УДК 004.414.2=161.1

Э.И. Митряев[1]

E.I. Mitryaev

АНАЛИТИЧЕСКИЙ МЕТОД ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО КРИТЕРИЮ ДОСТУПНОСТИ ИНФОРМАЦИИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

ANALYTICAL METHOD OF THE ASSESSMENT OF INFORMATION SECURITY BY CRITERION OF AVAILABILITY OF INFORMATION TO THE SOLUTION OF PROBLEMS OF CREATION OF THE PROTECTED DISTRIBUTED INFORMATION SYSTEMS

В статье рассматривается проблема построения устойчиво функционирующей территориально распределенной информационной системы при условии воздействия на нее потенциально возможных деструктивных факторов техногенного и антропогенного характера. Для решения практических задач инженерного проектирования предлагается аналитическая модель, построенная на основе применения математической теории графов. В статье излагается аналитическая методика и приводится пример ее использования для решения конкретной задачи.

Ключевые слова: *распределенная информационная система, защита информации, информационная безопасность, уязвимость информационной системы, доступность информации, связность каналов связи, граф структуры информационной системы, пропускная способность канала связи.*

In the article is considered the problem of creation of steadily functioning territorially distributed information system on condition of impact on it of potentially possible destructive factors of technogenic and anthropogenous character. For the solution of practical problems of engineering design is offered the analytical model constructed on the basis of application of the mathematical theory of counts. In the article is given the analytical technique is stated and the example of its use for the solution of a specific objective.

Keywords: *distributed information system, information protection, information security, vulnerability of information system, availability of information, connectivity of communication channels, columns of structure of information system, communication channel capacity.*

Современная тенденция развития информационных технологий определяется переходом в сторону создания распределенных информационных систем и сетей. При этом, основной характеристикой этих систем является территориальная распределенность компонентов системы и наличие интенсивного обмена информацией между ними.

Масштабы применения и приложения информационных технологий стали такими, что наряду с проблемами производительности, надежности и устойчивости функционирования информационных систем остро встает проблема обеспечения информационной безопасности по критерию доступности циркулирующей в системах информации.

Понятие «информационная безопасность» было нормативно закреплено в качестве самостоятельной составляющей безопасности Российской Федерации в 1992 году. За прошедшее время было многое сделано для наполнения этого термина конкретным содержанием, определе-

[1] Доктор технических наук, профессор, профессор кафедры информационной безопасности факультета информационных систем и компьютерных технологий НОУ ВПО «Российский новый университет».

ния наиболее важных направлений деятельности государства в этой области.

На сегодняшний день сформулированы базовые принципы информационной безопасности, среди которых наибольшее актуальное звучание принимает обеспечение доступности информации для всех авторизованных пользователей.

Широкое внедрение в повседневную практику компьютерных сетей, их открытость, масштабность делают проблему защиты информации исключительно сложной. При анализе данной проблемы выделяют две базовые подзадачи:

1) обеспечение безопасности обработки и хранения информации в каждом из компьютеров, входящих в сеть;

2) защита информации, передаваемой между компьютерами сети.

В Федеральном законе Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1] дается следующее определение защиты информации как принятие правовых, организационных и технических мер, направленных, в частности, на реализацию права на доступ к информации, которое можно также трактовать и как обеспечение доступности информации.

В ГОСТ Р50922-2006 [2] дано следующее определение доступности информации: «Доступность информации (ресурсов информационной системы) – это состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно».

Таким образом, доступность информации есть свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующаяся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда в обращении к ним возникает необходимость.

Исходя из большого разнообразия условий, при которых может возникнуть необходимость защиты информации, общая целевая установка заключается в разработке стратегий защиты информации, включающих рациональное обеспечение требуемой защиты и надлежащего использования информационных ресурсов в любых условиях, даже в случае, если эти ресурсы будут подвергнуты деструктивному воздействию как извне, так и изнутри.

