Відповідно до наведеного прикладу ця атака (що грунтується на МСІ) класифікується як: деполітизаційна, Т-віддалена, аверсна, АВВМ-маніпульована, К-дієва, монополічна, складна, ЕК-джерельна, ВК-доступу.

Запропонована в роботі ознакова класифікація МСІ розкриває багатогранність цього поняття та широту проявів соціотехнічних атак, а врахування цих чинників при розробці та виборі методів і засобів протидії дозволить підвищити ефективність відповідних впроваджуваних систем безпеки. Результати даної роботи можна також використати для побудови систем оцінки рівня підготовленості персоналу щодо протидії вторгненню, заснованому на певній множині визначених класів соціотехнічних атак.

Список літератури

1. *Корченко О.Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК – Пресс», 2006. – 320с.

2. *Конеев И.Р., Беляев А.В.* Информационная безопасность предприятия. – СПб:БХВ-Петербург, 2003. – 752с.

3. *Чириль Дж.* Защита от хакеров (+CD).-СПб.: Питер, 2002. – 480с.

4. *Мак-Клар Стюард, Спенбреб Джоел, Курц Джордж.* Секреты хакеров. Безопасность сетей – готовые решения. – 4-е изд.: Пер. с англ. – М.: Изд. дом «Вильямс», 2004. – 656с.

5. *Коул Ерик.* Руководство по защите от хакеров: Пер. с англ. – М.: Изд. дом «Вильямс»., 2002. – 640с.

6. *Бабак В. П., Корченко О. Г.* Інформаційна безпека та сучасні мережеві технології. Англ.-укр.-рос. слов. термінів. – К.: НАУ, 2003. – 670 с.

7. *Kevin D. Mitnik, William L. Simon, Steve Wozniak,.* The Art Of Deception: Wiley, 2002. – 304с.

8. *Корченко А. Г.* Несанкционированный доступ к компьютерным системам и методы защиты: Учеб. пособие. – К.: КМУГА, 1998. – 116 с.

9. *Robert B. Cialdini.* The Science of Persuasion // Scientific American Magazine. – 2001, – №2. – P.76-81.

10. *И. Н. Кузнецов* Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе. - М.: ООО Изд. Яуза, 2001. – 100с.

УДК 681.3.06 **Дóренський О.П.**

МЕТОД ВИЗНАЧЕННЯ ПОКАЗНИКА СТІЙКОСТІ ДО ЗАГРОЗ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Постановка проблеми

На сьогоднішній день більшість систем забезпечення безпеки інформації (СЗБІ) не повністю відповідають вимогам щодо організації надійної безпеки інформаційної системи (ІС), що пов'язано з рядом факторів, які не враховуються під час проектування і, відповідно, реалізації СЗБІ.

Аналіз

На основі проведеного дослідження [1, 2, 3] можна виділити основні напрямки вирішення комплексу задач, пов'язаних зі здійсненням оцінки та оптимального вибору варіантів побудови СЗБІ. При цьому аналіз впроваджених систем оцінювання СЗБІ [2, 4] показало, що більшість моделей СЗБІ окремо не виділяються та не розглядаються оцінювання показника стійкості самої СЗБІ до загроз, що є вірогідним. За умови відмови СЗБІ повністю унеможливлює організацію надійної безпеки інформації ІС.

Формулювання цілей

Метою проведення досліджень є вирішення проблеми отримання оптимальних методів оцінки та вибору альтернатив організації безпеки ІС на етапі обґрунтування показників стійкості СЗБІ до загроз, а також отримання ефективного методу визначення показника стійкості СЗБІ до загроз ІС, враховуючи при цьому вірогідні загрози самої СЗБІ. Крім того, дослідження [2, 4, 9] показало, що класифікації можливих вимог за критеріє ймовірності появи певної множини загроз та систематизація вжитих заходів щодо протидії цим загрозам проведено не було.

Основна частина

Вирішення проблеми моделювання СЗБІ, як показано в [2], потребує розробки принципів, методів та засобів скорочення розмірності опису СЗБІ, розробку методології, методів та засобів рішення задач забезпечення безпеки інформаційних технологій (ІТ) в умовах невизначеності, в результаті дослідження яких мають бути розроблені методологічні основи, методи та засоби вирішення некоректно поставлених задач в умовах невизначеності.

