Висновки

PCI Data Security Standard спрямований на визначення рівня забезпечення безпеки інформації про власників карт, а також на формування рекомендацій для торговосервісних підприємств, виробників і постачальників програмних рішень та термінального обладнання про заходи, необхідні для підвищення рівня захисту використовуваного програмного забезпечення.

Стандарт був введений для того, щоб допомогти тримачам платіжних карток, а також організаціям, що володіють інформацією про платіжні картки, вберегтися від щорічної втрати коштів через шахрайство. Він допомагає організаціям, що працюють з картками, підвищити рівень безпеки, але не є єдиною причиною для реалізації відповідних рішень безпеки.

1. Ricky Magalhaes PCI DSS Security // Section: Web-page.. – http://www.windowsecurity.com. 2. Гайкович В., Першин А. Безопасность электронных банковских систем "Единая Европа". – М., 1994. 3. Голдовский И. Безопасность платежей в интернете. – СПб.: "Питер", 2001. 4. Задірака В.К., Олексюк О.С., Недашковський М.О. Методи захисту банківської інформації. – К.: "Вища шк.", 1999. 5. Постанова Правління НБУ № 223 "Про здійснення операцій з використанням спеціальних платіжних засобів" від 30 квітня 2010 р.// Сайт Верховної Ради України: Веб-сторінка. – http://zakon1.rada.gov.ua/laws/show/z0474-10.

УДК 004.056.53:001.57

А.О. Петров
СНУ ім. В. Даля

ФОРМАЛІЗАЦІЯ ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ У МЕРЕЖАХ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Запропоновано підхід до формалізації проблеми системи захисту інформації у мережах загального користування.

Ключові слова: мережа загального користування, модель, граф, випадкова функція, загроза, захищеність, потік Пуассона.

The paper presents an approach to formalize the problem of information security in public networks.

Key words: public networks, model, graph, random function, risk, security, Poisson flow.

Вступ

Захист інформації в нинішніх умовах стає усе складнішою проблемою, зумовленою багатьма обставинами, основними з яких є: масове розповсюдження засобів електронної обчислювальної техніки; ускладнення шифрувальних технологій; необхідність захисту не тільки державних і військових секретів, але й промислової, комерційної та фінансової таємниць; можливості несанкціонованих дій з інформацією, що розширюються [1]. Однак наразі приділяється мало уваги факту екстенсивного збільшення мереж загального користування (МЗК), а також тому, що більша частина інформації передається саме за їх допомогою.

Сьогодні в Україні захист обміну інформацією між абонентами може бути забезпечений шляхом використання [2]:

– Державної системи урядового зв'язку;
– Національної системи конфіденційного зв'язку;
– мережі загального користування із забезпеченням захисту власними силами.

Перший спосіб, імовірно, не може бути застосований для громадян, що не належать до державного апарату, і не може бути використаний більшістю цивільних осіб.

Другий спосіб використання спеціальних мереж зв'язку подвійного призначення, до складу яких входить телекомунікаційна мережа, спеціальні мережі надання послуг стаціонарного і мобільного зв'язку, централізовані системи захисту інформації й оперативно-технічного керування [3]. Однак така система має перелік особливостей, які обмежують її застосування: суворі вимоги до захисту, необхідність у підключенні до системи спецзв'язку, обмеження у швидкості/якості передачі, висока вартість, недоступність деяким категоріям осіб.

Отже, третій спосіб – застосування відкритих комунікаційних каналів – найчастіше вибирають комерційні структури й фізичні особи, забезпечуючи захист за свій рахунок. Усунути цей недолік покликані системи захисту інформації, які створюють захищений закритий канал усередині відкритого каналу МЗК, запобігаючи в такий спосіб несанкціонованому зніманню інформації під час передачі від абонента до абонента за принципом точка-точка. У зв'язку з високою ресурсомісткістю захищених каналів зв'язку стає все актуальнішим завдання передавання конфіденційних даних по МЗК, тому роль наукового підходу у вирішенні цього питання істотно зростає. При цьому особливого значення набуває використання математичних методів і сучасних інформаційних технологій.

Вищезазначений стан речей визначив потребу теоретичних розробок та створення формалізованої математичної моделі захисту інформації в МЗК.

Основна частина

Наразі можна знайти доволоі повний перелік вимог і критеріїв [3–7], які можуть бути взяті за основу для оцінки ефективності засобів і заходів захисту інформації в МЗК.

