УДК 681.324.001:681.3.004

Пустовит С.Н., Степанов В.Д., Хорошко В.А.

РАСПРЕДЕЛЕНИЕ РЕСУРСОВ В МНОГОРУБЕЖНОЙ КОМПЛЕКСНОЙ СИСТЕМЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Целью защиты информации является деятельность, направленная на предотвращение утечки информации по различным каналам и их блокирование.

Защита включает в себя определение возможных каналов утечки информации, оценка важности самой информации и разработка мероприятий по предотвращению её утечки и хищения.

Определение потенциальной ценности информации позволяет подумать, в первую очередь, о безопасности наиболее важных секретов, утечка которых способна нанести ущерб.

Поэтому объектом технической защиты и является информация, которая попадает под действие Закона Украины "Об информации" или конфиденциальная информация переданная государству во владение или использование. Исходя из этого определяется цель защиты, которой является предотвращение утечки или нарушения целостности информации (1). Она может быть достигнута построением комплексной системы технической защиты информации (СТЗИ), которая представляет собой организованную совокупность методов и средств обеспечения защиты информации.

Техническая защита информации обеспечивается применением защищенных программ и технических средств обеспечения информационной деятельностью, программных и технических средств защиты информации (ТЗИ) и средств контроля, имеющих сертификат соответствующего требования нормативных документов по технической защите, также применением специально-технических сооружений, средств и систем. При этом средства ТЗИ могут функционировать автономно или совместно с техническими средствами обеспечения информационной деятельности в виде самостоятельных устройств или встроенных в них составных элементов (1).

Оперативное решение задач ТЗИ достигается организацией управления системой защиты информации, для чего необходимо (2):

- изучать и анализировать технологию прохождения информации в процессе информационной деятельности;
- оценивать подверженность информации воздействию угроз в конкретный момент времени;
- оценивать ожидаемую эффективность применения средств обеспечения ТЗИ;
- определять дополнительную потребность в средствах обеспечения ТЗИ;
- осуществлять сбор, обработку и регистрацию данных, относящихся к защите информации;
- разрабатывать и реализовывать предложения по корректировке СТЗИ в целом или отдельных ее элементов.

Основы стратегии защиты информации при общем подходе- это выбор основных и наиболее важных базовых системно-концептуальных положений и ориентиров при планировании, разработке и реализации этой стратегии. При этом центральным вопросом управленческого решения стратегического характера есть оценка объема необходимых ресурсов защиты и их оптимальное или наиболее распределение не только требуемого, но и непрерывного адаптивно-управляемого уровня гарантированной защиты. Гарантированность защиты- требование очень серьезное и с практических, и с теоретических позиций. Поэтому о гарантированности можно говорить только с

достоверностью и в контексте обязательного выполнения требований и рекомендаций используемых при этом стандартов безопасности.

Основы стратегии защиты информации включают в себя необходимость использования двух терминологических понятий: стратегия технической защиты информации и стратегия безопасности защищаемой информации с учетом последних требований нормативных документов по вопросам технической защиты информации Департамента специальных телекоммуникационных систем и защиты информации СБ Украины.

Из этого следует, что основной целью реализации стратегии ТЗИ является исключение или усложнение реализации угроз информации, снижение ущерба от реализации угроз и обеспечение безопасности информации.

Универсальных систем защиты на все случаи не существует, так как каждая защита создается для конкретного объекта, его окружения и внешней среды, под конкретные угрозы, функциональные требования и требуемый уровень защищенности. При их изменении защита должна быть способной адаптироваться к ним.

На практике в большинстве случаев система защиты состоит из нескольких звеньев и рубежей (3). Известно, что при попытке преодолеть защиту нарушитель попытается использовать наиболее слабое направление или рубеж в этой системе. По этой причине итоговая прочность СЗИ будет определяться прочностью наиболее слабого направления или рубежа в этой системе.

Если прочность слабого рубежа не удовлетворяет заданным требованиям, то этот рубеж укрепляется или заменяется на более прочный.

Следовательно, вероятность эффективной защиты информации при многорубежной системе определяется зависимостью:

$$P_{\Sigma} = P_{СЗИ1} * P_{СЗИ2} * \ldots * P_{СЗИN},$$

где $P_{СЗИN}$ – вероятность эффективной защиты N-го рубежа СЗИ, N – порядковый номер рубежа.

