УДК 681.3.004

РОЗПОДІЛ РЕСУРСІВ У БАГАТО РУБІЖНІЙ СИСТЕМІ ЗАХИСТУ

Володимир Хорошко, Юлія Ковальова, Дмитро Плус*
Національний авіаційний університет України
**МВС України*

Анотація: **Розглянуто методи розподілу ресурсів у багато рубіжній системі захисту інформації.**
Summary: **In work the methods of distribution of resources in much boundary system of protection of the information are considered.**
Ключові слова: **Система захисту інформації, ресурс, розподіл ресурсів.**

I Вступ

Метою захисту інформації є діяльність, спрямована на запобігання витоку інформації різними каналами і їх блокування.

Захист містить у собі визначення можливих каналів витоку інформації, оцінку важливості самої інформації і розробку заходів щодо запобігання її витоку і розкраданню.

Визначення потенційної цінності інформації дозволяє замислитись, у першу чергу, про безпеку найбільш важливих секретів, витік яких здатен завдати шкоди.

Тому об'єктом технічного захисту і є інформація, щодо якої чинний Закону України "Про інформацію", або конфіденційна інформація, передана державі в володіння чи використання. Виходячи з цього, визначається мета захисту, якою є запобігання витоку чи порушенню цілісності інформації [2]. Вона може бути досягнута побудовою комплексної системи технічного захисту інформації (СТЗІ), що являє собою організовану сукупність методів і засобів забезпечення захисту інформації.

Технічний захист інформації забезпечується застосуванням захищених програм і технічних засобів забезпечення інформаційної діяльності, програмних і технічних засобів захисту інформації (ТЗІ) і засобів контролю, що мають сертифікат, відповідний вимогам нормативних документів з технічного захисту, а також застосуванням спеціальних технічних споруджень, засобів і систем. При цьому засоби, ТЗІ можуть функціонувати автономно, або разом з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв, або вбудованих у них складних елементів [2].

Оперативне рішення задач ТЗІ досягається організацією керування системою захисту інформації, для чого необхідно [3]:

- вивчати й аналізувати технологію проходження інформації в процесі інформаційної діяльності;
- оцінювати схильність інформації впливу загроз у конкретний момент часу;
- оцінювати очікувану ефективність застосування засобів забезпечення ТЗІ;
- визначати додаткову потребу в засобах забезпечення ТЗІ;
- здійснювати збір, обробку і реєстрацію даних, що відносяться до захисту інформації;
- розробляти і реалізовувати пропозиції з коректування СТЗІ в цілому, або окремих її елементів.

II Основні положення

Основи стратегії захисту інформації при загальному підході – це вибір основних і найбільш важливих базових системно-концептуальних положень і орієнтирів при плануванні, розробці і реалізації цієї стратегії. Центральним питанням управлінського рішення стратегічного характеру є оцінка обсягу необхідних ресурсів захисту та їх оптимальний, або найбільше розподіл не тільки необхідного, але і неперервного адаптивно-керівного рівня гарантованого захисту. Гарантованість захисту – вимога дуже серйозна як з практичних, так і з теоретичних позицій. Про гарантованість можна говорити тільки з вірогідністю та в контексті обов'язкового виконання вимог і рекомендацій використаних при цьому стандартів безпеки.

Основи стратегії захисту інформації містять у собі необхідність використання двох термінологічних понять: стратегія технічного захисту інформації і стратегія безпеки інформації, що захищається, з урахуванням останніх вимог нормативних документів з питань технічного захисту інформації Департаменту спеціальних телекомунікаційних систем і захисту інформації СБ України.

З цього випливає, що основною метою реалізації стратегії ТЗІ є виключення, або ускладнення реалізації загрозам інформації, зниження збитку від реалізації загроз і забезпечення безпеки інформації.

Універсальних систем захисту на усі випадки не існує, бо кожен захист створюється для конкретного об'єкта, його оточення і зовнішнього середовища, під конкретні загрози, функціональні вимоги і необхідний

рівень захищеності. При їх зміні захист має бути здатним адаптуватися до них.

