УДК 004.413.4

В.І. ЧЕРНИШ

Харківський національний університет радіоелектроніки, Україна

МЕТОДИКА ОЦІНКИ ІНФОРМАЦИЙНИХ РИЗИКІВ З ВИКОРИСТАННЯМ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ

Пропонується методика оцінки інформаційних ризиків з використанням методу аналізу ієрархій, що добре відомий в теорії прийняття рішень. Визначена необхідність проведення оцінки інформаційних ризиків в корпоративних інформаційних системах підприємств. Досліджена математична модель використання методу аналізу ієрархій. Проаналізована процедура оцінки інформаційних ризиків згідно міжнародного стандарту ISO/IEC 27005:2008. Наведено обґрунтування використання методики аналізу інформаційних ризиків за допомогою методу аналізу ієрархій. Визначений напрям подальших досліджень методики.

Ключові слова: *інформаційна безпека, інформаційний ризик, метод аналізу ієрархій.*

Вступ та мета роботи

Постановка проблеми. У сучасному світі поняття ризику широко вживається в різних сферах діяльності. Це поняття, як правило, застосовується для опису будь-якого потенційно небезпечного явища. Задовго до появи поки що недосконалою теорії ризику та методів ймовірнісної оцінки негативних явищ з терміном «ризик» зазвичай пов'язувалося значення (якісне або кількісне), яке характеризувало потенційну ступінь небезпеки однієї або декількох загроз [1].

Управління інформаційними ризиками (ІР) є досить широке поняття, яке використовується в літературі як вид діяльності, що включає визначення загроз безпеці інформаційної системи (ІС), оцінку рівня небезпеки загроз (тобто розміру можливого збитку), а також ймовірностей реалізації цих загроз (тобто проведення повного аналізу ризиків системи [2]). На основі аналізу загроз приймається рішення про заходи щодо зниження загального рівня ризику для ІС. Причому конкретний зміст цього поняття залежить від розв'язуваної задачі.

На даний час в світі для оцінки ІР використовується стандарт ISO/IEC 27005:2008 [3]. В Україні застосовується в Методичних рекомендаціях щодо впровадження системи управління інформаційною безпекою (ІБ) та методики оцінки ІР відповідно до стандартів Національного банку України.

Метою роботи є дослідження можливості використання методу аналізу ієрархій (МАІ) в методиці оцінки ІР.

Актуальність дослідження. ІБ в даний час стає необхідною умовою успішного розвитку господарюючого суб'єкта. Ризик компрометації інформації впливає на матеріальні і нематеріальні активи організації і, в кінцевому рахунку, на результати її виробничо-економічної діяльності.

ІР – це небезпека виникнення збитків або втрати, пов'язаних зі створенням, передачею, зберіганням та використанням інформації. Аналіз ІР є інструментом, що дозволяє визначити:

- які об'єкти і в якому ступені потребують захисту;
- вартість засобів захисту (ЗЗ), без використання яких система ІБ не може бути ефективною.

Найбільш важливим етапом аналізу ІР є ідентифікація (ІД) ризиків. Аналіз відомих рішень демонструє, що загально прийнятої методики кількісної оцінки ІР не існує [4, 5]. Це пов'язано у першу чергу з відсутністю достатнього об'єму статистичних даних про ймовірності реалізації того чи іншого ризику. В теперішній час найбільше розповсюдження отримала якісна оцінка ІР, коли за відсутності точних даних значення параметрів встановлює експерт, що здійснює аналіз ІР. Суб'єктивність експертних оцінок знижує достовірність одержуваних результатів. Аналіз ІР потребує найчастіше залучання великої групи експертів, які добре знають ситуацію на підприємстві та чітко розуміють мету досліджень.

Основний матеріал

Вимоги міжнародних стандартів. Процес оцінки ІР представлений в [3] (рис.1). Оцінка ІР підрозділяється на два основних етапи:

1. Етап – Аналіз ІР;

2. Етап – Оцінювання ІР.

