УДК 681.3.06

ЗАДАЧА ОПТИМАЛЬНОГО СИНТЕЗУ СТРУКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ З МІНІМАЛЬНОЮ ВАРТІСТЮ ТА НЕОБХІДНИМ РІВНЕМ ЗАХИЩЕНОСТІ ІКС

І.В. АЛЕКСАХІНА, О.М. НОВІКОВ, А.М. РОДІОНОВ

Розглянуто задачу синтезу системи захисту інформації з оптимальними властивостями, а саме задачу синтезу структури системи захисту інформації з необхідним рівнем захищеності інформації та мінімальною вартістю системи захисту. У якості екстремального критерію використовується економічний показник (мінімізація вартості системи захисту), а обмеженням є фіксований рівень захищеності інформації. Для розв'язку зазначеної задачі запропоновано метод із використанням логіко-імовірнісного підходу. На його основі будується функція ймовірності успішності атаки, яка враховує структуру інформаційно-комунікаціної системи. У результаті отримаємо задачу нелінійної дискретної оптимізації булевого типу, для розв'язку якої застосовується метод меж та гілок. Працездатність та ефективність запропонованого методу показано за допомогою чисельного експерименту на модельному прикладі інформаційно-комунікаціної системи

ВСТУП

Під час проектування та побудови інформаційно-комунікаційних систем (ІКС) часто виникають задачі, пов'язані з необхідністю забезпечення низки технічних характеристик системи (пропускна здатність, кількість користувачів працюючих одночасно, рівень SLA, надійність та відмовостійкість тощо) за обмежень на вартість системи. До подібних технічних характеристик також відноситься і рівень захищеності ІКС, який забезпечується за допомогою системи захисту інформації. Цей рівень залежить від вартості системи захисту інформації, але ця залежність не є строго пропорційною.

У зв'язку з цим, під час створення системи захисту інформації, виникає низка задач пов'язаних з пошуком оптимального співвідношення між рівнем захищеності системи та вартістю системи захисту. Такі задачі належать до задач синтезу систем захисту інформації з оптимальними властивостями, для розв'язку яких успішно використовуються методи математичного програмування, пов'язані з пошуком екстремуму одного з критеріїв, показників.

У випадку інформаційно-комунікаційних систем в якості екстремальних критеріїв можна застосовувати економічні показники, які визначаються вартістю механізмів захисту, затратами на подолання наслідків вдалих атак

зловмисників та іншими затратами на функціонування ІКС. До таких задач відносяться структурний синтез та синтез параметрів системи захисту інформації з оптимальними економічними показниками. Також розглядають задачі визначення екстремальних показників надійності інформаційно-комунікаційних систем (задачі структурного синтезу та синтезу параметрів системи захисту інформації з оптимальним рівнем захищеності інформації) [1–3].

Серед наведених вище задач важливою є задача визначення структури механізмів захисту, яка б забезпечувала необхідний рівень захищеності ІКС відносно максимально можливого (згідно концепції прийнятного ризику [4]), при цьому мінімізуючи сукупну вартість системи захисту інформації.

Подібну задачу розв'язано у статтях [3, 5], але розглянуто лише показники надійності інформаційно-комунікаційних систем, без урахування вартісної складової. У роботі [6] розглядається задача синтезу систем захисту інформації з мінімальною вартістю механізмів захисту, де в якості технологічних обмежень використовується залишковий ризик в ІКС, проте наведена функція захищеності не враховує топологію ІКС.

Враховуючи наведене вище, актуальною є задача синтезу структури системи захисту інформації, за умови забезпечення необхідного рівня захищеності інформаційно-комунікаційної системи та мінімальної вартості системи захисту інформації, з урахуванням топології ІКС.

Мета роботи — розробка методу та алгоритму для розв'язку задачі оптимального розміщення механізмів захисту, які б мінімізували сукупну вартість системи захисту інформації та забезпечували б необхідний рівень захищеності ІКС.

ОСНОВНІ ЗАДАЧІ СИНТЕЗУ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ З ОПТИМАЛЬНИМИ ВЛАСТИВОСТЯМИ

Задачі синтезу систем захисту можуть розв'язуватися з використанням математичної теорії оптимізації, теорії системного аналізу та прийняття рішень [7]. Для формалізації задачі синтезу та пошуку її оптимального розв'язку, вводяться додаткові кількісні вимоги до якості побудови та функціонування системи захисту інформації у вигляді критеріїв якості та систем обмежень, які включають математичну модель. Тоді розв'язок задачі здійснюється шляхом пошуку екстремуму критерію якості з використанням методів математичного програмування.

