Модель інтегрального оцінювання рівня кіберзахищеності корпоративних мереж

УДК 004.056.5:004.7

Денис Трухан[1]

Державний університет інформаційно-комунікаційних технологій,
[1]d.truhan@stud.duikt.edu.ua

Зростання кількості кіберінцидентів у корпоративних інформаційних системах актуалізує потребу у кількісних методах оцінювання кіберзахищеності. На практиці адміністратор безпеки часто має справу не з окремою вразливістю або окремою загрозою, а з множиною взаємопов'язаних факторів: одна вразливість може використовуватися кількома типами атак, а один захисний механізм може одночасно знижувати ризик для групи вразливостей. Тому ізольоване оцінювання загроз, вразливостей і захисних заходів призводить до завищення або заниження реального рівня ризику [2].

Метою роботи є стислий виклад моделі інтегрального оцінювання рівня кіберзахищеності корпоративних мереж, яка враховує взаємне перекриття загроз, вразливостей та захисних механізмів. На відміну від підходів, що ґрунтуються лише на усередненні CVSS-оцінок або якісних матрицях ризику, запропонований підхід розглядає елементи кіберзахисту як єдину тріаду «загрози – вразливості – захист».

Корпоративну мережу доцільно подати у вигляді кортежу $N = < A, T, V, P, C, M, W >$, де A – множина активів; T – множина кіберзагроз; V – множина вразливостей; P – множина захисних механізмів; C – матриця покриття, що відображає можливість реалізації загрози через конкретну вразливість; M – матриця нейтралізації, що відображає вплив захисних механізмів на вразливості; W – система вагових коефіцієнтів. Таке подання дозволяє перейти від описового аналізу до формалізованого обчислення інтегрального показника.

Для визначення взаємного перекриття між елементами тріади використовується ідея подібності множин. Зокрема, перекриття двох загроз можна оцінити через частку спільних вразливостей, через які вони реалізуються. Якщо дві загрози використовують однакові або близькі набори вразливостей, їхній внесок у сукупний ризик не повинен дублюватися повністю. Аналогічно оцінюється перекриття вразливостей та захисних механізмів.

$$\Omega_T(t_i, t_j) = \frac{|V(t_i) \cap V(t_j)|}{|V(t_i) \cup V(t_j)|}, \qquad (1)$$

де $\Omega_T(t_i, t_j)$ – коефіцієнт перекриття двох загроз; $V(t_i)$ та $V(t_j)$ – множини вразливостей, через які можуть бути реалізовані відповідні загрози. Значення коефіцієнта належить інтервалу $[0; 1]$: 0 означає відсутність спільних вразливостей, а 1 – повний збіг множин.

На основі матриць C і M та коефіцієнтів перекриття формується інтегральний показник кіберзахищеності $I(N)$. Він поєднує критичність активів, залишкову уразливість, ефективність захисних механізмів і ступінь дублювання ризику. У практичній інтерпретації $I(N)$ набуває значень від 0 до

1, де значення, близьке до 1, відповідає високому рівню захищеності, а значення, близьке до 0, – критичному стану системи.

Процедура обчислення показника складається з п'яти етапів: інвентаризації активів і побудови матриць взаємозв'язків; обчислення коефіцієнтів перекриття; призначення вагових коефіцієнтів; визначення часткових метрик для активів; розрахунку інтегрального показника та його інтерпретації за шкалою рівнів захищеності. Перевагою такої процедури є можливість повторного перерахунку після появи нових вразливостей або впровадження додаткових засобів захисту.

Таблиця 1

Порівняння підходів до оцінювання кіберзахищеності

Метод	**Оцінка** / $I(N)$	**Достовірність, %**	**Облік перекриття**
Пентест (еталон)	0,71	100	-
Запропонована модель	0,68	95,8	повний
CVSS v3.1	0,54	73,9	відсутній
NIST SP 800-30	0,58	81,7	частковий
ISO/IEC 27005	якісна оцінка	64,8	відсутній

Як видно з табл. 1, у тестовому сценарії запропонована модель наблизилася до еталонної оцінки, отриманої за результатами пенетраційної перевірки, і продемонструвала вищу достовірність порівняно з підходами, які не враховують структурні взаємозв'язки між загрозами, вразливостями та засобами захисту. Основна причина покращення полягає в усуненні подвійного зарахування взаємопов'язаних ризиків.

