ТЕХНІЧНІ НАУКИ

УДК 004.056.8

А. А. ПЕТРОВ,
старший преподаватель кафедры компьютерных систем и сетей Восточноукраинского национального университета имени В. Даля,

В. А. ХОРОШКО,
доктор технических наук, профессор, заведующий кафедрой систем защиты информации Государственного университета информационно-коммуникационных технологий

ФОРМАЛИЗАЦИЯ ПРОБЛЕМЫ ОПТИМИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ОБЩЕГО ПОЛЬЗОВАНИЯ

Формализована проблема оптимизации защиты информации в сетях общего пользования.

Для оптимального выбора варианта системы комплексной защиты информации необходимо ввести критерии оценки эффективности системы защиты информации. Среди множества различных оценок основными представляются следующие:

1) вероятность реализации угрозы;

2) оценка возможных потерь (в стоимостном выражении);

3) оценка стоимости возможных мероприятий по недопущению реализации угроз.

Методика синтеза должна опираться на стабильные показатели. Поэтому за основу можно принять укрупненные структурные и сетевые модели информационной системы, угроз и защит, которые не зависят от конкретной реализации системы. В процессе создания подсистемы информационной безопасности и ее эксплуатации требования корректируются и конкретизируются так, что задача не теряет актуальности в следующие периоды жизненного цикла, как системы в целом, так и ее части – подсистемы информационной безопасности.

Остановимся на выделенных критериях более детально.

1. Вероятность реализации угрозы.

Пусть y – случайная величина, которая равна числу реализаций угрозы за период $[0,T]$, потери $F(y)$ случайны, зависят, вообще говоря, нелинейно от реализаций, и могут быть представлены в виде ряда Тейлора:

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

Тогда математическое описание случайной функции потерь будет иметь вид:

$$MF(y) = M \cdot \sum a_k y^k = \sum a_k My^k ,$$

где My^k – момент k-го порядка случайной величины y.

Таким образом, для вычисления критерия необходимо знать закон распределения случайной величины y на интервале $[0,T]$ и весовые коэффициенты a_k. Для неумышленных угроз можно принять пуассоновское распределение потока угроз по аналогии с простейшим потоком вызовов в системах массового обслуживания:

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

Для моментов получаем:

$$My = \lambda$$

$$My^2 = \lambda^2 + \lambda \quad \text{и т.д.}$$

Простейшая зависимость для случайной функции потерь – линейная:

$$U = a \cdot \xi \tag{1}$$

Тогда весовой коэффициент a имеет простое физическое содержание – потери от успешной одноразовой реализации угрозы Y. Переходим к математическому ожиданию и получаем:

$$MU = a \cdot \xi \cdot P \tag{2}$$

где P – достоверность реализации угрозы Y.

Для стационарного случайного потока угроз закон распределения случайной величины ζ может быть аппроксимирован пуассоновским

законом с интенсивностью. Тогда вероятность наличия n угроз в системе определяется формулами [1]:

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

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

где $p = \dfrac{\lambda}{m\mu}$,

μ – скорость обслуживания (ликвидации) угроз;

m – количество узлов графа ИС.

Введем матрицу потерь

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

где a_{ij} – потери от успешной одноразовой реализации угрозы y_i, которая направлена на j-ю компоненту информационной системы (далее – ИС).

Обозначим:

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

Тогда из (2–6) получаем простую оценочную формулу возможных потерь для неумышленных угроз:

$$\alpha_{\max} n p_n \le MU \le \alpha_{\min} n p_n \tag{7}$$

Потери от успешной одноразовой реализации угрозы могут быть оценены экспертами. Если в качестве экспертов выступает дельфийская группа [2], то оценки, которые дали эксперты, могут быть нормированы и тогда потери могут быть выражены действительным числом из интервала [0, 1], такой интерпретации границ:

1 – полное разрушение системы;

0 – полная защищенность от угроз (полное отсутствие потерь).

Отдельные параметры процесса для неумышленных угроз поддаются аналитическому определению: для m – очевидным образом, для λ, U – на основе статистических данных с помощью построения уравнения регрессии.