Розв'язання задачі розробки технології, методів та засобів адаптивного контроля параметрів й діагностування можливих станів системи можливе за умови розв'язку комплексу підзадач:

– формування динамічних зон, які характеризують різноманітні стани економічної системи та динамічних порогів, які розмежовують дані зони, виділення інтегральних динамічних векторів індикації стану системи;

– розробка ідеології і стратегії виконання адаптивного контроля векторів індикації (за часом виконання, кількістю та номенклатурі параметрів, які контролюються), прогнозування тенденції зміни їх значень в процесі функціонування системи;

– розробка методів та алгоритмів адаптивного одиночного та групового контроля й прогнозування значень окремих компонентів та векторів індикації в цілому;

– розробка методів та алгоритмів діагностування системи на основі аналіза отриманих результатів ідентифікації всіх векторів індикації.

Результатом розробки має бути створення методології, математичних методів та відповідних засобів для організації адаптивного контроля та діагностування станів СЗБІ.

Розв'язання проблеми розробки ґрунтовних принципів, методів та засобів самоорганізації СЗБІ можна етапізувати на наступні підзадачі:

– конструювання адаптивних моделей для опису структури та поведінки системи, прогнозування значення системних параметрів;

– конструювання адаптивних моделей для формування підмножин параметрів, які контролюються, та діапазону значень зон їх контроля на основі заданих вимог до стійкості функціонування системи;

– конструювання адаптивних моделей контроля роботоздатності та діагностування порушень роботоздатності системи;

– самоорганізація та саморозвиток сімейств моделей для опису структури, поведінки, прогнозування, контроля та діагностування з врахуванням забезпечення необхідності стійкості системи в умовах впливу факторів внутрішнього і зовнішнього середовища.

Рішенням досліджень повинні бути створені на основі відомих та спеціально розроблених методів та засобів, адаптивні моделі для опису структури та поведінки СЗБІ, а також контроля, діагностування та прогнозування її станів.

Розв'язування задачі розробки методів та засобів підтримки приймання рішень можна етапізувати на наступні підзадачі:

– розробка методів та засобів вибору рішень зі всієї множини альтернативних варіантів на основі дослідження стану та поведінки системи з врахуванням вимог керування, реального ресурса, які задовольняють цим вимогам, кваліфікованих оцінок близьких та віддалених наслідків виконання прийнятих рішень;

– розробка методів та засобів декомпозиції прийнятих рішень за рівнями керування системи;

– розробка методів та засобів підтримки прийняття рішень з самоорганізації системи в процесі її функціонування для вдосконалення всіх видів моделей та їх сімейств.

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

Для вирішення теоретичних і прикладних проблем необхідна цілеспрямована організація комплексних досліджень проблем забезпечення безпеки ІТ, в результаті чого можна отримати модель СЗБІ, яка виконує задані функції й відповідає визначеним параметрам та характеристикам [3].

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

В роботі [7] здійснено спробу системної класифікації загальних моделей систем і процесів забезпечення безпеки, які дозволяють здійснити оцінку загальних характеристик системи і процесів.

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

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

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

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

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

– складність отримання вхідних даних, необхідних для розв'язку задач аналіза та синтеза СЗБІ, особливо на ранніх етапах проектування.

