УДК 354.42

О.М. Косогов

Військова частина 1906

МЕТОДИЧНИЙ ПІДХІД ДО ФОРМАЛІЗАЦІЇ ПРОЦЕСУ ЗМІНИ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМИ

На основі аналізу методів забезпечення інформаційної безпеки системи запропоновано математичну модель, що описує динаміку зміни рівня інформаційної безпеки системи з урахуванням первинних і вторинних загроз. Модель може використовуватись для розроблення методик протидії цим загрозам.

***Ключові слова**: інформаційна безпека, загроза, динаміка загроз, матриця безпеки, наслідки реалізації загроз, ризик, експертне оцінювання.*

Вступ

Постановка проблеми. Аналіз літератури. Проблеми забезпечення інформаційної безпеки у воєнній сфері, з огляду на появу нових та зростання рівня існуючих ризиків і загроз в інформаційному просторі України, набувають великої значущості і потребують відповідного наукового підґрунтя для їх вирішення.

Одним з напрямів розв'язання цих проблем є постійне удосконалення науково-методичного забезпечення інформаційної безпеки, а саме визначення спрямованості загроз та оцінка їх рівня, виявлення об'єктів інформаційного впливу та вибір дієвих методів забезпечення інформаційної безпеки.

Існує низка публікацій, що присвячені проблемам інформаційної безпеки в інформаційних системах і мережах передачі й обробки інформації. Завдання створення, організації й дослідження процесів функціонування, удосконалювання й розвитку систем забезпечення безпеки інформації тою чи іншою мірою знайшли відбиття в працях ряду вітчизняних і закордонних учених [1 – 4].

Однак дотепер повною мірою не вивчені й залишаються дискусійними методологічні, методичні й практичні аспекти дослідження проблем моделювання безпеки складних інформаційних систем/

Метою статті є викладення методичного підходу до формалізації процесу зміни рівня інформаційної безпеки системи з урахуванням заходів протидії інформаційним загрозам.

Результати досліджень

Під рівнем інформаційної безпеки системи розуміється оцінка, яка отримана із сукупності показників і критеріїв, що характеризують стан системи на предмет захищеності критичних для неї елементів.

Рівень інформаційної безпеки системи можна характеризувати за такою матрицею:

$$B = \begin{pmatrix} K_1 & F_1 & V_1(T) & S_1 \\ \cdots & \cdots & \cdots & \cdots \\ K_n & F_n & V_n(T) & S_n \end{pmatrix}, \qquad (1)$$

де K_i – показник рівня безпеки за і-м критерієм;

F_i – тенденція зміни і-го критерію (зростає, убуває, незмінний);

$V_i(T)$ – швидкість зміни і-го критерію, що є функцією часу Т (наприклад: низька, нижче середнього, середня, вище середнього, висока);

S_i – ступінь критичності негативних наслідків при реалізації ризиків, яка погіршує значення і-го критерію.

Матрицю виду В в подальшому будемо називати матрицею безпеки (МБ).

Перший і четвертий стовпці МБ являють собою вектор часткових критеріїв безпеки і їх ваги та характеризують поточний стан комплексної інформаційної безпеки, дозволяючи оцінити ситуацію, що склалася на даний момент часу. Другий і третій стовпці матриці відображають динаміку розвитку процесів та дають змогу прогнозувати їх розвиток у подальшому.

У цьому випадку мультиплікативна згортка інтегрального критерію комплексної безпеки являє собою величину:

$$K = \prod_i (K_i)^{S_i} . \qquad (2)$$

Оцінки S_i можуть бути отримані експертним шляхом. Однак, експерту не завжди буде легко оцінити ці коефіцієнти.

Тому для цього доцільно використовувати різні рангові методи, реалізація яких вимагає лише впорядкувати ці критерії [5 – 8].

Наприклад, можна використати метод нестрогого ранжування. Відповідно до цього методу, експертом нумеруються всі критерії в порядку зниження рівня негативних наслідків, які пов'язані з даним критерієм безпеки. Причому допускається, що експерту не вдається розрізнити між собою деякі критерії. Провівши ранжування він розташовує їх

поруч у довільному порядку. Потім критерії, які уже пройшли процес ранжування, послідовно нумеруються. Оцінка (ранг) критерію визначається за його номером [6].

Якщо на одному місці знаходяться декілька не розрізнених між собою критеріїв, то оцінка кожного з них приймається за середнє арифметичне їх нових номерів [7, 8]. Однак, вважається за доцільне модифікувати такий метод оцінювання, прийнявши за ранг для кожного із не розрізнених критеріїв номер усієї групи як цілого об'єкта по ступеню впорядкування. Таким способом можуть бути оцінені як ступені впливу кожного параметра на часткові критерії безпеки K_i, так і ступені прийнятності наслідків реалізації загроз S_i.

