Application of the theory of counts at identification of potential threats to security of information

Popova M.[1], Karpov A.[2]

Применение теории графов при выявлении потенциальных угроз безопасности информации

Попова М. С.[1], Карпов А. П.[2]

[1]Попова Марина Сергеевна / Popova Marina – студент;
[2]Карпов Артём Павлович / Karpov Artem – студент,
специальность: информационная безопасность телекоммуникационных систем,
факультет приборостроения, информационных технологий и электроники,
Пензенский государственный университет, г. Пенза

Аннотация: *в данной статье рассматривается возможность применения теории графов при описании и анализе схем информационных потоков информационной системы с целью выявления потенциальных угроз безопасности информации и построения эффективной системы защиты информации.*
Abstract: *in this article the possibility application of the theory of counts is considered at the description and the analysis of schemes of information streams of an information system for the purpose of identification of potential threats to security of information and creation of effective system of information security.*

Ключевые слова: *информационная безопасность, модель угроз безопасности информации, схема информационных потоков, теория графов.*
Keywords: *information security, model of threats to security of information, scheme of information streams, theory of counts.*

Современный этап развития общества характеризуется возрастающей ролью информации, которая рассматривается как один из основных ресурсов информационного общества. Хранение, обработка и передача информации осуществляются с помощью информационных систем, являющихся совокупностью, содержащейся в базах данных информации и обеспечивающих обработку информационных технологий и технических средств [1].

В связи с высокими темпами развития информационных технологий и технических средств проблема защиты информации в информационных системах становится все более актуальной. Для обеспечения безопасности информационных систем необходимо разработать эффективную систему защиты информации, которая представляет собой комплекс организационно-технологических мер, программно-технических средств и правовых норм, направленных на противодействие источникам угроз безопасности информации.

Для построения адекватной системы защиты информации необходимо разработать модель угроз безопасности информации. Как правило, модель угроз включает в себя описание информационной системы, идентификацию угроз безопасности информации и их источников, а также оценку вероятности (возможности) реализации угроз безопасности информации [2].

Важным этапом разработки модели угроз безопасности информации является описание информационной системы, поскольку правильность и полнота общей характеристики информационной системы, включающей описание структурно-функциональных характеристик ИС, её алгоритма работы и технологий обработки информации, позволяет идентифицировать все актуальные угрозы безопасности информации, а, следовательно, и грамотно разработать систему защиты информации.

На данный момент разработано много подходов к описанию и анализу информационных систем. К наиболее популярным относятся структурный (функциональный) и объектно-ориентированный подходы.

В данной статье рассмотрен структурный (функциональный) подход описания информационной системы, который основан на описании компонентов информационной системы и информационных потоков между ними.

Для описания взаимодействия компонент информационной системы может быть разработана схема информационных потоков системы, наглядно отображающая маршруты информации между компонентами информационной системы.

Для разработки и описания схемы информационных потоков системы удобно использовать теорию графов. При этом информационная система представляется в виде ориентированного графа, состоящего из конечного множества вершин, соответствующих компонентам ИС, и рёбер, отражающих информационные потоки (взаимосвязи) между ними.

Любой информационный поток схемы может характеризоваться следующими параметрами: источник информации, получатель информации, тип передаваемой информации, уровень конфиденциальности информации, направление движения информационного потока и др.

Например, на рисунке 1 представлена схема информационных потоков информационной системы, которая является локальной сетью, обрабатывающей конфиденциальную (КИ) и неконфиденциальную (НКИ) информацию и не имеющей подключений к внешним информационным сетям.

