УДК 681.3.06

С.В. Павленко

Військова частина А0515, Київ

МЕТОД ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Розглянуто підходи до розв'язування багатокритеріальних задач синтезу моделей, побудованих на основі експертної інформації при нечіткому формулюванні переваг показників або їх важливості. Здійснено розробку методу оцінки захищеності інформаційних систем, що застосовується в умовах необхідності обліку великої кількості якісних показників, їх істотної взаємозалежності, а також різниці у важливості їх виконання.

Ключові слова: *інформаційна система, оцінка захищеності, метод, нечітка логіка, контроль, безпека, показники системи.*

Вступ

Постановка проблеми у загальному вигляді. Проведення внутрішнього контролю та самооцінки захищеності великих інформаційних систем (ІС) в умовах високого ступеня невизначеності середовища їх функціонування та постійного вдосконалення технологій, достатньо складна та багатокритеріальна задача. Для цього необхідно мати уяву про структуру ІС, про особливості технологічних процесів обробки, передачі та зберігання інформації в ній, про способи взаємодії з іншими ІС, про реалізовані заходи захисту та, нарешті, про основні принципи та підходи, що використовуються у системі безпеки.

Для того щоб оцінити захищеність ІС існують, в основному, якісні методи оцінки, які на виході дозволяють одержати не кількісну оцінку (система захищена на 4,2 бали або на 58%), а якісну – система відповідає певному класу або рівню захищеності, тому чи іншому стандарту безпеки.

Кількісні методи оцінки захищеності поки мало застосовуються на практиці, оскільки не враховують такий показник як якість функціонування захисних механізмів або ефективність систем захисту.

Необхідність же кількісної оцінки рівня захищеності ІС виникає щоразу під час об'єктивної оцінки загального стану захищеності інформаційних ресурсів. Кількісна оцінка може стати простим та зрозумілим засобом підтримки прийняття рішень, що базується на аналізі поточного стану ІС та враховує виконання вимог безпеки.

Формалізований опис узагальненої моделі безпеки ІС (1) містить у собі опис: характерних загроз безпеці, яким повинні протидіяти компоненти ІС $I_{ЗАГР}$, політики, здійснення якої повинно бути забезпечене механізмами безпеки компонентів ІС $I_{ПІБ}$, пропозицій безпеки відносно використання $I_{ПРОП}$, цілей безпеки, що відповідають компонентам ІС $I_{ЦІЛІ}$, часткових моделей безпеки компонентів, що враховують внутрішні та міжрівневі залежності функцій безпеки компонентів ІС та відповідають рівням управління та контролю ІС $I_{ЧМ}$ тощо.

$$I = I_{ЗАГР} \cup I_{ПІБ} \cup I_{ПРОП} \cup I_{ЦІЛІ} \cup I_{ЧМ} \ldots \qquad (1)$$

З огляду на вищезазначене, у рамках виконання досліджень, було поставлено задачу – розробки методу кількісної оцінки захищеності, що повинен враховувати наступні особливості ІС:

переважно якісний характер показників, що враховуються під час аналізу захищеності ІС;

необхідність обліку великої кількості показників або вимог безпеки;

складний опосередкований взаємозв'язок показників якості захисту з показниками якості функціонування ІС;

відмінності у важливості виконання вимог безпеки, що висуваються до ІС;

істотний взаємозв'язок та взаємозалежність показників різних продуктів ІТ, що входять в ІС;

труднощі одержання вихідних даних, необхідних для розв'язування задач контролю, аналізу та оцінки захищеності (велика кількість джерел даних).

Зазначені особливості впливають на вибір математичних методів розв'язування задачі, здійснення процедур контролю, аналізу, оцінки та удосконалення захисних механізмів.

Мета статті – розробка методу оцінки захищеності ІС та схеми його реалізації, побудованих на основі експертної інформації при нечіткому формулюванні переваг показників захищеності або їх важливості.

