УДК 004.056/005 **Соколов В. Ю.**

КІЛЬКІСНІ ПОКАЗНИКИ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ І РИЗИКІВ ВІД ПОРУШЕННЯ БЕЗПЕКИ У РОЗПОДІЛЕНИХ СИСТЕМАХ РУХОМОГО ЗВ'ЯЗКУ

Проблематика

На системи рухомого зв'язку постійно діє низка загроз: природні, техногенні, людські навмисні і людські ненавмисні. Природні (космічне випромінювання, іонізація іоносфери) і техногенні (випромінювання радіоапаратури) за результатом дуже схожі: вони викликають перешкоди у каналах зв'язку. Навмисні загрози набувають все більшого розповсюдження і проявляється, в вигляді порушень безпеки: введення в систему шкідливих кодів (комп'ютерних вірусів). Людські ненавмисні загрози можна розглядати як форс-мажорні, тому вони дуже важко піддаються узагальненому опису [1, 2].

З першого погляду здається, що проблему захисту від порушень безпеки можна вирішити, захищаючи саму інформацію, що передається мережею. Але така загроза зумовлена використанням в лініях зв'язку обчислювальної техніки в апаратурі, яка безпосередньо задіяна в передачі даних, наприклад, мультиплексори і демультиплексори, комутатори, маршрутизатори, підсилювачі, регенератори, пристрої керування тощо. Таким чином, мова йде не тільки про цілісність інформації, а і про працеспроможність системи в цілому [1].

Система в свою чергу складається з технічних засобів, програмного забезпечення, інформаційних ресурсів і організаційної структури. Кожен з цих елементів окремо можна розглядати як підсистему загальної системи і застосовувати ті самі принципи, що і для системи в цілому [3].

Теоретичні та практичні дослідження показують, що визначання точних кількісних оцінок можливого збитку дуже ускладнені або взагалі не є можливими. Через це широкого розповсюдження набули наближені оцінки, зібраних підчас роботи системи рухомого зв'язку, разом з експертними оцінками [4].

Через те, що результати порушень безпеки (кібератак і дій вірусів) призводять до погіршення роботи інфраструктури системи рухомого зв'язку, то можна розглядати їх аналогічними до перешкод. І навпаки, можна розглядати перешкоди, як результати дій вірусів.

Одночасно з визначенням показників захищеності необхідно розглядати і оцінку ризиків. Тільки сукупність цих двох показників надає повну картину про стан системи рухомого зв'язку, що досліджується.

Метою даного дослідження є аналіз існуючих засобів визначення рівня захищеності, доопрацювання їх для отримання методики порівняння кількох систем між собою, а також вдосконалення методів перевірки достовірності експертних оцінок.

Визначення рівня захищеності системи можна використовувати разом з методом дерева атак для своєчасного реагування на зміни в конфігурації системи, появу нових типів атак і змін у політиці безпеки організації

Підходи до оцінки загроз

Суб'єктивний процес отримання ймовірності можна розділити на три етапи:

- підготовчий (формується об'єкт дослідження: множина подій і початковий аналіз властивостей цієї множини; вибирається один за методів отримання суб'єктивної ймовірності; проводиться підготовка експерта або групи експертів);
- отримання оцінок (використання вибраного метода; отримання результатів в чисельній формі, можливо і суперечливих);
- аналіз отриманих оцінок (дослідження результатів опитування; уточнення відповідей експертів).

Інколи третій етап не проводиться, якщо метод сам використовує аксіоми ймовірного розподілення, що само по собі близьке до оцінок експертів. І навпаки особливо важливим цей етап стає, якщо результати отримані від групи експертів [5].

Також можна відокремити два підходи до багатокритеріальної оцінки ефективності розподілених систем рухомого зв'язку:

- пов'язаний з приведенням множини окремих показників ефективності до єдиного інтегрального показника;
- використовує методи теорії багатокритеріального вибору і прийняття рішень (при значній кількості окремих показників ефективності, приблизно однаково важливих) [4].

