УДК 621.391

Г.А. Вашакідзе, студент; В.В. Пасльон, к.т.н., доцент; І.Л. Щербов старший викладач, А.Є. Якушина старший викладач.

Донецький національний технічний університет, м. Донецьк

кафедра радіотехніки та захисту інформації

e-mail: schil@rtf.donntu.edu.ua gur.vash@yandex.ru

МЕТОДИКА ПРИЙНЯТТЯ РІШЕННЯ ПО ОЦІНКИ РИЗИКІВ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Г.А. Вашакідзе, В.В. Пасльон, І.Л. Щербов, А.Є. Якушина методика прийняття рішення по оцінки ризиків в телекомунікаційних системах. *Проведено аналіз послідовності прийняття рішення з управління інформаційною безпекою в телекомунікаційній системі (ТКС). Розглянуто найбільш поширені методи оцінки ризику. Запропоновано порядок дискретної оцінки ризику для інформаційно-телекомунікаційної системи на основі експертних оцінок очікуваного збитку в разі реалізації загроз.*

Ключові слова: *телекомунікаційна система, методи оцінки ризику, алгоритм прийняття ризику*

Постановка завдання

Застосування у повсякденному житті як окремо взятої людини, так і держави в цілому, сучасних інформаційно-телекомунікаційних технологій дозволяє отримувати всі блага досягнень сучасної науки і техніки. При цьому все значніше зростає залежність процесів життєдіяльності людини від навколишнього інформаційного простору. Дана залежність призводить до виникнення нових видів загроз - кібернетичних злочинів. Розробка ефективних моделей і методів управління безпекою телекомунікаційних систем з метою протидії кібернетичної злочинності, є актуальним завданням.

Вирішення даного завдання ускладнюється значною кількістю факторів, що впливають на його виконання. Найбільш суттєвими є:

- необхідність виконання сукупності технічних вимог для спільної роботи програмних продуктів та обладнання різних виробників;

- необхідність ефективного використання каналів зв'язку та дотримання вимог електромагнітної сумісності;

- врахування потенційних загроз для безпеки ІТС та оброблюваної в ній інформації;

- необхідність врахування перспектив модернізації системи;

- собівартість та ін [1] .

Безумовно, рішення даної задачі має базуватися на вимогах міжнародних стандартів і рекомендацій. При цьому обов'язковою умовою при прийнятті рішення є виконання вимог національного законодавства, що регламентує дану сферу діяльності .

Аналіз стану проблеми і вирішення завдання

Враховуючи широкий спектр юридичних та фізичних осіб, які надають послуги, обладнання та програмне забезпечення, що застосовуються в сфері телекоммунікацій Міжнародним союзом електрозв'язку в рекомендації МСЕ-Т Х.805 запропонована архітектура захисту для систем, що забезпечують зв'язок між кінцевими пристроями (рис.1). Дана архітектура дозволяє провести деталізацію складових частин ІТС, з метою спрощення прийняття рішення, спрямованого на ефективне управління, контроль і використання мережевої інфраструктури, послуг і програм. Архітектура захисту забезпечує комплексну, зверху донизу наскрізну область мережевого захисту і може застосовуватися до елементів мережі, послуг і програм, з тим, щоб виявляти, прогнозувати і виправляти уразливість захисту [3]

