УДК 004.281:681.3

Informatics and Mathematical Methods in Simulation
Vol. 3 (2013), No. 1, pp. 69-74

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ СИСТЕМ ЗАХИСТУ В МЕРЕЖАХ ПЕРЕДАЧІ ІНФОРМАЦІЇ

В.О. Хорошко, Ю.Є. Хохлачова

Національний авіаційний університет,
просп. Космонавта Комарова, 1, Київ, 03058, Україна; e-mail: professor_va@ukr.net

У даній статті розглянуто положення, які дозволяють сформулювати чи отримати ряд надзвичайно важливих для вирішення задачі захисту інформаційних ресурсів систем спеціального призначення умов, обмежень та оптимальних значень найбільш загальних параметрів системи захисту.

Ключові слова: захист інформації, системи захисту, мережі передачі інформації, захист інформаційних ресурсів

Вступ

Інформаційна безпека, поряд із економічною, військовою та іншими, займає одне з найважливіших місць у національній безпеці будь-якої держави. Забезпечення такої безпеки – складна наукомістка і багатогранна проблема.

Водночас необхідно чітко бачити протиріччя, що пов'язані з впровадженням інформаційних технологій взагалі і, зокрема, в системах спеціального призначення (ССП). З одного боку, автоматизація процесів збору, передачі, оброблення, збереження і відображення інформації істотно підвищує можливості органів керування, а з іншого боку – призводить до зростання залежності керування від надійності функціонування засобів автоматизації і надійності захисту інформації від несанкціонованого доступу і завад [1].

Тому величина шкоди ССП може бути визначеною у вигляді:

$$M\theta_2 = \sum_{i=1}^{i=n} p_{ві} \Delta T_{ki} C_i \,, \tag{1}$$

де

C_i — шкода за рахунок простою відповідних ресурсів ССП під час контролю в умовних одиницях в одиницю часу,

ΔT_{ki} — тривалість *i*-того виду контролю,

$p_{ві}$ — ймовірність виявлення і подальшої протидії загрозі *i*-го типу.

З урахуванням цього можна записати:

$$M\theta = M\theta_1 + M\theta_2 = \sum_{i=1}^{i=n} \left[G_i \left(T_{ki} - \Delta T_{ki} \right) \left(1 - p_{ві} \right) + p_{ві} C_i \Delta T_{ki} \right], \tag{2}$$

де $M\theta_1$ — максимальна величина можливої загальної шкоди.

Аналіз цього виразу дозволяє зробити висновок про те, що він може бути прийнятим як цільова функція системи технічного захисту інформації (ТЗІ).

У разі виявлення в процесі контролю факту порушення цілісності, здійснюється її поновлення із застосуванням резервних копій відповідної інформації. Характеристиками процесу поновлення є тривалість власне поновлення ($\Delta t_{пі}$) та ймовірність виникнення його необхідності; $p_{ві}$ — ймовірність виявлення порушення цілісності. Тоді математичне сподівання тривалості поновлення дорівнює:

$$\Delta t_{пі} p_{ві} + O(1 - p_{ві}) = \Delta t_{пі} p_{ві}.$$

Тобто тривалість усього процесу контролю та поновлення є винятковою величиною і визначається тривалістю власне процесу контролю $\Delta t_{кі}$, та тривалістю поновлення $\Delta t_{пі}$ з ймовірністю $p_{ві}$. Середнє значення величини $\Delta T_{кі}$, його математичне сподівання можна визначити як:

$$\Delta T_{кі} = \Delta t_{кі} + \Delta t_{пі} p_{ві}. \qquad (3)$$

Основна частина

Цільова функція (1), окрім умов доцільності застосування системи ТЗІ від загроз того чи іншого типу, дає змогу здійснити спробу знаходження оптимальних параметрів системи захисту – характеристик системи ТЗІ, наприклад, в сенсі максимуму шкоди, яка запобігається завдяки застосуванню системи захисту [2]. Зрозуміло, що величина цільової функції залежить від параметрів, які не є залежними від характеристик системи ТЗІ, але впливають на них, та і від параметрів, які не є залежними від помережної реалізації системи ТЗІ – їх характеристик. Деякі з них можуть бути параметрами управління, тобто тими параметрами, які можуть змінюватися залежно від умов застосування системи ТЗІ. Ці параметри залежать від типу загроз.

На інформаційні ресурси ССП, а також технічні засоби захисту цієї системи впливають виходи за межі допустимих значень температури, вологості, радіаційного чи електромагнітного випромінювання.