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

У [8] викладено основні принципи, які мають виконуватися у межах системного підходу під час вирішення довільної складної проблеми. У контексті документів [3–7] ці принципи можна сформулювати так:

1. Системний аналіз суті проблеми захисту інформації.
2. Розробка і обґрунтування повної, вільної від суперечностей, концепції й методології вирішення проблеми захисту інформації, у межах якої проблема захисту продукту або системи у конкретних умовах визначається у вигляді профілю та проекту захисту.
3. Системне використання методів і механізмів захисту інформації під час виконання завдань синтезу (проектування) безпечних продуктів і систем інформаційних технологій.

Із розгляду зазначених документів бачимо, що вони спрямовані на вирішення перших двох проблем. В одному з документів – стандарті ISO/IEC 15408 – здійснено повну декомпозицію проблеми захисту інформації. Механізм профілю й проекти захисту відображають суть концепції вирішення проблеми захисту інформації.

Сьогодні у нормативних документах відсутня методологія вирішення третьої проблеми – проблеми синтезу комплексної системи захисту інформації. Функціональні вимоги й вимоги щодо адекватності, як і методологія оцінки безпеки, спрямовані насамперед на вирішення проблеми оцінки безпеки продукту або системи, хоча їхнє використання має деякий регламентований вплив на проектування, розробку й експлуатацію систем. Тут необхідно забезпечити встановлення відповідності цілям захисту (їхня суть виражається через вимоги) множини засобів і механізмів, які є в розпорядженні.

Стандарт ISO/IEC 15408 передбачає створення електронного каталогу профілів захисту, що пройшли оцінку й сертифікацію, яка дасть можливість розроблювачам використовувати відомі профілі захисту під час розроблення нових систем і продуктів.

З іншого боку, профіль (проект) захисту є ніщо інше, як сертифіковане і обґрунтоване вирішення проблеми захисту інформації у конкретних умовах експлуатації.

Для оптимального вибору варіанта системи комплексного захисту інформації необхідно ввести критерії оцінки ефективності системи захисту інформації. Серед множини різних оцінок основними вважаються такі:

1. Імовірність реалізації загрози.
2. Оцінка можливих втрат (у вартісному виразі).
3. Оцінка вартості можливих заходів щодо недопущення реалізації загроз.

Методика синтезу повинна спиратись на стабільні показники. Тому за основу можна прийняти укрупнені структурні та мережеві моделі інформаційної системи (ІС), загроз і захистів, які не залежать від конкретної реалізації системи.

Зупинимось на виділених критеріях детальніше.

1. Імовірність реалізації загрози.

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

$$F(y) = \sum a_k y^k \,.$$

Тоді математичний опис випадкової функції втрат матиме такий вигляд:

$$M[F(y)] = M\left[\sum a_k y^k = \sum a_k M[y]^k\right],$$

де My^k – момент k-го порядку випадкової величини y .

Отже, для обчислення критерію необхідно знати закон розподілу випадкової величини y на інтервалі $[0,T]$ й вагові коефіцієнти a,k . Для ненавмисних загроз можна прийняти розподіл Пуассона потоку загроз за аналогією з найпростішим потоком викликів у системах масового обслуговування:

$$P(y \le k) = \frac{(l\,t)^k}{k!} e^{l\,t} \,.$$

Для моментів одержуємо:

$$My = l\,;$$

$$My^2 = l^2 + l\,.$$

Найпростіша залежність для випадкової функції втрат – лінійна:

$$U = a \cdot x \,. \tag{1}$$

Тоді ваговий коефіцієнт a має простий фізичний зміст – втрати від успішної одноразової реалізації загрози Y. Переходимо до математичного очікування й одержуємо:

$$M[U] = a \cdot x \cdot P\,, \tag{2}$$

де P – вірогідність реалізації загрози Y.

Для стаціонарного випадкового потоку загроз закон розподілу випадкової величини z може бути апроксимований законом Пуассона з інтенсивністю. Тоді вірогідність наявності n загроз у системі визначається за формулами [101]:

$$P_0 = \left(\sum_{m=0}^{n-1} \frac{(mr)^k}{k} + \frac{(mr)^m}{m(1-r)} \right)^{-1}, n = 0\,; \tag{3}$$

$$P_n = \begin{cases} P_0 \dfrac{(mr)^m}{n}, \, n \le m \\ P_0 \dfrac{m^m p^n}{m}, \, n \ge m \end{cases}, \tag{4}$$

де $r = \dfrac{l}{mm}$, m – швидкість обслуговування (ліквідації) загроз; m – кількість вузлів графа ІС.

