УДК 004.056.53

Г. А. Вашакідзе, В. В. Пасльон, І. Л. Щербо, А. Є. Якушина

Донецький національний технічний університет

МЕТОДИКА ПРИЙНЯТТЯ РІШЕННЯ З 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.

Проведен анализ последовательности принятия решения по управлению информационной безопасностью в телекоммуникационной системе (ТКС). Рассмотрены наиболее распространенные методы оценки риска. Предложен порядок дискретной оценки риска для информационно-телекоммуникационной системы на основе экспертных оценок ожидаемого ущерба в случае реализации угроз.

Ключевые слова: телекоммуникационная система, методы оценки риска, алгоритм принятия риска.

The analysis of decision making sequence on information security management in telecommunication system. The most common methods of risk assessment were considered. The risk discrete valuation order was proposed for information and telecommunication system based on expert estimation of the expected damage in case threat materializing.

Key words: telecommunication system, risk assessment methods, risk acceptance algorithm.

Вступ. Розробка ефективних моделей і методів управління безпекою інформаційно-телекомунікаційних систем (ІТС) з метою протидії кібернетичній злочинності, є актуальним завданням. З метою вирішення даної проблеми необхідно провести складний аналіз діючої ІТС та здійснити оцінку ризику щодо забезпечення захисту. Вирішення даного завдання базується на виконанні вимог діючих міжнародних стандартів і рекомендацій.

Так, Міжнародним союзом електрозв'язку в рекомендації МСЕ - Т Х.805 запропонована архітектура захисту для систем, що забезпечують зв'язок між кінцевими пристроями. Дана архітектура дозволяє провести деталізацію складових частин ІТС з метою спрощення прийняття рішення, спрямованого на ефективне управління, контроль і використання мережевої інфраструктури, послуг і додатків, дозволяє більш якісно провести аналіз ІТС [1].

Процес прийняття ризику щодо забезпечення безпеки ІТС доцільно здійснити, керуючись рекомендаціями міжнародного стандарту ISO / IEC 27005 «Менеджмент ризику інформаційної безпеки» [2].

В роботі запропоновано алгоритм роботи експертів по визначенню оцінки впливу загроз на властивості активів ТКС та порядок прийняття ризику інформаційної безпеки в ТКС.

Аналіз стану проблеми і вирішення завдання. Враховуючи широкий спектр юридичних та фізичних осіб, які надають послуги, обладнання та програмне забезпечення, що застосовуються в сфері телекомунікацій, Міжнародним союзом електрозв'язку в рекомендації МСЕ-Т Х.805 запропонована архітектура захисту для

систем, що забезпечують зв'язок між кінцевими пристроями. Порядок проведення деталізації активів ІТС та оцінку їх вразливості від ймовірних загроз розглянуто у роботах [3, 4, 5].

Кількісну оцінку вразливості конкретного активу ІТС від однієї загрози можна визначити за формулою:

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

Коефіцієнти a_k, c_k, i_k, s_k – визначають рівень вразливості таких властивостей інформаційних активів, як доступність, конфіденційність, цілісність та спостереженність (визначається групою призначених експертів). 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 успішного захисту активу ТКС за допомогою встановленого засобу захисту від загрози p_k.

Визначення вразливості активу від всіх імовірних загроз Q_i:

$$Q_i = \sum_{i=1}^{k} \frac{c_k + i_k + a_k + s_k}{4} * z_k * p_k \qquad (2)$$

Визначення загальної оцінки захисту сукупності активів Q_p здійснюється за формулою:

$$Q_p = \sum_{j=1}^{l} \sum_{i=1}^{k} \frac{c_k + i_k + a_k + s_k}{4} * z_k * p_k \qquad (3)$$

На підставі отриманої кількісної оцінки захищеності активів системи приймається рішення на прийняття ризику. Алгоритм даного процесу представлено на рисунку 1.

