УДК 621.391

І.Л. Щербов, В.Я. Воропаєва (канд. техн. наук, доц.), Г.А. Вашакідзе
ДВНЗ «Донецький національний технічний університет», м. Донецьк
кафедра радіотехніки та захисту інформації,
кафедра автоматики і телекомунікацій
e-mail: schil@rtf.donntu.edu.ua, voropayeva@donntu.edu.ua, gur.vash@yandex.ru

АЛГОРИТМ ПРИЙНЯТТЯ РИЗИКУ З МЕТОЮ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТКС

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.*

Загальна постановка проблеми

Стрімкий розвиток інформаційно-телекомунікаційних технологій все значніше впливає на процеси життєдіяльності людини, спрощуючи процес отримання необхідної інформації, сприяючи економічному розвитку, дозволяючи більш ефективно вирішувати проблеми державного управління. Але з іншого боку виникають нові глобальні проблеми – кібернетичні злочини. Розробка ефективних моделей і методів управління безпекою телекомунікаційних систем (ТКС) з метою протидії кібернетичній злочинності наразі є актуальним завданням. Його вирішення ускладнюється значною кількістю факторів, що впливають на його виконання. Найбільш суттєвими є [1]:

- 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 ТКС та інформації, що обробляється;
- необхідність врахування перспектив модернізації системи;
- собівартість та ін.

Постановка завдань дослідження

Для розробки ефективних моделей і методів управління безпекою телекомунікаційних систем в першу чергу необхідно вирішити наступні задачі:

1. Розробити алгоритм прийняття ризику при розробці системи захисту ТКС.
2. Запропонувати метод визначення експертних оцінок вразливості активів ТКС від ймовірних загроз.

Вирішення завдання та результати дослідження

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 (рис.1). Дана архітектура дозволяє провести деталізацію складових частин ТКС 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 вразливість захисту [2].

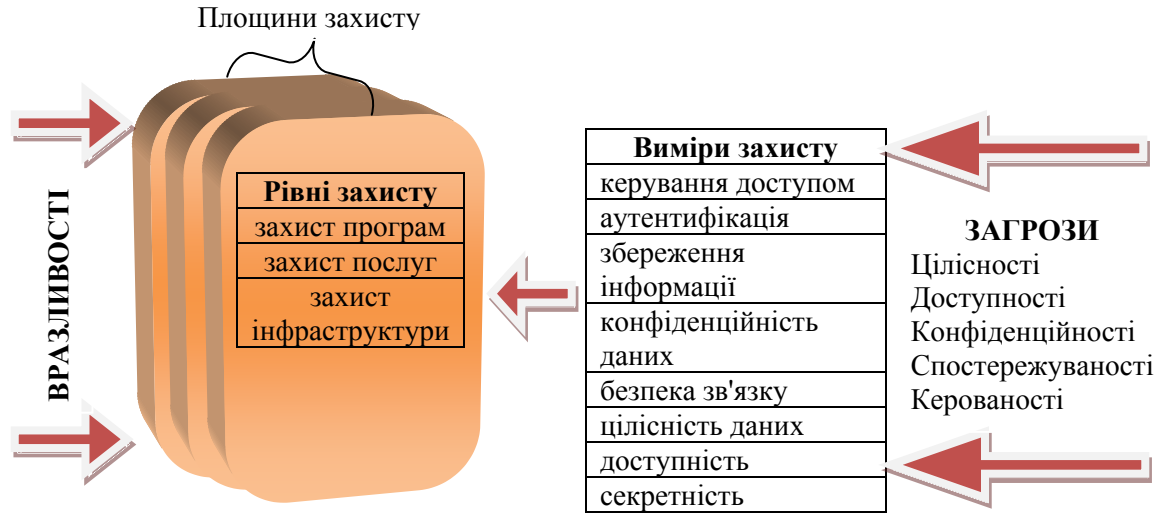

Рисунок 1 - Архітектура захисту систем

Прийнята архітектура захисту систем, що забезпечують зв'язок між кінцевими пристроями, дозволяє більш якісно провести оцінку ризику безпеки ТКС. З цією метою, виходячи з рекомендацій міжнародного стандарту ISO/IEC 27005 «Менеджмент ризику інформаційної безпеки», в початковій стадії прийняття рішення проводиться облік активів, вразливість яких може вплинути на ступінь захищеності ТКС [3].

