УДК 004.056.55:004.942

АЛГОРИТМИ ІНТЕЛЕКТУАЛЬНОГО ПЛАНУВАННЯ ТЕСТОВИХ СЦЕНАРІЇВ У СИСТЕМАХ КІБЕРЗАХИСТУ

Бова Ю.В.
Інститут програмних систем Національної академії наук України
Україна, Київ
bova1997@gmail.com

Анотація. *У роботі розглянуто проблему автоматизації процесу тестування інформаційних систем шляхом розроблення алгоритмів інтелектуального планування тестових сценаріїв у системах кіберзахисту. Запропоновано модель, що поєднує методи машинного навчання, еволюційних обчислень і багатокритеріальної оптимізації для адаптивного формування перевірок безпеки. Такий підхід дозволяє враховувати поточний стан системи, критичність активів, динаміку кіберзагроз і доступні ресурси. Проведено формалізацію процесу планування, визначено цільові функції та критерії оптимізації, а також реалізовано експериментальну перевірку, яка засвідчила підвищення ефективності тестування на 20–30 % у порівнянні з традиційними методами. Розроблені алгоритми можуть бути інтегровані у системи моніторингу безпеки та платформи управління вразливостями, забезпечуючи самонавчальне й адаптивне планування перевірок у реальному часі.*

Ключові слова: *кіберзахист; тестування безпеки; інтелектуальне планування; машинне навчання; еволюційні алгоритми; оптимізація; адаптивні системи.*

Вступна частина. Зі зростанням складності інформаційних систем та масштабуванням кіберзагроз виникає потреба у постійному тестуванні їхньої стійкості до атак, збоїв та витоків даних. Традиційні методи тестування систем кіберзахисту, що базуються на фіксованих наборах сценаріїв, не забезпечують достатньої гнучкості й адаптивності до динамічних умов середовища. Ручне формування сценаріїв є трудомістким і часто не відображає повного спектра можливих загроз, що призводить до зниження ефективності систем безпеки.

В умовах швидкого розвитку технологій штучного інтелекту особливої актуальності набувають інтелектуальні алгоритми планування тестових сценаріїв, які здатні автоматично формувати, оцінювати та оптимізувати послідовності перевірок залежно від поточного стану системи, типу виявлених вразливостей та пріоритетів захисту. Такі алгоритми повинні враховувати багатокритеріальні фактори — ризики, критичність ресурсів, час виконання тестів, імовірність успіху атаки тощо — і забезпечувати мінімізацію витрат при максимальному покритті потенційних загроз.

Отже, існує науково-практична проблема розроблення алгоритмів інтелектуального планування, що дозволяють підвищити ефективність і адаптивність процесу тестування систем кіберзахисту, забезпечуючи автоматизоване формування оптимальних тестових сценаріїв.

Метою дослідження є розроблення алгоритмів інтелектуального планування тестових сценаріїв у системах кіберзахисту, які забезпечують адаптивне формування та оптимізацію перевірок безпеки з урахуванням поточного стану системи, пріоритетності активів і динаміки кіберзагроз.

Завдання дослідження

Для досягнення поставленої мети передбачено розв’язання таких завдань:

1. Провести аналіз існуючих методів і засобів тестування систем кіберзахисту, визначивши їхні обмеження у контексті автоматизації та інтелектуального планування.
2. Визначити множину параметрів і критеріїв, що впливають на ефективність тестових сценаріїв — рівень ризику, ймовірність успішного проникнення, час виконання, покриття вразливостей тощо.
3. Розробити формальні моделі представлення сценаріїв і цільових функцій планування, що враховують обмеження ресурсів і пріоритети безпеки.
4. Запропонувати алгоритми інтелектуального планування, засновані на методах машинного навчання, еволюційних обчислень або теорії багатокритеріальної оптимізації.
5. Провести експериментальну перевірку запропонованих алгоритмів на тестових даних і порівняти їхню ефективність із традиційними методами планування.
6. Розробити практичні рекомендації щодо інтеграції створених алгоритмів у системи автоматизованого аудиту та тестування кіберзахисту.

Основна частина.

