політика безпеки об'єкта теж повинна доповнюватися і змінюватися у відповідності з усіма перерахованими критеріями та в залежності від змін цінності інформації, що захищається.

Список літератури

1. Информационно-методический журнал «Защита информации. Конфидент», 2002р., Петренко С.А. «Реорганизация корпоративных систем безопасности»;
2. Соколов А.В., Степанюк О.М. «Защита от компьютерного терроризма», Справочное пособие, БХВ-Петербург, «Арлит», 2002;
3. «Выработка официальной политики предприятия в области информационной безопасности», Internet;
4. Щеглов А.Ю. «Защита компьютерной информации от несанкционированного доступа», Санкт-Петербург, «Наука и техника», 2004.

Надійшла 18.06.2005
Після доробки 21.08.2005

УДК 681.3.06

В.К Белошапкін,С.М.Пустовіт, В.Д.Степанов

ФОРМАЛІЗАЦІЯ ПРОБЛЕМИ ОПТИМІЗАЦІЇ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

На сьогодні можна знайти достатньо повний перелік вимог та критеріїв [1-14] , які можуть бути взяті за основу для оцінки ефективності засобів і заходів захисту інформаційних ресурсів (ІР) інформаційно- телекомунікаційних систем.

Аналіз цих документів дозволяє оцінити перспективи використання існуючих розробок на практиці. При цьому такі оцінки важливо зробити з позицій системного підходу..

В [10] викладені основні принципи, які повинні виконуватися в межах системного підходу в ході вирішення довільної складної проблеми. В контексті документів [1-14] ці принципи можна сформулювати наступним чином:

1. Системний аналіз суті проблеми захисту інформації;

2. Розробка і обґрунтування повної, вільної від протиріч концепції і методології вирішення проблеми захисту інформації, в межах якої проблема захисту продукту чи системи в конкретних умовах визначається у вигляді профілю - проекту захисту;

3. Системне використання методів і механізмів захисту інформації при вирішенні задачі синтезу (проектування) безпечних продуктів і систем інформаційних технологій.

Із розгляду зазначених документів видно, що вони спрямовані на вирішення перших двох проблем. В одному з останніх документів - стандарті ISO/IEC 15408 здійснена повна декомпозиція проблеми захисту інформації. Механізми профілю і проекти захисту відображають суть концепції вирішення проблеми захисту інформації.

На сьогодні в нормативних документах відсутня методологія вирішення третьої проблеми -- проблеми синтезу комплексної системи захисту інформації. Функціональні вимоги і вимоги адекватності, як і методологія оцінки безпеки, направлені в першу чергу на рішення задачі оцінки безпеки продукту чи системи. Хоча їх використання, накладає деякий регламентований вплив на проектування, розробку і експлуатацію систем. Тут необхідно забезпечити встановлення відповідності цілям захисту (суть яких виражається через вимоги) множини засобів і механізмів , які маються в розпорядженні.

Стандарт ISO/IEC 15408 передбачає створення електронного каталогу профілів захисту, які пройшли оцінку та сертифікацію, що дозволить розробникам використати відомі профілі захисту при розробці нових систем і продуктів.

З іншої сторони профіль (проект) захисту є ні чим іншим як сертифікованим і обґрунтованим рішенням задачі захисту інформації в конкретних умовах експлуатації.

Метою статті є обґрунтування вибору оптимального варіанту системи комплексного захисту інформації. Для цього необхідно ввести критерії оцінки ефективності системи захисту інформації . Серед множини всіляких оцінок основними представляються наступні:

1.Вірогідність реалізації загрози.

2.Оцінка можливих втрат (у вартісному виразі).

3.Оцінка вартості можливих заходів по недопущенню реалізації загроз.

Методика синтезу повинна спиратися на стабільні показники . Тому за основу можна прийняти укрупнені структурні і мережівні моделі інформаційної системи , загроз і захистів , які не залежать від конкретної реалізації системи. В процесі створення підсистеми інформаційної безпеки та її експлуатації вимоги коректуються та конкретизуються ,так що задача не лишається актуальності, як і в наступні періоди життєвого циклу системи в цілому, так і в частині її підсистеми інформаційної безпеки.

Зупинимось на згаданих критеріях більш детально.