Доцільно активи телекомунікаційної системи розглядати окремо у відповідності до площини захисту: управління, контролю або 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.

Наступним кроком оцінки ризиків активів є визначення загроз для ідентифікованих активів. Загрози для ТКС 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 ТКС може впливати дана загроза.

Етап оцінки вразливості активів схематично представлені на рисунку 2.

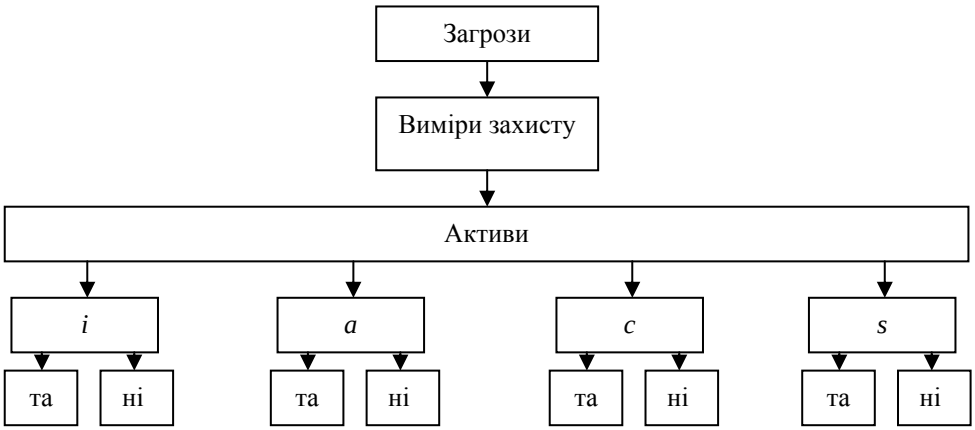

Рисунок 2 - Оцінка вразливості активів від імовірних загроз

Виміри захисту по своїй суті являють комплекс реалізованих заходів щодо захисту активів ТКС. У випадку успішної реалізації загрози активам може бути завдано шкоди, яка впливає на цілісність (i), доступність (a), конфіденційність (c), спостереженість та керованість (s). Таким чином визначається рівень стану захищеності ТКС від загроз.

Виділяється вісім основних вимірів захисту (рисунок 1): управління доступом; аутентифікація ; збереження інформації ; конфіденційність даних; безпека зв'язку; цілісність даних; доступність; секретність [2].

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

Таблиця 1

Загрози для інформаційної безпеки ТКС

№ 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 вразливості 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, коефіцієнт z_k визначає вірогідність захисту активу ТКС за допомогою встановленого засобу захисту від загрози p_k [4, 5].

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. 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).