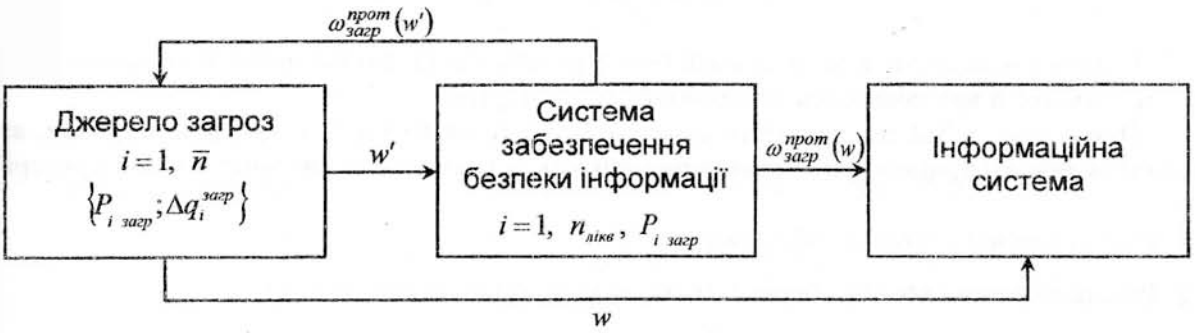

Рис 1. Модель процесу ЗБІ ІС

Проте побудова ефективної СЗБІ та її моделі можлива за умови ефективного апарату оцінювання показника стійкості спроектованої СЗБІ до загроз, на основі чого можна здійснити оцінку обраного варіанту СЗБІ. Нехай сукупність загроз, які можуть загрожувати ІС та СЗБІ надходять від джерела загроз. Проаналізувавши [2, 9] загальний вигляд моделі процесу забезпечення безпеки інформації (ЗБІ) в ІС наведено на рисунку 1, де сукупність загроз, які можуть загрожувати ІС та надходять від джерела загроз, є кінечними та підлягають підрахунку $i=1,\ \overline{n}$, кожна i-та загроза характеризується ймовірністю появи $P_{i\ загр}$ та збитком $\Delta q_i^{загр}$, який наноситься ІС.

Проаналізувавши сучасні методи та способи протидії загрозам [2], а також загрози, які можуть мати місце для ІС та СЗБІ, пропонується класифікувати можливі загрози ІС та СЗБІ на наступні чотири класи:

I. Малоймовірні;

II. Ймовірні;

III. Надймовірні;

IV. Критичні.

Схематично зобра́ження класифікації загроз ІС та СЗБІ наведено на рисунку 2, при чому множини загроз не можуть перетинатись, а загрози розподіляються за відповідними класами експертно та конкретно для заданого випадку.

Кожен клас загроз характеризується відповідною вагою – ймовірністю появи певного класу загроз $P_{i\ загр}$, $i = 1, 4$:

- малоймовірні $P_{1\ загр}$ – 0-10%,
- ймовірні $P_{2\ загр}$ – 10-50%;
- надймовірні $P_{3\ загр}$ – 50-80%;
- критичні $P_{4\ загр}$ – 80-100%.

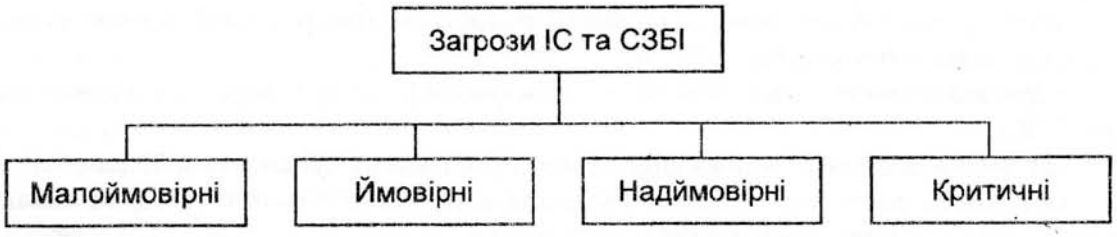

Рис 2. Класифікація загроз ІС та СЗБІ

Кожен з наведених класів складається з m елементів, які визначаються відповідно до даної ІС та СЗБІ й визначаються та оцінюються експертно.

При цьому, СЗБІ має володіти сукупністю методів та заходів протидії загрозам, які з метою можливості точного оцінювання пропонується типувати за наступні чотири критерії:

1. Рівень надійності носія інформації;
2. Рівень безпеки способу зберігання інформації (відповідно до п. 1);
3. Рівень безпеки місця зберігання інформації (відповідно до пп. 1, 2);
4. Можливість злоякісного впливу чи дії зовнішніх факторів та загроз на критерії пп. 1, 3.

Тобто, пропонуються основні критерії оцінювання вжитих заходів протидії загрозам відповідних класів I-IV. Кожен з наведених типів заходів має набір методів та засобів, за допомогою яких здійснюється повна або часткова протидія загрозам, та яка також характеризується відповідною ймовірністю $\omega_{загр}^{прот}$.