1. Особенности современных информационных систем как объектов защиты

Большинство современных информационных систем (ИС) обработки информации в общем случае представляет собой территориально распределенные системы, интенсивно взаимодействующие (синхронизирующиеся) между собой по данным (ресурсам) и управлению (событиям) локальных вычислительных сетей (ЛВС) и отдельных ЭВМ.

В распределенных ИС (РИС) возможны все традиционные для локально расположенных (централизованных) вычислительных систем способы несанкционированного вмешательства в их работу и доступа к информации.

В силу территориально распределенных компонентов системы и наличия интенсивного обмена информацией между ними, для РИС характерны новые специфические угрозы работе системы и нарушению доступности информации, в том числе:

– физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);

– отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);

– действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.).

2. Синтез распределенной информационной системы с гарантией информационной безопасности по критерию доступности информации

Проблема искусственных преднамеренных (умышленных) нарушений функционирования РИС различного назначения в настоящее время является одной из наиболее актуальных в связи с резко обострившейся геополитической обстановкой в мире. Наиболее справедливо это утверждение для стран с сильно развитой информационной инфраструктурой.

Создание информационной системы всегда связано с проблемой обеспечения ее информационной безопасности. Создание защищенной информационной системы заключается в выполнении совокупности мероприятий, направленных на разработку и/или практическое применение

таких информационных технологий, которые бы реализовали функции по защите информации в соответствии с требованиями стандартов и нормативных документов как во вновь создаваемых, так и в действующих системах.

Основные принципы и положения по созданию и функционированию защищенных систем изложены в нормативных документах. Согласно данным документам, информационная технология проектирования защищенной ИС в унифицированном исполнении включает в себя проведение следующих основных работ.

I. Анализ средств защиты

1. Представление организационно-структурного построения ИС в виде упорядоченного графа: узлы – типовые структурные компоненты, дуги – взаимосвязи между компонентами.

2. Представление технологии обработки защищаемой информации в виде строго определенной схемы.

3. Определение параметров защищаемой информации и условий ее обработки.

II. Оценки уязвимости информации

1. Определение значений вероятностей нарушения защищаемой информации в тех условиях, в которых она будет обрабатываться.

2. Оценки размеров возможного ущерба при нарушениях защищенности информации.

Учитывая активность, непрерывность, скрытность, количество и разнообразие потенциальных угроз информационной системе, проблему защиты информации относят к числу слабо формализуемых задач, т.е. задач, неразрешимых строго математически. В то же время, для решения проблемы проектирования защищенной ИС необходимы количественные оценки планируемых показателей информационной безопасности уже на этапе ее проектирования. На сегодня, для оценки различных показателей функционирования сложных систем в теории разработаны и доведены до практического применения различные аналитические методы.

3. Аналитический метод оценки показателя доступности информации

Распределенная информационная система (РИС) представляет собой многоуровневую иерархическую структуру, включающую множество узлов, связанных между собой определенным образом. Такой конструкции присуще свойство уязвимости, определяющейся тем, что за счет многочисленных узлов и связей между ними (учитывая, что нормальное функционирование нескольких узлов иерархической сети возможно только при нормальном функционировании одного основного узла, называемого управляющим) нередко проявляется «каскадный эффект», когда сбой в одном месте провоцирует перегрузки и выход из строя других элементов.

Проектирование новых РИС и развитие уже существующих связано с проблематикой принятия решений по использованию имеющихся сетевых структур:

– управлению потоками;

– распределению ресурсов между узлами.

Перечисленные проблемы тесно связаны с задачей определения связности и доступности информации в существующей или проектируемой ИС в условиях потенциально возможных деструктивных факторов техногенного или антропогенного характера.

Под связностью информационной системы понимается топологический вид сети межмашинных связей и надежностные характеристики компонентов этой сети.