Стійкість ССП до загроз визначається її надійністю, що забезпечується відповідними заходами, які включають засоби контролю та поновлення цілісності системи. Значної уваги для забезпечення стійкості ССП приділяється протидії випадковим або зловмисним спробам несанкціонованого доступу (НСД), або штучним загрозам, під якими розуміються заборонені дії користувачів, по відношенню до ресурсів ССП [3].

Спроби НСД можуть вплинути на ССП лише після подолання засобів управління доступом та відповідних засобів забезпечення тієї чи іншої функціональної послуги.

Таким чином, інформаційні ресурси ССП потребують захисту від спроб НСД, а також безпосередніх впливів.

Припустимо, що потоки кожного з типів загроз є найпростішими з інтенсивностями $\gamma_{зі}$, тоді ця інтенсивність дорівнює сумі інтенсивностей загроз штучних $\gamma_{ші}$ та природних γ_i, так що:

$$\gamma_{зі} = \gamma_{ші} + \gamma_i.$$

Звернемо увагу на те, що під величиною γ_i, на наш погляд, слід розглядати ту частину потоків відмов ССП з загальною інтенсивністю γ, яка створює лише загрози *i*-го типу, так що:

$$\gamma = \sum_{i=1}^{i=n} \gamma_i \ .$$

Слід враховувати те, що $p_{ві}$ — ймовірність виявлення і подальшої протидії загрози *i*-го типу є ймовірністю складної події, яка полягає в тому, що система ТЗІ запобігає (не допускає) впливу цієї загрози, чи встановила факт її впливу і ліквідувала відповідні наслідки.

Для вирішення першої задачі використовується система управління (обмеження) доступом до інформаційних ресурсів ССП, що забезпечується адміністратором безпеки. Стійкість (в розумінні імовірності неподолання) p_{gi} системи управління доступом визначається стійкістю процесів ідентифікації та автентифікації адміністратора, як користувача з найширшими повноваженнями [Same]. Останнє визначається можливостями системи ідентифікації та кількістю можливих варіантів паролів і надійністю їх конфіденційного збереження.

Оскільки штучні загрози можуть впливати тільки в разі їх не виявлення засобами управління доступом, то інтенсивність цих загроз, які впливають на засоби забезпечення відповідної функціональної послуги ССП, зменшується до

$$\gamma_{ші}\left(1 - p_{gi}\right).$$

Друга задача (установки факту впливу загрози і ліквідації відповідних наслідків) вирішується шляхом перевірки цілісності та доступності інформації і її поновлення, в разі виявлення такого порушення. Тому з урахуванням застосування відповідних засобів захисту – засобів забезпечення відповідної функціональної послуги ССП результуюча інтенсивність загроз γ_{pi} може бути розрахованою як:

$$\gamma_{pi} = \left[\gamma_{ші}\left(1 - p_{gi}\right) + \gamma_i\right]\left(1 - p_{ві}\right), \tag{4}$$

де $p_{ві}$ — ймовірність виявлення (усунення) засобами забезпечення відповідно функціонально послуги ССП загрози відповідного типу.

Будемо вважати закон розподілу ймовірностей впливу на ресурси пуассонівським [4]. Тоді ймовірність впливу на *i*-ий ресурс хоча б однієї загрози відповідного типу $p_{зі}$ на інтервалі $\left(T_{ki} - \Delta T_{ki}\right)$ при умові застосування системи ТЗІ, тобто коли система захисту не виявила і, зрозуміло, не протидіяла цій загрозі, дорівнює:

$$p_{зі} = 1 - p_{oi} = 1 - \exp\left\{-\left(T_{ki} - \Delta T_{ki}\right)\left[\left(\gamma_{mi}\left(1 - p_{gi}\right) + \gamma_i\right)\left(1 - p_{ві}\right)\right]\right\},$$

де p_{oi} — ймовірність відсутності впливів, або наявність рівня нуля впливів.