Сформулюємо задачу визначення показника стійкості СЗБІ до загроз: нехай функціонування СЗБІ забезпечує виконання повної або часткової компенсації загроз для ІС та самої себе. Основною характеристикою СЗБІ є ймовірність усунення загроз відповідного

класу $P^{усун}_{i\ загр}$, значення якої визначається сукупністю факторів забезпечення протидії загрозам $\omega_{j\ загр}$, $j = 1, 4$, з ймовірністю протидії загрозі системою ЗБІ $\omega^{прот}_{j\ загр}$.

Стійкість системи до загроз можна звести до визначення збитку w, який може завдатись ІС під дією загроз, а також збитку w', який може бути завданий безпосередньо СЗБІ (рисунок 1). Відповідно, загальний збиток W, який може бути завданий ІС та СЗБІ під дією зовнішніх загроз

$$W = w + w'. \tag{1}$$

Оскільки атаці може піддатись як ІС, так і сама СЗБІ, необхідно обов'язково врахувати збиток w', який з досить великою ймовірністю може загрожувати СЗБІ, а, відповідно, суттєво підвищити цим рівень небезпеки ІС. Тобто збитком w' виражаються загрози, які можуть спотворити процес обробки інформації та розмежування доступу до неї, що призведе до загальної небезпеки інформації, ІС вцілому.

Припустимо, що збиток W можна зменшити за допомогою загального запобіженого збитку $W_{зап}$ або збитку, якого запобігли за рахунок унеможливлення дії відповідного класу загроз, $W^{лікв}_{зап}$. Необхідно оцінити показник стійкості СЗБІ до загроз, який прямо залежить від величини збитку ІС, якого запобігли, $W_{зап}$.

Очевидно, збиток, якого запобігли, $W_{зап}$ у загальному вигляді виражається співвідношенням:

$$W_{зап} = F\left(P_{iзагр};\ \omega^{прот}_{j\ загр};\ i = 1,4;\ j = 1,4\right). \tag{2}$$

Збиток, якого запобігли за рахунок ліквідації дії i-го класу загроз

$$W^{лікв}_{зап} = P_{i\ загр} \cdot \omega^{прот}_{j\ загр};\ i = 1,4;\ j = 1,4. \tag{3}$$

З (3) слідує, що величина збитку, якого не вдалось запобігти,

$$W^{не\ лікв}_{зап} = P_{i\ загр}\left(1 - \omega^{прот}_{j\ загр}\right);\ i = 1,4;\ j = 1,4. \tag{4}$$

За умови незалежності загроз і адитивності їх наслідків отримуємо

$$W_{зап} = \sum_{i=1}^{4}\sum_{j=1}^{4} P_{i\ загр} \cdot \omega^{прот}_{j\ загр}. \tag{5}$$

Ймовірність появи загроз i-го класу $P_{i\ загр}$ визначається відповідно приналежністю до певного класу загроз з урахуванням експертної корекції значень $\acute{P}_{i\ загр}$ у межах величини ймовірності появи загроз i-го класу

$$P_{i\ загр} = \alpha_i, \tag{6}$$

де α_i – експертно встановлена величина загальної ймовірності загрози i-го класу загроз, яка лежить у проміжку, відповідно до запропонованої класифікації загроз ІС, тобто

$$\alpha_i = \begin{cases} \in [0;0,1), & \text{при} \quad i = 1, \\ \in [0,1;0,5), & \text{при} \quad i = 2, \\ \in [0,5;0,8), & \text{при} \quad i = 3, \\ \in [0,8;1), & \text{при} \quad i = 4. \end{cases} \tag{7}$$

Ймовірність усунення загроз i-го класу $\omega_{i\ загр}$ визначається за допомогою оцінки наявних засобів протидії загрозам до певного класу

$$\omega^{прот}_{j\ загр} \in [0;1], \quad j = \overline{1,\ 4}. \tag{8}$$

Тобто $\omega^{прот}_{j\ загр}$ визначається сукупністю визначених засобів протидії загрозам певного класу

$$\omega^{прот}_{j\ загр} = f_j(p_{j1}, ..., p_{jk}), \tag{9}$$

де p_{jk} – ймовірність протидії k-й загрозі ІС та СЗБІ $j = \overline{1,4}$; $k = \overline{1,m}$; m – загальна кількість загроз i-го класу, за якими проводиться оцінка надійності СЗБІ.