На практиці, в більшості випадків система захисту складається з декількох ланок і рубежів [4]. Відомо, що при спробі перебороти захист, порушник прагне використати найбільш слабкий напрямок, або рубіж у цій системі. З цієї причини підсумкова міцність СЗІ буде визначатися міцністю найбільш слабкого напрямку, або рубежу в цій системі.

Якщо міцність слабкого рубежу не задовольняє заданим вимогам, то цей рубіж зміцнюється, чи заміняється на більш міцний.

Отже, імовірність ефективного захисту інформації при багато рубіжній системі визначається залежністю:

$$P_{\Sigma} = P_{СЗІ1} * P_{СЗІ2} * \ldots * P_{СЗІ\,N},$$

де $P_{СЗІ}$ – імовірність ефективного захисту N-го рубежу *СЗІ*, N – порядковий номер рубежу.

Ефективність механізму захисту в значній мірі залежить від реалізації ряду принципів. По-перше, механізми захисту варто проектувати з урахуванням розподілу ресурсів між рубежами і можливістю їхнього перерозподілу. По-друге, питання захисту варто розглядати комплексно, в рамках єдиної системи захисту.

Системний підхід забезпечує адекватний багаторівневий богаторубіжний захист, який розглядається як комплекс організаційно-правових та технічних заходів. Крім цього, при реалізації механізмів захисту мають використовуватися передові, науково обґрунтовані технології захисту, що забезпечують необхідний рівень безпеки, прийнятність для користувачів і можливість нарощування і модифікації СЗІ в майбутньому.

Нехай комплексна СТЗІ характеризується множиною рубежів Р, що забезпечують протидію множині несанкціонованих дій **Д.** Оскільки Р складається з n рубежів, то **Д** містить **m** дій.

Кожен рубіж $p_i \in P$ характеризується доступною потужністю a_i ; відповідно до множини Р, маємо вектор $a=(a_1,\ldots,a_n)$ ресурсів рубежів.

Кожна несанкціонована дія $d_i \in Д$ відповідає набору дій зловмисника і має необхідний ресурс для виконання поставленої задачі (можливо і кількаразового) протягом доби z_i (опер/добу). За всіма діями множини Д маємо вектор $Z=(z_1,\ldots,z_m)$ необхідних ресурсів.

По кожній дії надано два вектори V_i і W_i , де $V_i=(v_{i1},\ldots,v_{in})$ множини Р, вектор $W_i=(w_{i1},\ldots,w_{im})$ - визначає інтенсивність нападів при нападі d_i із задачами інших протиправних дій множини Д. Тут $w_{ii}=0$. За всією сукупністю нападів маємо прямокутну матрицю V розміру mxn і квадратну матрицю W розміру mxm, складені з векторів V_i і W_i , $1 \le i \le m$, відповідно. Будемо вважати, що ресурси несанкціонованої дії $d_i \in Д$ можуть бути реалізовані тільки проти одного будь-якого рубежу множини Р, тобто дія виробляється проти конкретного рубежу.

Нехай дані множини Р и Д, представлені кортежами <P,a,R> і <Д,Z,V,W>, де а – вектор доступності до інформації, R – матриця відстаней між рубежами, Z – вектор ресурсів протиправної дії, V – матриця інтенсивності нападів. Отже, потрібно знайти повне відображення β: Д→Р, щоб середньоквадратична довжина L(β) маршруту несанкціонованих дій приймала мінімальне значення, тобто

$$L(\beta) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{i-1} s_{ij} z_{ij}}{\sum_{i=1}^{n}\sum_{j=1}^{i-1} s_{ij}},$$

де $S_{ij} = \begin{cases} \sum_{k=1}^{n} v_{kj} h_{ki} + \sum_{k=1}^{m}\sum_{\alpha=1}^{k-1} w_{k\alpha} h_{ki} h_{\alpha j} & \text{при } i \ne j \\ 0 \text{ при } i = j \end{cases}$,

$h_{ij}=\{0,1\}$ визначає цільову дію a_i на конкретний рубіж p_j,

$h_{ij} = \begin{cases} 1, \text{при } \beta(d_i) = p_j \\ 0 \text{ в зворотньому випадку} \end{cases}$ за умови $\sum_{i=1}^{m} z_i h_{ij} \le a_j$ для всіх $p_j \in P$.

