УДК 681.3.06

А.В. ЛЄНШИН

ЗАТ „Інститут інформаційних технологій", Україна

МЕТОДИ ОЦІНКИ ЗРІЛОСТІ ПРОЦЕСІВ ЗАХИСТУ ІНФОРМАЦІЇ В УМОВАХ НЕВИЗНАЧЕНОСТІ

Пропонуються методи оцінки зрілості процесів захисту інформації на основі використання математичного апарату суб'єктивної логіки та експертних оцінок.

безпека інформації, зрілість процесів, прийняття рішень, суб'єктивна логіка, вербальні оцінки

Вступ

Особливістю управління процесами захисту інформації є необхідність прийняття рішень в умовах невизначеності, яка в загальному випадку зумовлена множиною об'єктивних і суб'єктивних чинників. Важливою задачею у рамках процесного підходу до управління є оцінка зрілості процесів захисту інформації (ПЗІ). Але на цей час поки ще відсутній науково-методичний апарат оцінки зрілості, особливо ПЗІ. Це ускладнює підготовку та прийняття рішення з управління захистом інформації. З огляду на це, у статті розглядаються проблемні питання щодо оцінки зрілості ПЗІ в умовах невизначеності та описується сутність методів, що дозволяють проводити оцінку зрілості ПЗІ.

Загальна постановка задачі оцінки зрілості процесів захисту інформації

У відповідності до системодіяльнісного підходу захист інформації розглядається як систематична, стабільна, організована та цілеспрямована діяльність суб'єктів захисту (особи, організації, держави) відносно досягнення цілей та рішення задач захисту інформації.

Спираючись на загальні принципи забезпечення безпеки інформації, а також сучасні міжнародні [1,2] та національні стандарти, заходи у сфері захисту інформації можна розділити на управлінські, організаційні та програмно-технічні. При цьому близько 70% заходів є саме управлінськими та організаційними, тобто такими, що виконуються людиною. Саме для реалізації цих заходів найбільш ефективним є процесний підхід.

Сутність задачі оцінки зрілості процесів захисту інформації полягає в тому, що у конкретний момент часу з використанням конкретного науково-методичного апарату, що підтримується спеціальними додатками, визначити наявність та рівні прояви тих чи інших властивостей (ознак, рис, характеристик), що характеризують зрілість процесу, який є об'єктом оцінки.

Мета дослідження: розробка науково-методичного апарату оцінки зрілості ПЗІ, що забезпечує об'єктивність, порівнянність та повторюваність результатів оцінки та забезпечує формування рекомендацій щодо поліпшення (вдосконалення) ПЗІ та захисту інформації в цілому.

Науково-методичний апарат представляє собою сукупність методів, методик, способів та прийомів організації проведення оцінки зрілості ПЗІ.

Об'єкт дослідження – оцінка зрілості як процес оцінювання властивостей зрілості ПЗІ, що здійснюється в умовах невизначеності.

Предмет дослідження – методи оцінки властивостей зрілості на основі математичного апарату суб'єктивної логіки, положень теорії прийняття рішень та теорії нечітких множин.

Формування цільового профілю зрілості ПЗІ експертними методами

Одним з елементів управління захистом інформації є вибір цільових орієнтирів. При використанні процесного підходу в якості цільових орієнтирів пропонується використовувати „цільовий профіль зрілості" (ЦПЗ) [3]. Побудову ЦПЗ необхідно здійснювати на основі аналізу значущості різних напрямків практичної діяльності із захисту інформації за допомогою залучення експертної групи та урахуванням рівнів критичності інформації, що циркулює в інформаційно-телекомунікаційній системі (ІТС). Визначимо етапи розрахунку ЦПЗ.

1. На основі аналізу захищеності об'єктів, що підлягають захисту, існуючих загроз та вразливостей ІТС, рівня критичності інформації, яка циркулює в ІТС, визначається найвищий рівень вимог, що висуваються до конфіденційності, цілісності та доступності інформації, а отже і до ІТС в цілому.

Класифікацію інформації пропонується здійснювати за методикою, яка розроблена у відповідності до вимог НД ТЗІ 1.4-001-2000, на основі стандарту США FIPS 199 та німецького стандарту BSI.