Для формалізації задач синтезу систем захисту введемо деякі позначення. Представимо систему захисту як набір механізмів захисту, які позначимо через M, що характеризуються деяким параметром міцності K, і мають відповідну вартість C_M. В якості характеристики захищеності системи візьмемо деякий функціонал $F(M,K)$, що залежатиме від обраної структури механізмів захисту M та їх коефіцієнтів міцності K. Нехай $F_1(M,K)$ — деякий функціонал, який буде характеризувати вартісну (економічну) складову системи захисту. У найпростішому випадку цей функціонал буде визначатись як сумарна вартість обраних механізмів захисту $F_1(M,K)=\sum_i C_{M_i}$. Таке представлення відповідає моделі безпеки з повним

перекриттям (модель Клементса-Хофмана [8]). Ще одне необхідне позначення: F^* — фіксований рівень захищеності інформації.

Розрізняють декілька постановок задач синтезу систем захисту інформації, які враховують екстремальні показники надійності, економічні показники та інші критерії оптимальності. В табл. 1 наведено задачі оптимального синтезу систем захисту, можливі критерії якості та обмеження для зазначених задач. Крім того, представлено формальний запис задач синтезу системи захисту.

Таблиця 1. Задачі оптимального синтезу системи захисту

Класи задач оптимального синтезу	**Критерій**	**Обмеження**	**Формальний запис**
Синтез структури системи захисту інформації	Максимізація технологічного показника рівня захищеності	Фіксована вартість системи захисту інформації	$\begin{cases} F(M,K) \to \max \\ F_1(M,K) \le C_M^M \end{cases}$
	Мінімізація вартості системи захисту	Фіксований рівень захищеності інформації	$\begin{cases} F(M,K) \ge F^* \\ F_1(M,K) \to \min\limits_M \end{cases}$
Синтез параметрів системи захисту інформації	Максимізація технологічного показника рівня захищеності	Фіксована вартість системи захисту інформації	$\begin{cases} F(M,K) \to \max \\ F_1(M,K) \le C_M^K \end{cases}$
	Мінімізація вартості системи захисту	Фіксований рівень захищеності інформації	$\begin{cases} F(M,K) \ge F^* \\ F_1(M,K) \to \min\limits_K \end{cases}$

Також можуть бути комбіновані задачі структурного та параметричного синтезу. Тоді у ролі критеріїв та обмежень використовуються комбіновані показники.

Розглянемо задачу синтезу структури системи захисту інформації з мінімальною вартістю та фіксованим рівнем захищеності інформації більш детально.

ФУНКЦІЯ ЙМОВІРНОСТІ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ ІКС

ІКС є одним із видів структурно-складної системи. Тому для вирішення задачі оцінювання рівня захищеності ІКС та захищеності її об'єктів, з урахуванням топології та можливих шляхів доступу до неї зловмисників, використаємо логіко-ймовірнісний метод, запропонований та розвинутий академіком І.О. Рябініним [9].

Одними з основних понять логіко-ймовірнісної теорії безпеки є поняття небезпечного стану системи й відповідної логічної функції, що представляє розвиток цього небезпечного стану і описується функцією небезпечного стану (ФНС). У випадку ІКС розвиток небезпечного стану буде визначатися послідовністю дій або подій, які можуть вплинути на рівень захищеності об'єктів, що оцінюються, і будуть являти собою сценарій атак. Якщо зловмиснику вдасться успішно виконати усі дії зі сценарію атаки, тоді можна говорити про її успішність.

Таким чином, для оцінювання рівня захищеності об'єктів ІКС, послідовність дій зловмисника та всі шляхи, якими він може отримати доступ до об'єктів системи будуть формувати сценарії атак або ФНС логіко-ймовірнісної теорії. При цьому сценарій атаки становить кон'юнкцію подій Z_i, жодну з яких не можна вилучити не порушивши небезпечного функціонування системи. Таку кон'юнкцію можна записати у вигляді функції алгебри логіки (ФАЛ):

$$\varphi_l = \bigwedge_{i \in K_{\varphi l}} Z_i, \tag{1}$$

де K_{φ_l} — послідовність дій зловмисника у ІКС, що приводить до небезпечного стану визначеного об'єкта системи, яка відповідає *l-тому* сценарію атаки;

$$Z_i = \begin{cases} 1, \text{ якщо об'єкт } v_i \text{ захоплено,} \\ 0, \text{ якщо об'єкт } v_i \text{ незахоплено.} \end{cases}$$

Отже, для об'єкту v_i ІКС можна записати можливі атаки у вигляді ФАЛ та подій Z_j (де $j \in K_{\varphi_i}$) за допомогою операцій кон'юнкції та диз'юнкції:

$$y_i(Z_1,...,Z_m) = \bigvee_{l=1}^{d} \varphi_l = \bigvee_{l=1}^{d} \left(\bigwedge_{i \in K_{\varphi l}} Z_i \right), \tag{2}$$

де $d = \left| K_\varphi \right|$ — кількість сценаріїв атаки від джерел атак A для об'єкту v_i.

При умові, що булева функція $y_i(Z_1,...,Z_m) = 1$, можна говорити про успішність здійснення атаки на об'єкт v_i.