Практичне значення моделі полягає у можливості використовувати її як інструмент підтримки прийняття рішень під час аудиту корпоративної мережі. За допомогою інтегрального показника можна не лише визначати поточний рівень кіберзахищеності, а й порівнювати різні варіанти впровадження захисних механізмів, ранжувати їх за очікуваним впливом і прогнозувати залишковий ризик.

Отже, запропонований підхід дозволяє розглядати кіберзахищеність корпоративної мережі як системну характеристику, що залежить від взаємодії загроз, вразливостей і захисних механізмів. Подальші дослідження доцільно спрямувати на автоматизацію заповнення матриць C і M на основі даних SIEM, CVE/NVD та результатів сканування інфраструктури, а також на адаптацію моделі для хмарних і гібридних середовищ.

1. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. Gaithersburg: National Institute of Standards and Technology, 2012. 95 p.
2. CVSS v3.1 Specification Document. Forum of Incident Response and Security Teams (FIRST). 2019. URL: https://www.first.org/cvss/v3.1/specification-document (дата звернення: 10.01.2024).

3. ISO/IEC 27005:2018. Information technology - Security techniques - Information security risk management. Geneva: International Organization for Standardization, 2018. 87 p.
4. MITRE ATT&CK: Design and Philosophy. MITRE Corporation Technical Report. Bedford, MA, 2020. 57 p.

Система нечіткого логічного виводу вразливостей та загроз інформаційної безпеки

УДК 004.056

Володимир Джулій[1], Денис Вишневський[2]

Хмельницький національний університет,
[1]dzhuliivm@khmnu.edu.ua, [2]vushnya5495@gmail.com

Аналіз проведеного дослідження поточного стану в області інформаційної безпеки показує, що темпи розвитку інформаційних та комп'ютерних технологій значно випереджають процес створення програмно-апаратного забезпечення в області інформаційної безпеки. Пріоритетними, в даній ситуації, є задача аналізу, класифікації, виявлення діючих механізмів та засобів проведення атак і загроз інформаційній безпеці системи, які можуть призвести до отримання несанкціонованого доступу до конфіденційних даних, порушення функціонування інформаційної системи, визначення заходів протидії атакам та загрозам, оцінка заданої шкоди, розробка нормативно-правової бази, механізмів захисту та критеріїв інформаційної безпеки системи протидії.

Актуальною залишається задача проектування та розробки методу, системи прогнозування, виявлення вразливостей, загроз безпеки інформації. Як інструмент для досягнення поставленої задачі пропонується використовувати нечітку інформаційно-аналітичну систему прогнозування вразливостей та загроз інформаційної безпеки, що надає функціональні можливості, які представленні на рис. 1.

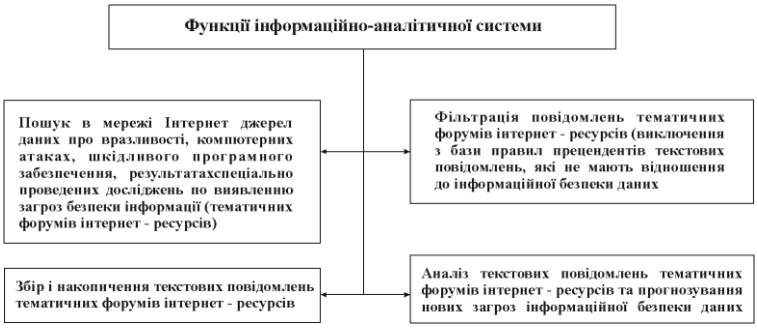

Рис.1. Функції інформаційно-аналітичної системи аналізу потоку повідомлень тематичних інтернет-форумів

Список тематичних джерел форумів містить адреси інтернет- ресурсів, на яких розміщуються текстові публікації про шкідливе програмне забезпечення, вразливості та комп'ютерні атаки [1].