Розгляд моделей порушень безпеки

Модель «зомбування»

Порушення безпеки за такою моделлю мають чітко відокремленні стадії, як показано на рисунку 1: поверхневе вивчення (рекогносцирування), глибоке вивчення (сканування каналів зв'язку), доскональне вивчення (складання карти), отримання доступу до операційної системи (ОС), розширення повноважень, «зомбування» ОС, маніпуляції з інформацією і видалення слідів злочину.

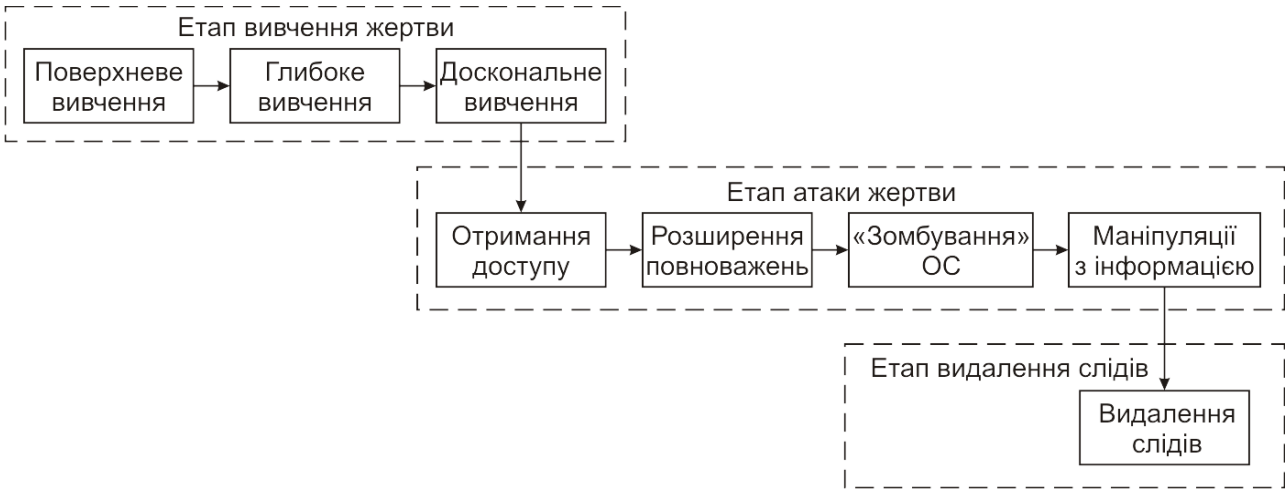

Рис. 1. Етапи моделі «зомбування»

«Зомбування» системи проходить за допомогою шкідливого коду, який вводиться в ОС для віддаленого доступу. Після цього з «зомбованої» ОС проводиться наступна атака і додавання нових робочих станцій до «зомбі»-мережі (так звана, ботнет, від англ. botnet від robot і network). Після закінчення атаки видаляються сліди перебування зловмисника в системі.

Для моделі «зомбування» ефективність eff [$с^{-1}$·грн.$^{-1}$] можна розрахувати за формулою:

$$eff = \frac{n \times s}{t \times cost},$$

де n — кількість потенційних серверів, на яких реалізована атака; s — кількість комп'ютерів, які безпосередньо працюють з одним сервером; t — час прибування системи в «зазомбованому» стані; cost — вартість атаки: вартість написання ботнету, додаткові витрати на введення і розповсюдження програного коду, додаткові витрати [6].

Модель «чорної скриньки»

Якщо розглядати порушення безпеки (CC_n) у вигляді множини підмножин, які характеризують об'єкт:

$$CC_n = \{X_n, Y_n, D_n, W_n\},$$

де X_n — підмножина зловмисників, Y_n — підмножина об'єктів, D_n — підмножина втрат, W_n — підмножина зовнішніх дій.

Модель атаки буде у вигляді «чорної скриньки» (див. рис. 2): на вхід об'єкта Y_n приходить зовнішні данні і команди W_n, а також дії зловмисника X_n, після чого виникає в результаті відповідь D_n (з втратою або без — в залежності від успішності атаки [6].