1.Вірогідність реалізації загрози.

Нехай y – випадкова величина , яка рівняється числу реалізацій загрози за період [0,T], втрати F(y) випадкові , залежать, взагалі кажучи, нелінійно від реалізацій , і можуть бути представлені у вигляді ряду Тейлора:

$F(y)= \sum \alpha_k y^k$

Тоді математичний опис випадкової функції втрат

$MF(y) = M\sum \alpha_k y^k = \sum \alpha_k My^k$

де My^k- момент k – го порядку випадкової величини y. Таким чином для обчислення критерію необхідно знати закон розподілу випадкової величини y на інтервалі [0,T] і вісові коефіцієнти α_k. Для ненавмисних загроз можна прийняти пуасонівський розподіл потоку загроз по аналогії з найпростішим потоком визовів в системах масового обслуговування.

$$P(y \le k) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}$$

Для моментів одержуємо

$My= \lambda$

$My^2= \lambda^2 + \lambda$

і т. ін.

Найпростіша залежність для випадкової функції втрат - лінійна

$$U = \alpha\zeta \qquad (1)$$

Тоді вісовий коефіцієнт α має простий фізичний зміст – втрати від одноразової успішної реалізації загрози Y. Переходимо до математичного очікування і одержуємо:

$$MU = \alpha\zeta P \qquad (2)$$

де P – вірогідність реалізації загрози Y.

Для стаціонарного ненавмисного потоку загроз закон розподілу випадкової величини ζ можна зробити апроксимацію пуасонівським законом з інтенсивністю λ, а за модель інформаційної системи (ІС) прийняти модель $\mu / \mu / m$. Тоді вірогідність наявності n загроз в системі визначається формулами [15]

$$P_0 = \left(\sum_{n=0}^{m-1} \frac{(m\rho)^k}{k} + \frac{(m\rho)^m}{m(1-\rho)} \right)^{-1}, \quad n = 0 \qquad (3)$$

$$P_n = \begin{cases} P_0 \dfrac{(mp)^n}{n} & , \quad n \le m \end{cases} \qquad (4)$$

$$P_0 \frac{m^m \rho^n}{m} \quad , \quad n \geq m$$

де $\rho = \frac{\lambda}{m\mu}$;

μ -швидкість обслуговування (ліквідації) загроз;

m - кількість вузлів графу ІС.

Введемо матрицю втрат

$$A = \begin{vmatrix} \alpha_{11} & \dots & \alpha_{1k} \\ \dots & \dots & \dots \\ \alpha_{s1} & \dots & \alpha_{sk} \end{vmatrix} \tag{5}$$

де α_{ij} - означає втрати від одноразової успішної реалізації загрози y_i, яка спрямована на j – у компоненту ІС.

Означимо

$$\alpha_{\max} = \max\{\alpha_{ij}\} \quad \forall_{ij}$$
$$\alpha_{\min} = \min\{\alpha_{ij}\} \quad \forall_{ij} \tag{6}$$

Тоді із (2-6 =5.7-5.11) одержуємо просту оціночну формулу можливих втрат для ненавмисних загроз:

$$\alpha_{\max} np_n \leq MU \leq \alpha_{\min} np_n \tag{7}$$

Втрати від одноразової успішної реалізації загрози можуть бути оцінені експертами. Якщо в якості експертів виступає дельфійська група [16], то оцінки, які дали різні експерти можуть бути нормовані і тоді втрати можуть бути виражені дійсним числом з інтервалу $[0,1]$, такою інтерпретацією меж:

1 –повне руйнування системи;

0 – повна захищеність від любих загроз (повна відсутність втрат).

Окремі параметри процесу для ненавмисних загроз піддаються аналітичному визначенню: для m – очевидним чином, для λ,U – на основі статистичних даних за допомогою побудови рівняння регресії.

При побудові моделі втрат для рішення задачі синтезу необхідно знати на які складові ІС може розповсюджуватися вплив загрози, що спрямована на і –у складову ІС, де вона ще може проявлятися і які втрати може принести. Для цього введемо поняття глибини проникнення загрози.

Визначення. Назвемо глибиною проникнення загрози кількість складових ІС, на які може розповсюджуватися її вплив при атаці однієї складової.

