УДК 004.056.5:004.4 DOI: https://doi.org/10.30837/IYF.IIS.2024.259

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ РИЗИКІВ КІБЕРЗАГРОЗ ТА ЕФЕКТИВНОСТІ ЗАХОДІВ БЕЗПЕКИ ДЛЯ ПІДПРИЄМСТВ

Сергійчук А. А.
Науковий керівник – к.т.н., доц. Малєєва Ю. А.
Національний аерокосмічний університет ім. М.Є. Жуковського «Харківський авіаційний інститут», каф. комп'ютерних наук та інформаційних технологій,
м. Харків, Україна
e-mail: juliabelokon84@gmail.com

Cybersecurity is an integral part of modern business, especially for small enterprises facing limited budgetary resources. The model using AnyLogic is proposed for risk assessment and identification of effective protection strategies. The model considers various aspects of cybersecurity, including network structure, control measures, and potential threats. Research results indicate that an appropriate defense strategy can be tailored for different types of small enterprises, taking into account their budgetary constraints. This approach allows for maximizing the return on investments in cybersecurity, contributing to protection of companies from potential threats.

Підприємства будь-якого масштабу стикаються зпостійно зростаючим ризиком кібератак. Успішні атаки можуть призвести до витоку конфіденційної інформації, що в свою чергу може призвести до фінансових втрат, перерв у бізнесі, а також понесення регулятивних штрафів та шкоди репутації. Особливо складно забезпечити захист від таких загроз для малих підприємств, які, з одного боку, мають обмежений бюджет і кадровий потенціал, а з іншого – прагнуть до розвитку.

Оцінка ризиків стає важливим інструментом для організацій у визначенні оптимального способу використання бюджету на кібербезпеку. Однак для малих підприємств проведення такої оцінки може вимагати значних витрат, які в іншому випадку могли б бути спрямовані на впровадження заходів контролю кібербезпеки.

Дане дослідження спрямоване на моделювання фішингових атак з метою виявлення ефективних стратегій захисту, які можуть використовувати малі бізнеси, а також оцінки ризиків. Отже, основною метою дослідження є підвищення ефективності заходів захисту від кібератак для малих підприємств з максимізацією віддачі від інвестицій в умовах обмеженого бюджету та недостатнього кадрового потенціалу.

Розглянуто та проаналізовано результати досліджень, які представляють структуру для встановлення пріоритетів засобів контролю на основі їх ефективності в змодельованій комп'ютерній мережі, відтвореній в AnyLogic.

AnyLogic – інструмент, який дозволяє здійснювати моделювання

бізнес-системи будь-якої складності з допомогою будь-якої комбінації трьох підходів: дискретно-подійного, агентного та системної динаміки.

Після побудови моделі в AnyLogic багато разів поспіль відбувається симуляція та фіксуються відмінності між прогонами й сукупними результатами, оскільки вхідні дані, наприклад, поведінка агента, змінюються відповідно до різних випадків використання.

В результаті аналізу існуючих досліджень запропоновано модель AnyLogic, що дозволяє здійснювати налаштування широкого спектру параметрів, які характеризують вузли мережі, засоби контролю, потенційні загрози, щорічний бюджет тощо. Модель імітує певну кількість атак щорічно та надає можливість отримувати усереднені значення за певний період.

Тестування моделі проводилось на декількох наборах вихідних даних, які характеризують різні види компаній за чисельністю персоналу. Крім того, модель відтворює різні кількості видів суб'єктів загрози.

Для багатьох невеликих або неприбуткових організацій моделювання симуляцій може бути чи не єдиним ефективним засобом для кількісної оцінки їхньої кібербезпеки. За результатами моделювання можна зробити висновки щодо доцільності використання певних заходів для захисту від кібератак для окремих категорій малого бізнесу з урахуванням обмежень наявного бюджету компанії. Також, очевидним є те, що точність результатів моделювання зростатиме, якщо відома точна інформація щодо вихідних даних конкретної компанії (статистика щорічних атак, існуючі засоби контролю безпеки та ін.).

Список використаних джерел:

1. ISACA, State of cybersecurity 2022, Information Systems Audit and Control Association, Schaumburg, IL, Tech. Rep. 2022. URL: https://www.isaca.org/resources/reports/state-of-cybersecurity-2022 (дата звернення: 13.03.2024).

2. Engström V., Lagerström R. Two decades of cyberattack simulations: A systematic literature review, Computers & Security. 2022. Vol. 116, 102681.

3. Dal Cin P., Fox J., Nunn-Price J., Sidhu H. State of cybersecurity resilience 2023, Accenture. Tech. Rep. 2023. URL: https://www.accenture.com/us-en/insights/security/state-cybersecurity (дата звернення: 17.03.2024).

4. Chronopoulos M., Panaousis E., Grossklags J. An options approach to cybersecurity investment, IEEE Access. 2018. Vol. 6. URL: https://www.researchgate.net/publication/321087294_An_Options_Approach_to_Cybersecurity_Investment (дата звернення: 03.03.2024).

5. Lerums J. E., La'Reshia D. P., Dietz J. E. Simulation modeling cyber threats, risks, and prevention costs, in 2018 IEEE International Conference on Electro/Information Technology (EIT). 2018. P. 96–101.