С учетом показателя связности, доступность информации будем характеризовать способностью информационной системы в любой момент времени функционирования использовать суммарную производительность всех исправных ЭВМ для решения задач обработки и передачи информации. Кроме того, на значение показателя доступности информации сети сильно влияет минимальная пропускная способность (число каналов связи) на информационном направлении, ниже которой связь считается отказавшей.

Данной проблеме ИС посвящен ряд работ (Винокуров Д.Е. [3], Додонов А.Г. [4], Дудник Б.Я. [5], Кривулец В.Г. [6], Мельников Ю.Е. [7],. Сарыпбеков Ж.С. [8], Хорошевский В.Г [9] и др.).

В настоящее время актуальной является задача разработки аналитических моделей и методов, использующих полученные по аналогичным проблемам оценки показателей надежности и живучести РИС, результаты для оценки информационной безопасности РИС по критерию доступности информации, позволяющих решать задачи расчета ИБ РИС большой размерности и сложной структуры.

На макроуровне РИС выглядит как ансамбль ЭВМ, между которыми есть линии связи (каналы связи).

Эти элементы составляют макроструктуру (или структуру) РИС. Структура РИС описывается однородным графом $G = \{N; M\}$.

N – множество вершин (множество ЭВМ или системных устройств);

M – множество ребер (линии, каналы, связи).

Мощность N равна числу ЭВМ в РИС.

Структура РИС характеризуется:

1) связностью требуемого числа работоспособных ЭВМ в системе при ненадежных линиях связи;

2) способностью к реализации обменов информацией между любыми ЭВМ ИС в течение заданного времени (иначе – задержками при передаче информации между ЭВМ, которые не превышают установленной нормы).

В рамках формальной теории графов, структуру ИС можно представить в виде вектор-функции доступности информации:

$$L(\mathrm{G}, Q) = \{L_r(\mathrm{G}, Q)\}, \qquad (1)$$

где $L_r(\mathrm{G}, Q)$ – вероятность существования подсистемы ранга r.

Подсистема ранга r – подмножество работоспособных ЭВМ, связность которых устанавливается через работоспособность линии связи.

G – структура РИС (граф).

Q – пропускная способность (трафик) каналов связи между ЭВМ.

Пропускная способность – один из важнейших с точки зрения пользователей факторов. Она оценивается количеством данных, которые сеть в пределе может передать от одного подсоединенного к ней устройства к другому.

Пропускная способность канала связи определяется максимальной скоростью передачи информации по каналу связи в единицу времени и выражается формулой:

$$q = V/\, t,$$

q – пропускная способность канала (в битах в секунду или подобных единицах);

($q \in Q$)

t – время передачи.

Доступность информации при передаче информации между ЭВМ РИС определяется расстоянием (в смысле графов – у нас это время передачи информации (трафик) между вершинами структуры графа G, сопоставленными взаимодействующими ЭВМ.

Для оценки доступности информации в ИС используем диаметр "d" и средний диаметр "d_c" структуры.

Диаметр "d" определим как максимальное расстояние, определенное на множестве кратчайших путей между парами вершин структуры РИС.

$$d = \max\ \{d_{ij}\}.$$

Средний диаметр: $d_c = (N-1)^{-1} \sum_{i=1}^{n} ln$

d_{ij} – расстояние – минимальное число ребер, образующих путь из вершины i в вершину j,

$i, j \in N$,

n – число вершин, находящихся на расстоянии l от любой выделенной вершины (однородного) графа G.

Получение аналитических выражений для координат вектор-функции доступности информации (1) является сложной задачей, разрешимой лишь для частных случаев.

Для решения данной задачи используем представление однородного графа G РИС в виде матрицы смежности порядка ($m \times n$), где $n \in N$ – число вершин однородного графа G (число ЭВМ РИС) , $m \in M$ – число ребер (число каналов связи между смежными ЭВМ РИС).

Используя матричное представление графа ИС значения пропускной способности каналов связи в качестве весовых характеристик ребер графа РИС, можно решать различные практические задачи проектирования РИС по критерию доступности информации.