Эффективность механизма защиты в значительной степени зависит от реализации ряда принципов. Во-первых, механизмы защиты следует проектировать с учётом распределения ресурсов между рубежами и возможностью их перераспределения. Во-вторых, вопросы защиты следует рассматривать комплексно в рамках единой системы защиты.

Системный подход обеспечивает адекватную многоуровневую многорубежную защиты, рассматриваемую как комплекс организационно-правовых и технических мероприятий. Кроме того, при реализации механизмов защиты должны использоваться передовые, научно обоснованные технологии защиты, обеспечивающие требуемый уровень безопасности, приемлемость для пользователей и возможность наращивания и модификации СЗИ в дальнейшем.

Пусть комплексная СТЗИ характеризуется множеством рубежей Р, которые обеспечивают противодействие множеству несанкционированных действий Д. Пусть Р состоит из n рубежей, а Д содержит m действий.

Каждый рубеж $p_i \in P$ характеризуется доступной мощностью a_i . в соответствии с множеством Р имеем вектор $a=(a_1,\ldots,a_n)$ ресурсов рубежей.

Каждое несанкционированное действие $d_i \in Д$ соответствует набору действий злоумышленника и имеет требуемый ресурс для выполнения поставленной задачи (возможно и неоднократного) в течение суток z_i (опер/сут). По всем действиям множества Д имеем вектор $Z=(z_1,\ldots,z_m)$ требуемых ресурсов.

По каждому действию даны два вектора V_i и W_i , где $V_i=(v_{i1},\ldots,v_{in})$ множества P, вектор $W_i=(w_{i1},\ldots,w_{im})$ определяет интенсивность нападений при нападении d_i с задачами других противоправных действий множества Д. Здесь $w_{ii}=0$. По всей совокупности нападений имеем прямоугольную матрицу V размера mxn и квадратную матрицу W размера mxm, составленные из векторов V_i иW_i , $1 \le i \le m$, соответственно. Будем считать, что ресурсы несанкционированного действия $d_i \in$ Д могут быть реализованы только против одного любого рубежа множества P, т.е. действие производится против конкретного рубежа.

Пусть даны множества P и Д, представленные кортежами <P,a,R> и <Д,Z,V,W>, где a - вектор доступности к информации, R – матрица расстояний между рубежами, Z – вектор ресурсов противоправного действия, V – матрица интенсивности нападений. Требуется найти полное отображение β: Д→P, чтобы среднеквадратичная длина $L(\beta)$ маршрута несанкционированных действий принимала минимальное значение, т.е.

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

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

$h_{ij}=\{0,1\}$ определяем, целевое действие a_i на конкретный рубеж p_j,

$$h_{ij} = \begin{cases} 1, \text{если } \beta(d_i) = p_j \\ 0 \text{ в противном случае} \end{cases}$$

при условии $\sum_{i=1}^{m} z_i h_{ij} \le a$ для всех $p_j \in P$.

Представим вектор Z в виде m-мерного вектора-столбца $Z = \begin{pmatrix} z_1 \\ \ldots \\ z_m \end{pmatrix}$, где z_i – объем противоправных действий при нападении d_i. Тогда функцию β можно представить характеристической функцией (характеристической матрицей) H её трафика, т.е.

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

Пусть p_i – номер некоторого рубежа. Двоичный m–мерный вектор-столбец H_j, содержащий единицу на местах с номерами составляющих противоправное действие, назовем характеристическим способом p_i – рубежа.

Используя [5] описывающее скалярное произведение векторов Z и $H_i - ZH_i = \sum_{i=1}^{m} z_i h_{ij}$ запишем, что $H_j c_j$ равно суммарному $a_i \in A$ со всеми рубежами, а произведение $H_i c_j$, где $i \neq j$, равно интенсивности потока между рубежами p_i и p_j. Это значение обозначено S_{ij}, т.е. $S_{ij}=H_i c_j$. Квадратную матрицу ранга n значений S_{ij} обозначим S.

Суммарный поток между рубежами

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

Тогда функционал

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

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

Таким образом, задача сводится к минимизации билинейного функционала на целочисленных (двоичных) векторах при линейных ограничениях вида

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

При выбранном критерии задач нападений распределяется рубежам и сводится к разбиению множества Д на подмножества и назначению этих подмножеств рубежам множества Р, что соответствует совместному решению задач разбиения графа на части и задачи назначения. Получение оптимального решения связано с полным перебором различных вариантов разбиения. Для решения таких задач используется, как правило, метод ветвей и границ. Недостатком этого метода [6] является сложность реализации при сравнительно невысокой эффективности.