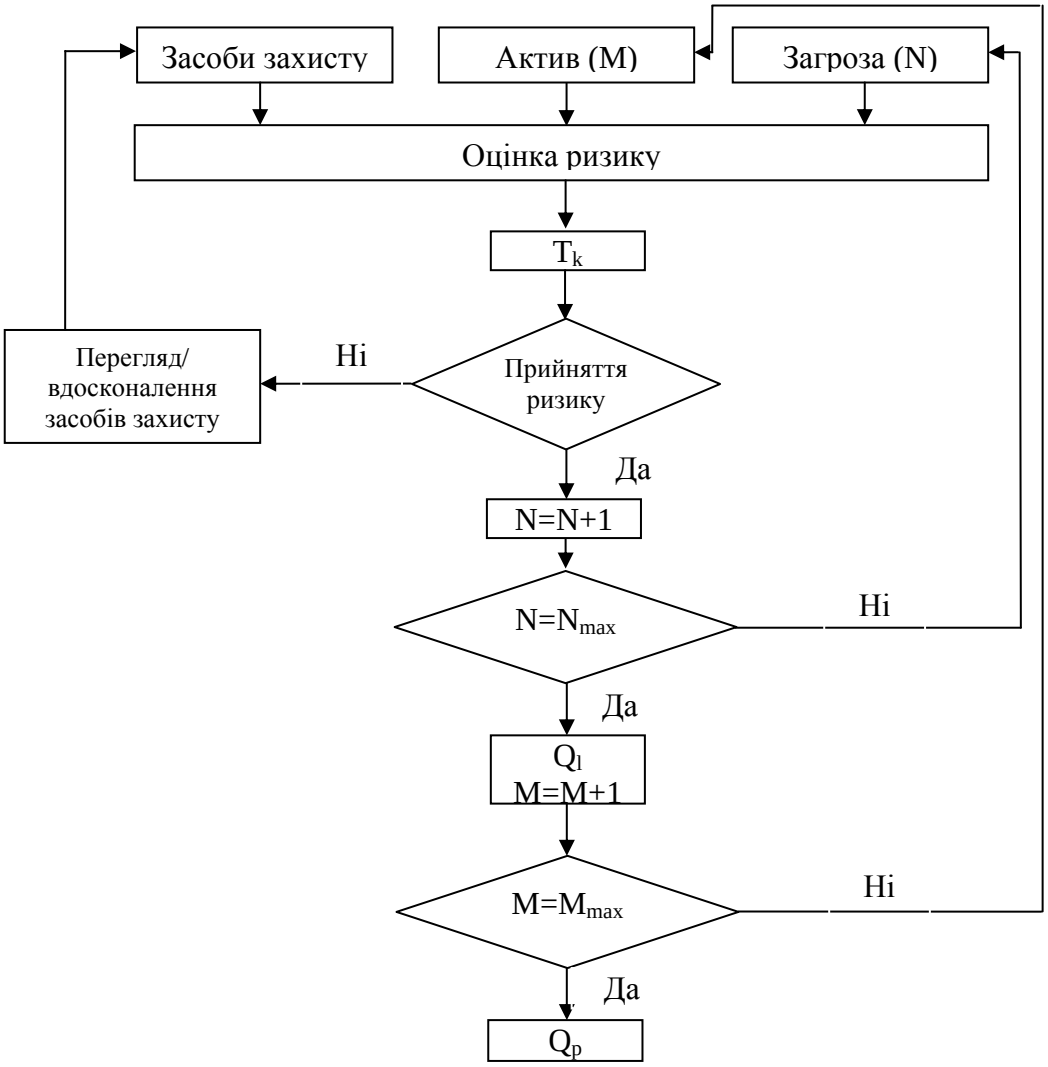

Рисунок 3 - Алгоритм прийняття ризику

У запропонованих формулах вагові коефіцієнти p_k – частота появи k-ї загрози щодо сукупності можливих загроз та коефіцієнт z_k – вірогідність захисту активу ТКС за допомогою встановленого засобу захисту від k-ї загрози, – визначаються на основі аналізу статистичних даних або з використанням відомих методик [6, 7]. 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 [8, 9, 10].

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.

Метод дослідження небезпеки і працездатності ґрунтується на ретельному аналізі систем обробки інформації та здійсненні ідентифікація небезпек і ризиків. Цей метод може

бути застосований до великої кількості систем і дозволяє найбільш повно їх описати, але є досить трудомістким, а отже, і досить тривалим.

Структурований аналіз сценаріїв методом «що, якщо?» 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 є досить трудомістким і тривалим.

Аналіз дерева подій 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, що потягли за собою подію.

Мультикритеріальний 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. Мультикритеріальний 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».

Таблиця 2

Експертна оцінка вразливості активу від ймовірної загрози

№ k	Загрози (threat)	E1	E2	E3	E4
1	Аналіз протоколів	80	90	70	70
2	Сканування мереж	90	70	90	90
3	Автоматичний підбір паролів	70	70	80	70
4	Spoofing	100	90	90	70
5	Захоплення мережевих підключень	80	85	90	80
6	Підміна мережевих об'єктів	50	60	50	70
7	Розподілена відмова в обслуговуванні	60	80	70	80
8	Віддалене проникнення	55	60	70	80

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.

Експерти (Е) на підставі знань проставляють бали імовірним загрозам за 100 бальною шкалою, як показано в таблиці 2. Експертна оцінка вразливості активу від ймовірної загрози є сумою оцінок впливу загрози на властивість активу. В таблиці 3 для прикладу представлено отримання оцінки вразливості активу від загрози «аналіз протоколів».

Для подальшого аналізу проводимо нормування експертних оцінок. Нормування експертних оцінок для першої загрози наведено у таблиці 4.

