КАЗАНСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
Институт физики
Кафедра радиофизики

Карпов А.В., Лапшина И.Р.

Имитационное компьютерное моделирование сложных радиосистем

Учебное пособие

Казань
2019

УДК 681.3.06
ББК 32.973.202
К26

Рекомендовано к изданию
Учебно-методическим центром КФУ

Рецензенты:
Кандидат физико-математических наук, доцент **Акчурин А.Д.**
Кандидат физико-математических наук, доцент **Ишмуратов Р.А.**

Карпов А.В.
К26 Имитационное компьютерное моделирование сложных радиосистем / А.В. Карпов, И.Р. Лапшина – Казань: Изд-во Казан. ун-та, 2019. – 61 с.

ISBN

Данное пособие предназначено для магистрантов Института физики направления магистратуры 03.04.03 – радиофизика. Учебное пособие посвящено основам компьютерного имитационного моделирования. Представлена классификация современных методов моделирования. Рассмотрены основные преимущества и недостатки имитационного эксперимента. Особое внимание уделено реализации имитационного эксперимента на персональном компьютере. Излагаемый материал сопровождается подробными графическими иллюстрациями и таблицами. Каждый раздел завершается списком контрольных вопросов, служащих для закрепления понимания учебного материала, или практическими заданиями. Целью практических заданий является создание программного комплекса, с помощью которого можно реализовать и протестировать компьютерную имитационную модель.

УДК 681.3.06
ББК 32.937.202

ISBN

ОГЛАВЛЕНИЕ

1.КЛАССИФИКАЦИЯ ВИДОВ МОДЕЛИРОВАНИЯ

Моделирование является одним из наиболее эффективных методов исследования сложных систем. В то же время сам термин «моделирование» используется практически во всех областях человеческой деятельности.

«Моделирование представляет собой один из основных методов познания, является формой отражения действительности и заключается в выяснении или воспроизведении тех или иных свойств реальных объектов, предметов и явлений с помощью других объектов, процессов, явлений, либо с помощью абстрактного описания в виде изображения, плана, карты, совокупности уравнений, алгоритмов и программ.

Возможности моделирования, то есть перенос результатов, полученных в ходе построения и исследования модели, на оригинал, основаны на том, что модель в определенном смысле отображает (воспроизводит, моделирует, описывает, имитирует) некоторые интересующие исследователя черты объекта».

Приведенное выше определение понятия моделирования подходит под любые приложения человеческой деятельности, от искусства до точных наук. Существует огромное число определений понятия «модель». Из этого огромного числа нас будет интересовать приложения к исследованию сложных радиотехнических систем. В то же время, такое определение должно быть достаточно лаконично и формализовано.

Корректное определение понятия «модель» должно отображать следующие признаки:

- наличие оригинала S (т.е. объекта, явления, системы);
- наличие модели M как объекта (явления, системы), не тождественного оригиналу ($S \neq M$);
- наличие исследующей системы I, относительно которой заданы оригинал и модель;
- указание на то, что результатом оперирования (исследования, наблюдения) исследующей системы с моделью и оригиналом являются знания (информация);
- указание на то, что исследующая система использует знания о модели для замещения знаний об оригинале.

Ключевым понятием, связывающим понятия оригинала и модели, является исследующая система. Это может быть:

- человек (наблюдатель);

- компьютер, формирующий модель внешних воздействий в процессе адаптации.

Примером последнего может служить центральный компьютер системы радиосвязи, функционирующий в режиме адаптации к условиям распространения радиоволн.

В рамках данных понятий определим модель следующим образом. Объект *M* называется моделью объекта *S* для исследующей системы *I*, если результаты Q_m исследования объекта *M* предназначаются системой I для исследования вместо результатов Q_s исследования объекта *S*.

