Система захисту інформації в умовах динамічних ризиків

Кіреєнко О.В.
Фб-41м
5 курс

Динамічні ризики

- Об’єкт дослідження - ризики, особливості побудови системи з ризиками
- Предметом дослідження є застосування ланцюгів Маркова та симплекс методу для існуючих моделей ризиків

Підходи до розробки системи захисту

- - Економічний (підхід Гордона-Лоеба)
- - Теоретичний (підхід Журиленко)
- - КІ-ЗКІ (підхід Маслова)

Класичні системи

- Для статичних ризиків зазначені підходи використовуються наступним чином
- Чистий прибуток - Expected Net Benefits from an Investment in Information Security
- $ENBIS(z) = [\,v - S(z,v)\,]L - z$
- *для підходу Г.-Л.*
- *1-(p+qp+(q^2)*p+ … + (q^(m-1))*p) = 0,99*
- *Для підходу Журиленко*

Класичні підходи

- Для підходу Маслова використовують цю формулу
- $1\text{-}P_R = \exp(-\tau_k k_R/R_0)$
- $\tau_k k_R$ – поточний рівень сигналу тривоги
- R_0 – критичний рівень сигналу тривоги
- T_k – час здійснення атаки
- $1\text{-}P_R$ – імовірність успіху

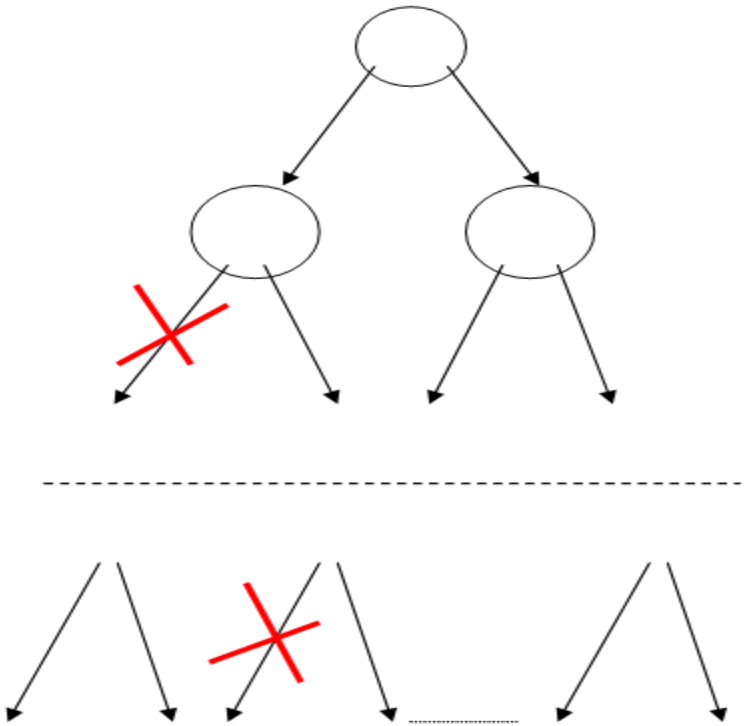
Адаптація засобів оптимізації та ланцюгів Маркова до класичних методів

- Для підходу Гордона-Лоеба знаходять не тільки оптимальну кількість коштів, що інвестують в захист, та їх розподіл між різними підсистемами (авторизація, цифровий підпис і т.д.)
- Жорсткі обмеження за часом суттєво обмежують застосування симплекс методу. Оптимальний розв’язок буде знайдено, але його неможливо впровадити.
- Для підходу Журиленко імовірності успіху зловмисника так само задаються функціями, але тепер параметри цих функцій є елементами ланцюга Маркова. Перевага – простота розрахунку, недолік – тільки для однорідних ланцюгів.

Ланцюг Маркова

- Функціонування будь-якої сучасної складної системи пов’язане з вибором дій. Навіть персональний комп’ютер має безліч застосувань. Його можна використовувати для ігор або для роботи. Рішення про поточний режим функціонування приймає користувач (або процес). Це рішення носить імовірнісний характер. Будь-яку послідовність станів функціонуючої системи (або системи, що проектується) можна представити у вигляді маршруту в дереві. Кожен маршрут відповідає одному з варіантів ланцюга Маркова.

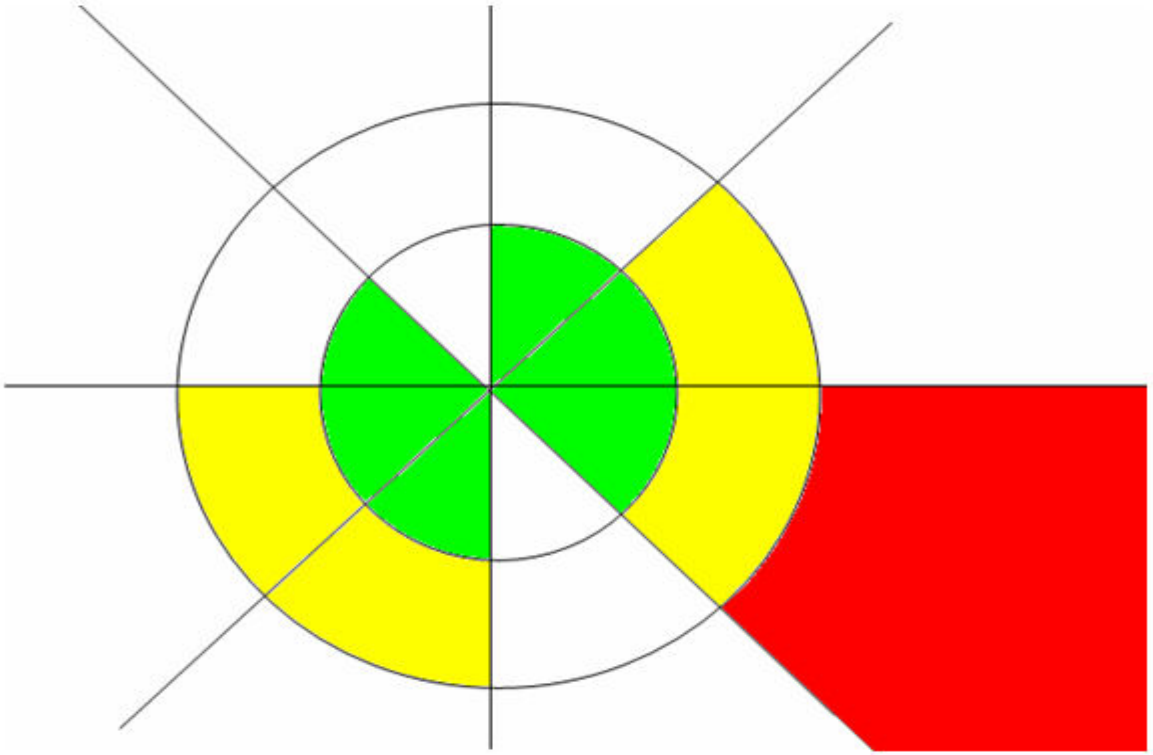
Дерево станів системи



Адаптація засобів оптимізації та ланцюгів Маркова до класичних методів

- Для підходу Маслова
- Формули розрахунку сигналу тривоги залишаються без змін
- Застосування даного підходу використовується в системах, що здатні відновлюватись навіть після серйозних збоїв.
- Ланцюг Маркова використовують для простого прогнозування дій, що виконуються системою. Якщо поведінка системи суттєво відрізняється від запланованої (наприклад якийсь процес запросив значну кількість ресурсів) – можливо завчасно виявити несанкціоновані дії в системі.

Діаграма сигналу тривоги



Дякую за увагу