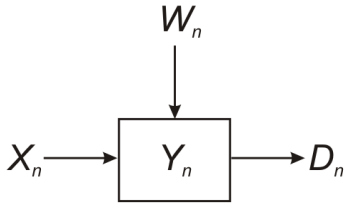

Рис. 2. Схема моделі «чорної скриньки»

Методи оцінки загроз

1. **Імовірність даних відмови в обслуговуванні** (в результаті стихійного лиха, форс-мажору, повній або частковій втраті даних, несанкціонованого доступу тощо) дозволяє отримувати результати у вигляді шкали оцінок потенційних загроз і їх наслідків. Метод оперує з набором показників і для кожного окремого випадку буде різним.

Значення показників виходять приблизні, основані на наявній статистиці або експертних оцінках, що унеможливлює аналіз при малій кількості накопичених статистичних даних [4].

2. **Очікуваний збиток уразливості від і-ї загрози** — емпіричний метод оцінки, був вперше запропонований спеціалістами американської фірми IBM:

$$R_i = 10^{(S_i + V_i - 4)},$$

де S_i і V_i — коефіцієнти, що характеризують можливу частоту виникнення загрози і значення можливого збитку при її виникненні (значення обох коефіцієнтів — цілі числа в проміжку [0, 7]; для S_i відповідно: 0 — майже ніколи, 7 — більше 1000 разів/рік; V_i відповідно 1-10 000 000 грн.) [4, 6, 7, 8].

Дану методику можна описати системою рівнянь, приводячи параметри на інтервалах:

$$\begin{cases} R_i = 10^{(S_i + V_i - 4)}, \\ S_i = 7 \times 10^{-3} \times s_i, 0 \le s_i \le 10^3, \\ S_i = 7, s_i > 10^3, \\ V_i = 7 \times 10^{-7} \times (v_i - 1), 1 \le v_i \le 10^7, \\ V_i = 7, v_i > 10^7; \end{cases}$$

де s_i — прогнозована або реальна кількість атак на рік, v_i — сума прогнозованого або реального збитку в грошових одиницях.

Але в даному випадку не враховано зростання на другому інтервалі, ми пропонуємо виправити формулу, враховуючи зростання на всій області визначення характеристик. В новій формулі пропонується використовувати гіперболічний тангенс (точніше тільки його додатну частину у першому квадранті). Виходячи з характеристик функції гіперболічного тангенсу, введено додаткові коефіцієнти:

$$f(x) = k_{max} \cdot th\frac{2 \cdot x}{b_{max}},$$

де k_{max} відповідає максимуму шкали, тобто 7, а b_{max} — максимальному значенню прогнозованої або реальної величини, коефіцієнт 2 введено для кращого масштабування по абсцисі. Тоді систему можна записати таким чином:

$$\begin{cases} R_i = 10^{(S_i + V_i - 4)}, \\ S_i = 7 \cdot th\frac{s_i}{500}, 0 \le s_i, \\ V_i = 7 \cdot th\frac{(v_i - 1)}{5 \cdot 10^5}, 1 \le v_i; \end{cases}$$

Формулу очікуваного збитку від і-ї загрози можна записати в загальному вигляді:

$$R_i = 10^{\left(7 \cdot th\frac{s_i}{500} + 7 \cdot th\frac{(v_i - 1)}{5 \cdot 10^5} - 4\right)}, 0 \le s_i, 1 \le v_i.$$

3. **Множина значень для визначення вимог безпеки** — інша запропонована в [7] методика оперує з нормованим рівнем безпеки в континуумі значень [0, 1], і показники надійності є функцією приналежності $\mu^A(x_i)$, де x_i — елемент множини X (вимог безпеки), а A — множина значень, визначаючих виконання вимог безпеки:

$$A = \frac{\mu^A(x_1)}{x_1} + \frac{\mu^A(x_2)}{x_2} + \ldots + \frac{\mu^A(x_n)}{x_n} = \sum_{i=1}^{n} \frac{\mu^A(x_i)}{x_i},$$

де $\frac{\mu^A(x_i)}{x_i}$ — нормована пара «функція приналежності/елемент». Тоді можливо проводити оцінку ефективності по чітко заданим критеріям безпеки.

Цей метод має головний недолік: оцінювати системи можна лише за попередньо визначеним набором критеріїв.