Аналіз останніх досягнень та публікацій. Принциповими особливостями задач контролю та оцінки захищеності ІС, що визначають метод її розв'язування, є: багатокритеріальність задач; не тільки кількісний, але і в основному якісний (нечіткий) опис показників, що задаються у вигляді вимог безпеки; вплив експертної інформації, що визначає переваги того або іншого показника, при нечіткій постановці задачі. Аналіз досліджень та публікацій [1 – 12] показує, що всі методи розв'язування багатокритеріальних задач можна звести до трьох груп методів: метод головного показника; метод результуючого показника; лексикографічні методи (методи послідовних поступок).

Метод головного показника базується на переведенні всіх показників, крім якого-небудь однорідного, що називається головним, у розряд обмежень типу рівностей та нерівностей. До недоліків методу головного показника можна віднести: труднощі виділення головного показника та встановлення припустимих значень для показників, що переводяться у розряд обмежень.

Метод результуючого показника базується на формуванні узагальненого показника шляхом інтуїтивних оцінок впливу часткових показників на результуючу якість виконання системою її функцій. Оцінки такого впливу даються групою фахівців – експертів.

Лексикографічний метод базується на впорядкованих за важливістю показниках. Суть методу полягає у виділенні безлічі альтернатив з найкращою оцінкою за найбільш важливим показником. Якщо така альтернатива єдина, то вона вважається найкращою; якщо їх декілька, то з їхньої підмножини виділяються ті, які мають кращу оцінку за другим показником тощо. За сукупністю показників може призначатися поступка, у межах якої альтернативи вважаються еквівалентними.

Вибір методу розв'язування багатокритеріальної задачі, як у класичній, так і в нечіткій постановці визначається тим, в якому вигляді представлена експертна інформація щодо переваг показників. Якщо представлено експертну інформацію про ступінь або важливість переваги показників та визначені їхні вагові коефіцієнти, то методом розв'язування багатокритеріальної задачі вважається метод результуючого показника.

Найбільш широке застосування серед результуючих показників одержали адитивний, мультиплікативний та мінімаксний показники.

Постановка задачі та викладення матеріалів дослідження

Моделі безпеки як складового компонента ІС запропоновано розглядати у термінах ISO/IEC 15408-1,3 з урахуванням загроз безпеці інформаційним ресурсам, політики та припущень безпеки у конкретному структурному підрозділі.

Розглянемо розробку моделі контролю, аналізу та оцінки захищеності ІС на прикладі узагальненої моделі безпеки.

При проведенні контролю може виявитися, що деякі показники не виконуються або не виконуються їхні залежності. Контроль реалізованих параметрів відображається в узагальненій моделі безпеки ІС ступенем виконання (повнотою реалізації) вимог.

Оцінка захищеності ІС грунтується на вихідних даних, представлених у вигляді бази даних, заповненої в процесі внутрішнього контролю фахівцями з безпеки. Приклад у скороченому вигляді наведено у табл. 1, де W_i – показники, згруповані за класами безпеки, J – рівні управління (серверної операційної системи (СОС), системи управління базами даних (СУБД), мережевих сервісів (ЛОМ), клієнтської операційної системи (КОС), прикладного програмного забезпечення (ППЗ) та документування ІС (ДІС)), $X_{i,j}$ – результат виконання показників.

Вважаємо, що якщо у розглянутої ІС забезпечені всі функції безпеки, що входять у її модель безпеки, то система перебуває у захищеному стані і її рівень захищеності відповідає встановленим нормативам.

Для визначення важливості показників та розрахунку вагових коефіцієнтів пропонується керуватися пріоритетами політики безпеки інформації (БІ). Наприклад, поширеною практикою є розподіл пріоритетів політики БІ відповідно до табл. 2.

Після ранжирування класів або показників за важливістю для кожного показника моделі визначаються вагові коефіцієнти, і проводиться їхнє нормування.

Визначення вагових коефіцієнтів A_i для кожного і-го показника або класу безпеки проводиться за формулою:

$$A_i = 1 - \frac{R_i - 1}{M}; \quad i = \overline{1, M}. \qquad (2)$$

де R_i – ранг, M – число класів або показників.