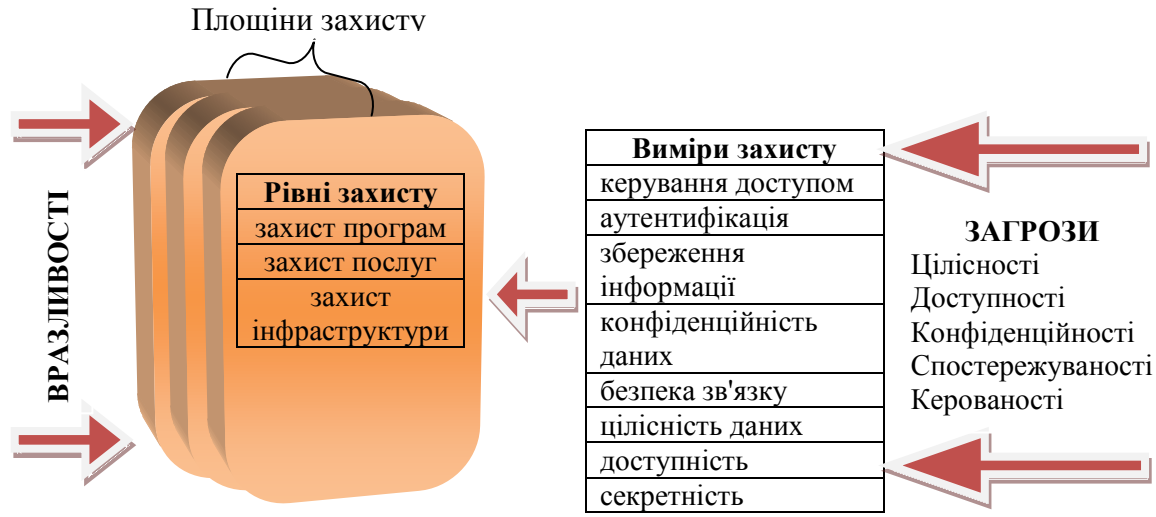

Рис.1. Архітектура захисту систем, що забезпечують зв'язок між кінцевими пристроями.

Прийнята архітектура захисту систем, що забезпечують зв'язок між кінцевими пристроями, дозволяє більш якісно провести оцінку ризику безпеки ІТС. З цією метою, виходячи з рекомендацій міжнародного стандарту ISO / IEC 27005 «Менеджмент ризику інформаційної безпеки», в початковій стадії прийняття рішення проводиться облік активів, уразливість яких може вплинути на ступінь захищеності ІТС [4].

Доцільно активи телекомунікаційної системи розглядати окремо у відповідності до площини захисту:

- управління;

- контролю;

- кінцевого користувача.

А для кожної площини захисту виділяти активи, що відносяться до відповідного рівня: інфраструктури, послуг, застосовуваних програм.

Враховуючи важливість початкового етапу прийняття рішення, до даного процесу повинен бути притягнутий персонал, що має відповідну кваліфікацію та досвід роботи.

Таки вимоги до експертів, наприклад, сформульовані у рекомендації в галузі стандартизації банку Росії:

- наявність вищої освіти;

- досвід роботи в даній професійній області не менше чотирьох років;

- систематичне підвищення кваліфікації;

- здатність ідентифікувати людей, здатних надати необхідну інформацію;

- володіння навичками ділового та управлінської взаємодії [5].

Наступним кроком оцінки ризиків активів є визначення загроз для ідентифікованих активів. Загрози для ІТС за своєю природою поділяються на природні та техногенні, останні в свою чергу поділяються на випадкові і навмисні. На даному етапі також визначається джерело загроз і «область» дії загрози, тобто, на які складові частини ІТС може впливати дана загроза.

Етап оцінки вразливості активів схематично представлені на рисунку 2.

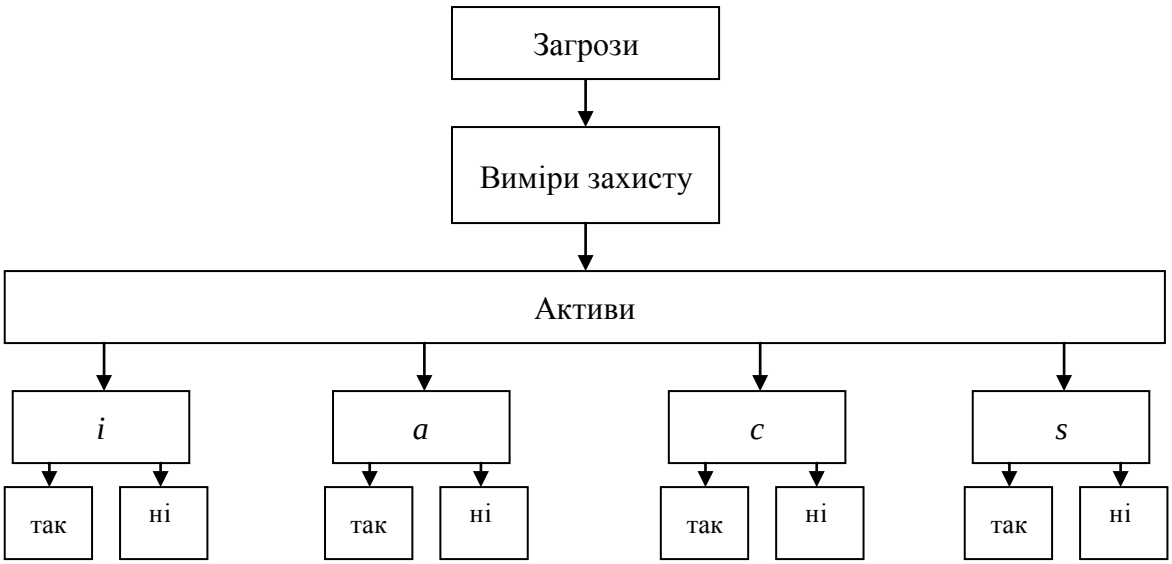

Рис.2. Оцінка вразливості активів від ймовірних загроз.