Наприклад, будемо вважати, що експерт упорядкував критерії в такий спосіб:

$$K_5,(K_3,K_7,K_2),K_1,(K_6,K_8),K_9,K_4. \qquad (3)$$

Критерії, які не розрізнені між собою, об'єднані в круглі дужки. Тоді оцінки для кожного із критеріїв, які обчислені відповідно до описаної вище процедури, дорівнюють:

$$\begin{gathered} S_5 = 1; \quad S_3 = S_7 = S_5 = 2; \quad S_1 = 3; \\ S_6 = S_8 = 4; \quad S_9 = 5; \quad S_4 = 6. \end{gathered} \qquad (4)$$

Застосуємо нормування за величиною, яка дорівнює сумі всіх оцінок:

$$S_{норм} = \sum\nolimits_i S_i . \qquad (5)$$

У нашому випадку $S_{норм} = 29$. Таким чином, після лінійного перетворення в шкалу [0; 1] за нормою $S_{норм}$ отримаємо:

$$\begin{gathered} S_5 = 1/29; \quad S_3 = S_7 = S_5 = 2/29; \quad S_1 = 3/29; \\ S_6 = S_8 = 4/29; \quad S_9 = 5/29; \quad S_4 = 6/29. \end{gathered}$$

Визначені, запропонованим способом оцінки являються узагальненням системи ваги Фішберна [9] у випадку змішаного розподілу переваг, коли поряд з перевагами в систему входять і відносини рівнозначності.

Критерії в матриці безпеки можна згрупувати за відповідними напрямами забезпечення безпеки, наприклад: економічні, екологічні, соціальні, технічні тощо.

Таким чином, кожний рядок матриці безпеки (K_i; F_i; $V_i(T)$; S_i) характеризує стан безпеки за *i*-м критерієм.

Часткові матриці, що складаються з рядків, що визначають певний напрям забезпечення безпеки, в свою чергу, описують стан у відповідній області.

Показники рівня безпеки K_i тісно пов'язані з наслідками від можливої реалізації наявних у системі загроз та заходами, які спрямовані на попередження, запобігання, локалізацію і усунення таких наслідків.

Слід особливо відзначити, що загрози можна розділити на первинні і вторинні. Первинні загрози існують незалежно від стану системи й апріорно мають певну безумовну ймовірність виникнення.

Імовірність виникнення вторинних загроз є умовною і залежить від стану системи та стану зовнішнього середовища.

Зокрема, деякі стани системи можуть спровокувати виникнення загроз, появлення яких в інших умовах була б неможливою.

Введемо такі позначення:

$\overline{U_i}$ і $\widetilde{U_j}$ (i, j = 1,2,3, … k) – сукупність первинних і вторинних загроз, що виникають з ймовірностями $\overline{P(U)_i}$ і $\widetilde{P(U)_j}$, відповідно, здійснюючи вплив $\bar{n}_{km}$ і $\tilde{n}_{km}$ на елемент (k,m) матриці безпеки B (k = 1,2,3,... n; m = 1- 4).

Вплив кожної з первинних або вторинних загроз можна описати матрицею впливу, що має вигляд:

$$N_{ij} = \begin{pmatrix} n_{11} & n_{12} & n_{13} & n_{14} \\ n_{21} & n_{22} & n_{23} & n_{24} \\ n_{31} & n_{32} & n_{33} & n_{34} \\ n_{41} & n_{42} & n_{43} & n_{44} \end{pmatrix}. \qquad (6)$$

Фактично матриця впливу являє собою матрицю ваги впливу і-го негативного фактора на елементи МБ. Необхідно відмітити, що вплив $\bar{n}_{km}$ і $\tilde{n}_{km}$ на відповідні елементи матриці безпеки B може бути як негативним так і позитивним.

Елементи матриці впливу, що здійснюють негативний вплив є негативними щодо елементів МБ; елементи, що роблять позитивний вплив - позитивними щодо елементів МБ; елементи, що не здійснюють ніякого впливу, є нейтральними.

Ризик реалізації і-ої первинної загрози

$$\overline{R_i} = \left(\overline{N_i}; \overline{P(U)_i}\right)$$

відображає появу наслідків із ймовірністю $\overline{P(U)_i}$, які змінюють стан системи через відповідні матриці впливу $\overline{N_i}$.

Імовірності виникнення первинних загроз $\overline{PUG_i}$ є незалежними. Однак сукупність превентивних заходів захисту дозволяє послабити вплив первинних загроз на ступінь комплексної безпеки системи.