Нормування коефіцієнтів здійснюється за залежністю

$$A_k = \frac{A_i}{\sum_{i=1}^{M} A_i}. \qquad (3)$$

Нормовані значення вагових коефіцієнтів класів, що відповідають пріоритетам політики БІ при обробці інформації з обмеженим доступом (табл. 2, ст. 2) наведені в табл. 3. Ранжирування класів або показників безпеки за важливістю може бути виконане і по-іншому, наприклад, відповідно до особистих переваг фахівців, що приймають рішення.

Результатом виконання показників можуть бути два стани, що взаємно виключають один одного, "0" – якщо показник не виконано, "1" – якщо показник виконано. Показники, що мають залежності, розраховуються з урахуванням виконання показників, від яких вони залежать і від ступеня впливу показників на захищеність (від ваги).

Наприклад, формула для розрахунку виконання показника FAU_GEN.2, що має пряму залежність від показників FAU_GEN.1 і FIA_UID.1 для рівня управління серверної ОС (табл. 1) буде виглядати таким чином:

$$X_{3,1} = \frac{A_2 \cdot X_{2,1} + A_{32} \cdot X_{32,1}}{A_2 + A_{32}}, \qquad (4)$$

де A_2, A_{32} – вагові коефіцієнти відповідних показників, $X_{2,1}$, $X_{32,1}$ – результати виконання показників, що входять у залежність.

Таблиця 1

Приклад вихідних даних для оцінки захищеності ІС

Клас	Показники (W_i)	Залежності	Рівні управління та контролю (J)					
			СОС	СУБД	ЛОМ	КОС	ППЗ	ДІС
FAU	FAU_GEN.2	FAU_GEN.1, FIA_UID.1	$X_{3,1}$	$X_{3,2}$	$X_{3,3}$	$X_{3,4}$	$X_{3,5}$	---
			…					
	FAU_STG.4	FAU_GEN.1	$X_{11,1}$	$X_{11,2}$	---	$X_{11,4}$	---	---
FCS	FCS_CKM.1	FCS_CKM.4	---	---	---	---	$X_{12,5}$	---
			…					
	FCS_COP.1	FCS_CKM.1	---	---	$X_{15,3}$	---	$X_{15,5}$	---
FDP	FDP_ETC.2	FDP_ACC.1 або FDP_IFC.1	---	---	$X_{18,3}$	---	---	---
			…					
	FDP_RIP.2	---	$X_{22,1}$	$X_{22,2}$	$X_{22,3}$	$X_{22,4}$	$X_{22,5}$	---
FIA	FIA_AFL.1	FIA_UAU.1	$X_{23,1}$	$X_{23,2}$	$X_{23,3}$	$X_{23,4}$	$X_{23,5}$	---
			…					
	FIA_USB.1	FIA_ATD.1	$X_{34,1}$	---	$X_{34,3}$	$X_{34,4}$	$X_{34,5}$	---
FMT	FMT_MOF.1	FMT_SMR.1	$X_{35,1}$	$X_{35,2}$	$X_{35,2}$	---	$X_{35,5}$	---
			…					
	FMT_SMR.3	FMT_SMR.1	$X_{45,1}$	$X_{45,2}$	$X_{45,2}$	---	$X_{45,5}$	---
FPR	FPR_ANO.1	---	---	---	---	---	$X_{46,5}$	---
	FPR_UNO.4	---	---	---	$X_{47,3}$	---	$X_{47,5}$	---
FPT	FPT_AMT.1	---	$X_{48,1}$	---	$X_{48,3}$	---	$X_{48,5}$	---
			…					
	FPT_TST.1	FPT_AMT.1	$X_{60,1}$	---	$X_{60,3}$	---	$X_{60,5}$	---
FRU	FRU_RSA.1	---	$X_{61,1}$	$X_{61,2}$	---	$X_{61,4}$	---	---
	FRU_FLT.1	FPT_FLS.1	---	---	$X_{62,3}$	---	$X_{62,5}$	---
FTA	FTA_MCS.1	FIA_UID.1	---	---	---	$X_{63,4}$	$X_{63,5}$	---
			…					
	FTA_TSE.1	---	---	$X_{69,2}$	$X_{69,3}$	$X_{69,4}$	$X_{69,5}$	---
FTP	FTP_ITC.1	---	---	---	---	---	$X_{70,5}$	---
	FTP_TRP.1	---	$X_{71,1}$	$X_{71,2}$	$X_{71,3}$	---	$X_{71,5}$	---
Довіра	ACM_CAP.3	---	---	---	---	---	---	$X_{72,6}$
			…					
	AVA_VLA.1	---	---	---	---	---	---	$X_{89,6}$

