УДК 681.3.06

О.П. До́ренський, Л.В. Помазан, Є.В. Мелешко

Кіровоградський національний технічний університет, Кіровоград

ВДОСКОНАЛЕННЯ МЕТОДА ВИЗНАЧЕННЯ ПОКАЗНИКА СТІЙКОСТІ ДО ЗАГРОЗ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

Розглядаються питання визначення показника стійкості до загроз системи забезпечення безпеки інформації (СЗБІ). Запропоновано вдосконалений метод визначення визначення показника стійкості до загроз системи забезпечення безпеки інформації (СЗБІ).

Ключові слова: *система забезпечення безпеки інформації, загрози безпеці інформації, показник стійкості.*

Вступ

Організація безпеки інформації (БІ) інформаційної системи (ІС) – основна функція системи забезпечення безпеки інформації (СЗБІ) ІС. Але на сьогоднішній день, як показали проведені дослідження [1, 2], більшість СЗБІ не задовільняють вимоги щодо забезпечення надійної безпеки ІС. Це пов'язано з рядом факторів та чинників, які не враховуються під час проектування і, відповідно, реалізації СЗБІ, що є досить об'ємною задачею, яка потребує нагального розв'язку [2]. Одним зі шляхів розв'язку цієї задачі є потужний апарат оцінювання показника стійкості до загроз інформаційній системі СЗБІ ще на етапі її проетування. Це дасть можливість на ранніх стадіях виявляти недоліки системи ЗБІ та ліквідовувати їх ще до її впровадження в експлуатацію [2, 3]. Метод оцінювання показника стійкості до загроз СЗБІ також забезпечить ефективним засобами оцінювання надійності існуючої, або проекта СЗБІ з метою усунення недоліків системи та, відповідно, підвищення рівня безпеки інформації ІС, яку вона забезпечує. Кількісно його можна представити як величину запобіжених збитків ІС завданих загрозою чи сукупністю загрозами в результаті атаки ІС [5]. Таким чином, розробка ефективного метода визначення показника стійкості до загроз СЗБІ є важливою задачею, яка на сьогоднішній день є розв'язаною частково та потребує нагального вдосконалення.

Аналіз. Дослідження методів визначення показника стійкості до загроз СЗБІ [4, 5] виявили комплекс недоліків запропонованих моделей системи оцінювання критерія якості СЗБІ до загроз ІС, що в свою чергу може викликати похибки під час визначення даної величини та, відповідно, призвести до прийняття хибних експертних висновків або результатів функціонування експертної системи.

Формулювання цілей. Метою проведення дослідження є одержання оптимізованого ймовірнісного методу визначення показника стійкості до загроз СЗБІ [4] шляхом усунення виявлених недоліків за допомогою застосування нових підходів і методів до визначення даної характеристики СЗБІ.

Основна частина

Побудова надійної СЗБІ та її моделі можлива за умови наявності ефективного метода одержання кількісного показника стійкості СЗБІ до загроз та його оцінювання за заданими характеристиками. На основі цього можна одержати комплексну оцінку обраного варіанту побудови, або вже існуючої та впровадженої СЗБІ. Зокрема, задача оцінювання діючої СЗБІ постає, як показує практика та дослідження [1, 2, 5, 6], набагато частіше. Це пов'язано з швидким моральним та фізичним старінням засобів протидії атакам ІС у зв'язку зі стрімким розвитком і вдосконаленням засобів та методів джерел загроз.