Згідно з логіко-ймовірнісною теорією, ймовірність переходу об'єкта v_i ІКС до небезпечного стану буде визначатись як ймовірність того, що функція алгебри логіки (2) буде дорівнювати:

$$P\{y_i(Z_1,...,Z_m) = 1\} = P\left\{ \bigvee_{l=1}^{d} \left(\bigwedge_{i \in K_{\varphi l}} Z_i \right) = 1 \right\},$$

де Z_i — події, які необхідні виконати зловмиснику для здійснення атаки,

$$Z_i = \begin{cases} 1, & i \text{ - та подія відбулась,} \\ 0, & i \text{ - та подія не відбулась;} \end{cases}$$

K_{φ_l} — послідовність дій зловмисника, що приводить до небезпечного стану визначеного об'єкта системи, яка відповідає *l*-му сценарію атаки; d — скінченний набір сценаріїв атак.

Значення функції $P\{y_i(Z_1,...,Z_m) = 1\}$ буде визначати ймовірність реалізації хоча б одного зі сценаріїв атак для об'єкту v_i.

Маючи ймовірність здійснення кожної з подій Z_i, можна обчислити ймовірність $P\{y(Z_1,...,Z_m) = 1\}$, де $P\{Z_i = 1\} = P_i$ — ймовірності захоплення об'єктів.

Для цього необхідно перетворити функцію алгебри логіки (2) у еквівалентну їй ортогональну диз'юнктивну нормальну форму. Для функції, представленої в такій формі, можна виконати пряме заміщення булевих змінних Z_i на їх ймовірнісні значення:

$$P\{y_i(Z_1,...,Z_N)=1\}=P(P_1,...,P_N). \qquad (3)$$

Таким чином, для кожного з об'єктів ІКС може бути побудовано функцію ймовірності, яка визначатиме рівень захищеності об'єкта v_i ІКС і буде залежати від ймовірностей захоплення проміжних об'єктів, що входять до сценарію атак.

Отже, функція ймовірності успішності атаки інформаційно-комунікаційної системи дозволяє визначити ймовірність переходу ІКС до небезпечного стану, враховує топологію мережі, множину об'єктів атак, множину джерел загроз та ймовірності захоплення кожного з об'єктів ІКС, сценарії атак та механізми захисту. Цю функцію було запропоновано в роботі [10]:

$$P\{y(Z_1,...,Z_m)=1\}\to P(P_1,...,P_N)\to P(P_1,...,P_N;M_1K_1,...,M_NK_N).$$

Використаємо отриману функцію, у якості цільової для синтезу структури системи захисту інформації з необхідним рівнем захищеності ІКС та мінімальною вартістю системи захисту інформації.

ПОСТАНОВКА ЗАДАЧІ ОПТИМАЛЬНОГО СИНТЕЗУ СТРУКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ З МІНІМАЛЬНОЮ ВАРТІСТЮ СИСТЕМИ ЗАХИСТУ ТА НЕОБХІДНИМ РІВНЕМ ЗАХИЩЕНОСТІ ІКС

Ця задача полягає у знаходженні оптимального розміщення механізмів захисту M_i, які б мінімізували сукупну вартість системи захисту інформації та забезпечували б значення функції ймовірності успішності атаки не більше деякого порогового значення $P_{\text{необх}}$:

$$\begin{cases} C=\sum\limits_i C_iM_i\to\min\limits_M; \\ P(P,M,K)=P(M_1,...,M_N)\le P_{\text{необх}}, \end{cases}$$

де $P_i\in[0,1]$ — ймовірність захоплення об'єктів; $M_i\in\{0,1\}$ — наявність або відсутність механізму захисту; $K_i\in[0,1]$ — коефіцієнт міцності відповідного механізму захисту M_i; C_i — вартість відповідного механізму захисту M_i.

В якості вхідних даних задачі оптимального розміщення механізмів захисту мають подаватись такі множини:

- множина ймовірностей захоплення об'єктів системи $P=\{P_1,P_2,...,P_N\}$, де $P_i\in[0,1]$ — ймовірність захоплення;
- множина механізмів захисту зі значенням їхньої міцності та вартості $M=\{M_1,M_2,...,M_N\}$, де $M_i\in\{0,1\}$ — факт наявності або відсутності механізму захисту.

Крім цього, кожен механізм захисту M_i буде мати такі характеристики:

- міцність механізму захисту — $K_i \in [0,1]$;
- вартість механізму захисту — $C_{M_i} \geq 0$.

