УДК 004.49:004.7

Касумов В.А., Мамедов С.З.
Gasimov V.A., Mamedov S.Z.

РАЗРАБОТКА ЭФФЕКТИВНОЙ СТРУКТУРЫ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ДЛЯ КОРПОРАТИВНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

THE DEVELOPMENT OF EFFICIENCY STRUCTURE OF INFORMATION SECURITY SYSTEM FOR CORPORATE COMPUTER NETWORKS

Аннотация. В статье предложена модель системы безопасности информации для корпоративных компьютерных сетей, разработаны методы определения структуры, а также вертикального (функционального) и горизонтального (географического) разбиения структуры системы безопасности информации.

Summary. In the article the model of information security system for corporate computer networks is offered, methods of definition, and also vertical (functional) and horizontal (geographical) decomposition of structure of information security system are developed.

В настоящее время существует проблема защиты информации. Средства обеспечения безопасности информации в корпоративных компьютерных сетях (ККС) можно разделить на два основных класса: локальные и сетевые. Локальные средства защищают отдельные абонентские системы и сервера, а также их ресурсы, в т.ч. информационные. Сетевые средства информационной безопасности обеспечивают управление потоками защищаемых данных в ККС, выполняют свои функции в тесном взаимодействии с другими компонентами и подсистемами сети согласно протоколам управления передачи данных. Сетевые средства размещаются на разных узлах сети и при необходимости используются (задействуются) системой безопасности информации [1-3].

Практика показывает, что применение отдельных средств безопасности (как локальных, так и сетевых) не всегда дает желаемый результат. Для достижения требуемого уровня защищенности необходимо реализовать множество методов и средств, которые применяются в совокупности. А для этого требуется разработка единой политики безопасности, а также реализация общей системы безопасности информации (СБИ) корпоративной сети на основе данной политики.

В работе [1,4] рассматриваются вопросы создания системы безопасности для открытых компьютерных сетей. Но особенности корпоративных сетей здесь остаются вне рассмотрения. В работе [2] основное внимание уделено механизмам защиты, основанные на криптографии, а также рассмотрены средства защиты в электронных платежных системах. В [3] рассмотрены основные концептуальные вопросы безопасности корпоративных сетей.

В этих и других работах сделаны серьезные шаги к разработке методов и средств защиты и информации в корпоративных сетях, однако не рассматривались задачи создания единой системы безопасности информации, которая включала бы все необходимые методы и средства, могла осуществить требуемые мероприятия и противодействовать возможным угрозам в сети.

СБИ должна иметь по крайней мере одно средство для обеспечения безопасности на каждом возможном пути проникновения в систему или доступа к объектам угроз. В такой системе должны точно определяться все защищаемые объекты, оцениваться методы и средства обеспечения безопасности [1,4,5].

Эффективность распределенной СБИ зависит от ее структуры, степени распределенности функций и компонентов по узлам корпоративной сети, а также от времени реакции системы на появляющиеся угрозы и эффективности протоколов взаимодействия.

Исходя из вышесказанного, цель данной статьи – решить задачу создания системы безопасности для корпоративных сетей.

1. Определение структуры СБИ для корпоративной сети. Пусть $O = \{o_1, o_2, ..., o_J\}$ – множество защищаемых объектов (ресурсов) ККС, $T = \{t_1, t_2, ..., t_I\}$ – множество угроз и злоумышленных действий, направленных на объекты ККС и нарушающих их безопасность. Вероятность появления угроз и злоумышленных действий относительно отдельных объектов системы определяет основную характеристику этого множества.

Модель системы безопасности можно построить на основе отношений "объект-угроза" [1, 5]. А эти отношения наглядно можно представить в виде двухдольного графа (рис. 1). Как видно из рисунка, первую часть графа составляют защищаемые объекты, а вторую – угрозы, направленные на эти объекты.

