УДК 681.3.06

О.А. Смірнов[1], О.П. До́ренський[2]

[1]*Кіровоградський національний технічний університет*
[2]*Кіровоградський юридичний інститут*
Харківського національного університету внутрішніх справ

ОЦІНЮВАННЯ ЗАГАЛЬНОГО ПОКАЗНИКА ЯКОСТІ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ

В статті запропоновано етапізування процесу організації надійної безпеки інформації автоматизованої системи (АС) та розглядається його основний етап, у рамках якого пропонується метод визначення показника якості системи забезпечення безпеки інформації автоматизованої системи. Визначено загальний алгоритм розв'язку задачі моделювання та загальну класифікацію системи забезпечення безпеки інформації (СЗБІ) автоматизованої системи.

безпека інформації, автоматизована система, показник якості, критерій якості

Вступ

Постановка проблеми. Основною задачею забезпечення безпеки інформації автоматизованої системи є належне оцінювання інформаційних загроз та врахування отриманих результатів під час проектування, реалізації та експлуатації СЗБІ АС. При цьому Під автоматизованою системою будемо розуміти систему, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення [1].

Аналіз. На основі проведеного дослідження сучасної літератури [2 – 8] можна виділити основні напрямки вирішення комплексу задач, пов'язаних зі здійсненням оцінки та оптимального вибору варіантів побудови СЗБІ АС.

Формулювання цілей. Метою проведення досліджень є вирішення проблеми отримання оптимальних методів оцінки та вибору альтернатив організації безпеки інформаційної підсистеми (ІПс) АС на етапі обґрунтування показників якості СЗБІ АС.

Основна частина

СЗБІ АС повинна мати комплекс організаційно-технічних заходів для запобігання заподіянню шкоди АС, спотворення інформації, її зміни та знищення, зокрема протидії спотворення самого процесу обробки інформації. Крім того, СЗБІ АС повинна забезпечувати організацію доступу до інформації, яка зберігається, обробляється і передається в АС. Це має здійснюватись виключно згідно з правилами розмежування доступу [1].

Захисту підлягає будь-яка інформація в АС, необхідність захисту якої визначається її власником або чинним законодавством України [9], а СЗБІ АС повинна організувати надійну безпеку інформації для відповідного функціонування АС, нормального протікання її внутрішніх процесів, залежних від інформації.

Вирішення проблеми моделювання СЗБІ АС потребує розробки принципів, методів та засобів скорочення розмірності опису СЗБІ АС, розробку методології, методів та засобів рішення задач забезпечення безпеки інформаційних технологій (ІТ) в умовах невизначеності, в результаті дослідження яких має бути розробка методологічних основ, методів та засобів вирішення некоректно поставлених задач в умовах невизначеності [6].

Розв'язання задачі розробки технології, методів та засобів адаптивного контроля параметрів й діагностування можливих станів системи можливе за умови розв'язку комплексу підзадач, наведених у [10]. Результатом розробки має бути створення ідеології, математичних методів та відповідних засобів для організації адаптивного контроля та діагностування станів самої системи ЗБІ АС [6].

Розв'язання проблеми розробки ґрунтовних принципів, методів та засобів самоорганізації СЗБІ АС можна етапізувати на чотири підзадачі [6, 10]. Рішенням досліджень повинні бути створені на основі відомих та спеціально розроблених методів та засобів, адаптивні моделі для опису структури та поведінки СЗБІ АС, а також контроля, діагностування та прогнозування її станів.

Розв'язування задачі розробки методів та засобів підтримки приймання рішень можна також етапізувати на три підзадачі [6, 10].

Дослідження базуються на використанні всіх отриманих раніше результатів та орієнтовані на створення банка знань про СЗБІ АС.

Для вирішення перерахованих та інших теоретичних і прикладних проблем необхідна цілеспрямована організація комплексних досліджень проблем забезпечення безпеки ІТ, в результаті чого можна отримати модель СЗБІ АС [10].

