

УДК 004.056.53

Савченко Ю.В.¹, Паршина О.А.², Воскобойник В.О.³

¹канд. техн. наук, доцент Університету митної справи та фінансів

²д-р економ. наук, професор Університету митної справи та фінансів

³канд. техн. наук, доцент НУ «Запорізька політехніка»

МЕТОДОЛОГІЯ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Процес діджиталізації сучасного суспільства породжує проблеми, які пов'язані з можливістю несанкціонованого доступу до ресурсів критично важливого об'єкта. Безпека ресурсів критично важливого об'єкта (КВО) має велике значення для забезпечення ефективної життєдіяльності як окремого підприємства зокрема, так і всієї держави загалом. Тому питання розробки і впровадження системи для оцінювання рівня захищеності інформації є, безумовно, актуальним.

Важливою умовою ефективної роботи системи захисту ресурсів критично важливого об'єкта є її керованість. Сучасна система захисту ресурсів КВО має складну, багатокомпонентну фізично і логічно розподілену структуру. Проектування оптимальної системи захисту передбачає використання якісної та кількісної інформації про важливість критеріїв та побудову багатокритеріального узагальненого критерію прийняття рішень на об'єктах критичної інфраструктури, в основі якого покладений певний набір таких необхідних підсистем—модулів, як: модуль захисту периметра мережі та між мережових взаємодій, модуль захисту серверів мережі, засоби захисту робочих станцій, модуль комплексного антивірусного захисту, засоби криптографічного захисту тощо. При побудові узагальненої системи захисту КВО необхідно витримувати певний баланс між необхідним рівнем захисту або ймовірними ризиками втрат та інвестиціями в систему захисту. Тому актуальним є питання розробки уніфікованих математичних моделей для системного проектування оптимальних систем захисту критично важливих об'єктів.

Метою дослідження є розробка багатокритеріальних узагальнених критеріїв для проектування інтегрованої оптимальної системи захисту ресурсів критично важливих об'єктів.

Методологія оцінювання захищеності інформаційних ресурсів. Комплексний підхід щодо оцінювання захищеності ресурсів КВО базується на формалізації вхідних даних до яких, у першу чергу, належать середні значення ймовірні загрози, характеристики та обмеження інформаційних потоків, що існують на об'єкті, специфічні ознаки технологічних процесів тощо. Такий загальносистемний підхід можна формалізувати у вигляді структури реалізації системи захисту КВО (рис. 1), де C_{vi} та $C_{уд}$ – критерії управління інформацією та даними, $C_{зі}$ та $C_{зд}$ – критерії загроз інформації та даним.

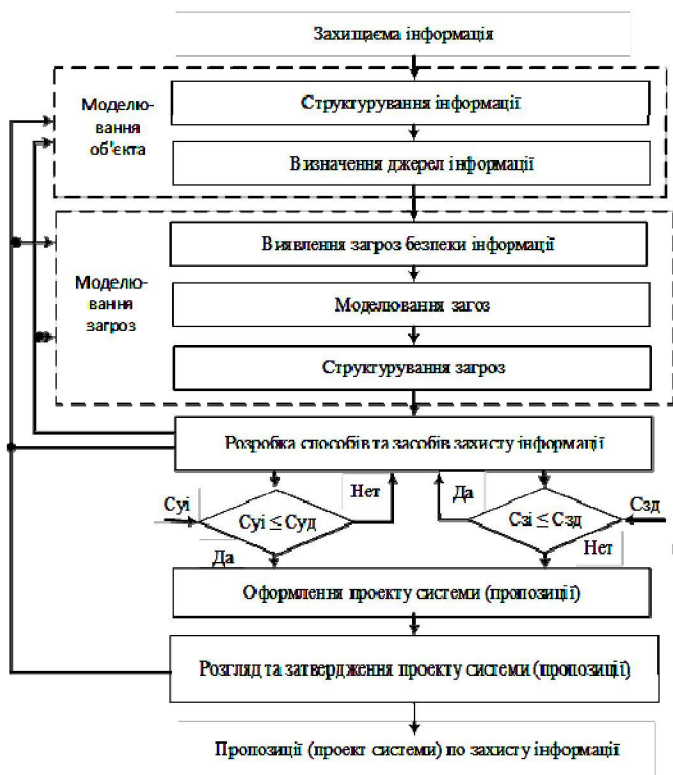


Рисунок 1 — Структура реалізації систем захисту КВО

Розв'язання задачі побудови оптимальної системи захисту почнемо з ідентифікації небезпек, які необхідно враховувати при оцінюванні загальної захищеності ресурсів КВО. Небезпеки у вигляді назв подій наведені в табл. 1.