Якщо сукупність інформаційних ресурсів (ІР) організації представити як множину $I=\{i_1,\ldots,i_n\}$, де n – кількість ІР організації, а множину вимог до конфіденційності, цілісності, доступності, позначити як $K=\{k_1,\ldots,k_n\}$, $Ц=\{u_1,\ldots,u_n\}$, $Д=\{\partial_1,\ldots,\partial_n\}$, то правило визначення (за принципом максимуму) загальних вимог безпеки до інформації здійснюється за такою формулою

$$ВБ_{\max}=\max_{j=\overline{1,n}} вб_j\ , \qquad (1)$$

де $ВБ$ – позначає одну із множин вимог безпеки.

2. Із врахуванням задач забезпечення захисту інформації проводиться декомпозиція загальної задачі захисту. Результатом декомпозиції є ієрархічний граф діяльності по забезпеченню безпеки інформації.

3. Експертна група здійснює оцінювання відносної значущості складових побудованої ієрархії та вагомості напрямків практичної діяльності для задоволення вимог безпеки. Проводиться обчислення коефіцієнтів відносної значущості напрямків практичної діяльності із захисту інформації.

Для визначення відносної значущості, запропоновано використовувати метод попарних порівнянь [4], з обов'язковою перевіркою узгодженості наданих експертних оцінок.

4. На основі одержаних на попередньому кроці коефіцієнтів відносної значущості за наступною формулою розраховується цільова зрілість ПЗІ:

$$цп_i=\max_{j=1,g}\left(L_j\cdot\left(v(КЦД)_{ji}/W_j\right)\right),\ \forall i=\overline{1,n}\ , \qquad (2)$$

де $W_j=\max_{a=1,n}(v(КЦД)_{ja})\forall\ a=\overline{1,n}$, L_j – максимальний підрівень зрілості у відповідності до $K_{\max}$, $Ц_{\max}$, $Д_{\max}$; g – кількість вимог безпеки, операція, а $V(КЦД)$ – матриця коефіцієнтів вагомості впливу напрямків практичної діяльності, елементи якої розраховуються за формулою

$$v_i(вб)=\gamma_j^{21}(вб)\cdot\gamma_i^{32},\ i=\overline{1,n},\ j=f(i),\ j\in\overline{1,t}\ , \qquad (3)$$

де n – кількість напрямків практичної діяльності; t – кількість сфер практичної діяльності, $f(i)$ – функція, що повертає порядковий номер сфери до якої відноситься i -й напрямок практичної діяльності.

Вимоги до математичного апарату оцінки зрілості ПЗІ. Застосування суб'єктивної логіки

З метою внесення ясності визначимо, що під математичним апаратом оцінки зрілості ПЗІ ми розуміємо сукупність математичних моделей, співвідношень, тверджень, припущень тощо, що складають основу методів оцінки зрілості ПЗІ.

Таким чином, математичний апарат повинен надавати змогу вирішувати задачі, які виникають при оцінці зрілості ПЗІ, а також дозволити коректно обробляти невизначеність, яка присутня в оцінках експертів. На роль такого математичного апарату може претендувати методи нечітких множин, апарат

суб'єктивної логіки, логіко-імовірнісний підхід тощо. Визначимо основні вимоги до математичного апарату:

– забезпечення можливості надання оцінок зрілості ПЗІ у зручній для експерта формі;

– врахування невизначеності, що присутня у експерта при оцінці зрілості ПЗІ;

– наявність математичних операторів, що дозволять коректно поєднувати як оцінки одного експерта по різним питанням, так і оцінки експертної групи по окремим питанням;

– забезпечення можливості ранжирування вихідних та узагальнених оцінок експертів;

– можливість його використання для побудови програмного засобу оцінки зрілості ПЗІ;

– можливість наочного представлення результатів оцінки.

Проведений аналіз дозволив визначити, що найкращим чином цим вимогам задовольняє апарат суб'єктивної логіки (СЛ). Центральним положенням СЛ є оперування трьома параметрами, що позначають ступінь довіри (b), недовіри (d) та невизначеності (u) у думці, що висловлюється стосовно істинності довільного твердження, та пов'язані таким співвідношенням:

$$b + d + u = 1 \quad . \qquad (4)$$

Таким чином, думка експерта A відносно істинності довільного твердження X може бути представлена у вигляді вектора $\omega_X^A = \{b, d, u\}$, або в графічному вигляді у просторі думок СЛ (рис. 1).

