УДК 621.391:004.056.5 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.063

ВИРІШЕННЯ ЗАВДАННЯ ОПТИМАЛЬНОГО ВИБОРУ ЗАСОБІВ ЗАХИСТУ ДЛЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА ОСНОВІ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ

Гонтар Д.Ю., Пшеничних С.В.
Науковий керівник – к.т.н., с.н.с. Пшеничних С.В., каф. ІКІ
Харківський національний університет радіоелектроніки
м. Харків, Україна
e-mail: daria.hontar@nure.ua

This document presents a variant of solving the problem of optimal selection of security tools to create an effective integrated information security system for a small computer network of an enterprise using the T. Saaty hierarchy analysis method. The main optimality criteria are the residual risk and the level of implementation costs. In the course of the work, a hierarchical system was built, the priorities of each of the criteria were calculated, and the global priorities of the proposed security measures were determined. Based on the data obtained, the optimal complex for a given computer network of an enterprise was proposed.

Велике різноманіття технічних і програмних засобів захисту інформації ставить завдання оптимального їх вибору для створення ефективної комплексної системи захисту інформації (КСЗІ). При розробці звертається увага на такі параметри, як залишковий ризик після її впровадження та рівень витрат на реалізацію. Метою даної роботи є використання методу аналізу ієрархій (МАІ) Т. Сааті, задля визначення оптимального комплекту програмно-технічних засобів забезпечення захисту від кіберзагроз для невеликої комп'ютерної мережі підприємства, яка складається зі 100 персональних комп'ютерів та двох файлових серверів. В таблиці 1 представлено перелік найпоширеніших кіберзагроз на комп'ютерну мережу та ризики їх реалізації, параметри для обрахування яких було визначено методом експертних оцінок.

Таблиця 1 – Можливі загрози безпеці та можливі збитки від їхньої реалізації на інтервалі часу один рік

Загроза	Ймовірність реалізації	Можливі збитки від реалізації, грн.	Ризик від реалізації, грн.
Витік конфіденційної інформації (загроза 1)	0,8	1800000	1440000
Несанкціоноване вторгнення в мережу (загроза 2)	0,6	500000	300000
Вірусна атака (загроза 3)	0,9	2900000	2610000

В таблиці 2 відображено перелік запропонованих засобів захисту, їх вартість та можливості запобігання обраним загрозам впродовж одного року, які також були визначені на основі експертних оцінок.

Таблиця 2 – Засоби захисту від загроз безпеки, вартості їхньої реалізації та можливості запобігання загрозам на інтервалі часу один рік

Засіб захисту	Вартість реалізації, грн.	Витрати на експлуатацію, грн.	Можливість запобігання загрозі		
			витоку конфіденційної інформації	несанкціонованого вторгнення в мережу	вірусної атаки
Logpoint SIEM (засіб 1)	138453	36000	0,5	0,8	0
ESET NOD32 Antivirus (засіб 2)	20088	0	0	0	0,9
ActivTrack Professional (засіб 3)	890712	34000	0,8	0	0
Quantum Rugged 1595R (засіб 4)	71857	44400	0,5	0,7	0,3

На рисунку 1 наведено розроблену ієрархічну систему, де на кожному рівні представлено критерії, які використовуються для оцінки альтернативних варіантів відповідно до головної мети [1]. Для зручності розрахунків для кожного елементу було визначено умовне позначення та індекси: перший визначає рівень у ієрархії, а другий – порядковий номер показника на певному рівні.

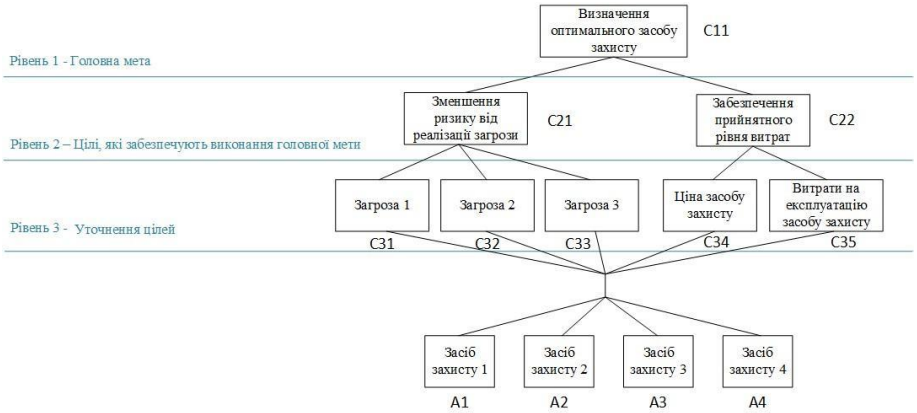
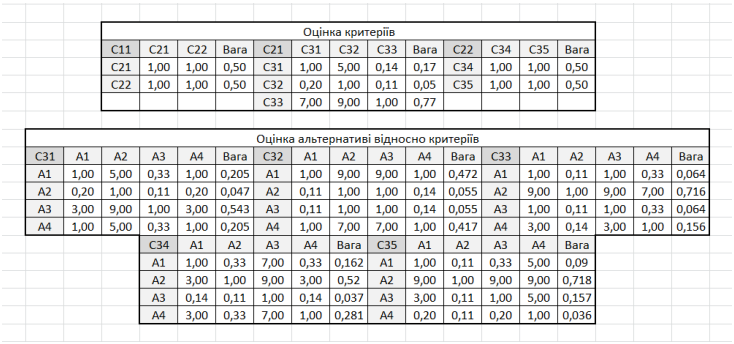