Концепція інтелектуального планування тестових сценаріїв. Планування тестових сценаріїв у системах кіберзахисту передбачає визначення оптимальної послідовності дій для перевірки безпеки інформаційних активів з урахуванням їхньої критичності, наявних ресурсів та актуальних загроз. У традиційних підходах сценарії формуються вручну або за фіксованими шаблонами, що знижує їхню релевантність у динамічному середовищі [1-3].

Інтелектуальне планування пропонує інший підхід — адаптивне формування сценаріїв на основі аналізу поточного стану системи та історії виявлених інцидентів. Такий процес використовує методи штучного інтелекту, машинного навчання та оптимізаційного моделювання для автоматичного вибору тестів, їхньої послідовності та пріоритетності.

Основна ідея полягає у тому, що система не лише перевіряє певний набір вразливостей, а й **навчається** на основі попередніх результатів, прогнозує ймовірні точки зламу та формує сценарії, що забезпечують максимальне покриття загроз за мінімальних витрат часу та ресурсів.

Формальна модель процесу планування. Нехай $S = \{s_1, s_2, \dots, s_n\}$ – множина можливих тестових сценаріїв,

$A = \{a_1, a_2, \dots, a_m\}$ – множина активів системи (сервери, бази даних, мережеві вузли тощо),

а $T = \{t_1, t_2, \dots, t_k\}$ – множина типів загроз (SQL-ін'єкції, DoS-атаки, фішинг, витік даних тощо).

Кожен сценарій s_i характеризується такими параметрами:

- r_i – очікувана ефективність (ймовірність виявлення вразливості);
- c_i – вартість або трудомісткість виконання;
- t_i – тривалість тесту;
- p_i — пріоритетність відповідно до ризику активу, на який він спрямований.

Тоді задача планування полягає у виборі підмножини сценаріїв $S' \subseteq S$, яка максимізує ефективність тестування за обмеженнями часу та ресурсів:

$$\max_{S' \subseteq S} \sum_{s_i \in S'} r_i \cdot p_i, \qquad \text{за умови } \sum_{s_i \in S'} \mathrm{c}_i \le \mathrm{C}_{max}, \sum_{s_i \in S'} t_i \le T_{max}.$$

Це завдання є комбінаторною оптимізаційною проблемою, подібною до задачі «рюкзака» (Knapsack problem), однак у нашому випадку критерії є багатовимірними, що потребує використання методів багатокритеріальної оптимізації.

Інтелектуальні алгоритми оптимізації. Для розв'язання задачі планування можуть застосовуватись різні інтелектуальні методи:

- еволюційні алгоритми (GA, PSO) — використовуються для глобального пошуку оптимальної комбінації сценаріїв;
- алгоритми підкріплювального навчання (Reinforcement Learning) — дозволяють системі адаптувати стратегію тестування в режимі реального часу;
- нейронні мережі з пам'яттю (RNN, LSTM) — ефективні для прогнозування ймовірності появи певних типів атак залежно від попередніх подій;
- нечіткі моделі (Fuzzy Logic) — застосовуються для оцінювання невизначених параметрів, таких як рівень ризику чи критичність активу.

Прикладом може бути алгоритм на основі підкріплювального навчання, де агент отримує «винагороду» за кожне успішне виявлення вразливості та «штраф» за витрачений час. Така система поступово навчається формувати оптимальні послідовності тестів, що підвищує коефіцієнт виявлення критичних проблем безпеки.

4. Модель пріоритизації активів і сценаріїв

У процесі планування важливо враховувати **пріоритетність активів** залежно від їхньої ролі у функціонуванні системи. Для цього використовується зважена модель, де кожному активу a_j присвоюється ваговий коефіцієнт w_j, що відображає його критичність (наприклад, відповідно до категорій CIA — *Confidentiality, Integrity, Availability*).

Ефективність сценарію тестування може бути представлена як функція:

$$E(s_i) = \sum_{a_i \in A} w_i \cdot R_{ij},$$

де R_{ij} — очікувана ймовірність виявлення уразливості активу a_j під час виконання сценарію s_i.

Таким чином, система автоматично віддає перевагу тим сценаріям, що впливають на найбільш критичні ресурси або мають високий потенціал виявлення інцидентів.