Для того, щоб визначити глибину проникнення побудуємо матрицю досягаємости ІС на основі мережевої моделі. Як відомо [13]вершина графа V_j називається досягаємою із вершини V_i якщо існує направлений шлях із V_i до V_j.

Введемо означення:

ΓV_i -множина вершин, які досягаються з V_i при використанні шляхів довжини 1;

$\Gamma(\Gamma V_i) = \Gamma^2 V_i$ – множина вершин, які досягаються з V_i при використанні шляхів довжини 2;

$\Gamma(\Gamma^{n-1} V_i) = \Gamma^n V_i$ – множина вершин, які досягаються з V_i при використанні шляхів довжини n.

Для рішення задачі визначення множини всіх вершин графа, які досягаються з даної вершини, достатньо знайти об'єднання множин

$$\{V_i\} \vee \{\Gamma V_i\} \vee \dots \vee \{\Gamma^n V_i\}$$

яке називається транзитивним замиканням $\bar{r}$ вершини V_i.

При вивченні досягаємості зручний матричний спосіб. Так одиничну матрицю Е можна розглядати, як матрицю досягаємості з використанням шляхів довжини 0; матрицю суміжності А – як матрицю досягаємості з використанням шляхів довжини 1. Але матриця суміжності А виражає відношення Г на множині вершин $\{V_i\}$. Тоді матриця A^2, яка виражає відношення $Г^2$ представляє собою матрицю досягаємості з використанням шляхів довжини 2 і т.д.

Таким чином, транзитивне замкнення $\bar{r}$ відношення Г, яке задане m вершинами графу, виражається матрицею $\bar{A}$, що визначається формулою

$$\bar{A} = A + A^2 + A^3 + \ldots + A^к.$$

Звідси, матриця $\bar{A}$ представляє собою матрицю досягаємості з використанням шляхів довжини 1. . . к , окрім к = 0.

Таким чином, матриця $\bar{A}$ і матриця досягаємості R знаходяться у співвідношенні

$$R = \bar{A} + E = E + A + A^2 + A^3 + \ldots + A^к.$$

Процес додавання матриць переривається, коли результат перестає змінюватися.

Визначимо тепер вірогідність p_{ki} – вірогідність реалізації загрози y_k, яка спрямована на і- у складову ІС. Для цього скористаємося теоремою ВСМР [17].

Але перед тим, як це зробити необхідно ввести ряд визначень.

Означимо через $n=\{n_{ir}\}$ - кількість загроз y_r спрямованих на і-у складову ІС. Число n визначає стан ІС.

Визначення 1. Вхідний потік загроз назвемо потоком першого типу, якщо із джерела поступає один пуасонівський потік, інтенсивність якого λ є функцією загальної кількості загроз в ІС у стані n.

Визначення 2. Вхідний потік загроз назвемо потоком другого типу, якщо мається l пуасонівських потоків загроз, які поступають у відповідні підсистеми ІС, інтенсивності яких λ_j є функцією кількості загроз у відповідній підсистемі (j=1 . . . l).

Будемо уявляти, що ІС складається із центрів типу 1, який характеризується наступним чином.

Центр типу 1. Ліквідація загроз в центрі здійснюється у відповідності з дисципліною FIFO. Тривалість ліквідації загроз має одне й теж експоненціальне розподілення з інтенсивністю $\mu_i(n_i)$ (і – номер даного центру в ІС), яка залежить від кількості загроз в центрі n_i.

По теоремі ВСМР стаціонарне розподілення вірогідностей $P(n_{ir}) = P_{ir}$ існує і має мультиплікативний вигляд:

$$P_{ir} = P(n_{ir}) = G^{-1} \lambda^*(n^*) \prod_{i=1}^{M} f_i(n_i) \qquad (8)$$

де $f_i(n_i) = \left(\frac{1}{\mu_i}\right)^{n_i} \prod_{j=1}^{n_i} e_j n_{ij}$ -коли вхідний потік першого типу;

$$\lambda^*(n^*) = \begin{cases} \prod_{i=0}^{\mu(n^*)-1} \lambda(i) \\ \prod_{j=1}^{l} \prod_{i=0}^{\mu(n^*,E_j)-1} \lambda_j(i) \end{cases}$$ -коли вхідний потік другого типу.

$$G = \sum_n \lambda^*(n^*) \prod_{i=1}^{m} f_i(n_i^*).$$

де e_{ir}- відносна інтенсивність потоку загроз y_r, який проходить через центр і,

μ - кількість загроз в ІС;

$\mu(n, E_j)$ -кількість загроз в підсистемі E_j.