В качестве примера рассмотрим следующую задачу.

В силу большой пространственной протяженности линий связи через неконтролируемую территорию практически всегда имеется возможность подключения к ним либо вмешательства в процесс передачи данных со стороны злоумышленников. При этом меняется объем (трафик) передаваемой информации – что может служить показателем данной угрозы.

Современные топологии и протоколы требуют, чтобы сообщения были доступны большому числу узлов при передаче данных сообщений по назначению. Это гораздо дешевле и легче, чем иметь прямой физический путь каждой пары машин.

Для повышения пропускной способности РИС, с учетом деструктивных факторов на каналы связи, можно их проектировать с использованием различной физической реализации каналов связи (кабельные, волоконно-оптические, широкополосные радиоканалы) по критерию доступности информации.

Математически данная задача формулируется следующим образом.

Между абонентами X_1, X_2, X_3 РИС и территориально удаленными абонентами Y_1, Y_2, Y_3 этой же РИС может быть установлена связь по телефонным или широкополосным радиоканалам.

Матрицами A и B задано время, которое необходимо затратить при использовании телефонного или широкополосного радиоканала для связи абонента X_i с абонентом Y_j.

$$\mathrm{A} = \begin{array}{c} \\ X_1 \\ X_2 \\ X_3 \end{array} \begin{array}{c} \begin{array}{ccc} Y_1 & Y_2 & Y_3 \end{array} \\ \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \end{array}$$

Элементы a_{ij} матрицы А – это пропускная способность телефонных каналов связи.

$$\mathrm{B} = \begin{array}{c} \\ X_1 \\ X_2 \\ X_3 \end{array} \begin{array}{c} \begin{array}{ccc} Y_1 & Y_2 & Y_3 \end{array} \\ \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix} \end{array}$$

Элементы b_{ij} матрицы В – это пропускная способность широкополосных радиоканалов.

Для выбора каналов связи проектируемой сети по критерию доступности информации надо построить матрицу $\mathrm{C} = (c_{ij})$, где $c_{ij} = \min \{a_{ij}; b_{ij}\}$

Решение данной задачи в матричном представлении графа РИС успешно реализуется на ЭВМ.

Литература

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).

2. ГОСТ Р50922-2006 Защита информации. Основные термины и определения.

3. Винокуров Д.Е. Исследование живучести информационных сетей / Ю.Ю. Громов, Д.Е. Винокуров, Т.Г. Самхарадзе, И.И. Пасечников // Инженерная физика. – М. : Научтехлитиздат, 2006. – № 3. – С. 123–139.

4. Додонов А.Г. Введение в теорию живучести вычислительных систем / А.Г. Додонов, М.Г. Кузнецова, Е.С. Горбачик. – Киев : Наук. думка, 1990. – 184 с.

5. Надежность и живучесть систем связи / под ред. Б.Я. Дудника. – М. : Радио и связь, 1984. – 243 с.

6. Кривулец В.Г. Что такое теория связности и живучести транспортных сетей? / В.Г. Кривулец, В.П. Полесский. – М. : Инофрмационные процессы, 2001. – Т. 1. – № 2. – С. 199–203.

7. Мельников Ю.Е. Модель комплексной оценки и обеспечения живучести распределенных информационно-вычислительных систем / Ю.Е. Мельников, Ж.С. Сарыпбеков : материалы II Всесоюзной науч.-техн. конф. – М., 1988.

8. Сарыпбеков Ж.С. Многокритериальная оценка живучести РВС / Ж.С. Сарыпбеков, Б.А. Ченсизбаев // Однородные вычислительные системы, структуры и среды : тез. докл. V Всесоюзн. науч.-техн. конф. – М., 1991. – Ч. III. – С. 219–220.

9. Хорошевский В.Г. Инженерный анализ функционирования вычислительных машин и систем / В.Г. Хорошевский. – М. : Радио и связь, 1987. – 155 с.