Визначити оптимальний варіант КВО з використанням узагальненого (інтегрального) адитивного критерію. Приватними критеріями, за допомогою яких оцінені варіанти КВО, є назви подій. Всі критерії «працюють» мінімум, тобто найкращими варіантами КВО є з тих, які забезпечують найменші її назви подій. Вихідні дані по варіантам 1-3 та нормам 1-3 вагових коефіцієнтів для вирішення задачі побудови оптимальної системи захист наведені у таблиці 1.

Цільова функція на основі адитивного критерію (по 23 приватних критеріях) запишеться таким чином:

$$F(X) = \sum_{i=1}^{23} C_i \cdot \frac{F_i(X)}{F_i^{(0)}(X)} \rightarrow \min, \quad (1)$$

де C_i – ваговий коефіцієнт і-го приватного критерію; $F_i(X)$ – числове значення і-го приватного критерію; $F_i^{(0)}(X)$ – і-й нормуючий дільник.

Таблиця 1 — Вхідні дані для визначення оптимального варіанта КВО

Назва події (приватні критерії)	Критерії (ймовірність)значення				Вагові коефіцієнти		
	позначення	Варіант 1	Варіант 2	Варіант 3	Норма 1	Норма 2	Норма 3
Загрози. пов'язані з програмним забезпеченням							
Вірусна атака	K11	0.1	0.163	0.120	0.043	0.046	0.064
Помилка коду	K12	0.005	0.007	0.006	0.043	0.032	0.019
Наявність мережі	K13	0.5	0.935	0.670	0.043	0.041	0.013
Зовнішня загроза	K14	0.1	0.114	0.120	0.043	0.050	0.015
Черви	K15	0.05	0.088	0.200	0.043	0.041	0.042
"Троянські" віруси	K16	0.03	0.052	0.050	0.043	0.025	0.058
Закладні об'єкти	K17	0.01	0.011	0.100	0.043	0.026	0.048
Загрози. пов'язані з персоналом							

Назва події (приватні критерії)	Критерії (ймовірність)значення				Вагові коефіцієнти		
	позначення	Варіант1	Варіант2	Варіант3	Норма 1	Норма 2	Норма 3
Помилки персоналу	K21	0.25	0.200	0.300	0.043	0.031	0.067
Ненадійні працівники	K22	0.2	0.130	0.500	0.043	0.058	0.037
Ворожа розвідка	K23	0.9	0.774	0.827	0.043	0.056	0.039
Неякісна політика інформаційної безпеки	K24	0.1	0.053	0.120	0.043	0.059	0.035
Людський фактор	K25	0.2	0.068	0.131	0.043	0.036	0.011
Помилка режиму	K26	0.1	0.056	0.065	0.043	0.047	0.028
Нестача ресурсів захисту	K27	0.07	0.017	0.080	0.043	0.050	0.070
Загрози, пов'язані з технічними засобами							
Зняття жучком	K31	0.15	0.270	0.029	0.043	0.040	0.043
Витік оптичної інформації	K32	0.3	0.200	0.030	0.043	0.036	0.072
Електромагнітне нав'язування	K33	0.05	0.077	0.009	0.043	0.059	0.019
Зняття стетоскопом	K34	0.005	0.007	0.008	0.043	0.037	0.073
Доступ до заземлення	K35	0.02	0.034	0.017	0.043	0.052	0.053
Підключення до каналу зв'язку	K36	0.35	0.800	0.385	0.043	0.057	0.035
Непомітне зняття	K37	0.1	0.146	0.034	0.043	0.043	0.017
Передача конфіденційної інформації	K38	0.05	0.095	0.042	0.043	0.046	0.030
Розпізнання інформації	K39	0.2	0.360	0.226	0.043	0.059	0.050

Приватні критерії мають різну фізичну природу і тому різну розмірність. А отже, просто підсумовувати їх некоректно. У зв'язку з цим у попередній формулі числові значення приватних критеріїв поділяються на деякі нормуючі дільники. В якості нормуючих дільників приймаються директивні значення параметрів або критеріїв. Вважається, що значення параметрів, закладені в технічному завданні, є оптимальними або найкращими.

Один із недоліків цього методу полягає в тому, що вагові коефіцієнти призначає керівник. Різні керівники можуть призначати різні вагові коефіцієнти.

Тому оптимальним варіантом системи захисту критично важливого об'єкта при різних нормах вагових коефіцієнтів відповідає мінімальне значення узагальненого адитивного критерію.