Представимо вектор Z у вигляді *m*-вимірного вектора-стовпця

$$Z = \begin{pmatrix} z_1 \\ \ldots \\ z_m \end{pmatrix},$$

де z_i – обсяг протиправних дій при нападі d_i.

Тоді функцію β можна представити характеристичною функцією (характеристичною матрицею) Н її

трафіка, тобто

$$H = \left\| h_{ij} \right\|_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} .$$

Нехай p_i – номер деякого рубежу. Двійковий m-вимірний вектор-стовпець H_j, що містить одиницю на місцях з номерами складових протиправної дії, назвемо характеристичним способом p_i – рубежу.

Використовуючи, [6], що описує скалярний добуток векторів $Z\ H_i - ZH_i = \sum_{i=1}^{m} z_i h_{ij}$, запишемо, що $H_j c_j$ дорівнює сумарному $a_i \in A$ із усіма рубежами, а добуток $H_i c_j$, де $i \neq j$, дорівнює інтенсивності потоку між рубежами p_i і p_j. Це значення позначене S_{ij}, тобто $S_{ij}=H_i c_j$. Квадратну матрицю рангу n значень S_{ij} позначимо через S.

Сумарний потік між рубежами

$$\lambda = \frac{1}{2}\sum_{j=1}^{n} H_j c_j .$$

Тоді можна записати функціонал

$$L(\beta) = L(H) = \frac{\sum_{i=1}^{n}\sum_{j=1}^{i-1} s_{ij} r_{ij}}{\lambda} ,$$

чи

$$L(\beta) = \frac{SR}{\frac{1}{2}\sum_{j=1}^{n} H_j c_j} .$$

Отже, задача зводиться до мінімізації білінійного функціоналу на цілочислових (двійкових) векторах при лінійних обмеженнях виду

$$ZH_j \le a_j, \text{ для усіх } 1 \le j \le n$$

і при обраному критерії задач нападів, розподіляється по рубежах зводиться до розбивки множини Д на підмножини та призначенню цих підмножин рубежам множини Р, що відповідає спільному рішенню задач розбивки графа на частини і задачі призначення. Одержання оптимального рішення зв'язано з повним перебором різних варіантів розбивки. Для рішення таких задач використовується, як правило, метод областей і границь. Недоліком цього методу [7] є складність реалізації при порівняно невисокій ефективності.

Оскільки в СЗІ значення m+n досить велике, доцільно використовувати для рішення даної задачі евристичні алгоритми оптимізації. Відомі евристичні алгоритми [8] можна віднести або до алгоритмів послідовної протидії підсистемі захисту, або до ітераційних алгоритмів послідовного поліпшення наближень за допомогою парних перестановок задач між рубежами.

На практиці часто мають місце ситуації, коли кожна неправомірна дія $d_i \in$ Д, представлена набором задач, яким можуть протистояти різні рубежі множин Р, і коли нападу d_i протистоїть тільки один рубіж. У цьому випадку розглянута задача трохи спрощується та може бути зведена до класичної транспортної задачі.

Нехай задані множини Р и Д, де Р має раніше вказаний зміст і представляється кортежем <P,a,R>.

Множина Д складена з m нападів $\{d_1,\ldots,d_m\}$... Кожен напад $d_i \in$ Д представлено набором задач і характеризується необхідним ресурсом Z_i для їхньої реалізації. По всіх протиправних діях Д маємо вектор необхідних ресурсів $Z=(z_1,\ldots z_m)$... Необхідний ресурс Z_i нападу d_i може бути припинений однією, чи декількома рубежами множини Р, при будь-якій розбивці Z_i між собою.

По кожному нападі $d_i \in$ Д, даний вектор $V_i=(v_{i1},\ldots,v_{in})$ визначає інтенсивність нападів d_i на рубежі множини Р. Передбачається, що всі задачі, зв'язані з нападом $d_i \in$ Д, володіють однакової питомою вагою щодо одиниці необхідного ресурсу, інтенсивністю f_{ij} протиправних дій проти рубежів $p_i \in$ Р, тобто

$$\forall d_i \in Д, p_i \in P \ \left| f_{ij} = \frac{v_{ij}}{r_i} \right.$$

Отже маємо вихідну інформацію множин Р та Д, представлених відповідно кортежами

<P,a,R> і <Д,Z,V>,

де V – матриця інтенсивності нападів множини Д на рубіж множини Р.