При построении модели потерь для решения задачи синтеза необходимо знать, на какие составляющие ИС может распространяться влияние угрозы, которая направлена на i-ю составляющую ИС, где на еще может проявляться и какие потери может принести. Для этого введем понятие глубины проникновения угрозы.

Назовем глубиной проникновения угрозы количество составляющих ИС, на которые может распространяться ее влияние при атаке одной составляющей.

Для того, чтобы определить глубину проникновения, построим матрицу досягаемости ИС на основе сетевой модели. Как считают В. М. Вишневский, В. А. Жожикашвили [3], вершина графа V_j называется досягаемой из вершины V_i, если существует направленный путь из V_i в V_j.

Введем определение:

ΓV_i – множество вершин, которые достигаются из V_i при использовании путей длины 1;

$\Gamma(\Gamma V_i) = \Gamma^2 V_i$ – множество вершин, которые достигаются из V_i при использовании путей длины 2;

$\Gamma(\Gamma^{n-1} V_i) = \Gamma^n V_i$ – множество вершин, которые достигаются из V_i при использовании путей длины n.

Для решения задачи определения множества всех вершин графа, которые достигаются из данной вершины, достаточно найти объединение множеств $\{V_i\} \vee \{\Gamma V_i\} \vee \dots \vee \{\Gamma^n V_i\}$, называемое транзитивным замыканием $\bar{r}$ вершины V_i.

При изучении досягаемости удобен матричный способ. Так, единичную матрицу E можно рассматривать как матрицу досягаемости с использованием путей длины 0; матрицу смежности A – как матрицу досягаемости с использованием путей длины 1. Но матрица смежности A выражает отношение Γ на множестве вершин $\{V_i\}$. Тогда матрица A^2, которая выражает отношение Γ^2, представляет собой матрицу досягаемости с использованием путей длины 2 и т.д.

Таким образом, транзитивное замыкание $\bar{r}$ отношения Γ, которое задано m вершинами графа, выражается матрицей $\bar{A}$, которая определяется формулой

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

Отсюда матрица $\bar{A}$ и матрица досягаемости R находятся в соотношении

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

Процесс добавления матриц прерывается, когда результат перестает изменяться.

Определим теперь вероятность p_{ki} – вероятность реализации угрозы y_k, которая направлена на i-ю составляющую ИС. Для этого воспользуемся теоремой ВСМР [3].

Однако прежде чем это сделать, введем ряд необходимых определений.

Обозначим через $n = \{n_{ir}\}$ – количество угроз y_r, направленных на i-ю составляющую ИС. Число n определяет состояние ИС.

Входной поток угроз назовем потоком первого типа, если из источника поступает один пуассоновский поток, интенсивность которого λ является функцией общего количества угроз в ИС в состоянии n.

Входной поток угроз назовем потоком второго типа, если имеется l пуассоновских потоков угроз, которые поступают в соответствующие подсистемы ИС, интенсивности которых λ_i являются функциями количества угроз в соответствующей подсистеме ($j=1,2,\ldots,l$).

Представим, что ИС состоит из центров типа 1, который характеризуется следующим образом.

Центр типа 1. Ликвидация угроз в центре осуществляется в соответствии с дисциплиной FIFO. Продолжительность ликвидации угроз имеет одно и то же экспоненциальное распределение с интенсивностью $\mu_i(n_i)$ (i – номер данного центра в ИС), которая зависит от количества угроз в центре n_i.

По теореме ВСМР стационарное распределение вероятностей $P(n_{ir}) = P_{ir}$ существует и имеет мультипликативный вид:

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

где $f_i(n_i) = \begin{cases} \left(\frac{1}{p_i}\right)^{n_i} \cdot \prod_{j=1}^{n_i} e_j n_{ij} \text{, если выходной} \\ \end{cases}$ поток имеет первый тип;

$\lambda^*(n^*) = \prod_{j=1}^{l} \prod_{i=0}^{\mu(n^*, E_j)-1} \lambda_j(i)$ – если выходной поток имеет второй тип;

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

где e_{ir} – относительная интенсивность потока угроз y_r, который проходит через центр i; μ – количество угроз в ИС; $\mu(n, E_j)$ – количество угроз в подсистеме E_j.

Перейдем теперь к формулированию задачи синтеза комплексной системы защиты информации.