Як правило, під інформацією в ІС розуміють всі її дані та програми, які виконують їх обробку, забезпечують функції введення/виведення і т.д. Тому, на основі проведеного аналізу моделей процесу забезпечення безпеки інформації ІС [4, 5], постає необхідність розрізняти загрози ІС та безпосереньо СЗБІ й окремо досліджувати й оцінювати їх вплив на безпеку інформації в ІС. При чому, інтуїтивно зрозуміло, що атаки СЗБІ несуть в собі значно більшу загрозу ІС. Це пов'язано з тим, від функціонування СЗБІ прямо залежить безпека інформації ІС. Тому разі успішності атаки СЗБІ інформація ІС стає частково або навіть повністю незахищеною, що є недопустимим. Нехай сукупність загроз ІС, які можуть становити небезпеку як для інформації ІС, так і безпосередньо СЗБІ, надходить від джерела загроз. Вони є скінечними та підлягають підрахунку $i = \overline{1, n}$. Кожна i-та загроза характеризується ймовірністю появи $P_{i\,загр}$ та збитком $\Delta q_i^{загр}$, який може бути нанесений ІС. Модель процеса забезпечення інформаційної безпеки ІС та СЗБІ наведено в [4].

Застосування системного підходу протидії загроам ІС та СЗБІ можливе виключно за умови наявності ефективного та зручного у практичній реалізації і використанні апарату ідентифікації загроз [5], що пропонується здійснити за допомогою класифікації загроз ІС [6]. Недоліком даного метода є не досить об'єктивна оцінка стійкості СЗБІ до загроз.

Математична модель методу визначає стійкість як унеможливлення загрозам завдати збитку ІС, який визначається в абсолютних одиницях [4].

Крім того, проведено класифікацію можливих загроз ІС на наступні чотири класи: 1) малоймовірні; 2) ймовірні; 3) надймовірні; 4) критичні. 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 $P^{кл}_{i\ загр}$, $i = 1,\ 4$: малоймовірні (i = 1) – 0-10%, ймовірні (i = 2) – 10-50%; надймовірні (i = 3) – 50-80%; критичні (i = 4) – 80-100%, тобто

$$P^{кл}_{i\ загр} \in \begin{cases} [0;0,1), & \text{при} \quad i = 1, \\ [0,1;0,5), & \text{при} \quad i = 2, \\ [0,5;0,8), & \text{при} \quad i = 3, \\ [0,8;1), & \text{при} \quad i = 4. \end{cases} \qquad (1)$$

Результати проведеного аналізу сучасних методів та способів протидії атакам ІС [2], а також загроз, які можуть мати місце для ІС та СЗБІ [5], дають підстави стверджувати про умовність та досить низьку практичну цінність наведеної класифікації, хоч вона й дозволяє реалізувати наведений метод [4] для визначення показника стійкості до загроз СЗБІ. Дослідження класифікації загроз ІС свідчать про не досить раціональний підхід до класифікаційного поділу, оскільки окрім ймовірності атаки загрози існують і інші ознаки, за допомогою яких має визначатись приналежність загроз до певного класу. З іншого боку, досліджена класифікація зберігає основне правило класифікаційного поділу [5], що в свою чергу доводить правильність підходу до проведення класифікаційного поділу загроз ІС. В [5] проведено детальний аналіз класифікаційного поділу загроз ІС та СЗБІ та запропоновано альтернативну класифікацію загроз ІС, де також наведено спосіб її приведення до вигляду (1) з відповідними ваговими характеристиками (коефіцієнтами) класів.

Новизною метода є розподіл загроз на дві основні групи: загрози ІС та загрози СЗБІ. При цьому під час визначення рівня небезпеки інформації ІС окремо оцінюються загрози ІС та загрози СЗБІ. Дослідження показали, що в деяких ситуаціях загрози СЗБІ становлять найбільшу небезпеку, оскільки за умови часткової або повної локалізації функцій СЗБІ чи спотворення процесу забезпечення БІ унеможливлюється протидія загрозам ІС. Це може призвести до високого рівня небезпеки інформації ІС. Перевагою методу є також типування вжитих заходів протидії загрозам ІС та СЗБІ, які враховуються під час визначення критерія безпеки ІС..

Отже, постає задача вдосконалення методу [4]. Для її розв'язку проведено детальний аналіз та дослідження можливих загроз, які можуть атакувати СЗБІ чи ІС [1 – 5], за результататами яких можна стверджувати, що раціональним підходом до вирішення проблеми є класифікація, проведена відносно джерела їх виникнення: I) апаратні; II) програмні; III) природні; IV) людські [5].