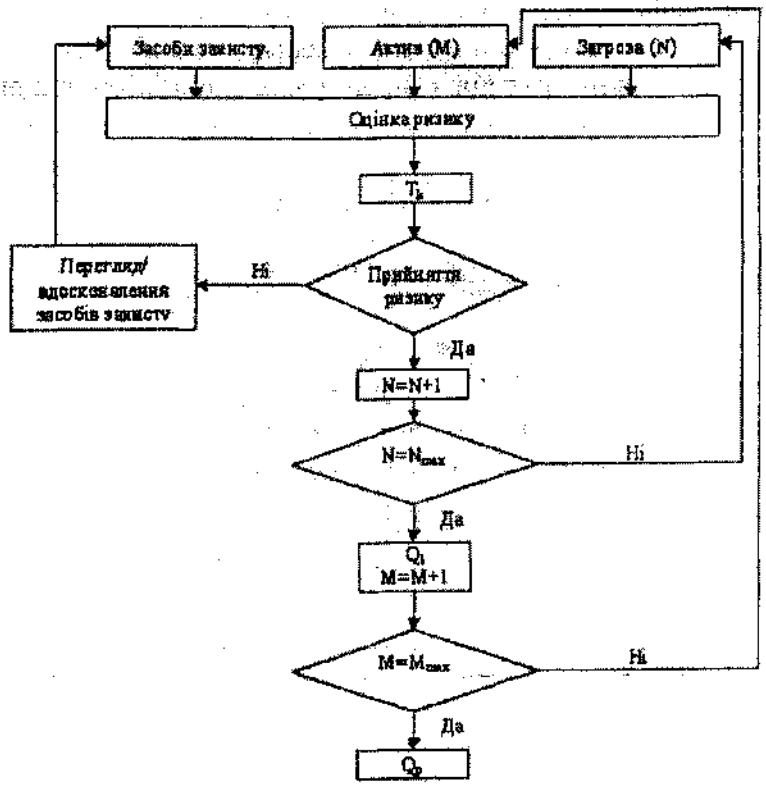

Рис. 1. Алгоритм прийняття ризику.

Як було зазначено, визначення вагових коефіцієнтів a_k, c_k, i_k, s_k – повинно здійснюватися групою призначених експертів.

Кількісну оцінку загрози для будь-якого активу визначимо на підставі порівняння наступних параметрів:

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

Коли ці параметри дорівнюють нулю, будемо вважати, що актив повністю захищено від даної загрози. Збільшення значення параметру від 0 до 1 призводить до зниження захищеності активу.

Отже, графічно загрозу можна уявити деякою точкою в тривимірному просторі, і чим далі вона від початку координат, тим більш вразливі властивості інформаційних активів.

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:

$$t_k = \sqrt{p_k^2 + z_k^2 + v_k^2} \tag{4}$$

Наприклад:

$$\begin{cases} p_k = 0{,}5 \\ z_k = 0{,}5 \\ v_k = 0{,}5 \end{cases}$$

Оцінка загрози буде визначена наступним чином:

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

Графічно цей результат наведено на рисунку 2.

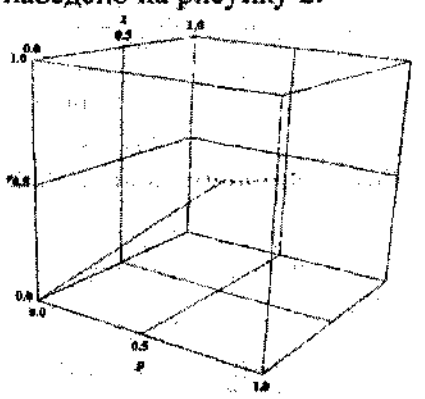

Рис. 2. Оцінка k-ї загрози для m-го активу.

Графік всіх k-х загроз для m-го активу наведен на рисунку 3.

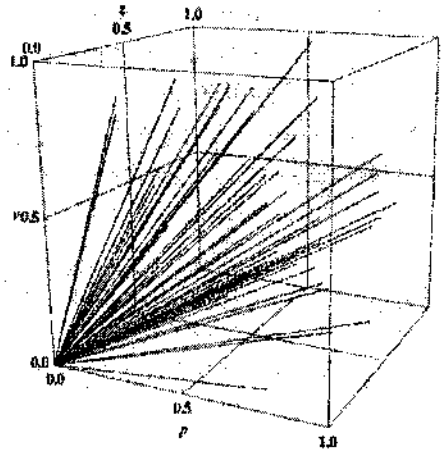

Рис. 3. Сукупність загроз для активу m.

Для більш наглядного представлення сукупність загроз для активу **m** відобразимо як поверхню (рисунок 4).