Аналіз ІР підрозділяється на ідентифікацію ІР (ІД ІР) та кількісну оцінку ІР.

Мета ІД ризику полягає в наступному:

- визначити що може трапитися;

- можливі втрати;
- отримати відомості: як, де і чому могла б трапитися втрата.

Кількісна оцінка ІР – оцінка ризику, результати якої можуть бути виражені в цифрах.

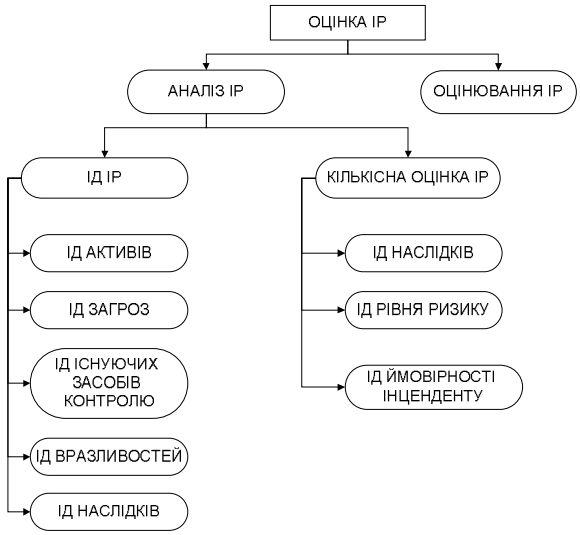

Рис. 1. Загальна структуризація процесу оцінки ІР згідно ISO/IEC 27005:2008

Загальна схема процесу оцінки ІР показує нам, що існує певний алгоритм оцінки ІР. Методика оцінки ІР може бути використана для кожної ланки цього алгоритму.

Методика, що пропонується дозволяє спростити процедуру оцінки ІР, знизити залежність оцінки від уподобань експерта, а також отримати кількісну оцінку ІР. Для цього пропонується використовувати МАІ, що добре відомий в теорії прийняття рішень для структуризації факторів, що оцінюються [6].

Використання ієрархічних структур дозволяє складну задачу розбити на під задачі або рівні ієрархій, оцінка яких представляється більш простою, а головне зробити розуміння задачі менш залежним від суб'єктивних уподобань експерта. МАІ передбачає:

- послідовну декомпозицію проблеми на все більш прості складові частини за допомогою побудови ієрархічної структури, що складається з альтернатив і критеріїв;
- експертну оцінку кожного елементу ієрархії;
- подальшу обробку експертних оцінок.

Сутність МАІ полягає в наступному [6]. Є певна мета і сукупність реалізацій методів (вирішуваних завдань), які забезпечують досягнення цієї мети. Зазначена ціль декомпозується на ряд підцілей або критеріїв (умов), виконання яких забезпечує досягнення поставленої мети.

Вибрані критерії попарно порівнюються між собою (кожен з кожним) та за n бальною системою визначається відносна ступінь важливості кожного критерію в парі. На основі отриманої матриці порівнянь визначається відносна величина ступеня важливості кожного із критеріїв для досягнення поставленої мети в цілому.

Аналогічним способом, шляхом попарного порівняння для кожного з критеріїв формуються матриці методів, на основі яких визначається ступінь відповідності кожного методу кожному з критеріїв. Надалі з урахуванням ступеня важливості кожного критерію визначається внесок (ваговий коефіцієнт) кожного з методів для досягнення поставленої мети.

МАІ досить ефективний при прийнятті рішень в умовах великого числа (більше 5... 7) критеріїв і великого числа реалізованих методів. Цей метод може успішно застосовуватися також у випадках, коли кількість критеріїв і методів не значне, але особа, що приймає рішення в силу недостатньої компетентності або з інших причин змушений звертатися до думки експертів.

