УДК 004.056.053

О.В. Сівіцький, А. М. Луцків, канд. техн. наук, доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ОЦІНЮВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

O. V. Sivitskiy, A. M. Lutskiv, Ph.D

COMPARATIVE ANALYSIS OF METHODS OF EVALUATION OF INFORMATION SECURITY

В умовах швидкого розвитку інформаційних технологій постійно виникають нові види загроз для апаратного і програмного забезпечення комп'ютерних систем. Тому над створенням єдиної моделі оцінювання захищеності інформації та ресурсів працюють багато відомих фахівців та науковців. Великої популярності протягом останнього часу набули кількісні моделі оцінювання СЗІ на основі аналізу ризиків. На основі їх алгоритмів було розроблено та модернізовано багато програмних продуктів, серед яких: Microsoft Baseline Security Analyzer (MBSA), CRAMM, CounterMeasures, BCM-Analyse та інші.

Таблиця 1 – Аналіз властивостей моделей оцінювання СЗІ

Назва моделі / Властивості	Модель оцінювання СЗІ «MATRIX» Домарьова В. В.	Модель оцінювання СЗІ Маслової Н. А. з використанням алгоритму оптимізації обчислень Балишева	Модель оцінювання СЗІ на основі графа захищеності
Метод оцінювання СЗІ	Комплексний	Кількісний	Кількісний
Обчислювальна складність моделі	Проста	Складна	Складна
Можливість програмної реалізації	+	+	+
Вираження можливості втрат інформації від НСД	В відсотковому співвідношенні	В відсотковому співвідношенні	В грошовому еквіваленті
Поетапне виконання оцінювання СЗІ	+	+	+
Оцінювання СЗІ за заданим критерієм	+	+	-
Врахування при оцінюванні СЗІ нормативно-правової бази України	+	-	-
Врахування структури мережі	+	-	+
Графічна реалізація методу	+	+	+
Оцінювання вразливостей і ризиків СЗІ	+	+	+
Оцінювання захищеності ПЗ	+	-	-
Склад експертної групи, кількість осіб	<=10	<=8	<=7

Метод оцінювання ефективності СЗІ з використанням алгоритму Балишева відноситься до кількісних методів оцінювання СЗІ і ключовою перевагою даного методу є можливість поетапного виконання процедури оцінювання ефективності СЗІ.

Недоліками цього методу, є те, що його програмна реалізація навіть із застосуванням методів оптимізації обчислень Балишева й методу гілок та границь є надзвичайно складною. Даний метод потребує великих затрат на обчислювальні ресурси та експертів, які б змогли реалізувати даний алгоритм та підтримувати програмний продукт. До недоліків даного методу також можна віднести те, що при оцінюванні ефективності СЗІ не враховується нормативно-правова база України, що на даний час є важливою складовою оцінювання СЗІ. Ще однією негативною рисою можна вважати і те, що даний метод оперує поняттям інформаційний ресурс. Тобто, деталізувати під час проведення оцінювання СЗІ чи це є вузол комп'ютерної мережі, чи це програмне забезпечення неможливо.

Суть методу оцінювання СЗІ з використанням графа захищеності полягає у тому, що рівень захисту інформації в мережі визначається захищеністю кожного із них незалежно один від одного. Даний алгоритм можна віднести до кількісних методів оцінювання. До переваг даного методу можна віднести те, що оцінювання СЗІ можна виконувати як комплексно, так і поетапно. Під час оцінювання ефективності СЗІ повністю оцінюється структура мережі, що є важливою складовою процесу оцінювання. Даний метод має просту графічну реалізацію у вигляді графа, звідки і походить назва алгоритму. Також, даний метод як і всі з представлених дозволяє ефективно оцінити вразливості і ризики СЗІ.

Недоліками методу на основі графів захищеності є складна модель обчислювальних задач, що в певній мірі ускладнює реалізацію програмного продукту. Вираження втрат інформації від НСД виражається в грошовому еквіваленті, що не дозволяє правильно і ефективно оцінити СЗІ. Під час оцінювання СЗІ в рамках даного методу неможливо оцінити ПЗ СЗІ, оскільки, в даному методі це розглядається як інформаційний ресурс. Також, недоліком є те, що як і в попередньому випадку, при оцінюванні СЗІ не враховується нормативно-правова база України, що на даний час є важливою складовою оцінювання СЗІ.

Суть методу В.В. Домарьова «Matrix» полягає в тому, що модель подається у вигляді трьох блоків показників, які об'єднуються в матрицю оцінювання. Кожен із елементів цієї матриці – це є кількісна оцінка експерта одного з критеріїв оцінювання СЗІ. Перевагами даного методу є невелика обчислювальна складність і простота програмної реалізації. Оцінювання СЗІ даним методом передбачає поетапне виконання за певним вибраним критерієм. Тобто, замовнику непотрібно проводити повністю аудит безпеки ІС, а тільки певного її параметру. За останнім критерієм даний метод можна вважати одним із кращих.

Критичною особливістю даного методу є рівень знань та навичок експертів, які проводитимуть оцінювання СЗІ, оскільки, від цього залежить результат оцінювання.

Проаналізувавши переваги та недоліки кожного із методів оцінювання СЗІ можна зробити висновок про доцільність використання моделі оцінювання СЗІ на базі математичного забезпечення В. В. Домарьова «Matrix».

Література.

1. Маслова Н.А. Построение модели защиты информации с заданными характеристиками качества // Штучний інтелект. – Донецьк: ІШІ, 2007. – № 1. – С. 51-57

2. Авраменко В.С., Козленко А.В. Модель для количественной оценки защищенностиинформации от несанкционированного доступа в автоматизированных системах покомплексному показателю // Труды СПИИРАН, №13, 2010. С. 172–181.

3. Домарев В. В. Оценка эффективности систем защиты информации [Електронний ресурс]. - Режим доступу: URL: http://domarev.com.ua/index.html/