Потрібно визначити розподіл ресурсів нападів Д по рубежах множини Р. У результаті розподілу ресурсів нападу формується матриця Q, в якій кожній протиправній дії має бути зіставлений вектор-рядок

$q_i=(q_{i1},\ldots,q_{in})$ розмірності n, що представляє собою розподіл ресурсів протиправних дій d_i за рубежами множини P, тобто k-й компонент q_{ik} вектора q_i являє собою обсяг задач нападу d_i на k-ий рубіж захисту. Сукупність розподілів протиправних дій множини Д визначимо як відображення γ: Д→N^n, тут N^n – векторний простір n-мірних векторів, компоненти яких є цілими числами. Якість розподілу γ буде оцінено значенням середньозваженої довжини L(γ) маршруту нападу.

Основою визначення L(γ) служить штраф для одиниці ресурсу нападу d_i, i=1,2,…,m=[Д], закріпленої за p_j-им рубежем. Якщо одиниця ресурсу нападу діє на p_j-ий рубіж, то їй відповідає штраф

$$c_{ij} = \sum_{k=1}^{n} f_{ik} r_{jk} = \sum_{k=1}^{n} r_{ik} \frac{v_{ik}}{z_i}$$

Отже для кожного нападу $d_i \in$ Д маємо вектор $c_i=(c_{i1},\ldots,c_{in})$, k-ий компонент c_{ik} якого визначає збиток за одиницю ресурсу нападу d_j, що закріплюється за рубежем $p_к$.

Функція збитку, що характеризує обраний розподіл протиправних дій γ за рубежами, має вигляд

$$F(\gamma) = \sum_{i=1}^{m} \sum_{j=1}^{n} q_{ij} c_{ij} \ .$$

При складанні розкладу γ бажано мінімізувати функцію

$$L(\gamma) = \frac{1}{\lambda} F(\lambda) \ ,$$

де λ – незалежна від розподілу γ величина, що визначає сумарний потік нападів відповідно до вираза

$$\lambda = \sum_{i=1}^{m} \sum_{j=1}^{n} v_{ij} \ \text{ або } \ \lambda = \sum_{i=1}^{m} \sum_{j=1}^{n} q_{ij} j_{ij} \ .$$

Якщо γ – обраний розподіл, то він, мабуть, має задовольняти наступним умовам:

1) $\forall d_i \in Д \ | \gamma(d_i) = q \geq 0 = 0,0,\ldots,0$ (позитивність),

2) $\forall d_i \in Д \, | \sum_{j=1}^{n} q_{ij} \leq z_i$ (обмеженість),

3) $\sum_{d_i \in Д} q_i \leq a = (a_1,\ldots,a_n)$ (можливість реалізації).

Отже, задача розподілу необхідних ресурсів нападу між рубежами в приведених вище поняттях і позначеннях може бути сформульована в такий спосіб.

Нехай задана система несанкціонованих дій <Д,Z,V> і система захисту <P,a,R>. Потрібно визначити такі позитивні, обмежені і реалізовані розподіли γ, щоб L(γ) приймало мінімальне значення.

Поставлена в такий спосіб задача, зводиться до класичної транспортної задачі.

Для цього поставимо у відповідність кожному p_i рубежу джерело ресурсу p_j, 1≤j≤n, з наявним ресурсом a_j, а кожному нападу $d_i \in$ Д поставимо відповідного зловмисника d_i, 1≤i≤m=$|$Д$|$, з необхідним ресурсом z_i. Вартість застосування одиниці ресурсу нападу d_i від зловмисника p_j є компонент c_{ij} вектора c_i. Обсяг ресурсу, споживаний нападом d_i від p_i, є q_{ij}. Тоді математична постановка класичної транспортної задачі набуває вигляду:

$$\text{мінімізувати } F = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} q_{ij} \text{ при обмеженнях,}$$

$$\sum_{i=1}^{m} q_{ij} \leq a_j, j = 1,2,\ldots, n \quad \text{(наявні ресурси),}$$