Перейдемо тепер до формулювання задачі синтезу комплексної системи захисту інформації.

Введемо матриці:

1. Матриця умовних вірогідностей реалізації загрози

$$P^y = \begin{array}{c|cccc} & Z_1 & \dots & \dots & Z_m \\ Y_1 & P_{11} & \dots & \dots & P_{1m} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ Y_n & P_{n1} & \dots & \dots & P_{nm} \end{array},$$

де значення P_{ij} означає вірогідність реалізації загрози y_i при наявності захисту Z_j.

2. Матриця вибору захистів

$$B = \begin{array}{c|cccc} & Z_1 & \dots & \dots & Z_m \\ Y_1 & b_{11} & \dots & \dots & b_{1m} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ Yn & b_{n1} & \dots & \dots & b_{nm} \end{array},$$

коли при загрозі y_i вибрано захист z_j,

де $b_{ij} = \begin{cases} 1 - \\ 0 - \end{cases}$

коли при загрозі y_i не вибрано захист z_j,

3. Матриця вартості захистів

$$C = \begin{array}{c|cccc} & Z_1 & \dots & \dots & Z_m \\ Y_1 & c_{11} & \dots & \dots & c_{1m} \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ Y_n & c_{n1} & \dots & \dots & c_{nm} \end{array},$$

де c_{ij} –вартість і-го захисту при атаці j-ої загрози.

Розглянемо вираз

1. $MU_z = \sum_i \sum_j \sum_r \alpha_{kj} p_{kj} r_j p^y_{ki} b_{ki} \varsigma_{ki} \xi_{ki}$.

2. $\overline{C} = \sum_i \sum_k c_{ki} b_{ki}$.

3. $MU = \sum_i \sum_j \sum_k \alpha_{kj} p_{kj} r_j \ \xi_{ki}$.

4. $\overline{e} = e_{ik} \ l_{ki}$

5. Матриця ефективності

$$|l| = E - P^y,$$

де Е-одинична матриця.

Перший вираз визначає інтегральні втрати від можливих загроз при наявності захистів та з урахуванням глибини проникнення загрози; r_j – строки матриці досягає мості R.

Другий вираз визначає можливу вартість захисту.

Третій вираз визначає інтегральні втрати від можливих загроз без використання захисту.

Четвертий вираз – визначає вибір компоненти l матриці ефективності.

Задача синтезу оптимальної комплексної системи захисту інформації формулюється тепер наступним чином. Знайти матрицю $\|b_{ki}\|$, таку що

$$\begin{gathered} U_z \longrightarrow \min \\ \overline{C} \longrightarrow \min \\ \overline{e} \longrightarrow \max \\ C \le U \end{gathered} \qquad (9)$$

Для вирішення задачі необхідно знати набір параметрів процесу:

1. λ - інтенсивність наступу загроз;
2. $\|\alpha_{ik}\|$ -матрицю втрат від одиничної успішної реалізації загрози y_k, яка спрямована на вузол i- ої ІС;
3. m – кількість вузлів мереженого структурного графу ІС;
4. R – матрицю досягає мості мереженого графу ІС;
5. P^y – матрицю умовних вірогідностей;
6. C - матрицю вартості засобів і заходів захисту.

Таким чином, в постановці (9) задача оптимального синтезу (або оптимального проектування) комплексної системи захисту інформації повністю формалізована і представляє собою багатокритеріальну задачу цілочисельного програмування, яка може бути вирішена відомими методами.