Провівши нормування [2], отримуємо

$$\omega^{прот}_{j\ загр} = \sum_{j=1}^{4} \sum_{k=1}^{m} p_{jk}. \tag{10}$$

З (6) та (10) слідує, що загальни збиток ІС, якого запобігли, має вигляд

$$W_{зап} = \sum_{i=1}^{4} P_{i\ загр} \cdot \sum_{j=1}^{4} \sum_{k=1}^{m} p_{jk}. \tag{11}$$

Таким чином, показник стійкості СЗБІ до загроз прямо пропорційний загальному збитку ІС W, якого запобігли,

$$W_{зап} = \sum_{i=1}^{4} P_{i\ загр} \cdot \sum_{j=1}^{4} \sum_{k=1}^{m} p_{jk}. \tag{12}$$

Отриманий показник $W_{зап}$, системою оцінювання показника стійкості СЗБІ наглядніше представляти у відсотковиму виді

$$W_{зап} = \left(\sum_{i=1}^{4} P_{i\ загр} \cdot \sum_{j=1}^{4} \sum_{k=1}^{m} p_{jk} \right) \cdot 100\%. \tag{13}$$

На цьому задачу визначення показника стійкості СЗБІ до загроз можна вважати розв'язаною.

Висновки

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

На основі досліджень [2, 8] перспективним напрямом розробки методів прийняття рішень при експертній вихідній інформації визначено лінгвістичний підхід на базі теорії нечітких множин та лінгвістичної змінної.

У результаті проведених досліджень за допомогою застосування теорії нечітких множин показано, що використання формального апарата за своїми потенційними можливостями і точністю має бути адекватним смисловому змісту та точності вхідних даних.

Проведено загальну класифікацію можливих загроз ІС й СЗБІ та визначено основні критерії оцінювання вжитих заходів протидії загрозам відповідних класів. У результаті проведених дослідження методів оцінювання показника якості СЗБІ [2, 4, 9] було запропоновано метод визначення показника стійкості системи СЗБІ до загроз, який порівняно з існуючими на сьогоднішній день [2, 6] є значно простішим та враховує загрози, які можуть зруйнувати стійкість СЗБІ й нанести інформаціний збиток як ІС так і самій СЗБІ. Вищевикладене має обов'язково враховуватись під час проектування системи ЗБІ, вибору методі та засобів захисту ІС та СЗБІ від негативної дії загроз.

Список літератури

1. *Sinder, F.* Die Grundlagen der Sicherheit der informativen Systeme. – Hamburg: Bücherei GmbH, 2006. -- 576 S.

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

3. *Мао Вембо.* Современная криптография: теория и практика.: Пер. англ. – М.: Издательский дом "Вильямс", 2005. – 768 с. : ил. – Парал. тит. англ.

4. *Смірнов О.А., Доренський О.П.* Метод оцінки показника якості системи забезпечення безпеки інформації. // У зб. наукових праць Кіровоградського національного технічного університету "Техніка в сільськогосподарському виробництві. Галузеве машинобудування. Автоматизація", вип. 18. – Кіровоград: КНТУ, 2007. – С. 282-289.

5. *Шевченко С.І., Волошанюк В.Г., Смірнов О.А., Доренський О.П.* Визначення ймовірності усунення заданої загрози інформаційної системи при наявності експертної інформації про загрози. – Х.: ХНУВС, 2007. – С. 23-24.

6. *Доренський О.П.* Метод визначення збитку інформаційної системи, якого запобігли, за умови наявності інформації про загрози. // У зб. тез доповідей Першої Міжнародної науково-правтичної конференції "Методи та засоби захисту й ущільнення інформації". – Вінниця: ВНТУ, 2007. – С. 53-54.

7. *Wei T.H.* The algebraik foundations of ranking theory Theses, Cambridge, 1952.

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

9. *Смірнов А.О., Доренський О.П.* Оцінювання загального показника якості системи забезпечення безпеки інформації автоматизованої системи // Системи обробки інформації. – Х.: ХУПС, 2007. – №7 (65). – С. 156-165.