Введемо матрицю втрат:

$$A = \begin{vmatrix} a_{11} & \dots & a_{1k} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nk} \end{vmatrix}, \tag{5}$$

де a_{ij} – втрати від успішної одноразової реалізації загрози y_i, спрямованої на *j*-у компоненту ІС.

Позначимо:

$$a_{\max} = \max_{\forall ij}\{a_{ij}\};$$
$$a_{\min} = \min_{\forall ij}\{a_{ij}\}. \tag{6}$$

Тоді з (2–5) одержимо просту оцінкову формулу можливих втрат для ненавмисних загроз:

$$a_{\max} np_n \le M[U] \le a_{\min} np_n . \tag{7}$$

Втрати від успішної одноразової реалізації загрози можуть бути оцінені експертами. Якщо експертами виступає дельфійська група [9], то оцінки, надані експертами, можуть бути нормовані. Тоді втрати можуть бути виражені дійсним числом з інтервалу [0, 1] такої інтерпретації границь:

1 – повне руйнування системи;

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

Окремі параметри процесу для ненавмисних загроз піддаються аналітичному визначенню: для m – в очевидний спосіб, для l, U – на основі статистичних даних за допомогою побудови рівняння регресії.

Під час побудови моделі втрат для вирішення проблем синтезу необхідно знати, на які складові ІС може поширюватися вплив загрози, спрямованої на *і*-у складову ІС, де вона може проявлятися і яку шкоду може спричинити. Для цього введемо поняття глибини проникнення загрози.

Визначення. Назвемо глибиною проникнення загрози кількість складових ІС, на які може поширюватися її вплив під час атаки однієї складової.

Для того, щоб визначити глибину проникнення, побудуємо матрицю досяжності ІС на основі мережевої моделі. Як відомо з [10], вершина графа V_j називається досяжною з вершини V_i, якщо існує спрямований шлях з V_i в V_j.

Введемо позначення:

ΓV_i – множина вершин, які досягаються із V_i під час використання шляхів довжини 1;

$\Gamma(\Gamma V_i) = \Gamma^2 V_i$ – множина вершин, які досягаються із V_i під час використання шляхів довжини 2;

$\Gamma(\Gamma^{n-1} V_i) = \Gamma^n V_i$ – множина вершин, які досягаються із V_i під час використання шляхів довжини *n*.

Для вирішення проблеми визначення множини усіх вершин графа, які досягаються з визначеної 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.

Визначаючи досяжність, використаємо матричний спосіб. Так, одиничну матрицю *E* можна розглядати як матрицю досяжності з використанням шляхів довжини 0; матрицю суміжності *A* – як матрицю досяжності з використанням шляхів довжини 1. Але матриця суміжності *A* виражає відношення Γ на множині вершин $\{V_i\}$. Тоді матриця A^2, яка виражає відношення Γ^2, є матрицею досяжності з використанням шляхів довжини 2 тощо.

Отже, транзитивне замикання $\overline{r}$ відносини *Г*, задане *m* вершинами графа, виражається матрицею $\overline{A}$, яка визначається формулою

$$\overline{A} = A + A^2 + A^3 + \ldots + A^k .$$

Отже, матриця $\overline{A}$ й матриця досяжності *R* перебувають у співвідношенні:

$$R = \overline{A} + E = E + A + A^2 + A^3 + \ldots + A^k .$$

Процес додавання матриць переривається, коли результат перестає змінюватися.

Визначимо тепер вірогідність p_{ki} – імовірність реалізації загрози y_k, спрямованої на *i*-у складову ІС. Для цього скористаємося теоремою ВСМР [10].

Однак перш ніж це зробити, уведемо ряд необхідних визначень.

Позначимо через $n = \{n_{ir}\}$ – кількість загроз y_r, спрямованих на *i*-у складову ІС. Число *n* визначає стан ІС.

Визначення 1. Вхідний потік загроз назвемо потоком першого типу, якщо із джерела надходить один потік Пуассона, інтенсивність якого l є функцією загальної кількості загроз в ІС у стані *n*.

Визначення 2. Вхідний потік загроз назвемо потоком другого типу, якщо є *l* потоків загроз, які надходять у відповідні підсистеми ІС, інтенсивності яких l_i є функціями кількості загроз у відповідній підсистемі (*j=1,2,…,l*).

Вважатимемо, що ІС складається із центрів типу 1, що характеризуються так.

