Салієва О. В.

ВИЗНАЧЕННЯ ВИТРАТ НА ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ РАНЖУВАННЯМ ЗАГРОЗ

Вінницький національний технічний університет
salieva8257@gmail.com

Анотація. Невід'ємною складовою ефективного функціонування системи захисту інформації є проведення аналізу можливих загроз безпеці досліджуваної системи та визначення допустимих витрат на забезпечення її захищеності. Одним із способів вирішення окреслених завдань є метод, що базується на ранжуванні загроз інформаційної безпеки на основі нечіткого відношення впливу та транзитивного замикання. У результаті визначення рангів загроз здійснюється розбиття множини загроз системи захисту інформації на класи, які не перетинаються та містять елементи еквівалентні за вагомістю. Для забезпечення захищеності даної системи пропонується розподіл допустимих витрат у пропорційній еквівалентності визначеним рангам загроз. Це сприятиме раціональному використанню ресурсів та засобів для попередження, усунення або ж зменшення сили впливу ймовірних загроз інформаційній безпеці.

Ключові слова: інформаційна безпека, загрози безпеці, нечітке відношення, транзитивне замикання.

Вступ

Проблема якісного функціонування системи захисту інформації, з огляду на появу нових та зростання рівня існуючих загроз в інформаційному просторі, набуває надзвичайної вагомості. Причому важливою практичною проблемою є встановлення оптимального балансу між забезпеченням захищеності системи безпеки та обсягом витрат на її підтримку, враховуючи раціональний розподіл між окремими напрямами захисту. У переважній більшості дане питання вирішується за допомогою методів статистичного аналізу, які потребують розгляду значного обсягу інформації, складних розрахунків та займають тривалий час для опрацювання. Тому для розв'язання даної задачі доцільно звернути увагуна метод ранжування загроз на основі теорії нечітких відношень, який не потребує трудомісткого навчання експертів та характеризується простотою і доступністю реалізації [1].

Результати дослідження

Запропоновано розподіл допустимих витрат на забезпечення захищеності системи захисту інформації пропорційно визначеним рангам загроз [2]. Для здійснення даного розподілу визначено множину найвагоміших, з точки зору вивчення даної проблеми, загроз [3] та критерії, у порушенні яких виражаються відповідні загрози. Вплив загроз на порушення відповідних критеріїв задано нечіткою множиною та розраховано ступені даного впливу шляхом порівняння з найменшим впливом за шкалою Сааті [4]. Відповідну інформацію формалізовано у вигляді нечіткого відношення впливу, яке перетворюється у нечітке відношення схожості та його транзитивне замикання. Для цього надано початковому не транзитивному відношенню схожості R властивість транзитивності, використовуючи операцію транзитивного замикання нечіткого відношення:

$$\overline{R} = R \cup R^2 \cup ... \cup R^\kappa \cup ...,$$

де відношення R^k знаходиться рекурсивно: $R^k = R^{k-1} \circ R$, $k = 2,3,...,n$;

$\cup$ – операція об'єднання нечітких відношень;

$\circ$ – операція нечіткої композиції.

Знайдено ранги, що відповідають загальному впливу i-тої загрози на виконання усіх критеріїв системи захисту інформації.

Розкладено нечітке відношення R заα – рівнями. Причому число α - рівень визначеності знань про систему. Чим складніша система і чим більше не враховуютьсяреальні події при моделюванні, тим більша невизначеність і тим менше число α. Чіткі відношення α – рівня утворюють класи загроз інформаційній безпеці, які за вагомістю еквівалентні, тобто загрози одного класу майже однакові за ступенем важливості й порівняльною динамікою їх наростання.

Побудовано дерево декомпозиції, яке наглядно представляє на кожному α - рівнічисло класів та перелік загроз, які належать даному класу.

У відповідності із визначеними рангами загроз, здійснено розподіл допустимихвитрат на забезпечення захищеності досліджуваної системи.

Висновки

На основі проведеного ранжування загроз, що базується на теорії нечітких відношень, було визначено, пропорційно рангам, допустимі витрати на забезпечення захищеності системи захисту інформації. З цією метою було здійснено розбиття множини загроз системі безпеки на класи, які не перетинаються та містять елементи еквівалентні за вагомістю. Побудовано дерево декомпозиції на класи еквівалентності. Отримані результати надають змогу доцільно вибудувати чіткий план організації захисту інформаційного простору, враховуючи ступінь впливу кожного класу загроз, забезпечити баланс між рівнем інформаційного ризику та допустимими витратами на проведення заходів інформаційної безпеки.

Література

1. А. П. Ротштейн, «Ранжирование элементов системы на основе нечеткого отношения влияния и транзитивного замыкания», *Кибернетика и системный анализ*, Том 53, №1, С. 68-78, 2017.
2. О. В. Салієва, Ю. Є. Яремчук, «Ранжування загроз для визначення витрат на забезпечення захищеності системи захисту інформації на основі теорії нечітких відношень», *Захист інформації*, Т. 22, №1, с. 51–59, 2020.
3. О. В. Салієва, Ю. Є. Яремчук, «Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання», *Безпека інформації*, №1, с. 42-49, 2020.
4. T. L. Saaty, Mathematical models of arms control and disarmament, New York: John Willey & Sons, 1968, 304 p.