Основне призначення загальних моделей полягає у створенні передумов для об'єктивної оцінки загального стану ІПс АС з точки зору вразливості або рівня захищеності інформації в ній. Необхідність в таких оцінках виникає під час дослідження існуючої ІПс АС з метою прийняття стратегічних рішень організації надійної системи забезпечення безпеки.

В роботі [5] здійснено спробу системної класифікації загальних моделей систем і процесів забезпечення безпеки, які дозволяють здійснити оцінку загальних характеристик системи і процесів (рис. 1).

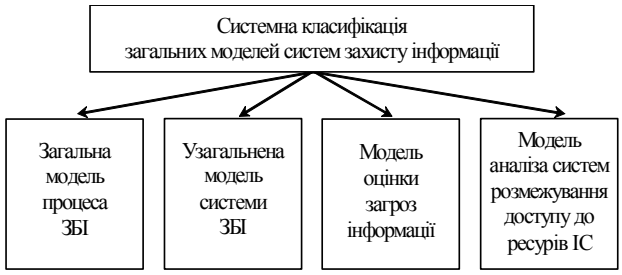

Рис. 1. Системна класифікація загальних моделей систем та процесів ЗБІ

Розв'язок задачі аналіза та синтеза СЗБІ АС ускладнюється рядом особливостей, основними з яких є:

– складний опосередкований взаємозв'язок показників якості СЗБІ АС з показниками якості ІПс АС;

– необхідність обліку великої кількості показників (вимог) СЗБІ АС під час оцінки та вибору їх раціонального варіанта;

– переважно якісний характер показників (вимог), які враховуються під час аналіза та синтеза СЗБІ АС;

– вагомий взаємозв'язок показників (вимог), які мають суперечливий характер;

– складність отримання вхідних даних, необхідних для розв'язку задач аналіза та синтеза СЗБІ АС, особливо на початкових етапах проектування [10].

У загальному вигляді модель процеса забезпечення безпеки інформації (ЗБІ) в АС можна зобразити у вигляді, показаному на рис. 2.

Нехай сукупність загроз, які можуть загрожувати ІПс АС та надходять від джерела загроз, є скінченими та підлягають підрахунку $i = \overline{1, n}$. Кожна і-та загроза характеризується ймовірністю появи $P_{i\,загр}$ та

збитком $\Delta q_i^{загр}$, який наноситься ІПс АС. СЗБІ АС виконує функції повної або часткової компенсації загроз для ІПс АС. Основною характеристикою СЗБІ АС є ймовірність усунення кожної і-ї загрози $P_{i\ загр}^{усун}$.

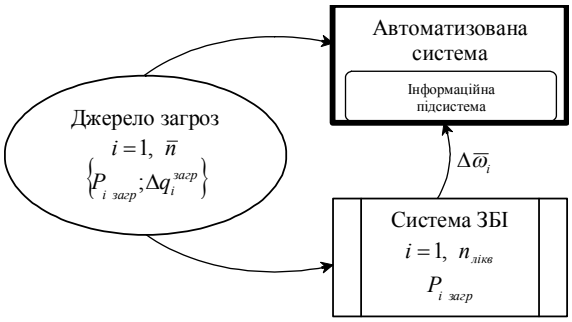

Рис. 2. Загальна модель процеса ЗБІ автоматизованої системи

За рахунок функціонування СЗБІ АС забезпечується зменшення збитку W, який наноситься ІПс АС під дією загроз. Припустимо, що збиток W можна зменшити за допомогою загального уникнутого збитку $\overline{W}$ або уникнутого збитку $\overline{\omega}_i$ за рахунок ліквідації дії і -ї загрози. Необхідно вибрати варіант реалізації СЗБІ АС, яка забезпечує максимум запобігання збитку від дії загроз за допустимих затрат на СЗБІ АС, тобто необхідно вирішити задачу

$$T^0 = \arg\ \max \overline{W}(T); \quad T^0 \in T^+, \tag{1}$$

при обмеженні

$$C\left(T^0\right) \le C_{доп}, \tag{2}$$

де T – деякий вектор, який характеризує варіант технічної реалізації СЗБІ АС; T^+ – допустиме значення вектора T; T^0 – оптимальне значення вектора T; $C_{доп}$ – допустимі затрати на СЗБІ АС.