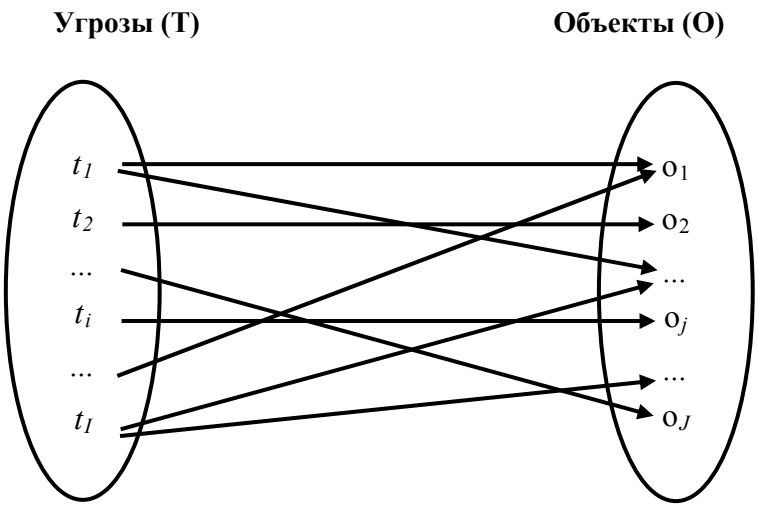

Рисунок 1 – Модель системы безопасности типа "объект-угроза"

Если угроза t_i может воздействовать на объект o_j, это значит, что в данном графе существует дуга (t_i, o_j). Здесь учитывается такое предположение, что отношения между угрозами и объектами не являются "один к одному". Другими словами, одна угроза может быть направлена к нескольким объектам, а также один объект может оказаться под воздействием нескольких угроз. Здесь целью обеспечения информационной безопасности является исключение всех дуг, показывающих возможные пути вхождения или воздействия угроз к объектам.

Для обеспечения безопасности информации в ККС в модель включается множество средств и методов защиты $M = \{m_1, m_2, ..., m_K\}$, в результате чего каждая дуга (t_i, o_j) делится на две дуги: (t_i, m_k) и (m_k, o_j). Узлы m_k в граф вводятся таким образом, что все дуги (t_i, o_j), которые ведут прямо от угрозы к объекту, были исключены.

Исходя из вышеприведенных определений систему безопасности можно представить в виде тройки {O,T,M}. Для определения структуры системы введем следующие матрицы:

– $P = \|p_{ij}\|_{I \cdot J}$, p_{ij} – вероятность появления угрозы t_i в отношении объекта o_j ККС;

– $V = \|v_{ij}\|_{I \cdot J}$, v_{ij} – коэффициент, определяющий уровень объема временного и материального расхода для защиты объекта o_j от угрозы t_i;

– $Z = \|z_{ij}\|_{I \cdot J}$, z_{ij} – объем ущерба владельца объекта o_j от действия угрозы t_i;

– $X = \|x_{ik}\|_{I \cdot K}$, $x_{ik} = 1$ – если средство защиты m_k может предотвратить угрозу t_i, иначе $x_{ik} = 0$.

С учетом вышесказанных предложен функционал, позволяющий определять такую структуру системы безопасности, которая дала бы оптимальное соотношение между величинами ущерба от нарушения безопасности информации и расхода (временного и материального) для предотвращения этой угрозы с помощью выше введенных параметров:

$$\sum_{i=1}^{I}\sum_{j=1}^{J}\sum_{k=1}^{K}\left(p_{ij} z_{ij} x_{ik} + v_{ij} p_{ij} x_{ik}\right) \to \min . \qquad (1)$$

Таким образом, задача определения требуемого уровня защиты ресурсов ККС сводится к задаче нахождения таких $x_{ik}, i = \overline{1, I}, k = \overline{1, K}$, которые минимизировали бы функционал (1) и удовлетворяли условиям:

$$\sum_{v=1}^{p} x_{iv} \geq 1, i = \overline{1, m} . \qquad (2)$$

Здесь условие (2) показывает, что в СБИ должно быть хотя бы одно средство для

предотвращения любой появляющейся угрозы.