Виміри захисту по своїй суті являють комплекс реалізованих заходів щодо захисту активів ТКС. У випадку успішної реалізації загрози активам може бути завдано шкоди, яка може привести до втрати властивостей інформації або керованості та спостереженості ТКС:

• цілісність (i);

• доступність (a);

• конфіденційність (c);

• спостереженость та керованість (s).

Таким чином визначається рівень стану захищеності ТКС від загроз.

Виділяється вісім основних вимірів захисту (рисунок 1):

1) управління доступом;

2) аутентифікація ;

3) збереження інформації ;

4) конфіденційність даних;

5) безпека зв'язку;

6) цілісність даних;

7) доступність;

8) секретність [3].

Результати оцінки уразливості активів на прикладі загроз, що можуть бути реалізовані з урахуванням недоліків протоколів міжмережевої взаємодії, наведені в таблиці 1.

Загрози для інформаційної безпеки ТКС Таблиця 1

№ k	Загрози (threat)	Конфіденційність (confidentiality)	Цілісність (integrity)	Доступність (availability)	Спостереженість та керованість (accountability and manageability)	Ваговий коефіцієнт
1	Аналіз протоколів	c_1	i_1	a_1	s_1	p_1
2	Сканування мереж	c_2	i_2	a_2	s_2	p_2
3	Автоматичний підбір паролів	c_3	i_3	a_3	s_3	p_3
4	Spoofing	c_4	i_4	a_4	s_4	p_4
5	Захоплення мережевих підключень	c_5	i_5	a_5	s_5	p_5
6	Підміна мережевих об’єктів	c_6	i_6	a_6	s_6	p_6
7	Розподілена відмова в обслуговуванні	c_7	i_7	a_7	s_7	p_7
8	Віддалене проникнення	c_8	i_8	a_8	s_8	p_8

Використовуючи отримані дані, можна отримати кількісну оцінку уразливості конкретного активу від однієї загрози за такою формулою:

$$T_k = \frac{(c_k+i_k+a_k+s_k)}{4} * z_k * p_k \quad (1)$$

Ваговий коефіцієнт p_k визначає частоту появи даної загрози щодо сукупності можливих загроз і обчислюється на основі аналізу статистичних даних або з використанням відомих методик. Коефіцієнт z_k визначає вірогідність захисту активу ТКС за допомогою встановленого засобу захисту від загрози p_k [2].

Визначення вразливості активу від всіх імовірних загроз Q_l визначаємо наступним чином:

$$Q_l = \sum_{i=1}^{k} \frac{(c_i+i_i+a_i+s_i)}{4} * z_i * p_i \quad (2)$$

Кожний із рівнів захисту (програм, послуг, інфраструктури), що представлено на рисунку 1, складається з обмеженої кількості активів. Тому для визначення загальної оцінки захисту одного рівню Q_p скористаємось наступною формулою:

$$Q_p = \sum_{j=1}^{l} \sum_{i=1}^{k} \frac{(c_i+i_i+a_i+s_i)}{4} * z_i * p_i \quad (3)$$

На підставі отриманої кількісної оцінки захищеності активів системи приймається рішення на прийняття ризику. Алгоритм даного процесу представлено на рисунку 3.