Центр типу 1. Ліквідація загроз у центрі здійснюється відповідно до дисципліни FIFO. Тривалість ліквідації загроз має той самий експонентний розподіл з інтенсивністю $m_i(n_i)$ (*i* – номер цього центра в ІС), який залежить від кількості загроз у центрі n_i.

За теоремою ВСМР стаціонарний розподіл імовірностей $P(n_{ir}) = P_{ir}$ існує і має мультиплікативний вигляд:

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

де $f_i(n_i) = \begin{cases} \left(\dfrac{1}{p_i}\right)^{n_i} \cdot \prod\limits_{j=1}^{n_i} e_j n_{ij} \end{cases}$ – якщо вихідний потік має перший тип;

$$l^*(n^*) = \prod_{j=1}^{l} \prod_{i=0}^{m(n^*, E_j)-1} l_j(i) ;$$

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

якщо вихідний потік має другий тип;

де e_{ir} – відносна інтенсивність потоку загроз y_r, який проходить через центр *i;* m – кількість загроз в ІС; $m(n, E_j)$ – кількість загроз у підсистемі E_j .

Висновки

Проведено формалізацію проблеми системи захисту інформації у мережах загального користування шляхом введення критеріїв оцінки ефективності системи захисту інформації. Створена формальна модель може використовуватися для синтезу систем захисту інформації у будь-якому класі мереж загального користування шляхом уточнення її критеріїв.

1. Ленков С.В. Методы и средства защиты информации: в 2 т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К.: Арий, 2008. –Т.2: Информационная безопасность. – 344 с. 2. Хома В.В. Методи та засоби забезпечення конфіденцийності телефонних повідомлень / В.В. Хома // Сучасна спеціальная техніка. – 2009. – №3(18).– С. 50–59. 3. Организация виртуального секретного канала связи // А.В. Лобанцев, А.Л. Гурков / "Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики". – 2005. – Вып. 20. 4. Степанов В.Д., Хорошко В.О. Захист інформації НДІ ГУР МОУ: зб. наук. пр. – К.: МОУ, 2003. – Вип.5. 5. Степанов В.Д., Хорошко В.О. Оценка стойкости многоуровневой комплексной системы защиты информации // Захист інформації. – 2003. – № 3. 6. Степанов В.Д., Хорошко В.О. Оцінка ефективності комплексної системи захисту інформації // Захист інформації. – 2004. – № 3. 7. Бєлошапкін В.К., Пустовіт СМ., Степанов В.Д. Формалізація проблеми оптимізації комплексної системи захисту інформації // Захист інформації. – 2005. – № 3. 8. Петров А.А. Определение технических характеристик систем активной защиты информации / А.А. Петров // Захист інформації. – 2009. – № 3(44). – С. 66–68. 9. Клейнрок Л. Вычислительные системы с очередями. – М.: Мир, 1973. 10. Петров А.А. Методы защиты информации в сетях общего пользования / А.А. Петров // Вісник СНУ ім. В. Даля. – 2008. – №126. – С. 81–86.

УДК 681.3

О.О. Щелконогов
Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ БЕЗДРОТОВОЇ СИСТЕМИ КОНТРОЛЮ РОЗКРИТТЯ АПАРАТУРИ

Розглянуто методи захисту системи контролю розкриття апаратури (СКРА) від несанкціонованих і випадкових впливів. Вона побудована на основі технології сенсорних мереж стандарту IEEE 802.15.4. Ця технологія містить деякі засоби захисту, проте їх недостатньо для постійного функціонування СКРА. На основі проведеного аналізу загроз описано систему захисту, яка включає вбудовані і додаткові засоби захисту, які утворюють замкнений контур навколо СКРА.

Ключові слова: методи захисту, бездротова система, контроль розкриття апаратури, сенсорна мережа, несанкціонований доступ, шифрування.

This paper deals with methods of protection equipment opening control system (EOCS) against unauthorized and accidental influences. It is based on sensor network technology standard IEEE 802.15.4. This technology contains certain protections, but they are not sufficient for stable operation EOCS. Based on analysis of threats in the security system is described that includes a built-in and additional means of protection. Together they form a closed loop around the EOCS.

Key words: protection methods, wireless system, equipment opening control, sensor network, unauthorized access, encryption.

Вступ

Система контролю розкриття апаратури (СКРА) інформаційної системи (ІС) призначена для перекриття доступу до внутрішнього монтажу з метою здійснення несанкціонованих дій. Ця система складається із трьох компонентів [1]:

- датчиків розкриття апаратури;
- ланцюгів збору сигналів;
- пристрою централізованого контролю.