Таблиця 3

Детальна оцінка вразливості активу

Загрози	Експерти (Е)	Оцінка впливу загрози на властивості активів				Сумарна кількість балів
		c	i	a	s	
Аналіз протоколів	Е1	20	10	30	20	80
	Е2	35	10	25	20	90
	Е3	20	10	25	15	70
	Е4	25	5	20	20	70

Таблиця 4

Нормовані експертні оцінки

Загрози	Експерти (Е)	Оцінка впливу загрози на властивості активів				Сумарна кількість балів
		c	i	a	s	
Аналіз протоколів	Е1	0.25	0.125	0.375	0.25	1
	Е2	0.39	0.1	0.282	0.228	1
	Е3	0.286	0.143	0.357	0.214	1
	Е4	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 формулою:

$$E1 = \left\| I_{ij} \right\|,\ I_{ij} = \begin{cases} 1, \textit{якщо } i \geq j; \\ 0, \textit{якщо } i < j. \end{cases} \quad (4)$$

Тоді:

Експерт 1	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 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:

$$S_{ij} = \sum_{k=1}^{k} I_{ij_k}, \quad (5)$$

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	1	4	0	4

Результуючу матрицю знаходимо за правилом:

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

де d – кількість експертів.

Сума	c	i	a	s
c	1	1	0	1
i	0	1	0	0
a	1	1	1	1
s	0	1	0	1

Для кожної властивості активу ТКС отримуємо результат у балах – таблиця 5.

Таблиця 5

Оцінка загрози для властивості активу

Властивість активу	Бали
c	3
i	1
a	4
s	2

Для подальшого використання цих балів, виконаємо їх нормування. Результати представлено у таблиці 6.

Таким чином, результатом роботи експертів є визначення вагових коефіцієнтів a_k, c_k, i_k, s_k, які за своєю суттю визначають оцінку впливу загрози на властивості активу.

Таблиця 6

Нормовані коефіцієнти

Властивість активу	Бали
c	0,75
i	0,25
a	1
s	0,5

Висновки

У статті розглянуто рекомендації міжнародної спілки електрозв'язку щодо архітектури захисту, яка дозволяє провести деталізацію складових частин ТКС з метою спрощення прийняття рішення, спрямованого на ефективне управління, контроль і використання мережевої інфраструктури, послуг і програм. Активи телекомунікаційної системи ідентифіковані у відповідності до площини захисту: управління, контролю або кінцевого користувача. Проведена класифікація імовірних загроз залежно від уразливості активів до цих загроз.

Розроблено новий алгоритм прийняття ризику при проектуванні системи захисту ТКС, який відрізняється від відомих тим, що базується на дискретній експертній оцінці захищеності активів системи від різних типів загроз.

Здійснено порівняльний аналіз методів, що можуть бути використані для оцінки ризику активів телекомунікаційної системи, та вибрано мультикритеріальний метод як найбільш ефективний. Запропоновано методику визначення експертних оцінок вразливості активів ТКС від імовірних загроз, що базується на мультикритеріальному методі, та приведений приклад розрахунку вагових коефіцієнтів експертної оцінки впливу загрози «аналіз протоколів» на властивості активів телекомунікаційної системи.

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. ITU-T X.805. Security architecture for systems providing end-to-end communications.
3. ISO/IEC 27005. Information technology — Security techniques — Information security risk management.
4. 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.
5. 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.
6. 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.
7. 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.
8. ISO/IEC 31010. Risk management – Risk assessment techniques.
9. 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.
10. Королев О. Л. Определение и управление рисками информационных систем // Ученые записки ТНУ им. ВИ Вернадского: Серия «Экономика». – 2006. – Т. 19. – №. 58. – С. 113-120.