Якщо підставити (3) в (1) з урахуванням (2), то величину шкоди можна записати у вигляді:

$$\begin{aligned} M\theta_i = {} & G_i\left(T_{ki} - \Delta T_{ki}\right)\left[1 - \exp\left\{-\left(T_{ki} - \Delta T_{ki}\right)\left[\left(\gamma_{mi}\left(1 - p_{gi}\right) + \gamma_i\right)\left(1 - p_{ві}\right)\right]\right\}\right] + \\ & + C_i \Delta T_{ki} \exp\left\{-\left(T_{ki} - \Delta T_{ki}\right)\left[\left(\gamma_{ші}\left(1 - p_{gi}\right) + \gamma_i\right)\left(1 - p_{ві}\right)\right]\right\}, \end{aligned} \tag{5}$$

Як слідує з останнього виразу, величина шкоди є функцією достатньо великого числа змінних. Серед цих змінних величини $G_i, C_i, \gamma_{ші}$ та γ_i є незалежними не тільки

від дій адміністратора безпеки, але і від характеристик підсистеми захисту ССП в цілому, тобто принципово не можуть розглядатися як параметри управління. Величини p_{oi}, $p_{вi}$ та ΔT_{ki} є залежними від якості розроблених та застосованих засобів управління доступом та засобів забезпечення відповідної функціональної послуги ССП і не можуть бути зміненими оперативно, але під час розробки системи ТЗІ їх значення принципово можна змінювати, тому ці параметри слід розглядати як параметри неоперативного управління. Після цих зауважень стає зрозумілим, що параметром оперативного управління слід вважати лише величину періоду контролю T_{ki}.

Слід показати, що ця функція має мінімум в точці:

$$T_{ki} = \Delta T_{ki} + d\,, \tag{6}$$

де величина ΔT визначається відповідно [3],

$$d = \frac{1}{z} + 0.5\sqrt{s}\,,$$

$$s = \Delta T_{ki}^2\left(1 + \frac{4C_i}{G_i}\right) + 4\left(\frac{1}{z^2} + \frac{C_i \Delta T_{ki}}{G_i z}\right),$$

а величина

$$z = \left\{\left[\gamma_{ші}\left(1 - p_{gi}\right) + \gamma_i\right]\left(1 - p_{вi}\right)\right\}$$

є не що інше, як результуюча інтенсивність загроз ($z = \gamma_{pi}$).

Отриманий результат має чітке і зрозуміле тлумачення [5]. Величина шкоди при зміні періоду контролю T_{ki} є мінімальною при такому його значенні, яке перевищує середнє значення його тривалості ΔT_{ki} на величину d яка, в свою чергу, визначається інтенсивністю потоку загроз, величинами шкод G_i та C_i характеристиками системи ТЗІ.

Вираз для розрахунку мінімального значення шкоди при цьому має вигляд:

$$\min M\theta_1 = G_i d\left[1 - \exp\left(-dz\right)\right] + C_i \Delta T_{ki} \exp\left(-dz\right),$$

з якого її легко розрахувати при відомих значеннях.

Цікавим є результат пошуку оптимального значення тривалості контролю ΔT_{ki}.

Неважко показати, що точка:

$$\Delta T_{ki} = \frac{\left[\left(2G_i T_{ki} z + \left(C_i - C_i T_{ki} z\right)\right)\right]}{\left[z_z\left(G_i - C_i\right)\right]} = \Delta T_{ki0\,pt}$$

є точкою максимуму шкоди. При цьому оптимальне значення тривалості контролю перевищує значення тривалості його періоду $\Delta T_{ki0\,pt} > T_{ki}$. Таке значення тривалості контролю є неможливим, але цей факт дозволяє зробити наступний, важливий для практики висновок: на інтервалі від $\Delta T_{ki} = 0$ до $\Delta T_{ki} = \Delta T_{ki0\,pt}$ значення шкоди із збільшенням ΔT_{ki} зростає, або чим меншим є значення тривалості контролю ΔT_{ki} тим меншим є значення шкоди у вигляді (3). Іншими словами, при побудові, проектуванні

чи виборі засобів ТЗІ перевагу слід віддавати таким засобам, які мають найменший час виконання операцій контролю.

Пошук екстремуму цільової функції (4) по результуючій інтенсивності загроз z призводить до висновку, що при надійних (високоефективних) системах управління доступом та виявлення і усунення загроз, коли на інтервал роботи ССП довжиною $(T_{ki} - \Delta T_{ki})$ попадає менше ніж один вплив, який є пропущений системою управління доступом і не виявленим та не усуненим системою контролю, тобто при виразі:

$$(T_{ki} - \Delta T_{ki})\left[\gamma_{ші}(1 - p_{gi}) + \gamma_i\right](1 - p_{ві}) < 1 \qquad (7)$$

величина шкоди є залежною лише від параметрів T_{ki} та ΔT_{ki} і має екстремуми в точках, які є близькими до

$$\Delta T_{ki0\,pt} = T_{ki}, \qquad \Delta T_{ki0\,pt} = T_{ki} / C .$$

Останній результат лише підтверджує вже отримані висновки і, при цьому його цінність полягає хіба що в підтвердженні адекватності моделі реальним процесам, пов'язаним з ТЗІ.

