УДК 519.718.2

Косогов О.М., к.військ.н., с.н.с.

Військова частина А1906, Київ

Модель динаміки зміни рівня інформаційної безпеки системи

Резюме. 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.

Постановка проблеми. 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 із 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 оцінка ефективності заходів протидії.

Аналіз досліджень і публікацій. 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 місце у 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.

Сучасні науково-практичні напрацювання в Україні, а так само ряд провідних міжнародних стандартів містять норми й вимоги, спрямовані в основному на захист від несанкціонованого доступу . При цьому вони часто не забезпечують базового рівня безпеки, оскільки дозволяють моделювати лише частину загроз. При цьому на сьогодні не існує загальноприйнятих стандартів або підходів, що дозволяють забезпечити підвищений або високий рівень захисту. Так само до негативного боку застосування сучасних стандартів варто віднести шаблонність пропонованого захисту й відсутність варіантності.

Метою статті є викладення математичної моделі, що описує динаміку зміни рівня інформаційної безпеки системи, яка вільна від зазначених недоліків.

Виклад основного матеріалу. 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 наступною матрицею:

$$B=\begin{pmatrix} K_1 & F_1 & V_1(T) & S_1 \\ K_2 & F_2 & V_2(T) & S_2 \\ K_3 & F_3 & V_3(T) & S_3 \\ \vdots & \vdots & \vdots & \vdots \\ K_n & F_n & V_n(T) & S_n \end{pmatrix}, \qquad (1)$$

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

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

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

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

Матрицю виду В у 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 із використанням різних рангових методів, реалізація яких вимагає впорядкувати ці критерії [5-8].

Наприклад, можна використати метод нестрогого ранжування, відповідно до якого експертом нумеруються всі критерії в порядку зниження рівня негативних наслідків, які пов'язані з цим критерієм безпеки. Критерії, які вже пройшли процес ранжування, послідовно нумеруються. Оцінка (ранг) критерію визначається за його номером [6].

Якщо на одному місці знаходяться декілька нерозрізнених між собою критеріїв, то оцінка кожного з них береться за середнє арифметичне їх нових номерів [7-8]. Однак вважається за доцільне модифікувати такий метод оцінювання, прийнявши за ранг для кожного з нерозрізнених критеріїв номер усієї групи як цілого об'єкта за ступенем впорядкування.

У такий спосіб 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:

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

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

$$S_5 = 1;\ S_3 = S_7 = S_2 = 2;\ S_1 = 3;$$
$$S_6 = S_8 = 4;\ S_9 = 5;\ S_4 = 6. \quad (4)$$

Застосуємо нормування за величиною, яка дорівнює сумі всіх оцінок:

$$S_{норм} = \sum_i S_i, \quad (5)$$

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

$$S_5 = \frac{1}{26};\ S_3 = S_7 = S_2 = \frac{2}{29};\ S_1 = \frac{3}{29};$$
$$S_6 = S_8 = \frac{4}{29};\ S_5 = \frac{5}{29};\ S_4 = \frac{6}{29}.$$

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

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

Часткові матриці, що складаються з рядків, які 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 неможливо.

Введемо наступні позначення:

$\overline{UG_i}$ і $\widetilde{UG_j}$ (i, j = 1,2,3,…) сукупність первинних і вторинних загроз, що виникають з імовірностями $\overline{PUG_i}$ і $\widetilde{PUG_j}$, відповідно, здійснюючи вплив $\overline{n_{km}}$ і $\widetilde{n_{km}}$ на елемент (k,m) матриці безпеки B (k = 1,2,3,...; m = 1,2,3,4,5).

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

$$N_{ij} = \begin{pmatrix} n_{11} & n_{12} & n_{13} & n_{14} \\ n_{21} & n_{22} & n_{23} & n_{24} \\ n_{31} & n_{32} & n_{33} & n_{34} \\ \vdots & \vdots & \vdots & \vdots \\ n_{n1} & n_{n2} & n_{n3} & n_{n4} \end{pmatrix} \quad (6)$$

Фактично матриця впливу є матрицією ваги впливу i-го негативного фактора на елементи МБ.

Необхідно відмітити, що вплив $\bar{n}_{km}$ і $\tilde{n}_{km}$ на відповідні елементи матриці безпеки В може бути як негативним, так і позитивним.

Кортеж $\overline{R_i} = (\overline{N_i}; \overline{PUG_i})$ назвемо ризиком реалізації і-ї первинної загрози.

Цей кортеж відображає появу наслідків з імовірністю $\overline{PUG_i}$, 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:

$$Z_i = \begin{pmatrix} z_{11} & z_{12} & z_{13} & z_{14} \\ z_{21} & z_{22} & z_{23} & z_{24} \\ z_{31} & z_{32} & z_{33} & z_{34} \\ z_{n1} & z_{n2} & z_{n3} & z_{n4} \end{pmatrix}, \quad (7)$$

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 усунення наслідків первинних загроз, такий стан системи може ініціювати появу вторинних загроз з імовірностями $\widehat{P(U)}_j$.

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.

Висновок. 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.

Напрямом подальших досліджень є апробація моделі на реальних даних та розроблення на її основі методик виявлення та аналізу загроз, а також протидії їм.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Киселев В.Д., Есиков О.В., Кислицын А.С. «Современные проблемы защиты в системах ее передачи и обработки» / Под ред. проф. Е.М. Сухарева. - М.:«Солид», 2000. - С. 200.
2. Шаньгин В.Ф., Соколов А.В. Защита информации в распределенных корпоративных сетях и системах. - Изд-во: ДМК, 2002. - 134 с.
3. Гарбарчук В., Зинович З., Свиц А. Кибернетический подход к проектированию систем защиты информации / 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 // Штучний інтелект. - Донецьк: ІШІ, 2007. - № 1. - С. 51-57.
5. Ажмухамедов И.М. Динамическая нечеткая когнитивная модель влияние угроз на информационную безопасность систем // Безопасность информационных технологий. 2010. №2. С. 68-72.
6. Ажмухамедов И.М. Математическая модель комплексной безопасности компьютерных систем и сетей на основе экспертых суждений // Инфокуммуникационные технологии Том 7, № 4, 2009, стр. 103-107.
7. Литвак Б.Г. Экспертная информация: методы получения и анализа. М.: Радио и связь, 1982.
8. Ажмухамедов И.М. Моделирование на основе экспертных суждений процесса оценки информационной безопасности // Вестник АГТУ. Серия: “Управление, вычислительная техника и информатика”, 2/2009г., С.101-109.
9. Фишберн П. Теория полезности для принятия решений. М.: Наука, 1978.

Стаття надійшла до редакції 15.09.2015

Косогов О.М., к.воен.н., с.н.с.
Войсковая часть А1906, Киев

Модель динамики изменения уровня информационной безопасности системы

Резюме. 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.

A. Kosogov
Military part A1906, Kyiv

Level change dynamics model of the information security of the system

Resume. 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.