Введем матрицы:

1. Матрица выбора защит

$$P^y = \begin{vmatrix} & Z_1 & \ldots & \ldots & Z_m \\ Y_1 & P_{11} & \ldots & \ldots & P_{1m} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ Y_n & P_{n1} & \ldots & \ldots & P_{nm} \end{vmatrix},$$

где значение P_{ij} означает вероятность реализации угрозы y_i при наличии защиты Z_j.

2. Матрица выбора защит

$$B = \begin{vmatrix} & Z_1 & \ldots & \ldots & Z_m \\ Y_1 & b_{11} & \ldots & \ldots & b_{1m} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ Y_n & b_{n1} & \ldots & \ldots & b_{nm} \end{vmatrix},$$

где

$b_{ij} = \begin{cases} 1 - \text{когда при угрозе } y_i \text{ выбрана защита } z_i, \\ 2 - \text{когда при угрозе } y_i \text{ не выбрана защита } z_j. \end{cases}$

3. Матрица стоимости защит

$$C = \begin{vmatrix} & Z_1 & \ldots & \ldots & Z_m \\ Y_1 & c_{11} & \ldots & \ldots & c_{1m} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ Y_n & c_{n1} & \ldots & \ldots & c_{nm} \end{vmatrix},$$

где c_{ij} – стоимость i-й защиты при атаке j-ой угрозы.

Рассмотрим выражения:

1) λ – интенсивность возникновения угроз;

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

3) $MU = \sum_i \sum_j \sum_r a_{kj} p_{kj} r_j \xi_{ki}$;

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

5) матрица эффективности $|l| = E \quad P^y$,
где E – единичная матрица.

Первое выражение определяет интегральные потери от возможных угроз при наличии защит и с учетом глубины проникновения угрозы; r_j – строки матрицы достижимости R.

Второе выражение определяет возможную стоимость защиты.

Третье выражение определяет интегральные потери от возможных угроз без использования защиты.

Четвертое выражение определяет выбор компоненты l матрицы эффективности.

Задача синтеза оптимальной комплексной защиты информации формулируется теперь следующим образом: найти матрицу $\|b_{ki}\|$, такую, чтобы

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

Для решения задачи необходимо знать набор параметров процесса:

1) λ – интенсивность наступления угроз;

2) $\|\alpha_{ki}\|$ – матрицу потерь от успешной единичной реализации угрозы y_k, которая направлена на узел *i*-й ИС;

3) m – количество узлов структурного сетевого графа ИС;

4) R – матрицу достижимости сетевого графа ИС;

5) P^y – матрицу условных вероятностей;

6) C – матрицу стоимости средств и мероприятий защиты.

Таким образом, в постановке (9) задача оптимального синтеза (или оптимального проектирования) комплексной системы защиты информации полностью формализована и представляет собой многокритериальную задачу целочисленного программирования, которая может быть решена известными методами [3].

Список использованной литературы

1. Бєлошапкін В. К. Побудова спеціалізованої моделі інформаційної системи з метою синтезу комплексної системи захисту інформації / В. К. Бєлошапкін, С. М. Пустовіт, В. Д. Степанов // Захист інформації. – 2005. – № 3. – С. 78–83.

2. Клейнрок Л. Вычислительные системы с очередями / Л. Клейнрок. – М. : Мир, 1973. – 600 с.

3. Вишневский В. М. Сети массового обслуживания: теория и применение к сетям ЭВМ / В. М. Вишневский, В. А. Жожикашвили. – М. : Радио и связь, 1988. – 192 с.

Надійшла до редколегії 11.05.2011

ПЕТРОВ А. О., ХОРОШКО В. О. ФОРМАЛІЗАЦІЯ ПРОБЛЕМИ ОПТИМІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ В МЕРЕЖАХ ЗАГАЛЬНОГО КОРИСТУВАННЯ
Формалізовано проблему оптимізації захисту інформації в мережах загального користування.

PETROV A., KHOROSHKO V. THE FORMALIZATION OF THE OPTIMIZATION PROBLEM OF INFORMATION SECURITY IN PUBLIC NETWORKS
The optimization problem of information security in public networks is formalized.