Для вирішення задачі необхідно сформувати показник якості функціонування СЗБІ АС $\overline{W}(T)$. Очевидно, уникнутий збиток у загальному вигляді виражається співвідношенням:

$$\overline{W} = F\left(P_{i\ загр}; \Delta q_i^{загр}; P_{i\,загр}^{усун}; i = 1,\overline{n}\right). \tag{3}$$

Уникнутий збиток за рахунок ліквідації дії і -ої загрози

$$\overline{\omega}_i = P_{i\ загр} \cdot \Delta q_i^{загр} \cdot P_{i\,загр}^{усун}; i = 1,\overline{n}. \tag{4}$$

За умови незалежності загроз і адитивності їх наслідків отримуємо

$$\overline{W} = \sum_{i=1}^{n} P_{i\ загр} \cdot \Delta q_i^{загр} \cdot P_{i\,загр}^{усун}. \tag{5}$$

Ймовірність появи і-ї загрози $P_{i\ загр}$ визначається статистично і відповідає відносній частоті її появи

$$P_{i\ загр} = \frac{\lambda_i}{\sum_{i=1}^{n}\lambda_i} = \overline{\lambda}_i, \tag{6}$$

де λ_i – частота появи і-ї загрози.

Збиток, який наноситься і-ю загрозою Δq_i, може визначатись в абсолютних одиницях:

– відмова підтримуваної інфраструктури;
– економічна втрата;
– об'єм знищеної, зіпсованої, зміненої (недостовірної) інформації;
– часові затрати і т.д.

Проте попередня оцінка збитків на етапі проектування СЗБІ АС досить складна. У зв'язку з цим необхідно використовувати поняття відносного збитку, який представляє собою ступінь межі небезпеки і-ї загрози для ІПс АС. Ступінь небезпеки може бути визначено експертним шляхом з припущенням, що всі загрози для ІПс АС складають повну групу подій [9], тобто

$$0 \le \Delta q_i \le 1;\ \sum_{i=1}^{n} \Delta q_i = 1.$$

Найбільш складною задачею є визначення ймовірності усунення і-ї загрози $P_{i\ загр}^{усун}$ під час проектування СЗБІ АС. Припустимо, ймовірність $P_{i\ загр}^{усун}$ визначається тим, на скільки повно враховано якісні та кількісні вимоги до СЗБІ АС під час їх проектування, тобто

$$P_{i\ загр}^{усун} = f_i\left(x_{i1},...,x_{ij},...,x_{im}\right), \tag{7}$$

де x_{ij} – ступінь виконання j-ї вимоги до СЗБІ АС для усунення і-ї загрози, $i = \overline{1,n}$; $j = \overline{1,m}$.

Нехай перші k вимог будуть кількісними $\left(j = \overline{1,k}\right)$, решта $m-k$ – якісними $\left(j = \overline{k+1,m}\right)$.

Ступінь виконання j-ї кількісної вимоги визначається його близькістю до оптимального (заданого) значення.

Для оцінки ступеня виконання j-ї кількісної вимоги до СЗБІ АС найзручніше використовувати його нормоване значення

$$\overline{x}_{ij} = \left(j = 1,k\right),\ 0 \le x_{ij} \le 1.$$

Як показано в [5], для нормування зручно використовувати функцію вигляду

$$\overline{x}_{ij} = \frac{x_{ij} - x_{ij}^{нг}}{x_{ij}^{нк} - x_{ij}^{нг}}, \tag{8}$$

де x_{ij} – поточне значення j-ї вимоги; $x_{ij}^{нг}$ – найгірше значення; $x_{ij}^{нк}$ – найкраще значення.