Наведена задача належить до класу задач математичного програмування, які в загальному вигляді формулюються наступним чином:

$$f(X) \to \min_X$$

за обмеженнь:

$$h_i(X) = 0,\ i = 1,...,m,$$

$$g_i(X) \leq 0,\ i = m+1,...,p.$$

Виходячи з того, що множина механізмів захисту M є скінченою, то ця оптимізаційна задача буде відноситись до задач дискретного програмування, загальний вигляд яких [11]:

$$f(x_1, x_2, ..., x_n) \to \min_X$$

за обмежень

$$g_1(x_1, x_2, ..., x_n) \leq 0;$$

$$\cdots$$

$$g_m(x_1, x_2, ..., x_n) \leq 0;$$

$$X = [x_1, x_2, ..., x_n] \in D,$$

де D — скінченна або злічена множина. Якщо $D \subset Z^n$ — маємо задачу цілочисельної оптимізації, при $D \subset B^n$ маємо частковий випадок — булеву оптимізацію.

Якщо одна з функцій $f(x_1, x_2, ..., x_n)$ або $g_i(x_1, x_2, ..., x_n)$ не буде лінійною, тобто не може бути представленою у вигляді $f(x) = \sum_{i=1}^{n} c_i x_i$, то оптимізаційна задача буде відноситись до задач нелінійної дискретної оптимізації.

Методи розв'язання задач дискретного програмування поділяються на точні та наближені методи. Обчислювальні труднощі розв'язку реальних прикладних задач з великою розмірністю та специфічними обмеженнями змушують звертатися до алгоритмів пошуку наближених розв'язків (метод локальної оптимізації, випадкового пошуку в області допустимих розв'язків та евристичні методи). Однак наближені методи мають недолік: вони не гарантують знаходження оптимального розв'язку та в більшості випадків не дозволяють оцінити відхилення наближеного розв'язку від оптимального [12].

Найбільш розповсюдженими точними методами для розв'язку задач дискретної оптимізації є методи, які реалізують схему послідовного аналізу варіантів, метод гілок і меж, та метод відсікаючих площин [13]. Однак останній використовується для розв'язку тільки цілочислених задач і часто викликає обчислювальні труднощі при необхідності порівняння сили відсі-

кань. При цьому методи послідовного аналізу варіантів та метод меж та гілок є доволі універсальними.

Зупинимось детальніше на методі меж та гілок. Цей метод вперше було запропоновано Лендом та Дойгом [14]. В його основі ідея послідовного розбиття множини допустимих розв'язків на підмножини. На кожному кроці елементи розбиття перевіряються для з'ясування, чи має ця підмножина оптимального розв'язку. Розглянемо цей метод детальніше [12].

Нехай маємо задачу дискретної оптимізації у вигляді: $\min\{f(x)\big|x\in\Omega_f\}$, де Ω_f — скінченна множина допустимих розв'язків. Введемо скінченну множину $\Omega\supseteq\Omega_f$, елементи якої назвемо розв'язками. Множина Ω необхідна для того, щоб полегшити застосування методів меж та гілок та позбавитись від найбільш жорстких обмежень, що задають Ω_f.

Головними операціями методів меж та гілок є операції розгалуження та обчислення меж.

Розгалуження. Припускається, що існує функція β, яка визначається на сукупності H всіх підмножин множини Ω. Розбиття множини розв'язків Ω за допомогою правила розгалуження β породжує розбиття множини допустимих розв'язків Ω_f на підмножини $\Omega_f^i=\Omega^i\cap\Omega_f$. Множини, що зустрічаються у процесі послідовного розгалуження Ω, впорядковані по включенню, і цей зв'язок між ними можна зобразити у вигляді дерева підмножин розв'язків (H,U) із коренем, що відповідає множині Ω, та висячими вершинами, які відповідають одноелементним множинам.

Найбільш розповсюдженими є два правила розгалуження. Перше правило пов'язане із розбиттям за деякою ознакою множини розв'язків Ω^i на дві множини, що не перетинаються: $\overline{\Omega^i}$ та її доповнення $\overline{\overline{\Omega^i}}$. Інше правило реалізовує так зване покомпонентне розгалуження, яке відбувається за рахунок фіксування значень змінних. У такому випадку кожний шлях від кореня до деякої вершини відповідає частковому розв'язку.

Обчислення меж. Використовуються два типи меж: нижня границя (оцінка) для значень $f(x)$ на кожній з підмножин допустимих розв'язків $\Omega_f^i=\Omega^i\cap\Omega_f$, що отримуємо в процесі розгалуження; верхня межа (рекорд) для оптимального значення функції $f(x)$ на Ω_f.

Оцінкою є функція $\gamma(\Omega^i)$, що задається на H та має такі властивості:

а) $\gamma(\Omega^i)\le f(x)$ при всіх $x\in\Omega_f^i$;

б) $\gamma(\Omega^i)=f(x)$, якщо $|\Omega^i|=1$ та $\Omega^i=\Omega_f^i=\{x\}$;

в) $\gamma(\Omega^i)=+\infty$, якщо $|\Omega^i|=1$ та $\Omega^i\cap\Omega_f=\varnothing$.

Останні дві умови визначають функцію $\gamma(\Omega^i)$ на одноелементних множинах Ω^i.