Таблиця 2

Розподіл пріоритетів політики БІ

Пріоритет	Умовна ступінь важливості інформації				ТКС і СС, що передають інформацію	
	1	2	3	4	технологічну та управляючу	зовнішніх організацій
1	конфідент-ційність	цілісність	доступність	цілісність	гарантованість доставки	цілісність
2	цілісність	конфіден-сть	цілісність	доступність	цілісність	доступність
3	доступність	доступність	конфідент-ційність	–	конфідент-ційність	конфідент-ційність

Формула для розрахунку виконання показника FDP_ETC.2, що має вибіркову залежність між показниками FDP_ACC.1 або FDP_IFC.1 для рівня мережевих сервісів (табл. 1) буде виглядати як

$$X_{18,3} = \max\left\lfloor A_{16} \cdot X_{16,3}; A_{19} \cdot X_{19,3} \right\rfloor, \qquad (5)$$

де A_{16}, A_{19}, $X_{16,3}$, $X_{19,3}$ – мають такий же зміст, як і у формулі (4).

Для розв'язування задачі оцінки захищеності ІС обрано метод результуючого показника, відповідно до якого визначається адитивний показник на кожному рівні управління (J).

$$\overline{X_j} = \sum_{k=1}^{n} A_k X_{kj}; 0 \le \overline{X_j} \le 1, \qquad (6)$$

де $0 \le A_k \le 1; \sum_{k=1}^{n} A_k = 1$, A_k – ваговий коефіцієнт важливості класів.

Таблиця 3

Нормовані значення вагових коефіцієнтів класів

№ з/п	Клас	Найменування	Ранг, R_i	Ваговий коеф-т, A_k
1.	FAU	Аудит безпеки	6	0,090
2.	FCS	Криптографічний захист	1	0,166
3.	FDP	Управління доступом	5	0,106
4.	FIA	Ідентифікація та автентифікація	3	0,136
5.	FMT	Управління безпекою	7	0,075
6.	FPR	Приватність	4	0,121
7.	FPT	Захист функцій безпеки	8	0,060
8.	FRU	Використання ресурсів	9	0,045
9.	FTA	Доступність сеансів	10	0,030
10.	FTP	Довірений канал	2	0,151
11.	Довіра	Управління конфігурацією, організаційні заходи	11	0,015