4. **Аналітичний метод оцінки загроз і втрат, пов'язаних з ними**, оперує з середнім показником появи загрози L і величиною розподілу ймовірності f(L). Для оцінки втрат використовується величина m з середнім відхиленням v.

Для аналізу обов'язково потрібно мати статистику порушень безпеки і виміряні значення втрат по цим атакам.

Проблемою методу є неможливість вирахувати вплив засобів захисту інформації (ЗІ) на L і відповідно на m, а тому і оцінити ефективність мір ЗІ [4].

5. **Ступень забезпечення безпеки** дозволяє отримати приблизну оцінку ефективності системи ЗІ. Метод оперує з суб'єктивними коефіцієнтами вагомості i-ї характеристики W_i і бальне значеннями кожної характеристики G_i, що визначається за експертними оцінками. Формула ступеню забезпечення безпеки має вигляд:

$$SR = \frac{1}{N} \sum_{i=1}^{N} W_i \cdot G_i,$$

де N — кількість характеристик.

Метод має два недоліки: неможливо порівняти системи з різним набором характеристик і не враховується залежність коефіцієнта вагомості і значення характеристики від самої характеристики [4, 7].

Автор статті пропонує використовувати для оцінки ступеня забезпечення безпеки системи нормовану характеристику SR*, і одночасно розглядати суб'єктивні коефіцієнти вагомості i-ї характеристики і бальне значення кожної характеристики, як функції від самої характеристики:

$$\begin{cases} W_i = f_{Wi}(x_i), \\ G_i = f_{Gi}(x_i); \end{cases}$$

де f_{Wi} і f_{Gi} — функції від характеристики x_i.

Загальна формула для монотонної f_W і непевної функції f_G має вигляд:

$$SR^* = \frac{1}{N} \sum_{i=1}^{N} W_i^*(x_i) \cdot G_i^*(x_i),$$

де $W_i^*(x_i) = \left| \frac{f_{Wi}(x_i)}{max[f_{Wi}]} \right|$ — нормований коефіцієнт вагомості суб'єктивної оцінки від значення параметру x_i, а $G_i^*(x_i) = \left| \frac{G_i^{\Sigma}}{G_{i\,max}^{\Sigma}} \right|$ — нормоване бальне значення функції, проміжні значення якої визначаються як інтегралі характеристики:

$$\begin{cases} G_i^{\Sigma} = \int_{x_i^{поч.}}^{x_i^{кін.}} f_{Gi}(x)dx, \\ G_{i\max}^{\Sigma} = \int_{x_i^{\min}}^{x_i^{\max}} f_{Gi}(x)dx; \end{cases}$$

де $x_i^{поч.}$ і $x_i^{кін.}$ — початок і кінець інтервалу значень для заданої характеристики, яка існує і неперервна на проміжку від x_i^{min} до x_i^{max}.

У приведеному випадку нормований ступень забезпечення безпеки системи завжди буде $S^* \leq 1$. S^* — абсолютно захищена система, коли розглянуті усі існуючі характеристики x_i. В загальному випадку запропонована модифікація методу дозволяє отримати нормований ступень забезпечення безпеки для будь-якої системи з кількістю характеристик (але не менше 3-ох), та проводити порівняльний аналіз ЗІ в системах з різним набором характеристик.

Так як метод оперує з результатами, отриманими за допомогою експертної оцінки, то перед початком обробки даних необхідно оцінити адекватність експертної групи. Для оцінки адекватності потрібно визначити коефіцієнт конкордації, для чого залучено елементи **функціонально-вартісного аналізу**.

Нехай маємо N суттєвих характеристик, які входять до множини X всіх характеристик системи: $[x_1, x_2 ... x_N] \in X$.