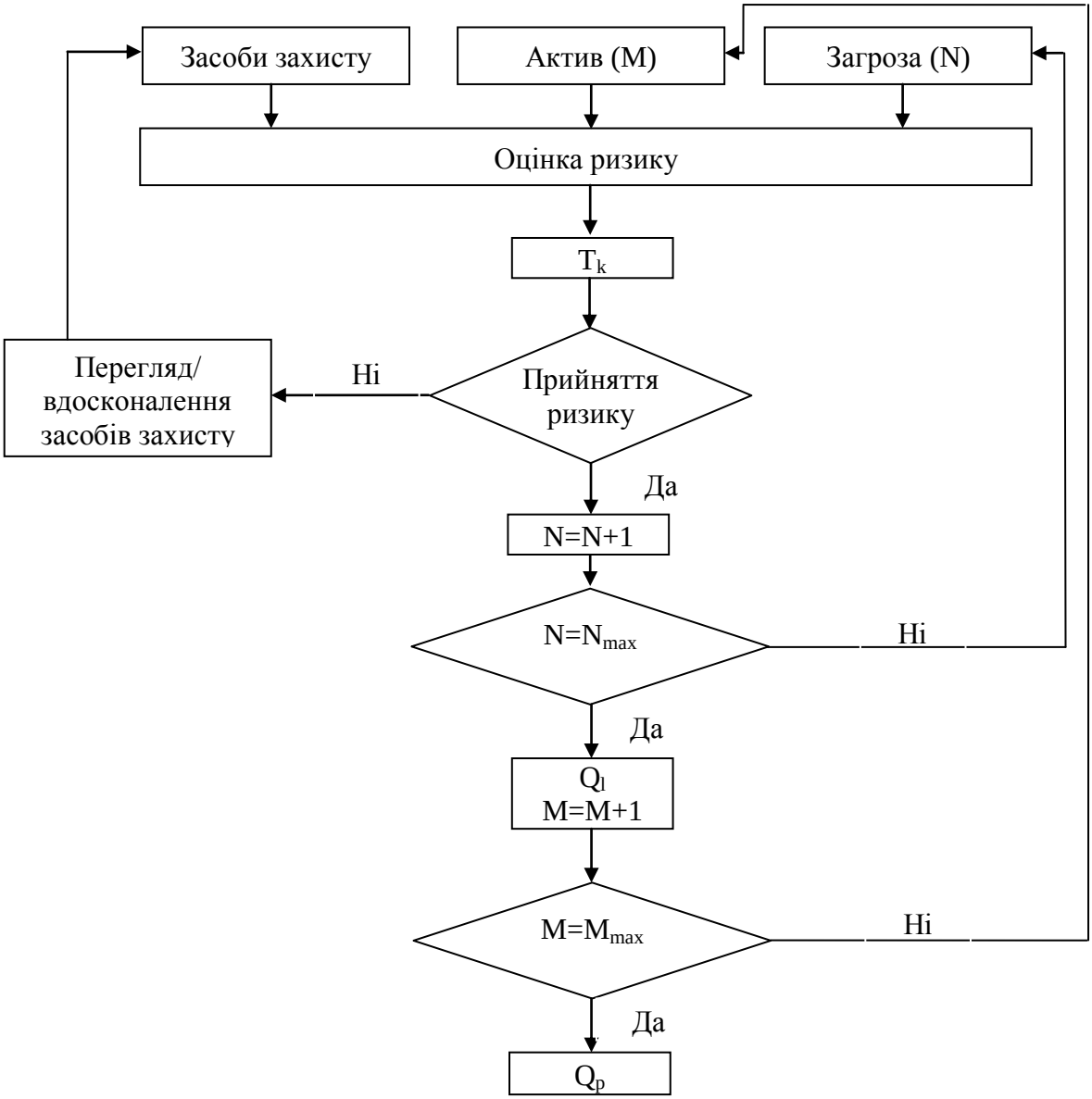

Рис.3. Алгоритм прийняття ризику.

Запропонований алгоритм оцінки та прийняття ризику може бути застосований для всіх розглянутих рівнів захисту (програм, послуг, інфраструктури) всіх трьох площин захисту (управління, контролю, кінцевого користувача).

У запропонованих формулах вагові коефіцієнти p_k - частоту появи k загрози щодо сукупності можливих загроз та коефіцієнт z_k - вірогідності подолання засобів захисту загрозою визначається на основі аналізу статистичних даних або з використанням відомих методик.

Визначення вагових коефіцієнтів $a_{k,}$ $c_{k,}$ $i_{k,}$ s_k. – повинно здійснюватися групою призначених експертів.

Методи, що можуть бути використані для оцінки ризику детально описані в додатках А і В міжнародного стандарту ISO/IEC 31010 «Менеджмент ризику. Методи оцінки ризику». Розглянемо деякі з них, що можуть бути застосовані до ТКС [6]:

1) мозковий штурм;

2) метод Дельфі;

3) дослідження небезпеки і працездатності;

4) структурований аналіз сценаріїв методом «що, якщо?»;

5) аналіз дерева подій;

6) аналіз «краватка-метелик»;

7) мультікрітеріальний аналіз рішень.

Мозковий штурм це ідентифікація групою фахівців можливих відмов, які з'явилися внаслідок, погроз, ризику, способів обробки ризику та критеріїв його оцінювання. Даний метод не може бути використаний самостійно або в поєднанні з іншими методами. Основне його призначення визначення можливостей прогнозування ситуацій учасниками обговорення.