Таблиця 4

Модель оцінки захищеності ІС, побудована за технологією клієнт-сервер

Ранг класу	Клас безпеки	Кількість показників, N	Узагальнений показник, $X_{k,j}$					
			СОС, J=1	СУБД, J=2	ЛОМ, J=3	КОС, J=4	ППЗ, J=5	ДІС, J=6
1	FCS	4	$X_{1,1}$	$X_{1,2}$	$X_{1,3}$	$X_{1,4}$	$X_{1,5}$	$X_{1,6}$
2	FTP	2	$X_{2,1}$	$X_{2,2}$	$X_{2,3}$	$X_{2,4}$	$X_{2,5}$	$X_{2,6}$
3	FIA	12	$X_{3,1}$	$X_{3,2}$	$X_{3,3}$	$X_{3,4}$	$X_{3,5}$	$X_{3,6}$
4	FPR	2	$X_{4,1}$	$X_{4,2}$	$X_{4,3}$	$X_{4,4}$	$X_{4,5}$	$X_{4,6}$
5	FDP	7	$X_{5,1}$	$X_{5,2}$	$X_{5,3}$	$X_{5,4}$	$X_{5,5}$	$X_{5,6}$
6	FAU	11	$X_{6,1}$	$X_{6,2}$	$X_{6,3}$	$X_{6,4}$	$X_{6,5}$	$X_{6,6}$
7	FMT	11	$X_{7,1}$	$X_{7,2}$	$X_{7,3}$	$X_{7,4}$	$X_{7,5}$	$X_{7,6}$
8	FPT	13	$X_{8,1}$	$X_{8,2}$	$X_{8,3}$	$X_{8,4}$	$X_{8,5}$	$X_{8,6}$
9	FRU	2	$X_{9,1}$	$X_{9,2}$	$X_{9,3}$	$X_{9,4}$	$X_{9,5}$	$X_{9,6}$
10	FTA	7	$X_{10,1}$	$X_{10,2}$	$X_{10,3}$	$X_{10,4}$	$X_{10,5}$	$X_{10,6}$
11	Довіра	18	---	---	---	---	---	$X_{11,6}$
Всього показників		89	41	35	48	26	52	18
Адитивний показник за рівнями, $\overline{X_j}$			$\overline{X_1}$	$\overline{X_2}$	$\overline{X_3}$	$\overline{X_4}$	$\overline{X_5}$	$\overline{X_6}$
Важливість рівнів, A_j			A_j=0,2	A_j=0,2	A_j=0,2	A_j=0,15	A_j=0,15	A_j=0,1
Підсумкова оцінка			$\overline{Q} = \sum_{j=1}^{6} A_j \overline{X_j}$					

Таблиця 5

Шкала відповідності Q~B~L

Інтервальна оцінка, *Q*	Бальна оцінка, *B*	Лінгвістична оцінка, *L*
0,9 – 1,0	5 – відмінно	Повністю задовольняє вимогам. Усі залежності функцій безпеки дотримані та виконані. Виконання вимог погоджено між компонентами ІС та описано в документації.
0,7 – 0,9	4 – добре	Майже задовольняє вимогам. Усі залежності функцій безпеки дотримані та виконані, але різними компонентами ІС, узгодження між компонентами не описано в документації.
0,5 – 0,7	3 – задовільно	Задовольняє вимогам в основному. Основні вимоги виконані, не всі залежності враховані та виконані.
0,3 – 0,5	2 – незадовільно	Не задовольняє вимогам. Вимоги розрізнені, виконані не всі основні вимоги.
0 – 0,3	1 – вкрай незадовільно	Повністю не задовольняє вимогам. Вимоги розрізнені, не виконано більшість основних вимог.

Підсумкова оцінка захищеності визначається за формулою

$$Q = \sum_{j=1}^{m} A_j \overline{X_j}; 0 \le Q \le 1, \qquad (7)$$

де $0 \le A_j \le 1; \sum_{j=1}^{m} A_j = 1$, A_j – важливість виконання на J-му рівні.

У табл. 4 представлена модель оцінки захищеності ІС, побудованої за технологією клієнт-сервер. Для ІС іншої структури в моделі можуть бути відсутні деякі зазначені рівні та/або бути присутні нові. Наприклад, для ІС, побудованою за технологією файл-сервер, у моделі буде відсутній рівень СУБД (J=2), а для автономної ІС будуть відсутні рівні СОС, СУБД, ЛОМ (J=1, 2, 3).

Формалізація критеріїв контролю дозволяє автоматизувати процес оцінки, тобто розробити засіб для оцінки відповідності заходів безпеки еталонному зразку (стандарту, політиці безпеки, профілю захисту, моделі безпеки) і автоматизувати дії, що пов'язані зі збором, зберіганням і обробкою результатів внутрішнього контролю захищеності.

Для підтримки прийняття рішень захищеність ІС зручно виражати в бальній або лінгвістичній оцінці. Для таких оцінок вводиться еталонна шкала, тобто така шкала, у якій відображено адитивну ознаку. У розглянутому прикладі оцінка захищеності представлена в інтервалі від 0 до 1, для переформатування її в інші оцінки в табл. 5 представлено шкалу відповідності Q~B~L.