Визначаємо дослідним або аналітичним шляхом інтервали значень для всіх характеристик (мінімальне і максимальне значення), а також середнє значення (яке не обов'язково буде співпадати з середнім арифметичним мінімального і максимального значень). В знайдених інтервалах експерти визначають бальне значеннями кожної характеристики G_i:

$$\begin{cases} G_1 = f_{G1}(x), x = \overline{x_{1\min}, x_{1\max}, x_{1cep.}}, \\ G_2 = f_{G2}(x), x = \overline{x_{2\min}, x_{2\max}, x_{2cep.}}, \\ \ldots \\ G_N = f_{GN}(x), x = \overline{x_{N\min}, x_{N\max}, x_{Ncep.}}; \end{cases}$$

За отриманими даними для наочності будуються графіки $G_i = f_{Gi}(x_i)$, яким оперують експерти для визначення наступних характеристик.

Вагомість параметрів визначаємо методом розстановки пріоритетів, згідно з яким пріоритети характеристик визначає експертна група (M — кількість експертів), а за результатами складається таблиця порівняння (див. табл. 1), в якій середня оцінка приводиться до числової форми за принципом: ">" відповідає 1,5; "=" — 1,0 і "<" — 0,5.

Таблиця 1. Експертна оцінка вагомості параметрів

Параметри	Експерти					Середня оцінка	Числове значення
	1	2	3	…	M		
x_1 и x_2	=	=	>	…	>	>	1,5
x_1 и x_i	>	>	>	…	>	>	1,5
…	…	…	…	…	…	…	…
x_1 и x_N	>	>	>	…	>	>	1,5
x_2 и x_i	>	>	<	…	=	<	0,5
…	…	…	…	…	…	…	…
x_2 и x_N	>	>	>	…	>	>	1,5
…	…	…	…	…	…	…	…
x_{i-1} и x_i	>	<	>	…	>	>	1,5
…	…	…	…	…	…	…	…
x_{N-1} и x_N	>	>	>	…	>	>	1,5

За отриманими даними заповнюється таблиця пріоритетів характеристик (див. табл. 2), в якій для пар x_i–x_i приймається коефіцієнт 1,0.

Таблиця 2. Визначення пріоритетів характеристик

	Характеристики						Важливість		Вагомість	
	x_1	x_2	…	x_i	…	x_N	b_i	φ_i	b'_i	$W_i=\varphi'_i$
x_1	1,0	1,5	…	1,5	…	1,5	7	0,28	34	0,292
x_2	0,5	1,0	…	1,5	…	1,5	5	0,2	22,5	0,193
…	…	…	…	…	…	…	…	…	…	…
x_i	0,5	0,5	…	1,0	…	1,5	4,5	0,18	20,5	0,176
…	…	…	…	…	…	…	…	…	…	…
x_N	0,5	0,5	…	0,5	…	1,0	3	0,12	14	0,12
∑								1,0		1,0

Ступінь важливості φ_i кожного параметру:

$$\varphi_i = \frac{b_i}{\sum\limits_{i=1}^{N} b_i},$$

$$\text{де } b_i = \sum_{j=1}^{N} a_{ij},$$

де b_i — вага і-го параметру по результатам експертних оцінок; a_{ij} — числове значення пріоритету.

Коефіцієнт W_i вагомості і-го параметра визначається на другому кроці:

$$W_i = \varphi'_i = \frac{b'_i}{\sum\limits_{i=1}^{N} b'_i},$$

$$\text{де } b'_i = \sum_{j=1}^{N} a_{ij} b_j .$$

Оцінка адекватність експертної групи проводиться після визначення залежності бального значеннями кожної характеристики від самої характеристики; функція з дискретної приводиться в неперервну: $G_i = f_{Gi}(x_i)$.

Сума рангів кожного параметра:

$$R_i = \sum_{j=1}^{M} r_{ij}, \text{ для } i = \overline{1,N}, j = \overline{1,M},$$

де r_{ij} — ранг і-ї характеристики, визначений j-м експертом.