Моделирование как форма отражения действительности широко распространено, и достаточно полная классификация моделирования крайне затруднительна, хотя бы в силу многозначности понятия модель, широко используемого не только в науке и технике, но и в искусстве, и в повседневной жизни. Тем не менее применительно к естественным и техническим наукам принято различать следующие виды моделирования:

концептуальное моделирование, при котором совокупность уже известных фактов или представлений относительно исследуемого объекта или системы истолковывается с помощью некоторых специальных знаков, символов, операций над ними или с помощью естественного или искусственных языков;

физическое моделирование, при котором модель и оригинал (моделируемый объект) представляют собой реальные объекты и процессы единой или различной физической природы, причем между процессами в объекте–оригинале и в модели выполняются некоторые соотношения подобия, вытекающие из схожести физических явлений;

структурно-функциональное моделирование, при котором моделями являются схемы (блок-схемы), графики, чертежи, диаграммы, таблицы, рисунки, дополненные специальными правилами их объединения и преобразования;

математическое (логико-математическое), при котором моделирование, включая построение модели, осуществляется средствами математики и логики;

имитационное моделирование, при котором логико-математическая модель исследуемого объекта представляет собой алгоритм функционирования объекта, реализованный в виде программного комплекса для компьютера.

Перечисленные виды моделирования не являются взаимоисключающими и могут применяться при исследовании сложных объектов либо одновременно, либо в некоторой комбинации. Кроме того, в некотором смысле концептуальное и структурно-функциональное моделирование неразличимы между собой,

так как блок-схемы, конечно же, являются специальными знаками с установленными операциями над ними.

Исторически случилось так, что первые работы по компьютерному моделированию были связаны с физикой, где с помощью моделирования решался целый ряд задач гидравлики, фильтрации, теплопереноса и теплообмена, механики твердого тела и т.д. Моделирование в основном представляло собой решение сложных нелинейных задач математической физики с помощью итерационных схем, и по существу было моделированием математическим. Подобный вид моделирования весьма широко распространен и в настоящее время. За время развития методов моделирования, при решении задач фундаментальных и смежных предметных областей, накоплены целые библиотеки подпрограмм и функций, облегчающих возможности моделирования.

И все же в настоящее время понятие «компьютерное моделирование» обычно связывают не с фундаментальными дисциплинами, а в первую очередь с системным анализом (совокупностью методологических средств, используемых для подготовки и принятия решений экономического, социального или технического характера) - направлением кибернетики, впервые заявившем о себе в начале 50-х годов прошлого столетия при исследовании систем в биологии, макроэкономике, при создании автоматизированных экономико-организационных систем управления. Объясняется этом тем фактом, что построение обобщенной модели, отображающей все факторы и взаимосвязи реальной ситуации, которые могут проявиться в процессе решения, является основой всего системного анализа, центральным этапом исследования и проектирования любой системы.

Сложная система — система, состоящая из множества взаимодействующих составляющих (подсистем), вследствие чего сложная система приобретает новые свойства, которые отсутствуют на подсистемном уровне.

Но не только при имитационном моделировании полезен компьютер. Например, при математическом моделировании выполнение одного из основных этапов – построение математической модели по экспериментальным данным просто немыслимо без компьютера. В последнее время, благодаря развитию графического интерфейса и графических пакетов, широкое развитие получило компьютерное структурно-функциональное моделирование. Положено начало привлечения компьютера даже к концептуальному моделированию, например, при построении систем искусственного интеллекта.

В настоящее время под компьютерной моделью понимают:

- Условный образ объекта (процесса), описанный с помощью взаимосвязанных компьютерных таблиц, блок-схем, диаграмм, графиков, рисунков, анимационных фрагментов, гипертекстов и отображающий структуру элементов объекта и взаимосвязи между ними. Компьютерные модели такого вида будем называть **структурно-функциональными;**
- Отдельную программу, совокупность программ, программный комплекс, позволяющий с помощью последовательности вычислений и графического отображения их результатов воспроизводить (имитировать) процессы функционирования объекта, системы объектов при условии воздействия на объект различных, как правило, случайных факторов. Такие модели будем называть **компьютерными имитационными.**

Компьютерное моделирование - метод решения задачи или синтеза сложной системы на основе использования ее компьютерной модели. Суть компьютерного моделирования заключена в получении количественных и качественных результатов по имеющейся модели. Качественные выводы, полученные по результатам анализа, позволяют обнаружить неизвестные ранее свойства сложной системы: ее структуру, динамику развития, устойчивость, целостность и др. Количественные выводы носят характер прогноза некоторых будущих или объяснения прошлых значений переменных, характеризующих систему.