Особливістю обраної системи оцінки є можливість її використання для обробки вихідної експертної інформації, а також для надання даної інформації в інтерпретованому вигляді, вираженою нетехнічною мовою та придатною для підтримки прийняття обґрунтованих рішень керівниками як завгодно високого рангу. Метод, що застосовано для визначення вагових коефіцієнтів – метод ранжирування, дозволяє одержати досить точні вагові коефіцієнти, при цьому час спілкування з експертами мінімальний.

Схема контролю та оцінки захищеності ІС і прийняття рішень на вибір варіантів захисту ІС або схема реалізації запропонованого методу представлена на рис. 1.

Реалізація методу розбита на три етапи:

1. Здійснюється побудова узагальненої моделі безпеки ІС і проводиться розрахунок вагових коефіцієнтів показників і класів, що входять у модель із урахуванням пріоритетів політики БІ.

2. Здійснюється контроль виконання показників, що входять у модель, заповнення бази даних поточного контролю та розрахунок підсумкової оцінки захищеності.

3. На основі результатів контролю та отриманої оцінки захищеності приймається рішення про вдосконалення захисних заходів або необхідність корегування моделі безпеки, зміни пріоритетів захисту та перерахування вагових коефіцієнтів.

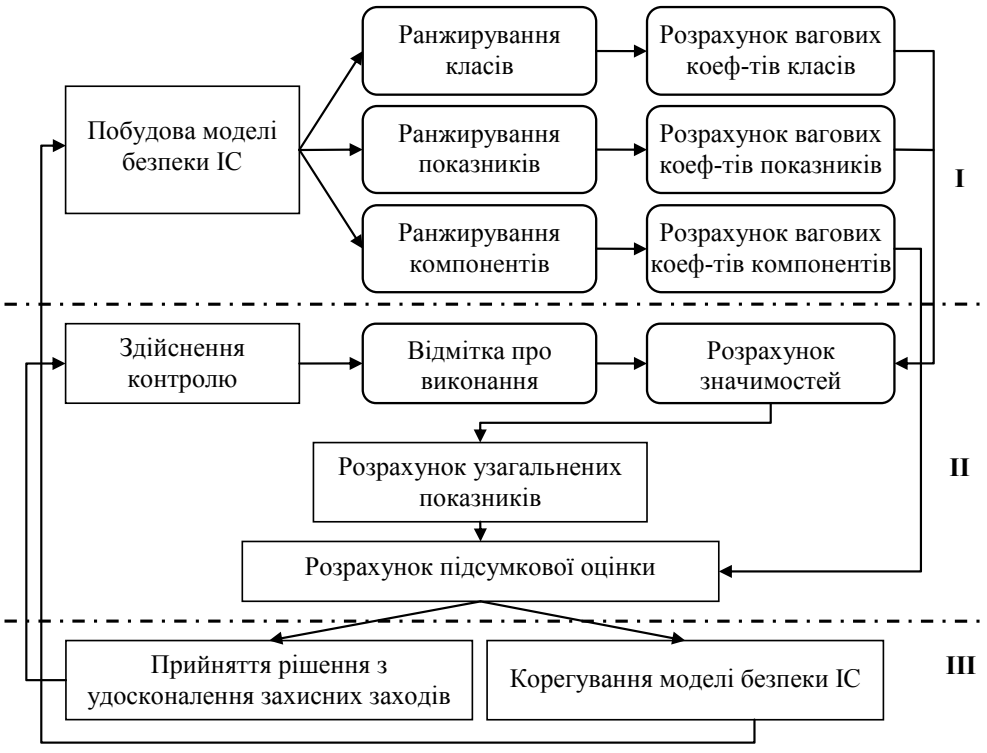

Рис. 1. Схема реалізації методу оцінки захищеності ІС

Висновки

Отже, розроблені метод та схема його реалізації дозволяють оцінити поточний або реалізований рівень захищеності ІС, провести порівняння із заданою моделлю безпеки та визначити слабкі показники. Розроблений інструментарій служить засобом підтримки прийняття рішень щодо вдосконалювання захисних заходів.