Метод Дельфі є одним з видів мозкового штурму. Основна відмінність - кожна група експертів висуває свою індивідуальну думку, при цьому зберігаючи анонімність. Даний метод використовується для отримання узгодженої оцінки ризику на різних етапах. Однак даний метод є досить тривалим і трудомістким.

Дослідження небезпеки і працездатності - даний метод ґрунтується на ретельному аналізі використовуваних систем обробки інформації. Виробляється ідентифікація небезпек і ризиків при використанні даного методу. Цей метод може бути застосований до великої кількості систем, і дозволяє найбільш повно їх описати, але в той самий час цей метод є досить трудомістким, а отже, і досить тривалим.

Структурований аналіз сценаріїв методом «що, якщо?». Спочатку даний метод був спрощеною копією методу «дослідження небезпеки і працездатності». Даний метод ґрунтується на дослідженні сценаріїв, з використанням слів-підказок (що , якщо) для ідентифікації небезпечних ситуацій і сценаріїв їх розвитку. Даний метод можна застосовувати у великих системах з високим рівнем деталізації. Також як і методу «дослідження небезпеки і працездатності» є досить трудомістким, а отже, і досить тривалим.

Аналіз дерева подій даний метод дозволяє ідентифікувати взаємовиключні послідовності подій, що з'являються за появою вихідної події, залежно від готовності систем призначених для зниження наслідків загрози. За допомогою цього методу встановлюються

всі варіанти розвитку події. Даний метод є досить наочним, але в той самий час для його існування необхідно знати всі початкові події, які потягли за собою ланцюжок інших подій.

Аналіз «краватка-метелик» це схематичний спосіб опису й аналізу шляху розвитку події, від його появи до завершення (появи загрози). Основна область ідентифікації даного методу зосереджена на кордонах між причиною і подією, подією і наслідком. Даний метод направлений на засоби управління попередженням і зменшенням наслідків створених загроз. Але даний метод не ідентифікує всі причини потягли за собою подію.

Мультікрітеріальний аналіз рішень використовує ранжування критеріїв для отримання об'єктивної оцінки ризику, в результаті чого необхідно вибрати доступні варіанти рішень. Даний метод дозволяє вибрати найбільш ефективне рішення виникаючих проблем, але в теж час багатокритеріальні проблеми можуть не отримати жодного рішення.

Мультікрітеріальний аналіз найбільш підходить для порядку прийняття рішення для управління безпекою ТКС відповідно до рекомендацій міжнародних стандартів ISO/IEC 31010 «Менеджмент ризику. Методи оцінки ризику» та ISO/IEC 27005 «Інформаційні технології. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки».

Враховуючи данні рекомендації розглянемо алгоритм роботи експертів по визначенню вагових коефіцієнтів a_k, c_k, i_k, s_k, які за своєю суттю визначають оцінку впливу загрози на властивості активу.

Першим кроком оцінки ризику є визначення переліку активів (A_i) що входять до складу ІТС.

Наступним кроком є визначення для кожного активу A_i загроз – їх оцінка, відповідно до вірогідності і використання існуючих вразливостей ІТС, а також існуючих засобів захисту. Тобто групою експертів дається оцінка загрози у відповідності до трьох параметрів:

- вірогідність загрози (p_k);
- вірогідності подолання засобів захисту загрозою (z_k);
- вірогідність використання вразливостей ІТС (v_k).

Коли ці коефіцієнти дорівнюють нулю, то будемо вважати, що актив повністю захищено від даної загрози, а у разі, коли коефіцієнти дорівнюють одиниці – на актив обов’язково буде здійснена загроза. Отже, графічно загрозу можна уявити деякою точкою в тривимірному просторі, і чим далі вона від початку координат, тим вище значимість для даного активу, тобто загальна оцінка загрози буде обчислюватися, як довжина відрізка лінії, яка з'єднує початок координат і отриману точку.

Тобто для оцінки загрози будемо використовувати наступну формулу:

$$t_k = \sqrt{p_k^2 + z_k^2 + v_k^2} \quad (4)$$

Задля прикладу візьмемо:

$$\begin{cases} p_k = 0.5; \\ z_k = 0.5; \\ v_k = 0.5; \end{cases}$$

Оцінка загрози буде визначена наступною чином:

$$t_k = \sqrt{p_k^2 + z_k^2 + v_k^2} = \sqrt{0{,}5^2 + 0{,}5^2 + 0{,}5^2} = 0{,}866$$

Графічно цей результат наведено, на рисунку 4.