Рекордом є функція $f^*(h_k)$, яка визначається для будь-якої сукупності (списку) h_k підмножин Ω^i та задовольняє співвідношенням:

а) $f^*(h_k) \geq \min\{f(x) | x \in \Omega_f\}$;

б) $f^*(h_k) \leq f(x)$, якщо $\Omega^i_f = \Omega^i = \{x\} \in h_k$.

Остання умова гарантує, що $f^*(h_k)$ не більше значення цільової функції на найкращому допустимому розв'язку, який відповідає «висячій» вершині з h_k.

Допустимий розв'язок x^*_k, що має властивість $f(x^*_k) = f^*(h_k)$, називається рекордним. Рекорд характеризує наближення до оптимального розв'язку. Саме тому важливо вдало вибрати початковий рекордний розв'язок x^*_0.

Метод меж та гілок у процесі послідовного розгалуження множини Ω виключає ті підмножини, про які стало відомо, що вони не містять допустимих розв'язків, які були б краще за рекордний. Виключення здійснюється за допомогою елімінуючого тесту, заснованого на обчисленні оцінок. Основним таким тестом є: якщо для деякої множини $\Omega^i \in h_k$ справедлива нерівність $\gamma(\Omega^i) \geq f^*(h_k)$, то множину Ω^i виключаємо із сукупності h_k. Проте для різних задач можливі різні тести, засновані на необхідних умовах оптимальності.

Схема методу меж та гілок має наступний вигляд. Нехай $h_0 = \{\Omega\}$, $f^*_0 = f^*_0(h_0) = +\infty$. Спільний k-й крок $(k = 1, 2, \ldots)$:

1. **Аналіз списку.** Якщо список h_{k-1} порожній, робота завершується, при цьому якщо $f^*_{k-1} < +\infty$, рекордний розв'язок є оптимальним. Інакше, вихідна задача не має допустимих розв'язків.

2. **Вибір кандидата.** Вибрати зі списку h_{k-1} одну з підмножин (кандидата). Якщо відомо оцінку $\gamma(\Omega^k)$, то перейти до п. 4, інакше — до п. 3.

3. **Аналіз кандидата.** Обчислити оцінку $\gamma(\Omega^i)$. При цьому можуть стати відомими допустимі розв'язки, тому необхідно оновити дані щодо рекорду. Отже, нехай X_k — множина допустимих розв'язків, отриманих при аналізі кандидата. Тоді $f^*_k = \min\{f^*_{k-1}, \min\limits_{x \in X_k} f(x)\}$ та рекордний розв'язок x^*_k є допустимим розв'язком, на якому досягається зазначений мінімум. Перевіряємо основний тест. Якщо нерівність тесту стверджується, то виключаємо зі списку h_{k-1} множину Ω^k, поклавши $h_k = h_{k-1} \setminus \Omega^k$, та переходимо до кроку $(k+1)$. Якщо ж нерівність не стверджується, то або необхідно змінити спосіб обчислення оцінки, або спробувати інші тести. У випадку, якщо після використання всіх тестів множина Ω^k не була виключена, то перейти до п. 4.

4. **Розгалуження.** Згідно правилу β, здійснити розбиття Ω_k, сформулювати список: $h_k = h_{k-1} \setminus \Omega^k \cup \beta(\Omega^k)$ та перейти до наступного кроку.

Скінченність алгоритму, побудованого за цією схемою, випливає зі скінченності множини Ω, припущень б) та в) з визначення оцінки та припущення б) у визначенні рекорду.

МОДЕЛЬНИЙ ПРИКЛАД

В якості прикладу використаємо невелику корпоративну мережу стандартної архітектури (рис. 1). В цьому випадку маємо сім об'єктів ($V = \{v_1, ..., v_7\}$) джерела атаки: $A = \{v_1, v_5\}$ та множина об'єктів атаки: $O = \{v_3, v_7\}$.