Застосований метод визначення вагових коефіцієнтів – метод ранжирування, при всій його простоті дозволяє одержати вагові коефіцієнти досить точні та близькі за значенням, що отримуються методом лінійної згортки, та потребує в 12 разів менше часу для спілкування з експертами.

У подальшому планується розробити програмну реалізацію відповідної бази даних з метою автоматизації процесу внутрішнього контролю, обробки його результатів, оцінки та вибору раціональних варіантів реалізації функцій безпеки, зіставлення і порівняльного аналізу результатів попереднього контролю.

Список літератури

1. Методы определения коэффициентов важности критериев / А.М. Анохин, В.А. Глотов, В.В. Павельев, А.М. Черкашин // Автоматика и телемеханика. – 1997. – № 8. – С. 3-35.

2. Поспелов Д.А. Нечеткие множества в моделях управления и искусственного интеллекта / Д.А. Поспелов. – М.: Наука, 1986. – 312 с.

3. Обработка нечеткой информации в системах принятия решений / [А.Н. Борисов, А.В. Алексеев, Г.В. Меркурьев и др.]. – М.: Радио и связь, 1989. – 304 с.

4. Заде Л. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л. Заде. – М.: МИР, 1976. – 165 с.

5. Литвак Б.Г. Экспертная информация: методы получения и анализа / Б.Г. Литвак. – М.: Радио и связь, 1982. – 184 с.

6. Кини Р.Л. Принятие решений при многих критериях предпочтений и замещения / Р.Л. Кини. – М.: Радио и связь, 1981. – 342 с.

7. Мулен Э. Кооперативное принятие решений: аксиомы и модели / Э. Мулен. – М.: МИР, 1991. – 463 с.

8. Жданов С.А. Экономические модели и методы в управлении / С.А.Жданов. – М.: Изд-во Дело и Сервис, 1998. – 176 с.

9. Шелобаев С.И. Математические методы и модели в экономике, финансах, бизнесе: учеб. пособие для вузов / С.И. Шелобаев. – М.: ЮНИТИДАНА, 2001. – 367 с.

10. Замков О.О. Математические методы в экономике: учебник / О.О. Замков, А.В. Толстопятенко, Ю.Н. Черемных. – М.: МГУ им. М.В. Ломоносова, Изд-во ДИС, 1998. – 368 с.

11. Балдин К.В. Математические методы в экономике. Теория, примеры, варианты контрольных работ: учеб. пособие / К.В. Балдин. – М.: Изд-во Московского психолого-социального института, 2003. – 112 с.

12. Герасименко В.А. Основы теории управления качеством информации / В.А. Герасименко. – М. : 1989. Деп. в ВИНИТИ. № 5392-В89.

Надійшла до редколегії 23.10.2009

Рецензент: д-р техн. наук, с.н.с. Г.В. Худов, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

МЕТОД ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

С.В. Павленко

Рассмотрены подходы к развязыванию многокритериальных задач синтеза моделей, построенных на основе экспертной информации при нечеткой формулировке преимуществ показателей или их важности. Осуществлена разработка метода оценки защищенности информационных систем, которая применяется в условиях необходимости учета большого количества качественных показателей, их существенной взаимозависимости, а также разницы в важности их выполнения.

Ключевые слова: *информационная система, оценка защищенности, метод, нечеткая логика, контроль, безопасность, показатели системы.*

METHOD OF ESTIMATION OF PROTECTED OF INFORMATIVE SYSTEMS

S.V. Pavlenko

Going is considered near untiing of multicriterion tasks of synthesis of models, built on the basis of expert information at unclear formulation of advantages of indexes or their importance. Development of method of estimation of protected of the informative systems, which is used in the conditions of necessity of account of plenty of high-quality indexes, their substantial interdependence, and also difference for importance of their implementation, is carried out.

Keywords: *informative system, estimation of protected, method, fuzzy logic, control, safety, indexes of the system.*