Проведені дослідження загроз ІС та запропонованої класифікації дають підстави зробити висновок, що загрози I-III класу мають функціональні зв'язки з класом IV. Тобто класи I-III можуть існувати для заданої ІС та СЗБІ як самостійно, так і породжуватись класом IV. Дана класифікація зберігає властивості класів, наведених в [4]. Множини загроз класу I-IV не перетинаються, тому окрема загроза може належати виключно одному класу загроз.

Класифікацію [5] можливо застосовувати у методі [4], якщо провести оцінювання кожного елемента класу I-IV і представити кожен клас у вигляді загальної ймовірності виникнення загрози i-го класу

$$P^{кл}_{i\ загр} = 1 - \prod_{k=1}^{n} \left(1 - p^{i}_{k}\right),\ i = 1,4, \qquad (2)$$

де p^{i}_{k} – ймовірність виникнення загрози i-го класу; n – кількість загроз i-го класу, які можуть атакувати дану ІС.

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 забезпечувати реалізацію сукупності заданих методів та заходів протидії загрозам, які з метою можливості точного оцінювання пропонується типувати за наступними критеріями [4]: 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 зловмисної дії зовнішніх факторів та загроз на характеристики 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 $\omega^{прот}_{загр}$.

Сформулюємо задачу визначення показника стійкості СЗБІ до загроз ІС: 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 БІ $\omega^{прот}_{j\ загр}$.

В [4] стійкість СЗБІ до загроз запропоновано звести до визначення завданого збитку w під дією

загроз, а також збитку w', який завдається безпосередньо СЗБІ. Так як СЗБІ безпосередньо не бере участі у процесі обробки інформації ІС, то загрози ІС та загрози СЗБІ з точки зору завданого збитку інформації є незалежними. Це твердження слідує з того, що навіть за умови успішної атаки СЗБІ, атака ІС може не здійснюватись. При цьому величина збитку СЗБІ визначається величиною витрат на її відлагодження. Таким чином, загальний збиток ІС W визначимо як суму збитків w та w'

$$W(n,k) = \sum_{i=1}^{n} w_i + \sum_{j=1}^{k} w'_j ,$$

де n – кількість загроз ІС; k – кількість загроз СЗБІ.

Збиток, якого запобігли, $W_{зап}$ у загальному вигляді виражається співвідношенням

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

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

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

За умови незалежності загроз і адитивності їх наслідків отримуємо

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

Ймовірність появи загроз i-го класу $P_{i\ загр}$ визначається відповідно приналежністю до певного класу загроз з урахуванням експертної корекції значень $P_{i\ загр}$ у межах величини ймовірності появи загроз i-го класу $P_{i\ загр} = \alpha_i$, де α_i – експертно встановлена величина загальної ймовірності загрози i-го класу загроз, яка лежить у проміжку, відповідно до запропонованої класифікації загроз ІС.

Ймовірність усунення загроз i-го класу $\omega_{i\ загр}$ визначається за допомогою оцінки наявних засобів протидії загрозам до певного класу $\omega^{прот}_{j\ загр} \in [0;1]$, $j = 1,\ 4$. Тобто $\omega^{прот}_{j\ загр}$ визначається сукупністю визначених засобів протидії загрозам певного класу 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.

Таким чином, показник стійкості СЗБІ до загроз прямо пропорційний загальному збитку ІС $W_{зап}$, якого запобігли,

$$W_{зап}(m) = \sum_{i=1}^{4} P_{i\ загр} \cdot \sum_{j=1}^{4} \sum_{k=1}^{m} p_{jk} . \qquad (3)$$

Але слід зауважити, що показник $W_{зап}$ не дає об'єктивної оцінки стійкості СЗБІ до загроз, а відображає якісну характеристику функціонування СЗБІ, не враховуючи при цьому загального. Тому пропонується стійкість S СЗБІ визначати як величину успішного запобігання дії загрози чи сукупності загроз ІС та СЗБІ. Тобто,

$$S = 1 - \prod_{i=1}^{4} \omega^{i\ прот}_{загр} , \qquad (4)$$

де $\omega^{i\ прот}_{загр}$ – ймовірність успішної протидії загрозі або загрозам i-го класу, величина якої визначається за допомогою відповідних методів [2].

