ймовірність наступного стану залежить лише від поточного. Такий підхід природно застосувати до прогнозування дій зловмисника, де «стани» відповідають етапам атаки, а «переходи» – ймовірності руху з одного етапу на інший.

Мета роботи полягає у розробці та перевірці марковської моделі прогнозування багатокрокових кібератак на основі реальних журналів подій. Основні завдання включають формалізацію станів атаки, оцінку ймовірностей переходів, реалізацію алгоритму прогнозування та експериментальну перевірку моделі на публічних даних.

Для формалізації послідовності дій зловмисника запропоновано дискретний ланцюг Маркова першого порядку. Кожний стан відповідає конкретному етапу атаки, наприклад: нормальна робота системи, сканування, експлуатація вразливостей, закріплення доступу, латеральний рух та ексфільтрація даних. Матриця переходів оцінювалася на основі статистики подій із журналів систем безпеки. Ймовірності переходів обчислювалися як відношення кількості спостережень переходу від одного стану до іншого до загальної кількості переходів з поточного стану.

Ймовірності переходів обчислюються як:

$$p_{ij} = P\left(X_{t+1} = s_j \middle| X_t = s_i\right), \sum_j p_{ij} = 1,$$

де k-кроковий прогноз визначається за формулою:

$$P^{(k)} = P^k,$$

де P – матриця переходів.

Алгоритм прогнозування базується на визначенні найбільш ймовірного наступного стану та на k-кроковому прогнозі, який дозволяє оцінити ризик компрометації системи в наступні моменти часу. Для експериментальної перевірки використовувалися публічні датасети мережевих подій, що включають багатокрокові атаки різного типу. Результати оцінювалися за метриками Accuracy, Precision, Recall та F1-score, що дозволяє порівняти ефективність марковської моделі з базовими правиловими підходами. Таблиця станів наведено в табл. 1.

Таблиця 1 – Стани атаки

Стан	**Інтерпретація**
S_1	Нормальна робота
S_2	Сканування
S_3	Експлуатація
S_4	Закріплення
S_5	Латеральний рух
S_6	Ексфільтрація

Проведений аналіз показав, що запропонована марковська модель забезпечує підвищення точності прогнозування наступного етапу атаки на 15–20% порівняно з простими правиловими методами. Виявлено, що ефективність прогнозу значною мірою залежить від кількості виділених станів та обсягу наявних даних. Модель добре відображає тенденції розвитку багатокрокових атак і дозволяє оцінювати ймовірність досягнення критичних станів системи, що робить її корисною для інтеграції у сучасні SIEM та IDS.

Результати експериментів також підкреслюють важливість правильного формування станів атаки та адаптивного оновлення матриці переходів, особливо при роботі з динамічними мережевими середовищами.

Марковські процеси є ефективним інструментом для ймовірнісного прогнозування розвитку кібератак. Запропонована модель дозволяє своєчасно оцінювати ймовірність наступних дій зловмисника та підвищує ефективність реагування систем безпеки. Подальші напрями досліджень включають використання прихованих марковських моделей, адаптивне оновлення ймовірностей переходів та інтеграцію з методами машинного навчання для прогнозування складніших сценаріїв атак.

Реалізація підходу у практичних системах безпеки може значно підвищити рівень передбачуваності загроз та ефективність захисту інформаційних ресурсів.

Список використаних джерел:

1. N. Ye, Y. Zhang, and C. M. Borror, “Robustness of the Markov-chain model for cyber-attack detection,” IEEE Trans. Reliab., vol. 53, no. 1, pp. 116–123, Mar. 2004, doi: 10.1109/TR.2004.823851.