Рисунок 1 – Ієрархія для визначення оптимального засобу захисту

Наступним кроком є оцінка критеріїв за допомогою попарного порівняння за шкалою від 1 до 9 для визначення їх відносної значущості до критерію вищого за рівнем. Після цього було обчислено вагу кожного

критерію, яка знаходиться як нормоване середнє геометричне елементів матриці [2]. Результат проведених обчислень представлено на рисунку 3.



Оцінка критеріїв

C11	C21	C22	Вага	C21	C31	C32	C33	Вага	C22	C34	C35	Вага
C21	1,00	1,00	0,50	C31	1,00	5,00	0,14	0,17	C34	1,00	1,00	0,50
C22	1,00	1,00	0,50	C32	0,20	1,00	0,11	0,05	C35	1,00	1,00	0,50
				C33	7,00	9,00	1,00	0,77				

Оцінка альтернативі відносно критеріїв

C31	A1	A2	A3	A4	Вага	C32	A1	A2	A3	A4	Вага	C33	A1	A2	A3	A4	Вага
A1	1,00	5,00	0,33	1,00	0,205	A1	1,00	9,00	9,00	1,00	0,472	A1	1,00	0,11	1,00	0,33	0,064
A2	0,20	1,00	0,11	0,20	0,047	A2	0,11	1,00	1,00	0,14	0,055	A2	9,00	1,00	9,00	7,00	0,716
A3	3,00	9,00	1,00	3,00	0,543	A3	0,11	1,00	1,00	0,14	0,055	A3	1,00	0,11	1,00	0,33	0,064
A4	1,00	5,00	0,33	1,00	0,205	A4	1,00	7,00	7,00	1,00	0,417	A4	3,00	0,14	3,00	1,00	0,156

C34	A1	A2	A3	A4	Вага	C35	A1	A2	A3	A4	Вага
A1	1,00	0,33	7,00	0,33	0,162	A1	1,00	0,11	0,33	5,00	0,09
A2	3,00	1,00	9,00	3,00	0,52	A2	9,00	1,00	9,00	9,00	0,718
A3	0,14	0,11	1,00	0,14	0,037	A3	3,00	0,11	1,00	5,00	0,157
A4	3,00	0,33	7,00	1,00	0,281	A4	0,20	0,11	0,20	1,00	0,036

Рисунок 3 – Результати обчислення ваг елементів ієрархії

На основі отриманих результатів було розраховано підсумкову вагу для кожного із запропонованих засобів захисту за допомогою адитивної згортки локальних ваг альтернатив за окремими критеріями з урахуванням ваг цих критеріїв [2]. Результати проведених обчислень представлено у таблиці 3.

Таблиця 3 – Результати обчислень підсумкових ваг для кожного із засобів захисту

Засіб захисту	Logpoint SIEM	ESET NOD32 Antivirus	ActivTrack Professional	Quantum Rugged 1595R
Підсумкова вага	0,10689	0,59217	0,122128	0,16829

Аналіз результатів розрахунків (табл. 3) показує, що для запобігання вірусної атаки оптимальним є засіб захисту 2. Засіб 4 забезпечує захист відразу від трьох загроз. Цей засіб є оптимальним за критерієм «ефективність-вартість» і забезпечує розумний баланс між вартістю реалізації засобу та ефективністю протидії загрозам. Тобто, для даного випадку оптимальний комплект засобів захисту складають засоби ESET NOD32 Antivirus та Quantum Rugged 1595R.

Таким чином, метод аналізу ієрархій може бути застосований для вирішення завдання оптимального вибору засобів захисту від загроз безпеки на об'єкті інформатизації.

Список використаних джерел:

1. Васильєв О. Б., Васильєва Н. С., Кічмаренко О. Д. Методи розв’язування задач багатокритеріальної оптимізації : метод. вказівки. Одеса, 2017. 48 с.

2. Файнзільберг Л. С., Жуковська О. А., Якимчук В. С. Теорія прийняття рішень : підручник. Київ, 2018. 246 с.