Відповідно, вразливість СЗБІ до загроз

$$\overline{S} = \prod_{i=1}^{4} \omega^{i\ прот}_{загр} .$$

Ймовірність усунення загроз i-го класу визначається за допомогою оцінки наявних засобів протидії загрозам класу I-IV [4]

$$\omega^{i\ прот}_{загр} \in [0;1],\ \ i = 1,\ \ 4 .$$

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

$$\omega^{i\ прот}_{j\ загр} = f_i\left(\alpha_{i1}, ..., \alpha_{ij} \right),$$

де α_{ij} – ймовірність успішної протидії j-й загрозі ІС та СЗБІ i-го класу, $j = \overline{1,m}$; m – загальна кількість загроз i-го класу, за якими проводиться оцінювання стійкості СЗБІ.

Провівши нормування [4], отримуємо

$$\omega^{i\ прот}_{загр} = 1 - \prod_{j=1}^{m} \left(1 - \alpha^i_j \right). \qquad (5)$$

Величина α_{ij} при цьому визначається як добуток ймовірності появи j-ї загрози i-го класу $p^{i\ загр}_j$ і ймовірності успішної протидії цій загрозі системою ІБ $\omega^{i\ прот}_j$

$$\alpha^i_j = \left(1 - p^{i\ загр}_j \right)\left(1 - \omega^{i\ прот}_j \right),$$

при $p^{i\ загр}_j \in (0;1)$, $\omega^{i\ прот}_j \in (0;1)$.

Щодо справедливості наступних виразів $p^{i\ загр}_j \in (0;1)$ та $\omega^{i\ прот}_j \in (0;1)$ свідчать дослідження, результати яких стверджують про неіснування жодної загрози, ймовірність успішної протидії якій можна наблизити до значення 1 або забезпечити її повну протидію, та про неіснування жодної системи БІ, стійкість якої рівна 1 і яку не можливо наблизити до значення 0 [7].

Зрозуміло, що при наближенні $\omega^{i\ прот}_j$ до значення 0 збільшується величина W. Тому під час проектування СЗБІ необхідно обрати такий варіант програмно-технічної реалізації, який би максималь-

но наближував значення $\omega_j^{i\ прот}$ до 1, щоб система забезпечувала високий рівень попередження та протидії даному класу загроз.

Якщо $p_j^{i\ загр} = 0$, то немає необхідності включати дану загрозу до множини загроз відповідної ІС та СЗБІ і забезпечувати функціями СЗБІ протидію даному класу загроз (частіше – даній загрозі).

Слід відзначити чутливість показника α_j^i до загроз, на протидію яким СЗБІ не має відповідних методів, способів та інструментарію ($\omega_j^{i\ прот} = 0$). Таким чином, величина показника α_j^i знижується до нуля, що є сигнатурою на вразливість СЗБІ і можливу небезпеку ІС.

Таким чином, з (4) та (5) випливає, що

$$S = 1 - \prod_{i=1}^{4}\prod_{j=1}^{m}\alpha_j^i . \qquad (6)$$

Виходячи з (6), вразливість (нестійкість) СЗБІ до загроз ІС та безпосередньо СЗБІ

$$\bar{S} = \prod_{i=1}^{4}\prod_{j=1}^{m}\alpha_j^i .$$

Таким чином, показник (6) характеризує величину уникнутих загроз на ІС та СЗБІ, що, як визначено вище, є стійкістю СЗБІ до загроз ІС та безпосередньо СЗБІ. Як показали дослідження оптимізованого методу, отриманий показник значно точніше та об'єктивніше оцінює рівень протидії загрозам.