Поскольку в СЗИ значение m+n достаточно большое, целесообразно использовать для решения данной задачи эвристические алгоритмы оптимизации. В основном известные эвристические алгоритмы [7] можно отнести либо к алгоритмам последовательного противодействия подсистемы защиты, либо к итерационным алгоритмам последовательного улучшения приближений с помощью парных перестановок задач между рубежами.

На практике часто имеют место ситуации, когда каждое неправомерное действие $d_i \in Д$ представлено набором задач, которым могут противостоять различные рубежи множества Р, и когда нападению d_i противостоит только один рубеж. В этом случае рассматриваемая задача несколько упрощается и может быть сведена к классической транспортной задачи.

Пусть заданы множества Р и Д, где Р имеет ранее указанны смысл и представляется кортежем <P,a,R>.

Множество Д составлено из m нападений $\{d_1,\ldots,d_m\}$. Каждое нападение $d_i \in Д$ представлено набором задач и характеризуется требуемым ресурсом Z_i для их реализации. По всем противоправным действиям Д имеем вектор требуемых ресурсов $Z=(z_1,\ldots z_m)$. Требуемый ресурс Z_i нападения d_i может пресечен одной или несколькими рубежами множества Р при любом разбиении Z_i между собой.

По каждому нападению $d_i \in Д$ дан вектор $V_i=(v_{i1},\ldots,v_{in})$, определяющий интенсивность нападений d_i на рубежи множества Р. Предполагается, что все задачи связанные с нападением $d_i \in Д$ обладают одинаковой удельной, относительно единицы требуемого ресурса, интенсивностью f_{ij} противоправных действий против рубежей $p_i \in P$, т.е.

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

И так, имеем в качестве исходной информации множества P и Д, представленные соответственно кортежами

$$<P,a,R> \text{ и } <Д,Z,V>,$$

где V – матрица интенсивностей нападений множества Д на рубеж множества P.

Требуется определить распределение ресурсов нападений Д по рубежам множества P . В результате распределения ресурсов нападения формируется матрица Q, в которой каждому противоправному действию должна быть сопоставлена вектор-строка $q_i=(q_{i1},\ldots,q_{in})$ размерности n, представляющая собой распределение ресурсов противоправных действий d_i по рубежам множества P, т.е. k-й компонент q_{ik} вектора q_i представляет собой объем задач нападения d_i на k-ый рубеж защиты. Совокупность распределений противоправных действий множества Д определим как отображение γ: $Д \rightarrow N^n$, здесь N^n – векторное пространство n-мерных векторов, компоненты которых являются целыми числами. Качество распределения γ будет оценено значением средневзвешенной длины $L(\gamma)$ маршрута нападения.

Основой определения $L(\gamma)$ служит штраф для единицы ресурса нападения d_i, $i=1,2,\ldots,m=[Д]$, закрепленной за p_j-ым рубежом. Если единица ресурса нападения действующая на p_j-ый рубеж, то ей соответствует штраф

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

Итак для каждого нападения $d_i \in Д$ имеем вектор $c_i=(c_{i1},\ldots,c_{in})$, k-й компонент c_{ik} которого определяет ущерб за единицу ресурса нападения d_j, закрепляемую за рубежом p_k.

Функция ущерба, характеризующая выбранное распределение противоправных действий γ по рубежам, имеет вид

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

При составлении расписания γ желательно минимизировать функцию

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

где λ – независимая от распределения γ величина, определяющая суммарный поток нападений в соответствии с выражением

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

Если γ – выбранное распределение, то оно, очевидно, должно удовлетворять следующим условием:

6 7 8

1) $\forall d_i \in Д \;\left|\gamma(d_i) = q \geq 0 = 0,0,\ldots,0\right.$ (положительность),

2) $\forall d_i \in Д \;\left|\sum_{j=1}^{n} q_{ij} \leq z_i\right.$ (ограниченность),

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

Таким образом, задача распределения требуемых ресурсов нападения между рубежами в приведенных выше понятиях и обозначениях может быть сформулирована следующим образом.