У СЛ також визначено набір операторів, які дозволяють обробляти оцінки експертів, основними з яких є: кон'юнкція, диз'юнкція, консенсус, заперечення та рекомендація.

Оскільки застосування СЛ для оцінки зрілості ПЗІ є новим, у табл.. 1 наведено результати порівняння змістовного значення параметрів.

Сформулюємо загальну постановку задачі, яку повинна вирішувати СЛ при проведені аудиту БІ.

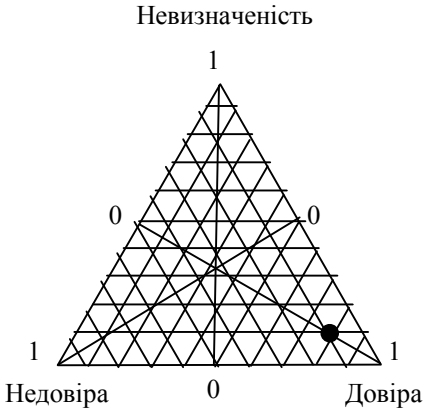

Рис. 1. Простір думок СЛ

Таблиця 1

Порівняння змістовного значення параметрів

Параметр	Область застосування	
	Стандартне застосування	Оцінка зрілості ПЗІ
Об'єкт оцінки	Довільне твердження	Твердження про наявність визначеної властивості зрілості у ПЗІ
Довіра	Ступінь, з якою оцінювач погоджується з твердженням, тобто вірить в його істинність	Ступінь задоволення ПЗІ критеріям зрілості на думку експерта
Недовіра	Ступінь, з якою оцінювач не згоден з твердженням	Ступінь з якою на думку експерта даний ПЗІ не задовольняє критеріям зрілості
Невизначеність	Невизначеність експерта щодо істинності твердження	Невизначеність експерта щодо зрілості процесу
Що перевіряється	Істинність твердження в умовах невизначеності	Ступінь задоволення ПЗІ критеріям зрілості в умовах невизначеності

Нехай $O = \{O_1, O_2, O_3, \ldots, O_m\}$ – це множина вербальних відповідей, які може надавати експерт, де m – мінімальна кількість відповідей, якої достатньо для оцінки будь-якого стану об'єкту оцінки.

$W = \{\omega_1, \omega_2, \omega_3, \ldots \omega_m\}$ – відображення цих оцінок у просторі СЛ у вигляді суб'єктивних думок. Необхідно сформувати таку функцію G, що забезпечить однозначне перетворення $G(O_i) = \omega_i$, де

$O_i \in O$, $\omega_i \in W$; $i = \overline{1,m}$ та зворотну функцію G^{-1}, за допомогою якою можна буде провести однозначне зворотне перетворення $G^{-1}(\omega_i) = O_i$, де $O_i \in O$, $\omega_i \in W$; $i = \overline{1,m}$.

Таким чином, загальна постановка задачі оцінки має такий вигляд (рис. 2).

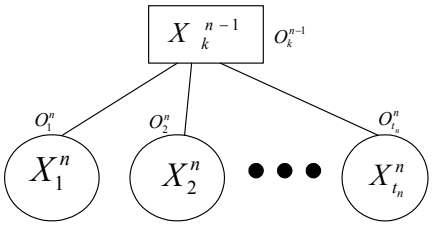

Рис. 2. Графічне представлення постановки задачі оцінки

Тобто в ході оцінки, необхідно отримати експертні оцінки ступеня задоволення критеріям зрілості кожного процесу X_j^n (де n – номер рівня у дереві цілей, j –порядковий номер ПЗІ) у просторі формалізованих вербальних оцінок $O_j^n \in O$, (де n – номер рівня у дереві цілей, j – порядковий номер ПЗІ). Наступним кроком перевести оцінки у простір СЛ за допомогою функції G, та обробити їх за допомогою спеціальних операторів. Отриману оцінку X_k^{n-1} для вищого рівня перевести в область вербальних оцінок O.