На основі показника стійкості СЗБІ до загроз (6) та за допомогою динамічної матриці знань реалізовано програмний додаток оцінки стійкості СЗБІ. Результати роботи програми дають підстави стверджувати про ефективність одержаного метода визначення показника S не тільки з точки зору практичного використання, але й програмної реалізації та подальшої інтеграції у системи оцінювання та аналізу якості СЗБІ.

Висновки

Результатом проведених досліджень є наступні висновки:

1) проаналізовано результати дослідження метода визначення показника стійкості СЗБІ, в результаті чого визначено її основні переваги та недоліки;

2) задачу вдосконалення метода визначення показника стійкості до загроз СЗБІ розв'язано шляхом усунення виявлених недоліків метода [4], зокрема застосування нового підходу до поняття стійкості системи до загроз ІС, інтеграції в метод класифікації загроз ІС та СЗБІ в результаті чого отримано більш ефективний цмовірнісний метод визначення показника стійкості до загроз СЗБІ;

3) наведено приклади практичного застосування одержаного ймовірнісного метода, а саме програмної реалізації у вигляді підсистеми оцінювання показника стійкості СЗБІ до загроз ІС та СЗБІ.

Список літератури

1. Смірнов А.О. Оцінювання загального показника якості системи забезпечення безпеки інформації автоматизованої системи / А.О. Смірнов, О.П. До́ренський // Системи обробки інформації. – Х.: ХУПС, 2007. – Вип. 7 (65). – С. 95-99.

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

3. Анохин А.М. Методы определения коэффициентов важности критериев / А.М. Анохин, В.А. Глотов, В.В. Павельев, А.М. Черкашин // Автоматика и телемеханика. – 1997. – № 8. – С. 30-35.

4. До́ренський О.П. Метод визначення показника стійкості до загроз системи забезпечення безпеки інформації / О.П. До́ренський // Вісник Державного університету інформаційно-комунікаційних технологій. – К.: ДУІКТ, 2007. – № 4. – С. 105-112.

5. До́ренський О.П. Дослідження потенційних загроз безпеці інформації інформаційної системи та аналіз їх класифікаційного поділу / О.П. До́ренський // Збірник наукових праць КНТУ. – Кіровоград: КНТУ, 2007. – Вип. 19. – С. 55-61.

6. Галатенко В.А. Основы информационной безопасности / В.А. Галатенко. – М.: ИУИТ, 2005. – 208 с.

7. Галатенко В.А. Стандарты и рекомендации в области информационной безопасности / В.А. Галатенко // Информационный бюлетень "Jet Informations". – № 1-3 (8-10). – 1996.

Надійшла до редколегії 13.05.2010

Рецензент: д-р техн. наук, проф. В.В. Сидоренко, Кіровоградський національний технічний університет, Кіровоград.

СОВЕРШЕНСТВОВАНИЕ МЕТОДА ОПРЕДЕЛЕНИЯ ПОКАЗАТЕЛЯ СТОЙКОСТИ К УГРОЗАМ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

А.П. Доренксий, Л.В. Помазан, Е.В. Мелешко

Рассматриваются вопросы определения показателя стойкости к угрозам системы обеспечения безопасности информации. Предложен усовершенствованный метод определения показателя стойкости к угрозам системы обеспечения безопасности информации.

Ключевые слова: *система обеспечения безопасности информации, угрозы безопасности информации, показатель стойкости.*

PERFECTION OF METHOD OF DETERMINATION OF INDEX OF FIRMNESS TO THE THREATS OF THE SYSTEM OF PROVIDING OF SAFETY OF INFORMATION

O.P. Dorensky, L.V. Pomasan, E.V. Meleshko

The questions of determination of index of firmness are examined to the threats of the system of providing of safety of information. The improved method of determination of index of firmness is offered to the threats of the system of providing of safety of information.

Keywords: *system of providing of safety of information, threats safety of information, index of firmness.*