Пусть задана система несанкционированных действий <Д,Z,V> и система защиты <P,a,R>. Требуется определить такое положительное, ограниченное и реализуемое распределения γ, чтобы $L(\gamma)$ принимало минимальное значение.

Поставленная таким образом задача, сводится к классической транспортной задаче.

Для этого поставим в соответствие каждому p_i рубежу источник ресурса p_j, $1 \le j \le n$, с наличным ресурсом a_j, а каждому нападению $d_i \in Д$ поставим соответствующего злоумышленника d_i, $1 \le i \le m = |Д|$, с требуемым ресурсом z_i. Стоимость применения единицы ресурса нападения d_i от злоумышленника p_j есть компонент c_{ij} вектора c_i. Объем ресурса, потребляемый нападением d_i от p_i, есть q_{ij}. Тогда математическая постановка классической транспортной задачи имеет вид:

минимизировать $F = \sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}q_{ij}$ при ограничениях,

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

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

$c_{ij} \ge 0$ и $q_{ij} \ge 0$ для всех i и j.

Чтобы задача имела допустимое решение, требуется, чтобы общие ресурсы злоумышленников были, по крайней мере, не меньше общей возможности защитника, т.е. чтобы выполнялось условие:

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

Однако при анализе транспортной задачи и построении алгоритма ее решения удобно принять, чтобы общая мощность злоумышленников была равна общей возможности защиты, т.е.

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

С этой целью достаточно ввести имитацию (n+1)-й наподения с ресурсом $a_{n+1} = \sum_{i=1}^{m} z_i$ и ложное (m+1)-й срабатывание, равное $z_{m+1} = \sum_{j=1}^{n} a_j$, и принять стоимость $c_{m+1,j} = 0$ для j=1,2,...,n+1, а стоимость $c_{i,n+1}$, i=1,2,...,m равной сколь угодно большой величине $b > \max_{\substack{1 \le i \le m \\ 1 \le j \le n}} (c_{ij})$.

Следовательно суммарная мощность имитируемого нападения равна суммарному ложному срабатыванию. Отсюда модель транспортной задачи принимает вид:

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

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

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

положительные целые числа, удовлетворяющие условию:

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

Данная модель транспортной задачи имеет n+m+1 переменных. Для ее решения может быть использована одна из модификаций симплекс-метода (метод потенциалов) [7].

Проведенные исследования позволяют оценить стойкость многорубежной комплексной системы технической защиты против действий злоумышленника. Причём полученные результаты дают возможность с достаточно высокой точностью оценить эффективность распределения ресурсов ТСЗИ между рубежами защиты при направленном и сконцентрированном преодолении определённого рубежа.

Список литературы

1. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

2. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

3. Шорошев В. В., Ильницкий А. Е. Основы стратегии защиты информации в компьютерных системах / Бизнес и безопасность, 2000, №2.-с.6-7.

4. Хорошко В. А. Модель системы защиты информации./ Захист інформації,1999, №1.-с.5-11.

5. Арфкен Г. Математические методы в физике. - М.: Атомиздат, 1970.-712 с.

6. Мину М. Математическое программирование. – М.: Наука, 1990.-488 с.

7. Сторский В. П. Математический аппарат инженера. – К.: Техніка, 1975.-768 с.

Поступила 25.04.2003г.

УДК 004.56.021.2: 510.22 (045)

А.Г. Корченко, В.А. Рындюк

ИССЛЕДОВАНИЕ МЕТОДОВ ФОРМИРОВАНИЯ ФУНКЦИЙ ПРИНАДЛЕЖНОСТИ НА ОСНОВЕ КОЛИЧЕСТВЕННЫХ ПАРНЫХ СРАВНЕНИЙ

В настоящее время все чаще при решении различных прикладных задач применяют аппарат теории нечетких множеств (НМ). Эта тенденция повлияла на создание моделей принятия решений в области информационной безопасности. Первым шагом при создании таких моделей является формализация нечетких понятий и отношений, используемых при описании их элементов. В этой связи важным является вопрос построения функции принадлежности (ФП) НМ по результатам опроса экспертов (ЭО) или путем анализа статистических данных. Этому вопросу посвящен ряд работ [1-7], в которых описывались прямые и косвенные методы формирования ФП одним или группой экспертов. Для эффективного решения подобных задач необходимо сделать правильный выбор нужного