Предметом компьютерного моделирования могут быть: экономическая деятельность фирмы или банка, промышленное предприятие, информационно-вычислительные сети, технологические процессы, любой реальный объект или процесс, например процесс инфляции, и вообще - любая сложная система.

Компьютерная модель сложной система должна, по возможности, отображать все основные факторы и взаимосвязи, характеризующие реальные ситуации, критерии и ограничения. Модель должна быть достаточно универсальной, чтобы описать близкие по назначению объекты, и в то же время достаточно простой, чтобы позволить выполнить необходимые исследования с разумными затратами.

Таким образом, структуру видов моделирования применительно к естественным и техническим наукам можно представить в виде следующей блок-схемы (рис.1.1).

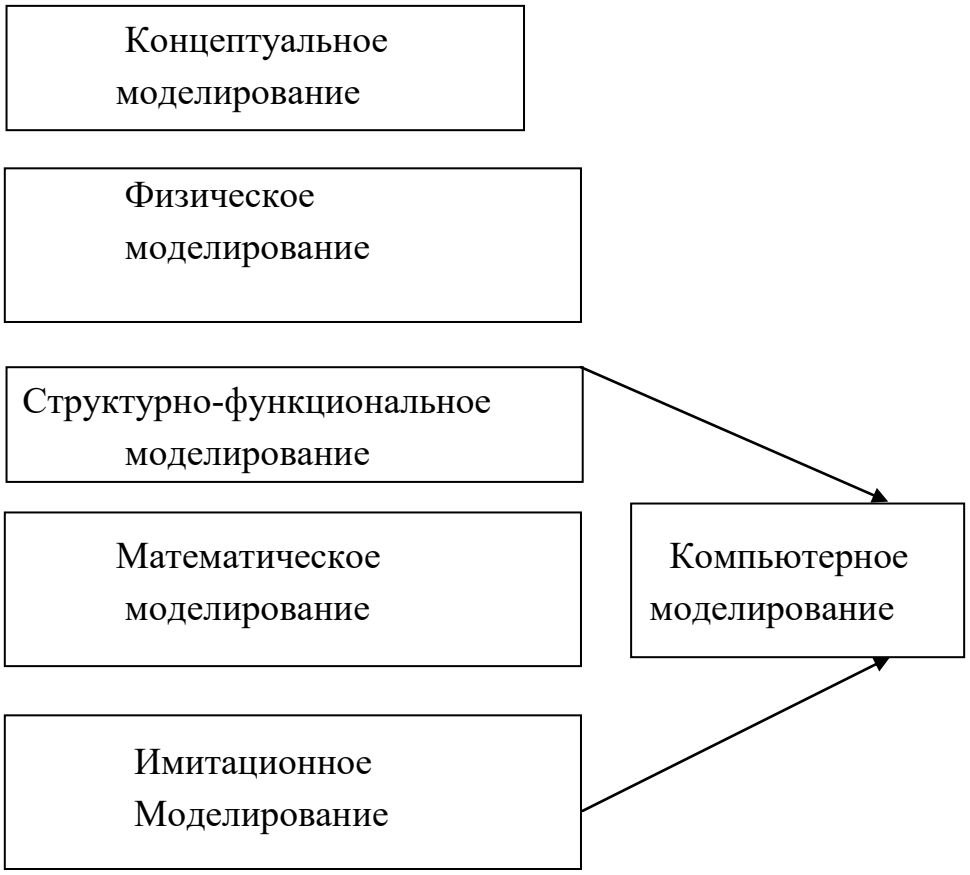

Рис.1.1 Структура видов моделирования

Контрольные вопросы

1. Перечислите основные виды моделирования.
2. Дайте определение концептуальному моделированию.
3. Дайте определение физическому моделированию.
4. Дайте определение структурно-функциональному моделированию.
5. Дайте определение математическому моделированию.
6. Дайте определение имитационному моделированию.
7. Какой вид моделирования является предтечей структурно-функционального моделирования?
8. Какие виды моделирования и как связаны с использованием компьютера?