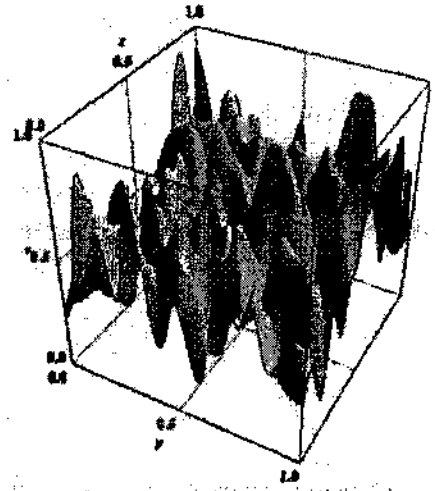

Рис. 4. Поверхня загроз для одного активу.

Провівши послідовну оцінку вразливості активів, експерти (Е) на підставі знань та отриманих даних проставляють бали ймовірних загроз по 100-бальній шкалі. В таблиці 1, для прикладу, приведено аналіз впливу загрози «Аналіз протоколів» на властивості інформаційного активу.

Таблиця 1

Експертна оцінка

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

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

Для подальшого аналізу проводимо стандартизацію (нормування) експертних оцінок (таблиця 2).

Таблиця 2

Нормовані експертні оцінки

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

Беремо до уваги факт, що оцінки експертів узгоджені. У цьому виладку 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:

$$E1 = \left\| I_{ij} \right\|, \tag{5}$$

де:

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

На наступному кроці необхідно підсумовувати матриці за всіма елементами, тобто формула має вид:

$$S_{ij} = \sum_{k=1}^{k} I_{ij_k}, \tag{6}$$

де: S_{ij} – елемент підсумованої матриці; k – номер експерта.

Результуючу матрицю знаходимо за правилом:

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

де: d – кількість експертів.

За кожною характеристикою активу ТКС отримуємо результат у балах – таблиця 3.

Таблиця 3

Результат

Характеристика	Бали
c	3
i	1
a	4
s	2

Для подальшого використання цих балів виконаємо їх нормування – таблиця 4.

Таблиця 4

Нормовані коефіцієнти

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

Отриманні бали використовуємо для розрахунку вразливості активу від даної загрози відповідно з формулою 1.

Таким чином, на підставі експертних оцінок, враховуючи такі параметри, як вірогідність загрози (p_k), вірогідності подолання засобів захисту загрозою (z_k) та вірогідність використання вразливостей активу (v_k), було отримано кількісну оцінку вразливості інформаційного активу від ймовірних загроз. Вибір параметрів, що використовуються для оцінки вразливості активу, здійснюється виходячи з особливостей, які йому притаманні.

Аналіз результатів. Запропонований алгоритм роботи експертів з визначення оцінки впливу загроз на властивості активів ТКС та порядок прийняття ризику інформаційної безпеки дозволяє в кількісній формі визначити реальний стан безпеки діючої ТКС, провести порівняльну оцінку отриманого результату з вимогами технічного завдання на реалізацію системи захисту, прийняти рішення на підвищення або зменшення фінансових витрат щодо організації захисту ІТС.

Висновок. 1. Розглянуто алгоритм роботи експертів з визначення оцінки впливу загроз на властивості активів ТКС.

2. Запропоновано порядок прийняття ризику інформаційної безпеки в ТКС.

Бібліографічні посилання

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

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

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

4. **Воропаєва В. Я.** Управління інформаційною безпекою інформаційно-телекомунікаційних систем на основі моделі «plan-do-check-act» / В. Я. Воропаєва, І. Л. Щербов, Е. Д. Хаустова // Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 25. – Донецьк, ДонНТУ, 2013. – С. 104-110.

5. **Воропаєва В. Я.** Алгоритм прийняття ризику з метою забезпечення безпеки ТКС / В. Я. Воропаєва, І. Л. Щербов, Ващакідзе Г. А.// Наукові праці Донецького національного технічного університету. Серія: Обчислювальна техніка та автоматизація. Випуск 26. – Донецьк, ДонНТУ, 2014. – С. 135-145.

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

7. **Дядин И. П.** Исследование распределенных информационных атак и методов борьбы с ними / И. П. Дядин, В. В. Червинский // 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.** Подготовка данных при разработке медицинских экспертных систем/ Т. А. Васяева, Ю. А. Скобцов// Вестник Херсонского национального технического университета, №4(27) –Херсон, ХНТУ, 2007. – С. 49-55.

9. **Аноприенко А. Я.** Особенности моделирования и оценки эффективности работы сетевой инфраструктуры/ А. Я. Аноприенко, С. Н. Джон, С. В. Рычка.– 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, радиоэлектроник,. – 2013. – Т. 13. – №. 1.

Надійшла до редколегії 04.06.2014