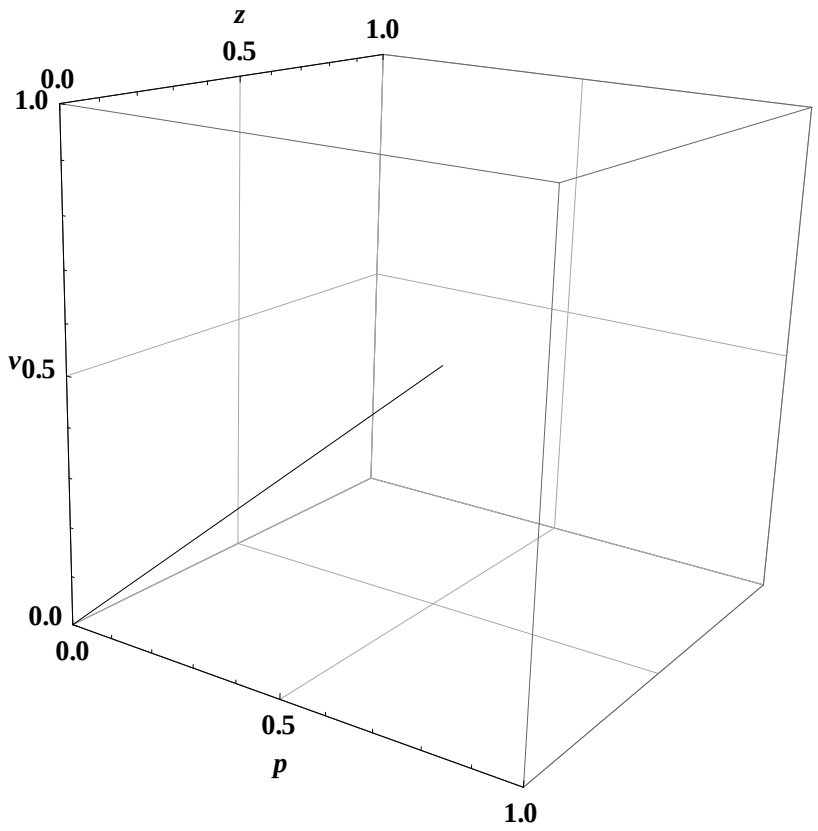

Рис. 4 Оцінка k-ї загрози для m-го активу.

Графік всіх k-х загроз для m-го активу наведен на рисунку 5.

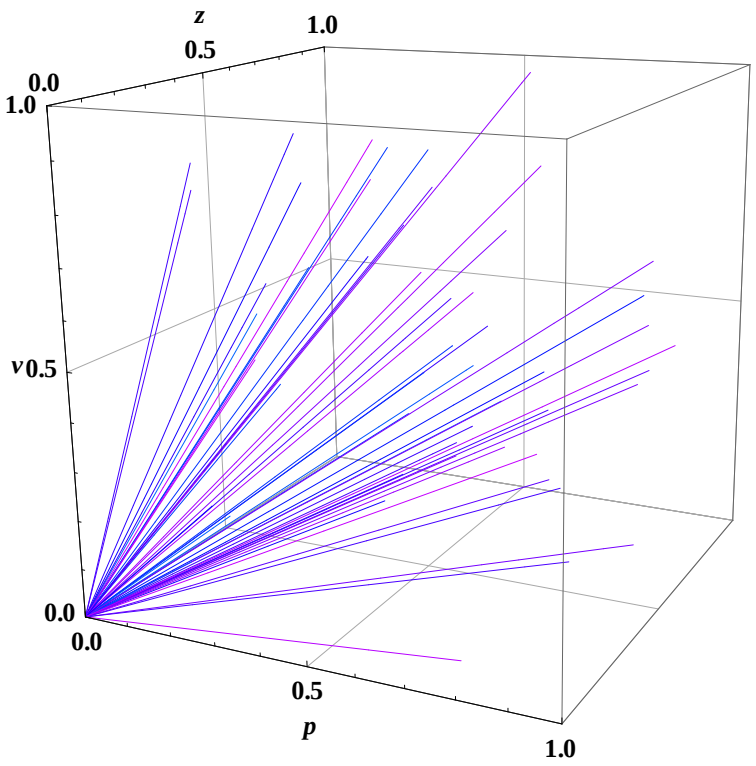

Рис. 5 Загрози, які впливають на m-й актив.