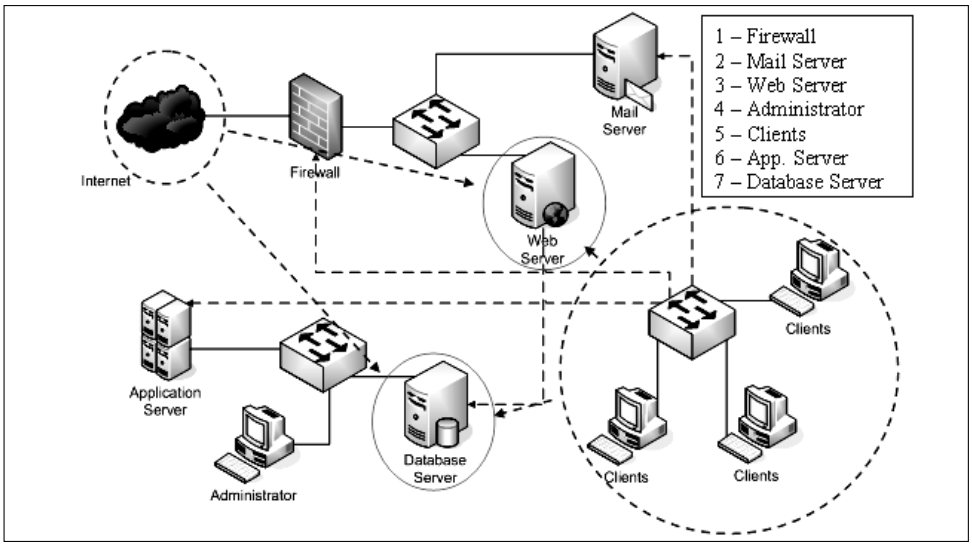

Рис. 1. Схема мереж ІКС

В табл. 2 наведено загрози об'єктів інформаційно-комунікаційної системи, а також відповідні значення ймовірностей реалізації цих загроз.

Таблиця 2. Загрози об'єктів ІКС та ймовірності їх реалізації

Об'єкти		P		**Загрози**
v_1	Firewall	P_1	0,2	Знаходження помилки у налаштуваннях
v_2	Mail Server	P_2	0,5	Зараження вірусом
v_3	Web Server	P_{31}	0,6	SQL ін'єкція або Cross Site Scripting (XSS)
		P_{32}	0,6	Перехоплення сесії
		P_{33}	0,9	Сканування портів та знаходження вразливостей
v_4	Administrator	P_4	0,2	Підбір паролю адміністратора
v_5	Clients	P_{51}	0,5	Підбір паролю користувача
		P_{52}	0,9	Зараження вірусом
v_6	Application Server	P_6	0,6	Слабка авторизація
v_7	Database Server	P_7	0,8	Слабкий пароль

Для такої топології мережі за допомогою логіко-ймовірнісного методу було отримано наступну функцію ймовірності успішності атаки [15]:

$$P(K) = P_1(1 - K_1M_1)P_{33}(1 - K_{33}M_{33}) +$$

$$+ P_1(1-K_{11}M_{11})P_{32}(1-K_{32}M_{32}) * (1-P_{33}(1-K_{33}M_{33})) +$$

$$+ P_1(1-K_1M_1)P_{31}(1-K_{31}M_{31})(1-P_{32}(1-K_{32}M_{32}))(1-P_{33}(1-K_{33}M_{33})) +$$

$$+ (1-P_1(1-K_1M_1))P_{52}(1-K_{52}M_{52})P_6(1-K_6M_6)P_7(1-K_7M_7) +$$

$$+ P_1(1-K_1M_1)(1-P_{31}(1-K_{31}M_{31}))(1-P_{32}(1-K_{32}M_{32}))(1-P_{33}(1-K_{33}M_{33}))\times$$

$$\times P_{52}(1-K_{52}M_{52})P_6(1-K_6M_6)P_7(1-K_7M_7) +$$

$$+ (1-P_1(1-K_1M_1))P_{51}(1-K_{51}M_{51})(1-P_{52}(1-K_{52}M_{52}))P_6(1-K_6M_6)\times$$

$$\times P_7(1-K_7M_7) + P_1(1-K_1M_1)(1-P_{31}(1-K_{31}M_{31}))P_{51}(1-K_{51}M_{51})\times$$

$$\times (1-P_{32}(1-K_{32}M_{32}))(1-P_{33}(1-K_{33}M_{33}))\times$$

$$\times (1-P_{52}(1-K_{52}M_{52}))P_6(1-K_6M_6)P_7(1-K_7M_7).$$

Для цієї функції обчислюємо мінімальне значення функції ймовірності успішності атаки, припустивши, що наявні всі механізми захисту з максимальними значеннями відповідних коефіцієнтів міцності. За таких умов отримаємо мінімальне значення ймовірності успішності атаки $P^* = 0.$

Нехай необхідним та достатнім рівнем захищеності системи буде значення, що складає 80% від значення, що відповідає стану максимальної захищеності системи. Тоді, прийнявши $\lambda = 0{,}8,$ отримаємо допустиме значення ймовірності незахищеності системи $P_{\text{необх}} = 1-\lambda(1-P^*) = 0{,}2.$