У рамках МАІ немає загальних правил для формування структури моделі прийняття рішення. Це є відображенням реальної ситуації прийняття рішення, оскільки завжди для однієї і тієї ж проблеми є цілий спектр думок. Метод дозволяє врахувати цю обставину за допомогою побудови додаткової моделі для узгодження різних думок, за допомогою визначення їх пріоритетів. Таким чином, метод дозволяє враховувати «людський фактор» при підготовці прийняття рішення. Це одне з важливих переваг даного методу перед іншими методами прийняття рішень.

Математична модель МАІ. Припустимо, що n видів дій або об'єктів розглядаються групою експертів. Припустимо, що цілі групи такі:

- висловити судження про відносну важливість цих об'єктів;
- гарантувати такий процес отримання суджень, який дозволить кількісно інтерпретувати судження по всіх об'єктах [6].

Очевидно,що для досягнення кількісного інтерпретування судження потрібна розробка відповідного методу, а саме опис методу отримання з кількісних суджень групи (тобто з відносних величин, асоційованих з парами об'єктів) множини ваг, асоційованих з окремими об'єктами, в тому сенсі, що визначені нижче ваги повинні відображати кількісні судження групи. Завдяки такому підходу інформацію приводимо в зручну форму без інформаційних втрат, властивих якісним судженням.

Нехай $C_1,C_2,..,C_n$ – сукупність об'єктів (можливих дій). Кількісні судження о парах об'єктів (C_i,C_j) представляються матрицею розміру n x n

$$A=(a_{ij}),\ (i,j=1,2,\ldots,n).$$

Елементи a_{ij} визначені за наступними правилами :

Правило 1. Якщо $a_{ij}=\alpha$, то $a_{ji}=1/\alpha$, $\alpha\neq 0$, де α - коефіцієнт судження.

Правило 2 Якщо судження такі, що C_i має однакову з C_j відносну важливість, то $a_{ij}=1$, $a_{ji}=1$, зокрема, $a_{ij}=1$ для усіх і. Тому, матриця А має наступний вигляд:

$$A=\begin{bmatrix} 1 & a_{12} & ... & a_{1n} \\ 1/a_{12} & 1 & ... & a_{2n} \\ ... & ... & ... & ... \\ 1/a_{1n} & 1/a_{2n} & ... & 1 \end{bmatrix}$$

Після представлення кількісних суджень про пари (C_i, C_j) в числовому вираженні через a_{ij}, задача зводиться до того, щоб n можливим діям $C_1,C_2,..,C_n$ поставити у відповідність множину числових ваг ω_1, $\omega_2,\ldots,\omega_n$, які відповідали б зафіксованим судженням.

Для цього, по-перше, необхідно для задачі, що сформульована нечітко надати сувору математичну форму. Цей істотний крок є найбільш важливим у будь-якій задачі, в якій потрібно представити життєву ситуацію в термінах абстрактної математичної структури. Особливо важливий він в розглянутій задачі, оскільки в ній процес математичного формулювання включає в себе ряд неявно видимих переходів. Тому в даній задачі бажано чітко визначити основні етапи процесу її формулювання і як можна детальніше описати кожен етап, щоб потенційний користувач міг скласти власну думку про значимість і цінність цього методу для вирішення його конкретного завдання.

Використання МАІ при оцінці ІР. Загальний вид ієрархічної структури для оцінки ІР представлений на рис. 2. Під альтернативами в даному випадку розуміють ризики, що виникають в ІС, що розташовані на нижньому рівні ієрархії. Стан захищеності проміжних рівнів ієрархії характеризують оцінки ІР (технічні, економічні, фінансові та інші). Побудова ієрархії залежить як від самої ІС, так і від точки зору на оцінку ІР. Єдиним рівнем захищеності найвищого рівня є інтегральна оцінка ризиків (ІОР).