З цього можна зробити висновок, що всі загрози, які впливають на актив, у сукупності будуть мати вид якоїсь поверхні. Вид поверхні загроз, що впливають на актив, наведено на рисунку 6.

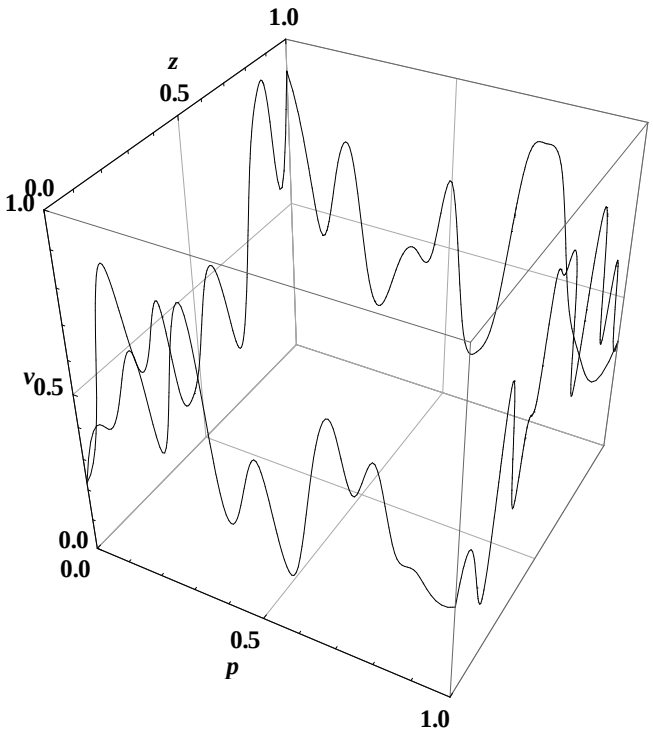

Рис. 6 Поверхня загроз для одного активу.

Експерти (Е) на підставі знань, та отриманих графіків проставляють бали імовірним загрозам по 100 бальній шкалі, при цьому розбивають оцінку на різні характеристики інформації – таблиця 2.

Експертна оцінка Таблиця 2

Загрози	**Експерти (Е)**	**Оцінка впливу загрози на властивості активів**				
		c	i	a	s	Кількість балів
Аналіз протоколів	E1	20	10	30	20	80
	E2	35	10	25	20	90
	E3	20	10	25	15	70
	E4	25	5	20	20	70
Сканування мереж	E1	c_1	i_1	a_1	s_1	t_1
	E2	c_2	i_2	a_2	s_2	t_2
	E3	c_3	i_3	a_3	s_3	t_3
	E4	c_4	i_4	a_4	s_4	t_4
⋮	⋮	⋮	⋮	⋮	⋮	⋮
Розподілена відмова в обслуговуванні	E1	c_1	i_1	a_1	s_1	t_1
	E2	c_2	i_2	a_2	s_2	t_2
	E3	c_3	i_3	a_3	s_3	t_3
	E4	c_4	i_4	a_4	s_4	t_4

Оцінка у 100 балів відповідає загрозі для якої t_k=1.

Для подальшого аналізу проводимо стандартизацію (нормування) експертних оцінок. Для прикладу розглянемо першу загрозу. Нормування експертних оцінок для першої загрози наведено у таблиці 3.

Нормовані експертні оцінки Таблиця 3

Загрози	**Експерти (Е)**	**Оцінка впливу загрози на властивості активів**				
		c	i	a	s	Кількість балів
Аналіз протоколів	E1	0.25	0.125	0.375	0.25	1
	E2	0.39	0.1	0.282	0.228	1

	E3	0.286	0.143	0.357	0.214	1
	E4	0.286	0.071	0.357	0.286	1

Візьмемо до уваги факт, що оцінки експертів узгоджені. У цьому випадку для побудови узагальненої експертної оцінки використаємо метод попарних порівнянь.