References

1. Voropaeva, B.Y. and Shcherbov, I.L. (2012), "Adaptirovanie informacionno-telekommunikacionih sistem k vneshnim vozdeistviyim", *Proceedings of Donetsk National Technical University. Series: Computers and Automation*, no.23 (201), pp. 83-88.
2. ITU-T X.805. Security architecture for systems providing end-to-end communications.
3. ISO/IEC 27005. Information technology - Security techniques - Information security risk management.
4. Dyadin, I.P. and Cherwinski, V.V. (2012), "Issledovanie raspredelenih informacionnih atak i metodi borbi s nimi", *Automation of technological objects and processes. Search young. Collected Works of XII scientific conference and students in Donetsk on 17-20 April 2012*, Donetsk, Ukraine, 2012, pp.32-34.
5. Voropaeva, V.Y., Shcherbov, I.L. and Haustova, E.D. (2013), "Upravlenie informacionnoi bezopasnostiu informacionno-telekommunikacionih system na osnove modeli «plan-do-check-act»", *Proceedings of Donetsk National Technical University. Series: Computers and Automation*, no. 253 (201), pp. 104-110.
6. Vasyaeva, T.A. and Skobtsov, Y.A. (2007), "Podgotovka dannih pri razrabotke medicinskih ekspertnih system", *Bulletin of Kherson National Technical University*, no. 4(27), pp. 49-55.
7. Anoprienko, A.Y., Djon, S.N. and Richka, S.V. (2002), "Osobenosti modelirovania I ocenki effektivnosti raboti setevoi infrastrukturi", *Proceedings of Donetsk National Technical University. Series: Computers and Automation*, no. 38, pp. 205-210.
8. ISO/IEC 31010. Risk management – Risk assessment techniques.
9. Astahov, L.V. (2013), "Problema identifikacii i ocenki kadrovih uyazvimostei informacionnoi bezopasnosti organizacii", *Bulletin of the South Ural State University. Series: computer technology, management, electronics*, vol. 13, no. 1.
10. Korolov, O.L. (2006), "Opredelenie i upravlenie riskami informacionnih system", *Scientific notes of TNU. Vernadsky Series "Economy"*, vol. 19, no. 58, pp. 113-120.

Надійшла до редакції:
02.04.2014 р.

Рецензент:
докт. пед. наук, проф. Стефаненко П.В.

И.Л. Щербов, В.Я. Воропаева, Г.А. Вашакидзе
ГВУЗ «Донецкий национальный технический университет»

Алгоритм принятия риска с целью обеспечения безопасности телекоммуникационных систем. *Проведен анализ последовательности принятия решения по управлению информационной безопасностью в телекоммуникационной системе. Предложен математический аппарат по определению общей оценки защищенности составных элементов ТКС. Рассмотрены наиболее распространенные методы оценки риска. Разработан алгоритм принятия риска при проектировании системы защиты. Разработана методика определения экспертных оценок уязвимости активов ТКС.*

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

I.L. Shcherbov, V.Y. Voropaeva, G.A. Vashakidze
Donetsk National Technical University

Risk acceptance algorithm aiming to provide safety of telecommunications systems *The analysis of decision making sequence on information security management in the telecommunications system was done. The model for analysis is security architecture of systems, which provide connection between users ITU-T X.805). Application of this architecture allows assessing the risk of telecommunications system.*

Mathematical tool for security rating definition of the telecommunication systems compound elements was offered. Security rating estimation is based on analysis of: assessment of the hazard impact on assets property, frequency of hazard occurrence, probability of hazard avoidance using existing security equipment.
The routine methods of risk assessment were considered. Multi-criterion method was chosen according to special aspects of telecommunications system structure and operating. An algorithm of risk acceptance during security system design was developed on the base of offered mathematical tool for telecommunications system security rating definition. The algorithm is based on quantitative assessment of system assets security.
Method of expert estimation definition of telecommunications system assets vulnerability was developed. The order of risk discrete valuation for telecommunications system was developed on the base of expert estimation of expected damage in case of hazard materializing.
***Key words**: telecommunications system, risk assessment methods, risk acceptance algorithm.*

Щербов Ігор Леонідович, Україна, Краснодарське вище військове училище ім. г.а. Штеменко С.М., ст. викладач кафедри радіотехніки та захисту інформації ДВНЗ «Донецький національний технічний університет» (вул. Артема, 58, м. Донецьк, 83001, Україна). Основний напрям наукової діяльності – управління інформаційною безпекою в телекомунікаційних системах та мережах.

Воропаєва Вікторія Яківна, Україна, закінчила Донецький національний технічний університет, канд. техн. наук, доцент, професор кафедри автоматики та телекомунікацій ДВНЗ «Донецький національний технічний університет» (вул. Артема, 58, м. Донецк, 83001, Україна). Основний напрямок наукової діяльності – сучасна теорія телетрафіку, оптимізація телекомунікаційних та інформаційно-комунікаційних систем та мереж.

Вашакідзе Гурам Аміранович, Україна, магістрант Донецького національного технічного університету, кафедра радіотехніки та захисту інформації (вул. Артема, 58, м. Донецьк, 83001, Україна). Основний напрям наукової діяльності – дослідження методів прийняття рішень щодо захисту інформації в інформаційно-телекомунікаційних мережах.