2. Синтез структуры распределенной СБИ. Задача синтеза эффективной структуры СБИ заключается в классификации ее функций в виде отдельных подмножеств и расположении их по узлам ККС таким образом, чтобы при этом достигались повышение быстродействия, надежности, мобильности, облегчение реализации системы. Синтез структуры СБИ осуществляется с помощью двух подходов – вертикального и горизонтального распределения структуры СБИ [1]. Иногда вертикальное разбиение называют функциональным разбиением, а горизонтальное – географическим.

3. Вертикальное (функциональное) разбиение структуры СБИ. Пусть $F = \{f_1, f_2, ..., f_s\}$ – множество функций, реализуемых в СБИ. Матрицей $A = \left\| a_{ij} \right\|_{s \times s}$ обозначим взаимозависимость выполнения функций $f_i, i = \overline{1, s}$, элементы которой определим следующим образом: $a_{ij} = 1$, если функция f_i выполняется в зависимости от функции f_j, $a_{ij} = 0$, если отсутствует такая зависимость. Введем матрицу $X = \left\| x_{iq} \right\|_{s \times n}$, элементы которой определим как $x_{iq} = 1$, если функция f_i попала в q-е подмножество, иначе $x_{iq} = 0$.

При такой постановке количество подмножеств, на которые разбивается множество F (следовательно, число уровней), задается жестко, в данном случае оно равно n.

Введем матрицу штрафов $C = \left\| c_{pq} \right\|_{n \times n}$ между уровнями, элементы которой будут определяться как $c_{pq} = k \cdot |p - q|, p, q = \overline{1, n}$. Здесь $k > 1$ произвольно выбираемое число. Чем больше это число, тем больше штрафные веса между уровнями.

Таким образом, задача вертикального разбиения структуры СБИ сводится к нахождению таких $x_{iq}, i = \overline{1, s}, q = \overline{1, n}$, которые бы минимизировали функционал:

$$\sum_{i=1}^{s} \sum_{j=1}^{s} \sum_{p=1}^{n} \sum_{q=1}^{n} x_{iq} x_{jp} a_{ij} c_{pq} \to \min \tag{3}$$

и удовлетворяли условиям:

$$\sum_{q=1}^{n} x_{iq} = 1, i = \overline{1, s}. \tag{4}$$

Решение задачи (3) … (4) дает оптимальное разбиение функций СБИ на уровни, что позволяет достичь максимальную независимость выполнения, а также осуществлять правильный контроль за ее функционированием.

4. Горизонтальное (географическое) разбиение структуры СБИ. При реализации СБИ ее функции могут распределяться по узлам сети, что приводит к образованию различных структур. Примерами таких структур являются: централизованные, децентрализованные (распределенные), централизованно-децентрализованная (гибридные), централизованные с полным или частичным копированием и децентрализованные с полным или частичным копированием функций СБИ.

При горизонтальном разбиении ставится задача распределения функций СБИ по узлам сети в зависимости от сетевых и внешних требований таким образом, чтобы время реакции СБИ было наименьшим.

Пусть $F = \{f_1, f_2, ..., f_s\}$ – множество функций СБИ, $N = \{n_1, n_2, ..., n_n\}$ – множество узлов ККС. Тогда географическую структуру СБИ можно определять тройкой $\{F, N, A\}$. Здесь A определяет отношения между функциями СБИ и узлами ККС, т.е. схему распределения функций обеспечения безопасности по узлам сети. Элементы матрицы A определяются следующим образом: $a_{ij} = 1$, если функция f_i реализована на узле n_j, $a_{ij} = 0$ – в обратном случае.

Для централизованной структуры СБИ выполнятся следующие выражения:

$$\sum_{i=1}^{s} x_{iq} = 1, \quad \sum_{i=1}^{s} \sum_{j=1}^{h} x_{ij} = 0, \quad j \neq q.$$

Здесь узел n_q является центральным узлом.