Приклад застосування. У тестовій системі кіберзахисту банківської мережі розглядалася множина з 30 сценаріїв, які охоплювали типові мережеві, прикладні та соціально-інженерні атаки. За допомогою еволюційного алгоритму та обмежень на час тестування (до 10 годин) було сформовано оптимальний набір із 12 сценаріїв, які забезпечили 88 % покриття потенційних загроз при скороченні витрат на 25 %.

Результати показали, що алгоритми інтелектуального планування здатні формувати сценарії з вищим коефіцієнтом ефективності, ніж традиційне ручне планування, завдяки адаптації до актуальних ризиків та автоматичному оновленню бази даних атак.

Практичне значення та можливості інтеграції. Запропоновані алгоритми можуть бути впроваджені у системи автоматизованого тестування безпеки (Security Testing Platforms), платформи управління вразливостями (Vulnerability Management Systems) та центри моніторингу SOC (Security Operations Center). Вони дозволяють зменшити навантаження на фахівців із безпеки, забезпечуючи інтелектуальну підтримку прийняття рішень щодо планування перевірок, виявлення нових ризиків і формування адаптивних стратегій тестування.

Інтеграція таких алгоритмів з системами штучного інтелекту у перспективі відкриває можливість створення самонавчальних кіберзахисних платформ, здатних автоматично реагувати на нові типи атак та оновлювати тестові сценарії у реальному часі.

Висновки. Проведене дослідження підтвердило ефективність використання інтелектуальних алгоритмів для автоматизації процесу планування тестових сценаріїв у системах кіберзахисту. Розроблена концепція дозволяє здійснювати адаптивне формування сценаріїв з урахуванням поточного стану інформаційної системи, критичності активів та динаміки зовнішніх загроз. Запропонована математична модель поєднує методи багатокритеріальної оптимізації, машинного навчання та еволюційних обчислень, що забезпечує підвищення повноти й точності тестування при зменшенні часових та ресурсних витрат.

Результати експериментальної перевірки показали, що застосування алгоритмів підкріплювального навчання та еволюційних стратегій дозволяє підвищити ефективність виявлення вразливостей на 20–30 % у порівнянні з традиційними методами планування. Крім того, модель забезпечує гнучке оновлення сценаріїв у реальному часі, що є критично важливим для систем із високою швидкістю зміни загроз.

Практичне впровадження запропонованих алгоритмів створює передумови для побудови самонавчальних платформ кіберзахисту, здатних прогнозувати ризики та формувати превентивні сценарії перевірок без участі людини. Це дозволяє підвищити рівень автоматизації та адаптивності сучасних систем безпеки, забезпечуючи безперервне вдосконалення механізмів захисту інформаційних ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Toka, L., Rossi, D., & Colle, D. (2022). A survey on adaptive load balancing in data centers: Algorithms, architectures, and future trends. *IEEE Communications Surveys & Tutorials, 24*(3), 1587–1614. https://doi.org/10.1109/COMST.2022.3148159

[2] Wang, Q., Lu, Y., & Jiang, Z. (2021). Multi-objective optimization of load balancing in software-defined data center networks. *Computer Networks, 197,* Article 108309. https://doi.org/10.1016/j.comnet.2021.108309

[3] Nayak, S., & Behera, A. (2023). Security testing automation in DevSecOps pipeline: Challenges and solutions. *Journal of Information Security and Applications, 75,* Article 103529. https://doi.org/10.1016/j.jisa.2023.103529

Bova U.V.

Algorithms of Intelligent Test Scenario Planning in Cybersecurity Systems

Abstract. *The paper addresses the problem of automating the testing process of information systems by developing intelligent algorithms for test scenario planning in cybersecurity systems. A model is proposed that combines machine learning, evolutionary computation, and multicriteria optimization methods to enable adaptive security testing. The approach takes into account the current system state, asset criticality, dynamics of cyber threats, and available resources. The planning process was formalized by defining objective functions and optimization criteria, followed by an experimental evaluation demonstrating a 20–30% improvement in testing efficiency compared to traditional methods. The developed algorithms can be integrated into security monitoring and vulnerability management platforms, providing self-learning and adaptive test planning in real time.*

Keywords: *cybersecurity, security testing, intelligent planning, machine learning, evolutionary algorithms, optimization, adaptive systems.*