Перевірка загальної суми рангів, яка має дорівнювати:

$$R_{ij} = \frac{1}{2} \cdot M \cdot N \cdot (N+1).$$

Середня сума рангів $R_{сер.}$:

$$R_{сер.} = \frac{1}{N} R_{ij}.$$

Відхилення суми рангів для кожної і-ї характеристики від середньої суми (сума відхилень за всіма характеристиками повинна дорівнювати нулю):

$$\Delta_i = R_i - R_{сер.}.$$

Загальна сума квадратів відхилень Δ_i^2:

$$S = \sum_{i=1}^{N} \Delta_i^2.$$

Коефіцієнт конкордації:

$$W = \frac{12 \cdot S}{M^2 \cdot (N^3 - N)}.$$

Коефіцієнт конкордації може приймати значення: $0 \le W \le 1$. У випадку повної узгодженості поглядів експертів коефіцієнт становить: $W = 1$. Якщо $W \ge W_{норм.}$ визначені дані заслуговують на довіру и придатні для використання. Для засобів обчислювальної техніки прийнято $W_{норм.} = 0{,}67$, те саме значення можна використовувати і для розподілених систем рухомого зв'язку [9, 10]:

$$W_{розпод.\ сист.\ рух.\ зв'язку} \ge 0{,}67.$$

Методики оцінки ризиків

Існує декілька методик у вимірюванні ризиків, але найбільш розповсюджені оцінки: за двома, трьома і кількома факторами.

1. **Оцінка ризиків за двома факторами** проводиться для аналізу ризиків на базовому рівні і оперує з імовірністю події $P_{події}$ (успішної атаки) і важкістю втрати $C_{втрати}$ (ціною втрати). Ризик і-ї події R_i є прямо пропорційним до $P_{і\ події}$ і $C_{і\ втрати}$ і визначається як добуток цих факторів [5]:

$$R_i = P_{і\ події} \cdot C_{і\ втрати}.$$

Якщо змінні — кількісні, то R_i — математичне очікування витрат.

Якщо змінні — якісні (найчастіший метод оцінки), то метрична операції добутку не визначена. Тому в явній формі цю формулу неможливо використати, але можна використати шкали ймовірності події і важкості втрати. Значення шкал повинні бути чітко обґрунтовані і визначені (в мовній формі) і однаково зрозумілі всіма експертами.

Можна задати суб'єктивну шкала ймовірностей подій, наприклад (приведені у душках ймовірності отримані за допомогою опитування 16-ти експертів-носіїв мови):

A — подія майже ніколи не виникає (~0,05);
B — подія стається рідко (~0,20);
C — середня ймовірність виникнення події (~0,50);
D — подія скоріш за все виникне (~0,20);
E — подія майже обов'язково виникне (~0,05).

Також потрібно визначити суб'єктивну шкалу важливості подій:

- неважливі;
- незначні наслідки і легко ліквідуються;
- помірні наслідки і неважко ліквідуються;
- значні наслідки і важко ліквідуються;
- критичні.

А кінцевий результат оцінки ризику буде складатися за трьох значень: низький, середній і високий ризик. Таким чином, формулу можна замінити на таблицю відповідностей (табл. 3), вид і кількість якої параметрів можуть бути іншими.

Таблиця 3. Таблиця відповідностей

	Неважливі	Незначні наслідки	Помірні наслідки	Значні наслідки	Критичні
A	низький	низький	низький	Середній	середній
B	низький	низький	середній	Середній	високий
C	низький	середній	середній	Середній	високий

D	середній	середній	середній	Середній	високий
E	середній	високий	високий	Високий	високий

2. **Оцінка ризиків за трьома факторами** оперує з поняттями загрози (сукупності умов і факторів, які можуть стати причиною порушення цілісності, доступності і конфіденційності інформації) і уразливості (слабкості в системі ЗІ, яка надає можливість реалізувати загрозу). В такому випадку ймовірністю події $P_{події}$ прямо пропорційна ймовірностям загрози і уразливості [5, 6]:

$$P_{події} = P_{загрози} \cdot P_{уразливості}.$$

Тоді ризик і-ї події R_i має вигляд:

$$R_i = P_{i\ події} \cdot C_{i\ втрати} = P_{i\ загрози} \cdot P_{i\ уразливості} \cdot C_{i\ втрати}.$$

Як і в першому випадку можуть використовуватися як в кількісній, так і в якісній формі. Також можна використовувати комбінації кількісних і якісних форм.