Цей факт може бути описаний за допомогою матриці превентивних заходів

$$Z_i = \begin{pmatrix} z_{11} & z_{12} & z_{13} & z_{14} \\ z_{21} & z_{22} & z_{23} & z_{24} \\ z_{31} & z_{32} & z_{33} & z_{34} \\ z_{41} & n_{42} & z_{43} & z_{44} \end{pmatrix}, \qquad (7)$$

де $j = \overline{1,M}$, M – загальна кількість превентивних заходів.

Елементи матриці Z_i назвемо демпферними коефіцієнтами.

Якщо, незважаючи на превентивні заходи безпеки, реалізація визначеної множини первинних загроз призвела до виникнення наслідків то необхідно розпочати заходи для їх локалізації та усунення.

У випадку недостатності превентивних заходів, а також заходів з локалізації та усуненню наслідків первинних загроз , то такий стан системи може ініціювати появу вторинних загроз із ймовірностями $\widetilde{P(U)_j}$.

Зауважимо, що ймовірності виникнення вторинних загроз не є безумовними, як для первинних загроз. Вони залежать від поточного стану системи. До первинних загроз вживають заходи протидії ще до їх настання, тобто фактично зводяться до мінімуму їх наслідки, не впливаючи на сам факт їх виникнення.

У випадку з вторинними загрозами необхідно намагатися взагалі не припустити їх, тобто нейтралізувати їх причини.

Висновки

Таким чином, на основі формалізації процесу динаміки безпеки інформаційних систем запропонована модель зміни рівня інформаційної безпеки системи, яка враховує ризики та наслідки реалізації інформаційних загроз, а також вплив превентивних заходів на безпеку системи.

Зазначена модель може використовуватись при розробленні методик виявлення та аналізу загроз, а також протидії їм.

Список літератури

1. Киселев В.Д. Современные проблемы защиты в системах ее передачи и обработки / В.Д. Киселев, О.В. Есиков, А.С. Кислицын. Под ред. проф. Е.М. Сухарева. – М.: Солид, 2000. – 200 с.

2. Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах / В.Ф. Шаньгин, А.В. Соколов. – ДМК, 2002. – 134 с.

3. Гарбарчук В. Кибернетический подход к проектированию систем защиты информации / В. Гарбарчук, З. Зинович, А. Свиц. Украинская академия информатики; Волынский гос. ун-т им. Леси Украинки; Люблинский политехнический ун-т. – К.; Луцк; Люблин, 2003. – 658 с.

4. Маслова Н.А. Построение модели защиты информации с заданными характеристиками качества / Н.А. Маслова // Штучний інтелект. – Донецьк: ІШІ, 2007. – № 1. – С. 51-57.

5. Ажмухамедов И.М. Динамическая нечеткая когнитивная модель влияние угроз на информационную безопасность систем / И.М. Ажмухамедов // Безопасность информационных технологий. – 2010. – № 2. – С. 68-72.

6. Ажмухамедов И.М. Математическая модель комплексной безопасности компьютерных систем и сетей на основе экспертных суждений / И.М. Ажмухамедов // Инфокоммуникационные технологии. – 2009. – Т. 7, № 4. – С. 103-107.

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

8. Ажмухамедов И.М. Моделирование на основе экспертных суждений процесса оценки информационной безопасности / И.М. Ажмухамедов // Вестник АГТУ. Серия: "Управление, вычислительная техника и информатика". – 2009. – 2. – С. 101-109.

9. Фишберн П. Теория полезности для принятия решений / П. Фишберн. – М.: Наука, 1978. – 352 с.

Надійшла до редколегії 14.07.2016

Рецензент: д-р техн. наук, проф. О.Б. Леонтьєв, Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків.

МЕТОДИЧЕСКИЙ ПОДХОД К ФОРМАЛИЗАЦИИ ПРОЦЕССА ИЗМЕНЕНИЯ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ

А.Н. Косогов

На основе анализа методов обеспечения информационной безопасности предложена математическая модель, которая описывает динамику изменения уровня информационной безопасности с учетом первичных и вторичных угроз. Модель может быть использована при разработке методик противодействия этим угрозам.

Ключевые слова: *информационная безопасность, угроза, динамика угроз, матрица безопасности, последствия реализации угроз, экспертная оценка.*

METHODICAL APPROACH TO THE FORMALIZATION OF THE CHANGE PROCESS THE LEVEL OF INFORMATION SYSTEM SECURITY

O.M. Kosogov

On base of the analysis of the methods of the provision to information security it is offered mathematical model, which describes the level change dynamics of the information security of the system with provision for primary and secondary threats. The model can be used at development of the methods of the reluctance this threat.

Keywords: *information security, threat, track record of the threats, matrix to security, consequences to realization of the threats, expert estimation*.