Підхід до вибору стратегії застосування методів протидії кібератакам

УДК 621.395.7 (043.2)

Сергій Веретюк[1], Катерина Молодецька[2]

Поліський національний університет,
[1]kateryna.molodetska@polissiauniver.edu.ua, [2]mail2@nau.rdu.ua

Зростання кількості кібератак свідчить про динамічний характер взаємодії в кіберпросторі між кіберзлочинцями та системами кіберзахисту. Більшість існуючих систем, підходів та стандартів стикаються з певними обмеженнями, такими як застосування статичних моделей, відсутність урахування спільної еволюції стратегій та відсутність синхронізованого налаштування, що не враховує динамічний характер кібератак і захисту. Постійна коеволюція вимагає від захисників не лише реактивної, але й прогнозованої стратегії.

Ефективний захист передбачає синхронізацію стратегій на різних рівнях захисту, включаючи мережевий, рівень застосунків та фізичний захист, для ефективного запобігання вразливостям. Застосування динамічних моделей дозволяє краще розуміти та передбачати змінність в діях кіберзлочинців і захисників, що допомагає вчасно реагувати на потенційні загрози. Нарешті, стратегічне планування є ключовим елементом в розробці майбутніх стратегій захисту, дозволяючи захисникам адаптуватися до швидких змін у загрозах та технологіях.

Таким чином, пошук нових адаптивних динамічних підходів до забезпечення ефективного кіберзахисту об'єктів інформаційної діяльності є актуальним науковим завданням.

Дослідження спрямоване на розроблення підходу до підвищення ефективності стратегічного планування заходів із забезпечення кібербезпеки об'єктів інформаційної діяльності в умовах динамічного антагоністичного середовища.

Нехай є набір методів протидії кібератакам на об'єкт інформаційної діяльності

$$M = \{m_i\},\ i \in [1; N]. \quad (1)$$

Кожний метод формалізовано трьома параметрами $\{P, T, C\}$, де:

P_i – потенціал протидії, тобто здатність методу адекватно протидіяти окремому типу кібератаки або її складовій *i*-того методу протидії кіберзагрозі;

T_i – час імплементації *i*-того методу або час перехідного процесу від початку дії методу;

C_i – вартість застосування *i*-того методу.

Стратегією протидії $S_j = \{m_{j,i}\}$ називатимемо довільний набір методів, який ефективно протидіє кіберзагрозі Z_j. У свою чергу кіберзагрозу Z_j будемо описувати параметром збитків L_i.

Ефективністю *i*-того методу E_i визначимо через наступне співвідношення

$$E_i = \frac{P_i}{T_i C_i}. \quad (2)$$

Тоді загальну ефективність стратегії S_j формалізуємо через величину

$$E_{s_j} = \sum E_{ij}, \quad (3)$$

де E_{ij} – ефективність застосування *i*-того методу в *j*-тій стратегії.

Опишемо загальні втрати від потоку атак таким співвідношенням

$$L_{\text{заг}} = \lambda\tau L_A\left(1 - E_j^*\right), \quad (4)$$

де E_j^* – нормована відносно 1 ефективність обраної стратегії, λ- інтенсивність потоку атак (пуассонівського потоку подій).

Тоді принцип вибору стратегії повинен забезпечувати мінімізацію $L_{\text{заг}}$

$$\lambda\tau L_A\left(1 - E_j^*\right) \to min \quad (5)$$

за таких умов

$C_j = \sum C_i < C_{max}$ – обмеження на вартість;

$P_j = \sum P_i < P_{max}$ – обмеження, які накладаються на потенціал методу;

$T_j < T_{max}$ – обмеження по часу;

$C_j < \lambda\tau L_{A\tau}$ – виконання умови доцільності, а саме використовувати стратегію, якщо вартість її реалізації менша за втрати від кібератак.

Вираз (5) можемо переписати як

$$\lambda\tau L_A\left(1 - \frac{E_j}{E_{max}}\right) \to min,$$

де E_{max} – максимальна ефективність обраної стратегії.

При фіксованих значеннях $L_A, \lambda, \tau, E_{max}$ задача зводиться до мінімізації співвідношення

$$E_{max} - E_j \to min. \quad (6)$$

Для вирішення скористаємось методом Лагранжа. Розв'язок системи диференціальних рівнянь, отриманих шляхом диференціювання рівняння Лагранжа дасть можливість визначити параметри $\{P, T, C\}$ оптимальної стратегії S_j для протидії кіберзагрозі Z_j за критерієм ефективності за сукупністю показників: потенціалу методів, що входять до стратегії, вартості та часу реагування цих методів. Отже, розуміння коеволюції засобів здійснення кібератаки та методів кіберзахисту надає можливість дослідити та спрогнозувати зміни в системі «загроза-захист» на макрорівні.

1. Van der Kleij, Rick, et al. Developing decision support for cybersecurity threat and incident managers. *Computers & Security*. – 2022. – 113:102535.
2. Yevseiev S., Hryshchuk R., Molodetska K., Nazarkevych M. and others. Modeling of security systems for critical infrastructure facilities: monograph. Kharkiv: PC Technology Center, 2022. 196 p.
3. Yin, Yimin. Information Security and Risk Control Model Based on Plan-Do-Check-Action for Digital Libraries. *Journal of Cyber Security and Mobility*. – 2024. – PP. 305–326.
4. Lippert, Kari J., Robert Cloutier. Cyberspace: a digital ecosystem. *Systems*. – 2021. – 9.3: 48.
5. Fedushko, S., Molodetska, K., Syerov, Y. Analytical method to improve the decision-making criteria approach in managing digital social channels. *Heliyon*. – 2023. – 9(6). – e16828.