З врахуванням формули (8) отримуємо наступні розрахункові співвідношення:

при

$$x_{ij}^{нк} = x_{ij}\,;\quad x_{ij}^{нг} = x_{ij\ \min}\,; \tag{9}$$

$$\overline{x}_{ij} = \frac{x_{ij} - x_{ij\ \min}}{x_{ij\ \max} - x_{ij\ \min}}, \tag{10}$$

при

$$x_{ij}^{нк} = x_{ij\ \min}\,;\quad x_{ij}^{нг} = x_{ij\ \max}\,; \tag{11}$$

$$\overline{x}_{ij} = \frac{x_{ij\ \max} - x_{ij}}{x_{ij\ \max} - x_{ij\ \min}}\,; \tag{12}$$

$$\overline{x}_{ij} = \begin{cases} 0, \text{ при } x_{ij} > x_{ij\ \min};\quad x_{ij} < x_{ij\ \max}; \\ 1, \text{ при } x_{ij} = x_{opt}; \\ \dfrac{x_{ij} - x_{ij\ \min}}{x_{ij\ opt} - x_{ij\ \min}}, \text{ при } x_{ij\ \min} \le x_{ij} \le_{ij\ opt}; \\ \dfrac{x_{ij\ \max} - x_{ij}}{x_{ij\ \max} - x_{ij\ opt}}, \text{ при } x_{ij\ opt} \le x_{ij} \le_{ij\ \max}. \end{cases} \tag{13}$$

Ступінь виконання j-ї якісної вимоги визначається функцією приналежності до найкращого значення $\mu(x_{ij})$.

Розклавши функцію (7) в ряд Маклорена та обмежившись тільки першими членами ряда, одержимо

$$P_{i\ загр}^{усун} = P_{i\ загр}^{усун}(0) + \sum_{\gamma=1}^{m} \frac{\partial P_{i\ загр}^{усун}}{\partial x_{ij}} \cdot x_{ij}, \tag{14}$$

де $P_{i\ загр}^{усун}(0) = 0$ – ймовірність усунення і-ї загрози при невиконанні вимог до СЗБІ АС; $\dfrac{\partial P_{i\ загр}^{усун}}{\partial x_{ij}} = \alpha_{ij}$ – величина, яка характеризує ступінь впливу вимог на ймовірність усунення і-ї загрози (важливість виконання j-ї вимоги для усунення і-ї загрози).

Очевидно, що $0 \le \alpha_{ij} \le 1$; $\sum_{j=1}^{m} \alpha_{ij} = 1$ для $i = \overline{1,n}$.

Після підстановки у (13) відповідних значень отримуємо

$$P_{i\ загр}^{усун} = \sum_{j=1}^{k} \alpha_{ij} \cdot x_{ij} + \sum_{j=k+1}^{m} \alpha_{ij} \cdot \mu(x_{ij}). \tag{15}$$

Кінцева формула (5) для оцінки величини збитка $\overline{W}$, якого запобігли, приймає вигляд

$$\overline{W} = \sum_{j=1}^{n}\sum_{j=1}^{k} \overline{\lambda_i} \cdot \Delta q_i \cdot \alpha_{ij} \cdot \overline{x}_{ij} + \sum_{i=1}^{n}\sum_{j=k+1}^{m} \overline{\lambda_i} \cdot \Delta q_i \cdot \alpha_{ij} \cdot \mu(x_{ij}). \tag{16}$$

Таким чином, задача синтеза СЗБІ АС у вигляді (1), (2) зводиться до оптимального обґрунтування кількісних та якісних вимог до СЗБІ АС при допустимих затратах і приймає вигляд:

знайти

$$\max \overline{W}(x_{ij}; i = \overline{1,n}; j = \overline{1,m}), \tag{17}$$

при обмеженні

$$C(x_{ij}) \le C_{доп}\,;\quad i = \overline{1,n};\ j = \overline{1,m}\,.$$

У відповідності з формулювання задачі (16) можна визначити етапізований алгоритм її вирішення:

– збір та обробка експертної інформації про характеристики загроз: часта поява і-ї загрози $\overline{\lambda_i}$ та збитку $\Delta q_i\left(i = \overline{1,n}\right)$;

– збір та обробка експертної інформації для визначення важливості виконання j-ї вимоги для усунення і-ї загрози α_{ij} і функції приналежності $\mu(x_{ij})$, $(i = \overline{1,n};\ j = \overline{1,m})$;

– оцінювання вартості СЗБІ АС для конкретної альтернативи її реалізації, яка залежить від ступеня виконання вимог $C(x_{ij}; i = \overline{1,n}; j = \overline{1,m})$;

– розробка математичної моделі та алгоритма вибору раціональних вимог до СЗБІ АС у відповідності з (17) як задачі нечіткого математичного програмування.