Метод визначення думок у просторі суб'єктивної логіки

Однією із першочергових задач, яку необхідно вирішувати при застосуванні СЛ, є визначення думок, що будуть використовуватися у якості вхідних даних подальших розрахунків. Стандартний алгоритм визначення думок зводиться до ітераційного призначення коефіцієнтів з діапазону $[0;1]$ на користь аргументів за, проти, а також аргументів, що зумовлюють невизначеність, з їх подальшим нормуванням. Значним недоліком цього алгоритму є практична складність висловлення думок (та зменшення їх якості) при зростанні кількості об'єктів оцінки, а також непритаманний для людини спосіб висловлювати думки у відсотках. Для усунення цього недоліку авторами було розроблено метод визначення думок у просторі СЛ, що базується на понятті зони базової думки [5].

Визначення. Нехай R – множина усіх можливих думок експерта, а N – кількість підмножин (зон), на які розбито цю множину. Тоді $R = \{r_1, r_2, ..., r_N\}$, де r_i – зона базової думки, тобто сукупність точок у просторі трикутника думок, що характеризується однаковим співвідношенням головного (домінуючого) та другорядних параметрів, що дозволяє надати їй вербальний опис.

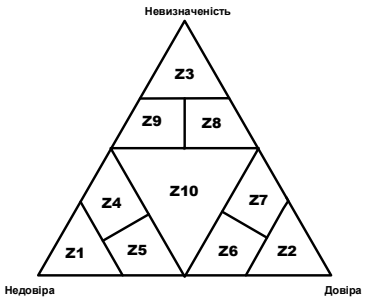

Рис. 3. Зони базових думок

У роботах [5] детально описано цей метод та надано математичний опис границь зон базових думок. Для визначення належності розрахованої думки до певної зони використовуються розроблено суб'єктивні функції належності [6].

Метод формування вербальних порад щодо поточного рівня зрілості ПЗІ

Для формування вербальних відповідей-оцінок ПЗІ у даному методі пропонується поєднати зміст твердження про відповідність ПЗІ критеріям зрілості та оцінку цього процесу у просторі СЛ переведену в типову відповідь на основі зон базових думок [7].

Приклад.

Твердження: З метою вірного формулювання вимог безпеки проводиться первина оцінка ризиків.

Отримана оцінка: $\omega = \{0{,}6; 0{,}3; 0{,}1\}$.

Розрахований номер базової зони (використовуючи функцію належності $\mu(p)$): 6 [6].

Типова відповідь для базової зони: Вважаю, що виконується, але присутні аргументи і проти.

Відповідь-оцінка: Вважаю, що в цілому з метою формулювання вимог безпеки проводиться первина оцінка ризиків, але ця оцінка не завжди є вичерпно задовільною.

На практиці при вирішенні задачі формування відповідей-оцінок для кожного із тверджень виникають труднощі пов'язані із обробкою великого обсягу інформації. Автоматизація даної задачі може бути проведена за умови можливості представлення будь-якого вхідного твердження у формалізованому вигляді та наявності процедури (правил) формування типових відповідей на основі обробки вхідних даних. У роботі [7] пропонується представити вхідні твердження та відповіді у вигляді лінгвістичних змінних, що мають визначену структуру.

Дослідження принципів побудови тверджень дозволило виділити такі складові: обставини дії, джерело дії, об'єкт дії, спосіб дії, умова дії, мета дії.

Для формулювання вербальних відповідей-оцінок було визначено правила їх побудови. Оскільки відповіді оцінки будуються на основі типових відповідей для зон базових думок у просторі СЛ, то структура речення буде подібна до їх структури. Симетричність трикутника думок відносно центра дозволило розбити зони базових думок, а отже і типові відповіді, що відповідають їм, на три множини за принципом домінуючого параметру. Для кожної множині є три випадки співвідношення параметрів: випадок, коли базовий параметр домінує цілком ,та два випадки домінації базового параметра та переваги одного другорядного параметру над іншим. Для роз'яснення сутності методу стисло розглянемо правила побудови вербальних відповідей-оцінок для першої множини.

Оскільки для першої множини домінуючим параметром є довіра до відповідності критерію зрілості, базою для побудови конструкції відповідей-оцінок є „позитивне речення", для позначення якої використовується лінгвістична змінна $\{Pos\}$. Під терміном „позитивне речення" розуміється твердження про відповідність ПЗІ критерію зрілості. У випадку, коли беззаперечним домінантом є ступінь відповідності, у якості відповіді-оцінки використовується позитивне речення. У випадку, коли домінантом є ступінь відповідності, а ступінь невідповідності критерію переважає над ступенем невизначеності: на початок позитивного речення ставиться вираз, що свідчить про відповідність ПЗІ в цілому, а на кінець додається вираз, в якому вказується на недоліки у загальному вигляді У випадку, коли домінантом є ступінь відповідності критерію зрілості, а ступінь невизначеності переважає над ступенем невідповідності: на початок позитивного речення ставиться вираз, що свідчить про відповідність ПЗІ в цілому, а на кінець додається вираз, в якому вказується, що кількість інформації не дозволяє беззаперечно стверджувати про відповідність ПЗІ критерію.