З урахуванням необхідного рівня захищеності ІКС, вартості кожного з механізмів захисту та необхідності мінімізувати сукупну вартість системи захисту, маємо наступну оптимізаційну задачу, що відноситься до класу задач нелінійної дискретної оптимізації булевого типу:

$$P(K) = P_1(1-K_1M_1)P_{33}(1-K_{33}M_{33}) + P_1(1-K_1M_1)P_{32}(1-K_{32}M_{32})\times$$

$$\times (1-P_{33}(1-K_{33}M_{33})) + P_1(1-K_1M_1)P_{31}(1-K_{31}M_{31})(1-P_{32}(1-K_{32}M_{32}))\times$$

$$\times (1-P_{33}(1-K_{33}M_{33})) + (1-P_1(1-K_1M_1))P_{52}(1-K_{52}M_{52})P_6(1-K_6M_6)\times$$

$$\times P_7(1-K_7M_7) + P_1(1-K_1M_1)(1-P_{31}(1-K_{31}M_{31}))(1-P_{32}(1-K_{32}M_{32}))\times$$

$$\times (1-P_{33}(1-K_{33}M_{33}))P_{52}(1-K_{52}M_{52})P_6(1-K_6M_6)P_7(1-K_7M_7) +$$

$$+ (1-P_1(1-K_1M_1))P_{51}(1-K_{51}M_{51})\times$$

$$\times (1-P_{52}(1-K_{52}M_{52}))P_6(1-K_6M_6)P_7(1-K_7M_7) +$$

$$+ P_1(1-K_1M_1)(1-P_{31}(1-K_{31}M_{31}))P_{51}(1-K_{51}M_{51})(1-P_{32}(1-K_{32}M_{32}))\times$$

$$\times (1-P_{33}(1-K_{33}M_{33}))(1-P_{52}(1-K_{52}M_{52}))P_6(1-K_6M_6)P_7(1-K_7M_7)\times$$

$$\times C_1M_1 + C_{31}M_{31} + C_{32}M_{32} + C_{33}M_{33} + C_{51}M_{51} + C_{52}M_{52} +$$

$$+ C_6M_6 + C_7M_7 \to \min_M.$$

Також задамо значення коефіцієнтів міцності для механізмів захисту та вартість кожного з них. Ці дані наведено в табл. 3.

Таблиця 3. Вартість та значення коефіцієнтів міцності для механізмів захисту

M / K, C	M_1	M_{31}	M_{32}	M_{33}	M_{51}	M_{52}	M_6	M_7
K_i	0,5	0,7	0,3	0,4	0,2	0,1	0,8	0,6
C_i	7	2	3	5	1	4	11	3

Треба зауважити, що вартість застосування механізмів захисту подана в деяких умовних одиницях.

Використаємо для розв'язку поставленої задачі метод меж та гілок. Представимо задачу у вигляді дерева, беручи в якості кореня максимальний набір механізмів захисту, тобто коли всі механізми захисту наявні й $M_i = 1$. На кожному наступному кроці побудови дерева змінюємо одну зі складових набору. Таким чином, на останньому кроці маємо перелік усіх можливих варіантів, яких всього 256. Далі трансформуємо дерево у таблицю, де кожний стовпчик є шляхом від кореня до вершини із найменшим ступенем, тобто до кінцевих вершин, ступінь яких дорівнює одиниці (кожен стовпчик є множиною h_i, впорядкованою у напрямку від кореня).

Далі перевіряємо кожний набір з підмножини h_i. Обчислюємо оцінку $\gamma(\Omega^i)$. У цьому випадку в якості оцінки використовуємо виконання умови $P(M_1,...,M_N) \le P_{\text{необх}}$. Якщо оцінка вже відома (цей набір вже зустрічався в одній з попередніх підмножин), то переходимо до наступного кроку. Якщо умови нерівності виконуються, то з таких наборів формуємо множину розв'язків Ω. У протилежному випадку, якщо нерівність не виконується, то ця множина виключається з множини допустимих розв'язків. Також виключаються $2^p - 1$ наступних множин, де p — кількість наборів з множини h_i, які не були перевірені, оскільки автоматично не містять розв'язку.

Коли сформовано множину розв'язків Ω, то серед її елементів знаходимо оптимальний розв'язок за допомогою основного тесту, а саме: критерій мінімізації сукупної вартості системи захисту інформації, тобто $\sum_i C_i M_i \to \min\limits_M$.

У результаті розв'язку задачі, отримуємо, що оптимальним набором механізмів захисту в цьому випадку є наступний: $M = \{M_1, M_6\}$, тобто $M = \{M_1, M_{31}, M_{32}, M_{33}, M_{51}, M_{52}, M_6, M_7\} = \{1,0,0,0,0,0,1,0\}$. Це означає, що в цьому випадку доцільно використовувати тільки два механізми захисту, а саме: достатньо ретельно перевірити наявність помилок та неправильних налаштувань на міжмережевому екрані та підвищити рівень авторизації на сервері застосувань. При цьому вартість системи захисту буде мінімальною ($C = 18$ умовних одиниць), а рівень захищеності системи буде відповідати заданому, тобто буде становити не менше 0,8 (майже 0,82, тобто значення

ймовірності успішності атаки складає $P = 0{,}181)$ від значення, що відповідає стану максимальної захищеності системи.

Треба також зауважити, що використання методу меж та гілок є ефективним, тому що для отримання результату за допомогою повного перебору всіх можливих комбінацій, необхідно перевірити 256 варіантів. Якщо ж використовувати зазначений метод, то алгоритм зупиняється через 116 кроків, що більш ніж вдвічі швидше за метод повного перебору.