Після побудови ієрархії і присвоювання елементам номерів для забезпечення подальших посилань необхідно оцінити і-й елемент ієрархії з точки зору j-го рівня захищеності, тобто визначити значення C_{ij}.

Оцінений ІР може приводитися за такими критеріями:

- частота виникнення ІР (%);
- частота реалізації ІР окремо для технічного і програмного забезпечення ІС(%);
- ступінь збитку від реалізації ІР (вимірюється в грошових одиницях).

Після того як обраний критерій оцінки і визначено C_{ij}, розраховуються векторні оцінки ІР для кожного елемента ієрархії за формулою:

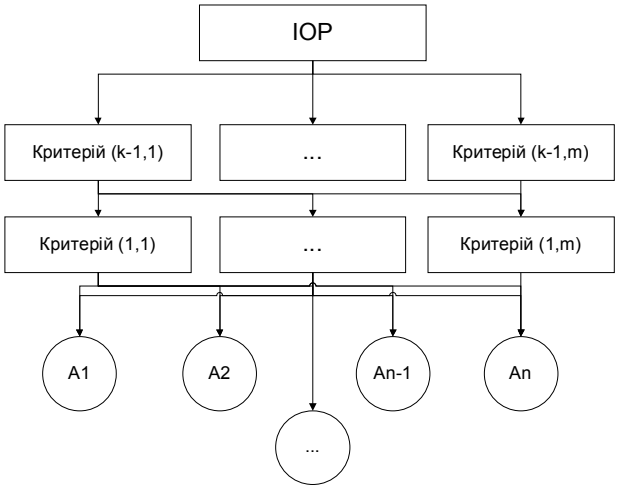

Рис. 2. Ієрархічне представлення проблеми оцінки ІР в загальному вигляді

$$\overline{V_i}=\frac{\sum_i C_{ij}\overline{V_j}}{\sum_i C_{ij}},$$

де і отримує значення з множини номерів елементів ієрархії найближчого нижнього рівня. На самому нижньому рівні ієрархії векторна оцінка ІР отримується наступним чином:кожному ризику ставиться у відповідність вектор, який має одиничну компоненту в позиції, яка відповідає номеру ризику,і нулі у всіх інших позиціях. Ієрархія відображає реальні зв'язки, які існують між об'єктами інформаційного середовища, тому побудована ієрархічна структура дозволяє оцінити не тільки самі ІР,а й ефективність ЗЗ від них.

Оцінка ефективності ЗЗ від ІР може проводитися за такими критеріями:

- зменшення частоти виникнення ІР (%);
- зменшення частоти реалізації ІР окремо для технічного та програмного забезпечення ІС (%);
- зменшення ступеня шкоди від реалізації ІР (вимірюється в грошових одиницях).

Запропонована методика вводить кілька рівнів ієрархії і тим самим систематизує і спрощує процедуру оцінки, ми можемо розглядати ризик з різних точок зору. Виникають розбіжності в оцінці одного і того ж ризику, і тим самим зменшується суб'єктивність оцінки. Наприклад, один рівень захищеності може оцінювати ризики з точки зору вартості ЗЗ, інший – з точки зору ефективності застосування.

На наступному рівні ієрархії оцінюються вже самі точки зору, тобто критерії стають альтернативами до верхнього рівня ієрархії. Таким чином складна проблема оцінки декомпозується на ряд більш простих.

Для детальної наочності продемонструємо практичне застосування ієрархій. Розглянемо ***дві умови функціонування ІС***:

1 умова – дрібне підприємство, що використовує автоматизовану систему класу 2 (АС2);

2 умова – велике підприємство, що використовує автоматизовану систему класу 3 (АС3).

Виділимо ***п'ять основних груп загроз***:

- загрози в зв'язку з форс-мажорними обставинами;
- загрози на організаційному рівні;
- загрози, що пов'язані з помилками людей;
- загрози, що пов'язані з технікою;
- загрози, що виникають на предпроектному етапі розробки ІС.