Время реакции, вернее среднее время обслуживания СБИ – $T^{Б}$ можно выразить как

$$T^{Б} = \sum_{q=1}^{n} T_q^{уз} P_q ,$$

где $T_q^{уз}$ – среднее время обслуживания частью СБИ, расположенной на узле n_q, P_q – относительная вероятность обращения к части СБИ, расположенной на узле n_q, здесь $\sum_{q=1}^{s} P_q = 1$. Под частью СБИ подразумевается как сама СБИ (в случае централизованной структуры), так и ее отдельные модули или группа модулей и т.п.

Время $T_q^{уз}$ вычисляется следующим образом:

$$T_q^{уз} = \lambda \cdot T_q^{ф} + \nu \cdot T_q^{в}, \lambda + \nu = 1 , \tag{5}$$

здесь $T_q^{ф}$ – время передачи запросов между модулями СБИ для согласования выполнения функций, $T_q^{в}$ – время обслуживания внешних запросов, λ и ν относительные вероятности выполнения соответственно, внешних и внутренних функций СБИ.

Для корректности поставленной задачи должно быть удовлетворено условие, что каждая функция СБИ должна быть реализована хотя бы на одном узле:

$$\sum_{q=1}^{n} x_{iq} \geq 1, i = \overline{1,s} . \tag{6}$$

Таким образом, задача определения структуры и схемы размещения частей СБИ приведена к задаче целочисленного программирования, которая формулируется как нахождение таких $x_{iq}, i = \overline{1,s}, q = \overline{1,n}$, которые дали бы минимум функционалу (5) и удовлетворяли условиям (6).

В заключение отметим следующее. Предложенные выше методы позволяют реализовать такую структуру СБИ, которая обеспечивала бы желаемую эффективность и надежность функционирования системы, улучшение времени реакции ее на появляющиеся угрозы.

Решение задачи (1) … (2) позволяет гарантировано обеспечить безопасность информации в ККС и минимизировать объем ущерба от нарушения безопасности при разумных временных и материальных расходах. Результатом вертикального разбиения структуры СБИ является расслоение ее функций на уровни таким образом, чтобы при этом достигалась их максимально возможная независимость. Такой подход позволяет, с одной стороны, облегчить процесс реализации и дальнейшее совершенствование СБИ, с другой – осуществлять правильный контроль за ее функционированием. При горизонтальном разбиении, путем оптимального распределения функций СБИ по узлам сети в зависимости от сетевых и внешних требований достигается оптимальное значение времени реакции СБИ.

Путем анализа проведенных исследований можно сделать следующие выводы: время реакции в СБИ зависит от распределенности ее структуры, значение распределенности растет с ростом внешнего потока сети, данная зависимость ослабевает с уменьшением времени задержки в сети связи. Следует отметить, что минимум времени реакции системы достигается (в большинстве случаев в гибридных структурах) тогда, когда централизуются основные (часто используемые) функции обеспечения безопасности. Если централизованные функции реализуются на самом мощном узле сети, то можно обеспечить максимальную эффективность.

Литература

1. *Аббасов А.М., Алгулиев Р.М., Касумов В.А.* Проблемы информационной безопасности в компьютерных сетях. – Баку: "Елм", 1998. – 235 с.
2. *Соколов А.В., Шангин В.Ф.* Защита информации в распределенных корпоративных сетях и системах. – ДМК Пресс, 2002. – 656 с.
3. *Биячуев Т.А.* Безопасность корпоративных сетей. – С.Пб.: СПб ГУ ИТМО, 2004. – 161 с.
4. *Ярочкин В.И.* Информационная безопасность. – М.: Трикста, 2005. – 544 с.
5. *Касумов В.А., Мамедов С.З.* Моделирование системы информационной безопасности в корпоративных компьютерных сетях // Научные труды Аз.ТУ. – 2007. – № 1. – С. 6-10.