Для цього виконаємо ранжування оцінок кожного експерта:

$$E1: a > c = s > i$$

$$E2: c > a > s > i$$

$$E3: a > c > s > i$$

$$E4: a > c = s > i$$

Далі складемо матриці попарних порівнянь кожного експерта за такими формулами:

$$E1 = \|I_{ij}\| \quad (5)$$

де:

$$I_{ij} = \begin{cases} 1, \text{якщо } i \geq j \\ 0, \text{якщо } i < j \end{cases}$$

Тоді:

Експерт 1	c	i	a	s
c	1	1	0	1
i	0	1	0	0
a	1	1	1	1
s	1	1	0	1
Експерт 2	c	i	a	s
c	1	1	1	1
i	0	1	0	0
a	0	1	1	1
s	0	1	0	1
Експерт 3	c	i	a	s
c	1	1	0	1
i	0	1	0	0
a	1	1	1	1
s	0	1	0	1

Експерт 4	c	i	a	s
c	1	1	0	1
i	0	1	0	0
a	1	1	1	1
s	1	1	0	1

На наступному кроці необхідно підсумовувати матриці по всім елементам, тобто формула має вид:

$$S_{ij} = \sum_{k=1}^{k} I_{ij_k} \quad (6)$$

де:

S_{ij} - елемент підсумованої матриці;

k – номер експерта.

Результат має вид:

Сума	c	i	a	s
c	4	4	1	4
i	0	4	0	0
a	3	4	4	4
s	2	4	0	4

Результуючу матрицю знаходимо за правилом:

$$R_{ij} = \begin{cases} 1, \text{якщо } S_{ij} \geq d/2 \\ 0, \text{якщо } S_{ij} < d/2 \end{cases}$$

де: d – кількість експертів.

Результат	c	i	a	s
c	1	1	0	1
i	0	1	0	0
a	1	1	1	1
s	0	1	0	1

За кожною характеристикою активу ТКС отримуємо результат у балах – таблиця 4.

Результат Таблиця 4

Характеристика	Бали
c	3
i	1
a	4
s	2

Для подальшого використання цих балів, виконаємо їх нормування – таблиця 5.

Нормовані коефіцієнти Таблиця 5

Характеристика	Бали
c	0,75
i	0,25
a	1
s	0,5

Висновок.

1. Проведений аналіз стандартів і рекомендацій Міжнародної організації з стандартизації, Міжнародної електротехнічної комісії та Міжнародного союзу електрозв'язку, приводить до висновку про необхідність як найшвидшого впровадження даних документів у повсякденну діяльність, з метою підвищення захищеності ТКС держави.

2. Розглянуто алгоритм роботи експертів по визначенню оцінки впливу загроз на властивості активів ТКС.

3. Запропоновано порядок прийняття ризику інформаційної безпеки в ТКС.

Список використаної літератури

1. Воропаєва В. Я., Щербов І.Л. Адаптування інформаційно-телекомунікаційних систем до зовнішніх впливів // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 23 (201). - Донецьк, ДонНТУ, 2012. С - 83-88.

2. Воропаєва В. Я., Щербов І.Л., Е.Д.Хаустова Управління інформаційною безпекою інформаційно-телекомунікаційних систем на основі моделі «plan-do-check-act» // Наукові

праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 25. - Донецьк, ДонНТУ, 2013. С - 104-110.

3. ITU-T X.805. Security architecture for systems providing end-to-end communications.

4. ISO/IEC 27005. Information technology — Security techniques — Information security risk management.

5. Рекомендациями в области стандартизации банка России РС БР ИББС -2.2-2009

6. ISO/IEC 31010. Risk management – Risk assessment techniques.

7. Дядин_И.П., Червинский В.В. Исследование распределенных информационных атак и методов борьбы с ними // Автоматизація технологічних об'єктів та процесів. Пошук молодих. Збірник наукових праць XII науково-технічної конференції аспірантів та студентів в м. Донецьку 17-20 квітня 2012 р. - Донецьк, ДонНТУ, 2012. – с.32-34.

8. Васяева Т.А., Скобцов Ю.А. Подготовка данных при разработке медицинских экспертных систем // Вестник Херсонского национального технического университета, №4(27) –Херсон, ХНТУ, 2007. С. 49-55.

9. Аноприенко А.Я., Джон С.Н., Рычка С.В. Особенности моделирования и оценки эффективности работы сетевой инфраструктуры Наукові праці Донецького національного технічного університету. Серія: "Обчислювальна техніка та автоматизація". Випуск 38 – Донецьк: ДонНТУ, 2002, С. 205 – 210.

10. Астахова Л. В. Проблема идентификации и оценки кадровых уязвимостей информационной безопасности организации // Вестник Южно-Уральского государственного университета. Серия: компьютерные технологии, управление, радиоэлектроника. – 2013. – Т. 13. – №. 1.

11. Королев О. Л. Определение и управление рисками информационных систем // Ученые записки ТНУ им. ВИ Вернадского: Серия «Экономика». – 2006. – Т. 19. – №. 58. – С. 113-120.