Для кожної групи визначимо по три основних загрози. Структуруємо та результати занесемо в табл. 1.

Далі побудуємо загальну ієрархічну систему (рис. 3) з наступними характеристиками:

- *альтернативами* є ІР (А1, А2, А3 та А4);
- *критеріями першого рівня* є джерела ІР (перелік загроз);
- *критеріями другого рівня* є групи загроз, що впливають на ІР*;*
- *критеріями третього рівня* – умови функціонування ІС.

Таблиця 1

Ієрархічна модель загроз

Рівні критеріїв	Найменування критеріїв	Умовні позначення	Характеристики критеріїв
1 рівень	(1,1)	U1	Блискавка
	(1,2)	U2	Відмова ІС
	(1,3)	U3	Втрата даних через вплив інтенсивних магнітних полів
	(1,4)	U4	Відсутність або недоліки регламентуючих документів
	(1,5)	U5	Недоліки адміністрування прав доступу
	(1,6)	U6	Некоректна система управління криптографічними ключами
	(1,7)	U7	Порушення конфіденційності / цілісності даних в результаті помилок користувачів
	(1,8)	U8	Руйнування обладнання чи даних в результаті недбалості
	(1,9)	U9	Заборонені дії в ІС
	(1,10)	U10	Втрати даних через старіння (погіршення якості) носія даних
	(1,11)	U11	Руйнування системи електропостачання
	(1,12)	U12	Відмова бази даних
	(1,13)	U13	Неавторизоване використання ІС
	(1,14)	U14	Несанкціонований доступ до конфіденційних даних, збереженим в процесі інсталяції офісної АТС
	(1,15)	U15	Загрози, які виходять від сторонніх фахівців, які залучаються для обслуговування елементів ІС
2 рівень	(2,1)	T1	Загрози в зв'язку з форс-мажорними обставинами
	(2,2)	T2	Загрози на організаційному рівні
	(2,3)	T3	Загрози, що пов'язані з помилками людей
	(2,4)	T4	Загрози, що пов'язані з технікою
	(2,5)	T5	Загрози, що виникають на предпроектному етапі
3рівень	(3,1)	АС2	Дрібне підприємство
	(3,2)	АС3	Велике підприємство