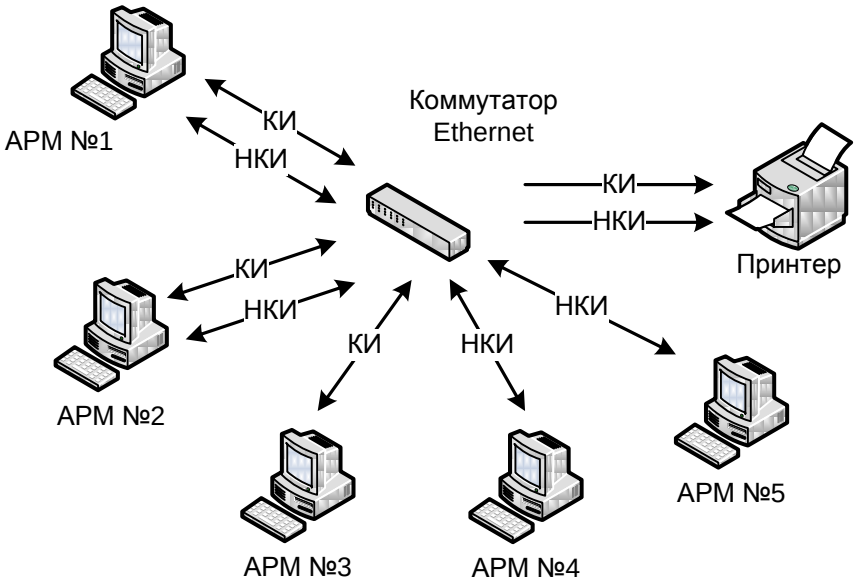

Рис. 1. Схема информационных потоков

Описание схемы информационных потоков можно провести с помощью описания трактов прохождения информации (маршрутов графа), при описании которых последовательно указывается источник информации, промежуточная аппаратура и получатель информации, а также вид передаваемой информации.

Например, источником конфиденциальной информации является автоматизированное рабочее место № 1 (АРМ №1), которое осуществляет её передачу (приём) через коммутатор Ethernet на АРМ №2-3 и принтер. Информационный поток может быть описан в следующем виде: АРМ №1 $\xleftarrow{КИ}$ Коммутатор Ethernet $\xleftarrow{КИ}$ АРМ №2 – 3 (Принтер).

Также схема информационных потоков может быть описана с помощью матриц, например, матриц смежности и инцидентности.

Матрица смежности графа отражает смежность вершин графа, т.е. смежность компонентов ИС, а матрица инцидентности отражает связи между вершинами и рёбрами (компонентами и информационными потоками).

Использование матриц смежности и инцидентности позволяет выявить все возможные тракты передачи информации в информационной системе, которые могут быть разделены на разрешённые (например, передача конфиденциальной информации с АРМ №1 на АРМ № 2) и запрещённые (например, передача конфиденциальной информации с АРМ №1 на АРМ № 5). При построении системы защиты информации в информационной системе необходимо учитывать выявленные запрещённые тракты передачи защищаемой информации и предусмотреть средства защиты от их возникновения.

Также матрица инцидентности позволяет определить компоненты информационной системы, которые обрабатывают информацию различных уровней конфиденциальности и являются потенциально опасными с точки зрения утечки конфиденциальной информации. Для этого можно использовать понятие «степени вершины», определяющего количество рёбер графа, инцидентных данной вершине. Например, степень вершин «АРМ № 1» и «АРМ № 2» равна двум, в связи с чем на данных технических средствах необходимо предусмотреть разграничение доступа к информации.

Это только часть методов теории графов, которые могут быть использованы при анализе схем информационных потоков с целью определения потенциальных угроз безопасности информации. Однако даже с их помощью можно сделать вывод о необходимости выделения в рассматриваемой информационной системе двух сегментов сети, осуществляющих обработку конфиденциальной и неконфиденциальной информации соответственно, и осуществлении их взаимодействия через межсетевой экран.

Таким образом, можно отметить практическую ценность применения теории графов при описании и анализе схем информационных потоков информационной системы с целью выявления потенциальных

угроз безопасности информации и построения эффективной системы защиты. Также стоит отметить, что применение математического аппарата теории графов позволяет автоматизировать процесс анализа схемы информационных потоков и исключить при этом человеческий фактор.

Литература

1. Федеральный закон от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Проект методического документа ФСТЭК «Методика определения угроз безопасности в информационных системах». [Электронный ресурс]. Режим доступа: http://fstec.ru/component/attachments/download/812/ (дата обращения: 21.11.2016).