Виходячи з усього розглянутого вище, за умови відсутності інформації про загрози для вирішення задачі (17) може бути застосовано показник вигляду

$$\overline{W} = \sum_{j=1}^{n}\sum_{j=1}^{k} \alpha_{ij} \cdot \overline{x}_{ij} + \sum_{i=1}^{n}\sum_{j=k+1}^{m} \alpha_{ij} \cdot \mu(x_{ij}). \tag{18}$$

Висновки

Наведені у статті особливості дослідження та синтеза СЗБІ АС роблять практично неможливе застосування традиційних математичних методів, у тому числі й методів оптимізації для вирішення задач аналіза та синтеза СЗБІ АС. Складність процеса прийняття рішень, відсутність математичного апарата призводить до того, що під час оцінки та вибору альтернатив можливо використовувати та обробляти якісну експертну інформацію.

Перспективним напрямом розробки методів прийняття рішень при експертній вихідній інформації визначено лінгвістичний підхід на базі теорії нечітких множин та лінгвістичній змінній. Теорія нечітких множин показала, що застосування формального апарата за своїми потенційними можливостями і точністю має бути адекватним смисловому змісту та точності вхідних даних.

У результаті досліджень основних методів, способів та засобів побудови надійної та ефективної СЗБІ АС визначено загальний алгоритм розв'язку задачі моделювання СЗБІ АС, загальну класифікацію моделей СЗБІ АС, запропоновано метод визначення показника якості безпеки ІПс АС за умови наявності

інформації про загрози, тобто величини загального уникнутого збитку $\overline{W}$, що дало можливість звести до оптимального обґрунтування кількісних та якісних вимог до СЗБІ АС за допустимих затрат. Також запропоновано метод визначення показника якості СЗБІ АС за умови відсутності інформації про загрози.

На основі дослідження, проведеного у даній статті, сформуємо проблему розв'язку задачі визначення важливості (ваги) вимог, які мають бути пред'явлені до параметрів СЗБІ АС. Вирішенню цієї проблеми будуть присвячені подальші дослідження існуючих методів визначення коефіцієнтів важливості СЗБІ АС.

Список літератури

1. Закон України "Про захист інформації в автоматизованих системах" від 05.07.1994 р.

2. Sinder F. Die Grundlagen der Sicherheitder informativen Systeme. – Hamburg: Bücherei GmbH, 2006. – 576 S.

3. Zeleny M. Compromise programming in M.K. – Starr and M. Zelleny, Columbia, 1973. – 404 p.

4. Thurstone L.L. The measurement of valnes. – Chicago, 1959. – 158 p.

5. Rosner B.S. A new scaling technique for absolute judgement // Psychometrica. – 1956. – V. 21, No. 4 – P. 14-19.

6. Wei T.H. The algebraik foundations of ranking theory Theses, Cambridge, 1952. – 504 p.

7. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО "Тид "ДС", 2004. – 992 с.

8. Мао Вембо. Современная криптография: теория и практика: Пер. англ. – М.: Издательский дом "Вильямс", 2005. – 768 с.

9. 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.

10. Смірнов О.А., До́ренський О.П. Метод оцінки показника якості системи забезпечення безпеки інформації // Зб. наук. праць Кіровоградського національного технічного університету "Техніка в сільськогосподарському виробництві. Галузеве машинобудування. Автоматизація". – Кіровоград: КНТУ. – 2007. – Вип. 18. – С. 282-289.

Надійшла до редколегії 16.06.2007

Рецензент: д-р фіз.-мат. наук, проф. Ю.І. Волков, Кіровоградський національний технічний університет, Кіровоград.