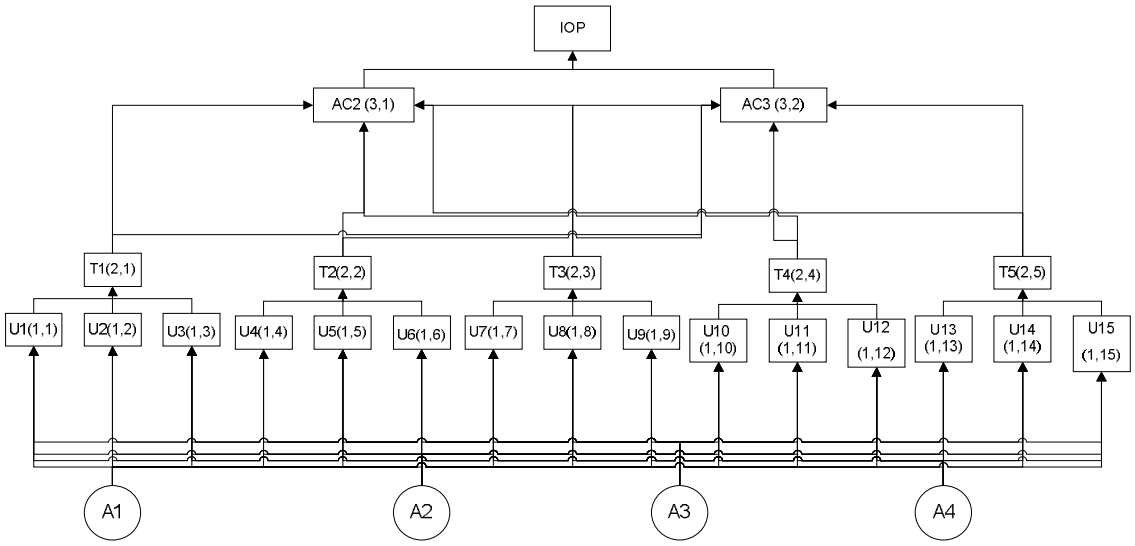

Рис. 3. Ієрархічна структура оцінки інформаційних ризиків

Висновки

Розроблена універсальна методика і тому може служити науковою базою для інженерів - розробників при побудові корпоративної системи захисту від ІР ІС підприємств різного призначення і масштабу. Методика буде корисна широкому колу осіб, зайнятих проблемами захисту від ІР.

Напрям подальших досліджень пов'язаний з дослідженням ієрархічної композиції пріоритетів загроз ІР та розрахунок інтегральних оцінок впровадження методики даної методики оцінки ІР.

Література

1. Черныш, В.И. Методы оценивания информационных рисков компании [Текст] / В.И.Черныш // Материалы XV Международного юбилейного молодёжного форума «Радиоэлектроника и молодежь в XXI веке»: сб. тезисов, 18–20 апреля 2011 р., Т.5. - Харьков: ХНУРЭ, 2011. – С. 195.

2. Замула, О.А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки [Текст]/ О.А. Замула, В.І. Черниш // Системи обробки інформації: збірних наукових праць ХУПС. – Вип.2(92). – Харків: ХУ ПС, 2011. – С. 53-56.

3. ISO 27005 ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management [Text]. – ISO / IEC, 2008. – 70 с.

4. Марка, Д., Методология структурного анализа и проектирования [Текст]: пер. с англ. / Д. Марка, К. Мак-Гоуэн. – М.: Мета Технология, 1993. – 240 с.

5. Могилевский, В.Д. Методология систем [Текст]/ В.Д. Могилевский. – М.: Экономика, 1999. – 251 с.

6. Саати, Т. Принятие решений. Метод анализа иерархий [Текст] / Т. Саати. – М.: Радио и связь, 1993. – 278 с.

Поступила в редакцию 20.01.2012

Рецензент: д-р техн. наук, професор, завідувач кафедри безпеки інформаційних технологій І.Д. Горбенко, Харківський національний університет радіоелектроніки, Харків.

МЕТОДИКА ОЦЕНКИ РИСКОВ С ИСПОЛЬЗОВАНИЕМ МЕТОДА АНАЛИЗА ИЕРАРХИЙ

В.И. Черныш

Предлагается методика оценки информационных рисков с использованием метода анализа иерархий, хорошо известной в теории принятия решений. Определена необходимость проведения оценки информационных рисков в корпоративных информационных системах предприятий. Исследована математическая модель использования метода анализа иерархий. Проанализирована процедура оценки информационных рисков согласно международного стандарта ISO / IEC 27005:2008. Приведены обоснования использования методики анализа информационных рисков с помощью метода анализа иерархий. Определено направление дальнейших исследований методики.

Ключевые слова: информационная безопасность, информационный риск, метод анализа иерархий.

METHOD OF ASSESSMENT RISKS OF INFORMATION USING THE METHOD OF ANALYSIS OF HIERARCHIES

V.I. Chernish

A method of assessing information risks by using the analytic hierarchy process, well known in decision theory. Determined by the need to assess information risk in corporate information systems companies. Investigated a mathematical model of the use of the analytic hierarchy process. Analyzed the information risk assessment procedure in accordance with International Standard ISO / IEC 27005:2008. We present a method of analysis justify the use of information risks by using the analytic hierarchy process. Set the direction for further research methodologies.

Key words: information security, information risk, method of analysis of hierarhies.

Черниш Владислав Ігорович – магістрант кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки, Харків, Україна, e-mail: vlad.chernish@gmail.com.