3. **Оцінка ризиків за кількома факторами** формується з добутку декількох ймовірностей, пов'язаних між собою послідовністю етапів сценарію можливого порушення безпеки, наприклад [11]:

$$P_{події} = P_{перелік} \cdot P_{вибір} \cdot P_{брандмауер} \cdot P_{успіх} \cdot P_{збиток},$$

де $P_{перелік}$ — ймовірність входження інформаційної системи в перелік можливих цілей; $P_{вибір}$ — ймовірність вибору з переліку і атаки; $P_{брандмауер}$ — ймовірність обходження захисту каналів (шлюзів); $P_{успіх}$ — ймовірність успішності атаки, досягнення основної мети; $P_{збиток}$ — ймовірність нанесення передбачуваного збитку.

Тоді аналогічно до оцінки за трьома факторами ризик і-ї події R_i має вигляд:

$$R_i = P_{i\ події} \cdot C_{i\ втрати} = P_{i\ перелік} \cdot P_{i\ вибір} \cdot P_{i\ брандмауер} \cdot P_{i\ успіх} \cdot P_{i\ збиток} \cdot C_{i\ втрати}.$$

Висновки

В статті розглянуто існуючі моделі і методи оцінювання захищеності і ризиків, але всі вони мають свої недоліки. Запропоновані модифікації призначені для вдосконалення існуючих методів і включають в себе більш точну апроксимацію (для очікуваного збитку уразливості) і узагальнення функції (для ступеню забезпечення безпеки). Крім того, запропоновано використовувати елементи функціонально-вартісного аналізу для перевірки достовірності експертної оцінки.

З вищезазначеного можна сказати, що методі оцінки ще не достатньо досконалі і потребують більш детального розгляду і введення покрокових інструкцій при комплексному оцінюванні захищеності і ризиків для розподілених систем рухомого зв'язку.

Використовуючи наведену у статті послідовність визначення захищеності системи можна створити програмне забезпечення для автоматизації процесу аналізу і визначення адекватності системи до засобів її захисту.

Список літератури

1. Шварцман В. О. Количественная оценка защищенности информации и сетей святи от несанкционированных действий// Электросвязь. — 2008. — № 5. — С. 5-8.

2. Нечунаев В. М. Оценка рисков информационной безопасности корпоративной информационной системы // Доклады ТУСУРа. — 2009. — № 1 (19), ч. 2. — С. 51-53.

3. Нечунаев В. М. Методика описания корпоративной информационной системы для процедуры управления рисками информационной безопасности // Доклады ТУСУРа. — 2008. — № 2 (18), ч. 1. — С. 116-117.

4. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО «ТИД «ДС», 2001. — 688 с.

5. Симонов С. В. Технологии и инструментарий для управления рисками // Информационный бюллетень Jet Info. — 2003. — № 2 (117). — С. 9-13.

6. Давыдов И. В. Формализация модели совершения киберпреступлений, совершаемых с использованием вредоносных кодов / И. В. Давыдов, А. А. Шелупанов // Известия Томского политехнического университета. — 2006. — Т. 309, № 8. — С. 126-129.

7. Чипига А. Ф. Оценка эффективности защищённости автоматизированных систем от несанкционированного доступа / А. Ф. Чипига, В. С. Пелешенко // Вестник СевКавГТУ. Серия «Физико-химическая». — 2004. — №1 (8). — С. 40.

8. Мещеряков Р. В. Основы информационной безопасности / Р. В. Мещеряков, А. А. Шелупанов, Е. Б. Белов, В. П. Лось. — М.: Горячая линия — Телеком, 2006. — 350 с.

9. Методичні вказівки до виконання організаційно-економічного розділу дипломних проектів / за ред. А. Т. Чернявського. — К.: НТУУ «КПІ», 1999. — 66 с.

10. Методические указания к использования ФСА при разработке программного продукта / сост. А. Т. Чернявский, Л. В. Швец, В. Ф. Шудра, Л. С. Маевская. — К.: НТУУ «КПИ», 1990. — 69 с.

11. Галатенко В. А. Управление рисками: обзор употребительных подходов. Часть II // Информационный бюллетень Jet Info. — 2006. — № 12 (163). — С. 15.

Рецензент: д.т.н., проф. Корченко О.Г.
Надійшла 17.03.2010 р.