АНАЛІЗ РЕЗУЛЬТАТІВ

У результаті проведених обчислень можна зробити висновок, що для забезпечення необхідного рівня захищеності системи (ймовірність успішності атаки складає $P = 0{,}181)$ достатньо використовувати лише два механізми захисту з восьми. Також, при цьому сукупна вартість системи захисту буде мінімальною.

За відсутності обмеження на вартість системи захисту, можна було б застосувати всі механізми захисту $(M_i = 1)$, причому з максимальним коефіцієнтом міцності. Тоді, значення функції ймовірності успішної атаки стало б мінімальним, тобто $P^* = 0$. Якщо ж не застосовувати жодного з механізмів захисту $(M_i = 0)$, то вартість системи захисту буде дорівнювати нулю, а значення функції ймовірності успішності атаки буде залежати лише від ймовірностей захоплення об'єктів, співпадатиме з функцією ймовірності успішності атаки і буде максимальним — $P = 0{,}56$. Таким чином, бачимо, що використання лише двох зазначених механізмів захисту підвищує рівень захищеності системи на 36%, що є істотним показником.

Чисельний експеримент показав працездатність та ефективність запропонованого методу.

ВИСНОВКИ

У цій роботі розроблено метод та алгоритм для розв'язку задачі оптимального розміщення механізмів захисту, з мінімальною вартістю системи захисту інформації та необхідним рівнем захищеності інформаційно-комунікаційної системи, при цьому враховується топологія ІКС.

Алгоритм було розроблено на основі методу меж та гілок та застосовано для розрахунку структури механізмів захисту для ІКС.

За результатами модельного експерименту було виявлено, що для забезпечення необхідного рівня захищеності достатньо використовувати два механізми захисту. При цьому ймовірність захищеності системи складає 0,819, що на 36% більше у порівнянні із випадком, коли жоден механізм захисту не використовується.

Ефективність методу було продемонстровано за допомогою чисельного прикладу — для пошуку оптимального розв'язку було перевірено менше половини можливих варіантів (116 із 256).

ЛІТЕРАТУРА

1. *Новіков А., Тимошенко А.* Визначення множини механізмів захисту, що забезпечують оптимальний рівень захищеності інформації // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2002. — Вип. 4. — С. 98–105.
2. *Боня Ю.Ю., Новіков О.М.* Синтез системи захисту інформації, оптимальної за рівнем ризику // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2007. — Вип. 1. — С. 26–33.
3. *Новіков О.М., Родіонов А.М., Тимошенко А.О.* Оптимальний синтез параметрів системи захисту інформації // Наукові вісті НТУУ «КПІ». — 2007. — № 4. — С. 146–151.
4. *Концепция* абсолютной безопасности и приемлемого риска. — http://for-engineer.info/general/koncepciya-absolyutnoj-bezopasnosti-i-priemlemogo-riska. html.
5. *Новиков А., Тимошенко А.* Определение множества механизмов защиты, обеспечивающих оптимальный уровень защищенности информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2002. — Вип. 4. — С. 98–105.
6. *Боня Ю.Ю., Новиков А.Н.* Синтез систем защиты информации с минимальной стоимостью механизмов защиты информации // Проблемы управления и информатики. — 2006. — № 3. — С. 147–156.
7. *Грайворонський М.В., Новиков О.М.* Безпека інформаційно-комунікаційних систем — К.: BHV, 2009. — 608 с.
8. *Хоффман Л.Д.* Современные методы защиты информации. — М.: Советское радио, 1980. — 286 с.
9. *Рябинин И.А.* Надежность и безопасность структурно-сложных систем. — СПб: Политехника, 2000. — 248 с.
10. *Родіонов А.М., Новіков О.М.* Логіко-імовірнісна модель захищеності компонентів інформаційно-комунікаційних систем // Інформаційні технології та комп'ютерна інженерія. — 2008. — № 1. — С. 170–175.
11. *Зайченко Ю.П.* Дослідження операцій. — К.: Слово. — 2001. — 688 с.
12. *Ковалев М.М.* Дискретная оптимизация. Целочисленное программирование. — М.: Едиториал УРСС, 2003. — 192 с.
13. *Сергиенко И.В*. Математические модели и методы решения задач дискретной оптимизации. — К.: Наук. Думка, 1988. — 472 с.
14. *Land A.H., Doig A.G.* An autmatic method of solving discrete programming problems // Econometrica. — 1960. — **28**. — P. 497–520.
15. *Родіонов А.М.* Логіко-ймовірнісний підхід до побудови захищених інформаційно-комунікаційних систем: автореф. дис. канд. техн. наук: 05.13.21: захист 14.06.11 / Нац. техн. ун-т. України «КПІ» — К., 2011. — 24 с.

Надійшла 12.03.2013