Список літератури

1. Trusted Computer Systems Evaluation criteria, US DoD 5200 28-STD. 1985/
2. Information Technology Security Evaluation criteria, V.1.2. – Office for Official ublications of the European Communities,1991.
3. Canadian Trusted Computer Product Evaluation criteria,v.3.0. Canadian Systems Security Centre, Communications Security Establishments Covernment of Canadian,1993.
4. Federal criteria for Information Technology security. NIST, NSA, US Covernment, 1993.
5. ISO/IEC 15408-1: 1999- Information Technology security techniques- Evaluation criteria for IT Security- Part 1: Information and general model.
6. ISO/IEC 15408-2: 1999- Information Technology security techniques,- Evaluation criteria for IT Security- Part 2: Security functional requirements.
7. ISO/IEC 15408-3: : 1999- Information Technology security techniques- Evaluation criteria for IT Security- Part 3: Security assurance requirements.
8. CEM-97/017. Common Evaluation Methodology for Information Technology security – Part 1: Information and general model.
9. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. Кн.1.М., Энергоатомиздат,1994.
10.И.Д.Горбенко, А.В.Потий, П.И.Терещенко. Критерии и методолбгия оценки безопасности информационных технологий. Радиотехника. Выпуск 114. Харьков. 2000. с.25-38.
11.Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. -НД ТЗІ 1.1-002-99, ДСТСЗІ СБ України, Київ, 1999.
12.Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. -НД ТЗІ 1.1-003-99, ДСТСЗІ СБ України, Київ, 1999.
13.Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. -НД ТЗІ 2.5-004-99, ДСТСЗІ СБ України, Київ, 1999.

14.Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. -НД ТЗІ 2.5.-005 -99, ДСТСЗІ СБ України, Київ, 1999.

15. IT Baseline Protection Manual Bundesamt far Sicherheit in der Informationstechnik. 1998.
16. Клейнрок Л. Вычислительные системы с очередями. М. Мир.1973.
17. В.А. Жожикашвили, В.М.Вишневський. Системы массового обслуживания. Теория и применение к сетям ЕВМ. М., Радио и связь. 1988.

Надійшла 30.06.2005

УДК 681.3

І.Ю.Мануйлов

ТОНАЛЬНИЙ АЛГОРИТМ ВИЯВЛЕННЯ РАДІОМІКРОФОНІВ

Для напівавтоматичного й автоматичного виявлення радиозакладок у даний час широко застосовуються програмно-апаратні комплекси. У них реалізовані найбільш надійні принципи виявлення радіомікрофонів. До них відноситься просторово-тимчасова селекція, аналіз на гармоніки, перевірка на кореляцію акустичного сигналу усередині приміщення з прийнятим сигналом.

У даній статті розглядаються алгоритми виявлення радіомікрофонів, засновані на кореляції низькочастотних сигналів. Передбачається, що приймач апаратури виявлення набудований на радіосигнал і має відповідний тип детектора. Потрібно прийняти рішення про тім, є присутнім чи сигнал, випромінюваний усередині приміщення, у прийнятому радіосигналі чи ні. Для виявлення кореляції в апаратурі виявлення мається можливість формувати різні акустичні сигнали.

Розглянемо класичний алгоритм виявлення радіомікрофонів, застосовуваний у сучасних апаратно-програмних комплексах. Цей алгоритм був запозичений з теорії радіолокації і являє собою процедуру виявлення детерминированного сигналу з невідомою затримкою приходу і невідомим масштабним множником на тлі нормального гауссовского шуму невідомої інтенсивності [1, 2].

Постановка задачі для синтезу цього алгоритму припускає апріорну популярність форми сигналу, що виявляється. Це має місце тільки у випадку повної відсутності акустичних перекручувань. У результаті реверберації уку з'являються додаткові спотворювання, що у даному алгоритмі не враховуються. Як тестовий сигнал звичайно вибирається сигнал з лінійною частотною модуляцією (ЛЧМ), тому що він володіє відмінною автокорреляційною функцією.

Передбачається, що заважаючий сигнал представлений у вигляді нормального гауссовского шуму. Нехай на вхід обнаружителя надходить послідовність відліку сигналу s(n),

де n - номер відліку сигналу $\mathbf{n = \overline{0, N}}$. При справедливій гіпотезі H_0 вхідний сигнал являє собою шумову послідовність

$$\mathbf{S(n) = \xi_0(n)},$$

де $\xi_0(n)$ -відлік шумового сигналу. При справедливій гіпотезі H_1 сигнал на вході обнаружителя являє собою аддитивну суміш детермінірованого тестового сигналу a(n) і шуму

$$\mathbf{S(n) = ka(n) + \xi_1(n)},$$