Сутність підходу до формування порад по підвищенню зрілості ПЗІ

Найважливішим етапом проведення оцінки зрілості ПЗІ є прийняття рішень на основі зібраних даних, сутність якого полягає в тому, що особа, яка приймає рішення (начальник підрозділу захисту інформації), повинна:

– сформувати оцінку поточної зрілості ПЗІ;

– визначити ступінь відповідності цільових орієнтирів та отриманих результатів оцінки зрілості ПЗІ;

– визначити перелік та черговість заходів безпеки, зрілість яких необхідно підвищити негайно, та заходів безпеки, зрілість яких потребує покращення, але вони не є критичними для організації;

– визначити типові недоліки, які присутні системі управління зрілістю ПЗІ та сформувати поради щодо їх усунення.

З метою формалізації представлення найважли-

віших чинників, що мають бути враховані при прийнятті рішень щодо управління зрілістю ПЗІ, було введено поняття „маркер зрілості процесу" (МЗП). МЗП – структура даних, використання якої дозволяє оцінити поточну зрілість ПЗІ, стан, а також здійснювати порівняння черговості та значущості підвищення зрілості ПЗІ. МЗП складається з полів, що містять: опис ПЗІ, вектор оцінки зрілості на досягнутому рівні зрілості, кількість експертів на основі думок яких розрахована оцінка, досягнутий рівень зрілості, вартість підвищення зрілості ПЗІ та величина збитку, якому можна запобігти, ступінь задоволення вимог цільового профілю зрілості, кількість підпроцесів, необхідність застосування в конкретній організації, рівень в ієрархії процесів та відносна значущість ПЗІ на цьому рівні.

На основі аналізу алгоритму прийняття рішень було визначено правила, які дозволяють приймати рішення щодо черговості та необхідності прийняття заходів по підвищенню зрілості ПЗІ, формалізувати процес прийняття рішень начальником підрозділу захисту інформації.

Висновки

В статті зроблено постановку задачі оцінки зрілості процесів захисту інформації в умовах невизначеності. У відповідності до поставленої мети дослідження визначено об'єкт та визначено вимоги до математичного апарату, надано огляд розроблених у ході досліджень методів та підходів до оцінки зрілості ПЗІ на основі використання математичного апарату суб'єктивної логіки та експертних оцінок, а саме:

– метод визначення ЦПЗ для ПЗІ;

– метод визначення думок у просторі СЛ;

– метод формування вербальних порад щодо поточного рівня зрілості ПЗІ;

– підхід до формування порад по підвищенню зрілості ПЗІ на основі використання МЗП.

Література

1. ISO/IEC 17779:2000 Code of practice for information security management.

2. NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

3. Потій О.В., Лєншин А.В. Методика визначення цільового профілю зрілості процесів захисту інформації з використанням методу вирішуючих матриць // Науково-технічний збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – К., 2005. – Вип. 11. – С. 83-95.

4. Саати Т. Принятие решений. Метод анализа иерархий. – М: Радио и связь, 1999. – 341с.

5. Потій О.В., Лєншин А.В. Методика визначення думок експертів відносно зрілості безпеки інформації із застосуванням математичного апарату суб'єктивної логіки // Науково-технічний збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – К., 2004. – Вип. 9. – С. 38-47.

6. Лєншин А.В. Побудова функцій належності експертних оцінок до зон базових думок у просторі суб'єктивної логіки // Науково-технічний збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – К., 2005. – Вип. 11. – С. 95-103.

7. Потій О.В., Лєншин А.В. Методика формування вербальних оцінок щодо захищеності ІТС на основі вимог нормативних документів // Науково-технічний збірник „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – К., 2005. – Вип. 10. – С. 8-18.

Надійшла до редакції 14.02.2006

Рецензент: канд. техн. наук, проф. О.А. Замула, Харківський національний університет радіоелектроніки, Харків.