$$\sum_{j=1}^{n} q_{ij} \leq z_i, i = 1,2,\ldots, m \quad \text{(попит),}$$

$$c_{ij} \geq 0 \text{ і } q_{ij} \geq 0 \text{ для всіх } i \text{ та } j.$$

Щоб задача мала припустиме рішення, потрібно, щоб загальні ресурси зловмисників були, принаймні, не менше загальних можливості захисника, тобто щоб виконувалася умова:

$$\sum_{j=1}^{n} a_j \geq \sum_{i=1}^{m} z_i \ .$$

Однак при аналізі транспортної задачі і побудові алгоритму її рішення зручно прийняти, щоб загальна потужність зловмисників дорівнювала загальної можливості захисту, тобто

$$\sum_{j=1}^{n} a_j = \sum_{i=1}^{m} z_i .$$

З цією метою досить ввести імітацію (n+1)-го нападу з ресурсом $a_{n+1} = \sum_{i=1}^{m} z_i$ і помилкове (m+1)-ше спрацьовування, рівне $z_{m+1} = \sum_{j=1}^{n} a_j$, і прийняти вартість $c_{m+1,j} = 0$ для j=1,2,…,n+1, а вартість $c_{i,n+1}$, i=1,2,…,m рівною як завгодно великій величині $b > \max_{\substack{1 \le i \le m \\ 1 \le j \le n}} (c_{ij})$.

Отже сумарна потужність нападу, що імітується, дорівнює сумарному помилковому спрацьовуванню. Звідси модель транспортної задачі приймає вид:

мінімізувати $F = \sum_{i=1}^{m+1} \sum_{j=1}^{n+1} c_{ij} q_{ij}$ при обмеженнях,

$$\sum_{i=1}^{m+1} q_{ij} \le a_j, j = 1,2,...,n+1 \quad \text{(пропозиція)},$$

$$\sum_{j=1}^{n+1} q_{ij} \le z_i, i = 1,2,...,m+1 \quad \text{(попит)},$$

де a_j, z_j – позитивні цілі числа, що задовольняють умову:

$$\sum_{j=1}^{n+1} a_j = \sum_{i=1}^{m+1} z_i .$$

Дана модель транспортної задачі має n+m+1 змінних. Для її рішення може бути використана одна з модифікацій симплекса-методу (метод потенціалів) [8].

III Висновки

Проведені дослідження дозволяють оцінити стійкість багато рубіжної комплексної системи технічного захисту. Отримані результати дають можливість з досить високою точністю оцінити ефективність розподілу ресурсів ТСЗІ між рубежами захисту при спрямованому і сконцентрованому подоланні визначеного рубежу.

Література: ***1****. Аналіз структури автоматизованої інформаційної системи ДПС України як об'єкту дослідження. Звіт про НДР частина 1, 2002р.* ***2****. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.* ***3****. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.* ***4****. Шорошев В. В., Ильницкий А. Е. Основы стратегии защиты информации в компьютерных системах / Бизнес и безопасность, 2000, №2.-с. 6-7.* ***5****. Хорошко В. А. Модель системы защиты информации./ Захист інформації,1999, №1.-с. 5–11.* ***6****. Арфкен Г. Математические методы в физике. - М.: Атомиздат, 1970.-712 с.* ***7****. Мину М. Математическое программирование. – М.: Наука, 1990.– 488 с.* ***8****. Сигорский В. П. Математический аппарат инженера. – К.: Техніка, 1975.-768 с.*

УДК 681.3

ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ В ІНТЕРНЕТ

Михайло Гуцалюк
Міжвідомчий НДЦ при Координаційному комітеті по боротьбі з корупцією і організованою злочинністю при Президентові України

Анотація: **Розглянуто деякі аспекти захисту інформації в мережі Інтернет.**
Summary: **Some aspects of information safety in a network the Internet are considered.**
Ключові слова: **Інформаційна безпека, Інтернет, провайдер, браузер.**

I Вступ

Геополітична спрямованість сучасного цивілізаційного процесу визначається його глобалізацією, прогресуючим зростанням значущості гуманітарної сфери, високих інформаційних технологій,