Якщо розглядати вираз (7) як таке обмеження при (4), що при певних умовах [4] перетворюється на окрему цільову функцію, тоді отримаємо важливі для практики вимоги щодо допустимих значень:

1) Тривалості періоду контролю (з урахуванням раніше отриманого результату щодо величини ΔT_{ki} (T_{ki}):

$$T_{ki} < \frac{1}{\left(\gamma_{mi}(1 - p_{gi}) + \gamma_i\right)(1 - p_{ві})}. \qquad (8)$$

2) Або щодо результуючої інтенсивності впливів загроз

$$\left[\gamma_{ші}(1 - p_{gi}) + \gamma_i\right](1 - p_{ві}) < \frac{1}{T_{ki}}. \qquad (9)$$

Умова (8) дозволяє визначити вимоги щодо тривалості періоду контролю T_{ki} при відомих інтенсивностях загроз γ_i, $\gamma_{ші}$ та реалізованих в системі ТЗІ ймовірностях p_{gi} та $p_{ві}$.

В свою чергу, умова (9) при заданій тривалості періоду контролю T_{ki} дозволяє визначити вимоги щодо таких параметрів системи ТЗІ як ймовірності p_{gi} та $p_{ві}$ при відомих інтенсивностях загроз γ_i, $\gamma_{ші}$.

З виразу (4) можна отримати значення екстремумів цієї ж функції і по будь-яким іншим параметрам неоперативного управління.

Висновки

Таким чином, розглянуті положення, які дозволяють сформулювати чи отримати цілу низку надзвичайно важливих для вирішення задачі захисту інформаційних ресурсів ССП: умов, обмежень та оптимальних значень найбільш загальних параметрів системи захисту, але не дають змоги сформулювати більш конкретні вимоги щодо складу та параметрів системи захисту чи її складових.

Список літератури

1. Основи надійності інформаційних систем [Текст] : підручник / С.М. Головань [та ін.]. — Луганськ : Ноулідж, 2012. — 334 с.
2. ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт [Текст] = Техническая защита информации. Порядок проведения работ : стандарт. — Введ. с 1997-07-01. — К. : Держстандарт України, 1997. — 27 с.
3. Василенко, В.С. Оцінювання ризиків безпеці інформації в локальних обчислювальних мережах *[Електронний ресурс]* / В.С. Василенко, О.С. Бордюк, С.М. Полонський. — Режим доступу: http://www.rusnauka.com/11_EISN_2010/Informatica/64068.doc.htm (Дата звернення 14.03.2013 р.)
4. Справочник по вероятностным расчетам [Текст] / Г.Г. Абезгауз [и др.]. — 2-е изд., испр. и доп. — М. : Воениздат, 1970. — 536 с.
5. Відновлення та оптимізація інформації в системах прийняття рішень [Текст] : підруч. для студ. вищ. навч. закл., які навч. за напрямом «Інформаційна безпека» / В.Л. Баранов [та ін.] ; Державний ун-т інформаційно-комунікаційних технологій. — К. : ДУІКТ, 2009. — 132 с.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ СИСТЕМ ЗАЩИТЫ В СЕТЯХ ПЕРЕДАЧИ ИНФОРМАЦИИ

В.А. Хорошко, Ю.Е. Хохлачева

Национальный авиационный университет,
просп. Космонавта Комарова, 1, Киев, 03058, Украина; e-mail: professor_va@ukr.net

В данной статье рассмотрены положения, позволяющие сформулировать или получить ряд важнейших для решения задачи защиты информационных ресурсов систем специального назначения: условий, ограничений и оптимальных значений наиболее общих параметров системы защиты.

Ключевые слова: защита информации, системы защиты, сети передачи информации, защите информационных ресурсов

OPTIMIZATION OF PARAMETERS FOR DEFENCE SYSTEMS IN DATA TRANSMISSION NETWORK

Vladimir O. Khoroshko, Yulia E. Khokhlachova

National Aviation University,
1 Kosmonavta Komarova Ave., Kyiv, 03058, Ukraine; e-mail: professor_va@ukr.net

This article discusses provisions that allow to formulate or to get a number of extremely important conditions, constraints, and the optimal values of the most common parameters of protection for solving the problem of protecting information resources in special use systems.

Keywords: information security, security systems, data transmission network, protection of information resources