2. ВВЕДЕНИЕ В ИМИТАЦИОННОЕ КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

Имитационное моделирование появилось раньше структурно-функционального, хотя, по логике вещей, при моделировании сложных объектов это следующая фаза моделирования. Причина в том, что структурно-функциональное моделирование окончательно сформировалось лишь с развитием графических оболочек, которые совершенно необходимы для решения этих задач; в то время как имитационное моделирование, хотя и может использовать графический интерфейс, зависит от него в гораздо меньшей степени.

Имитационное моделирование основано на применении логико-математической модели сложной системы - со всеми вытекающими особенностями. Построение математической модели, в отличие от структурно-функционального моделирования, требует большого объема детальной информации о системе, включая всевозможные логические и количественные соотношения.

Среди методов прикладного системного анализа имитационное компьютерное моделирование является мощнейшим инструментом исследования сложных систем, управление которыми связано с принятием решений в условиях неопределенности. По сравнению с другими методами имитационное компьютерное моделирование позволяет рассмотреть большее число альтернатив, улучшить качество управленческих решений и точнее прогнозировать их последствия. Эффективность моделирования значительно возросла с появлением мощных компьютеров. Идея имитационного моделирования проста и в то же время интуитивно привлекательна. Она дает возможность пользователю экспериментировать с системами (существующими или предлагаемыми) в тех случаях, когда делать это невозможно или нецелесообразно.

Имитационное моделирование является одним из наиболее широко распространенных количественных методов, используемых при решении проблем управления.

В таблице 2.1 приведены результаты обследования 1000 крупнейших фирм США с точки зрения анализа пригодности определенных методов для внутрифирменного планирования.

Таблица 2.1

Результаты обследования 1000 крупнейших фирм США

Методы	Частота использования в %
Имитационное моделирование	29
Линейное программирование	21
Сетевые методы	14
Теория управления запасами	12
Нелинейное программирование	8
Динамическое программирование	4
Целочисленное программирование	3
Теория массового обслуживания	3
Прочее	6
Всего:	100

С точки зрения системного анализа имитационное моделирование есть процесс конструирования модели реальной системы и постановки экспериментов на этой модели с целью:

- либо понять поведение системы,
- либо оценить (в рамках ограничений, накладываемых некоторыми критериями) различные стратегии, обеспечивающие функционирование данной системы.

С методологической точки зрения наиболее полно имитационное моделирование характеризует следующее определение:

Имитационное моделирование является экспериментальной и прикладной методологией, имеющей целью:

- описать поведение систем;
- построить теории и гипотезы, которые могут объяснить наблюдаемое поведение;
- использовать эти теории для предсказания будущего поведения системы.

2.1. Преимущества и недостатки имитационного моделирования

Использование модели в качестве средства осмысления действительности несет за собой как некоторые преимущества, так и недостатки. К числу первых относится возможность реализации большого числа режимов работы, которые сложно или практически невозможно реализовать, гибкость и относительно простое применение компьютерной математической обработки результатов моделирования. Естественно, что информация, полученная в математическом эксперименте, носит вторичный характер и может быть самостоятельной лишь в том случае, если математическая модель достаточно адекватна реальному объекту и результаты моделирования имеют физическое объяснение и удовлетворяют натурному эксперименту.

Преимущества имитационного эксперимента особенно проявляются при наличии любого из следующих условий:

1. Не существует аналитических методов решения сформулированной задачи. К этой категории относятся многие модели телетрафика (теории сетей передачи информации).
2. Аналитические методы решения существуют, но математические процедуры столь сложны и трудоемки, что имитационное моделирование дает более простой способ решения.
3. В натурном эксперименте может оказаться сложным поддержание одних и тех же рабочих условий при каждом повторении эксперимента или в течение всего времени проведения серии экспериментов.
4. Для получения одной и той же величины выборки (и, следовательно, статистической значимости результатов экспериментирования) могут потребоваться чрезмерные затраты времени и средств.
5. При экспериментировании с реальными системами может оказаться невозможным исследование множества альтернативных вариантов.
6. Имитационное моделирование позволяет пользователю экспериментировать с системами (существующими или предлагаемыми) в тех случаях, когда делать это на реальном объекте практически невозможно или нецелесообразно.

С другой стороны нельзя забывать, что имитационное моделирование - методология, а не теория. Для получения необходимой информации о системе необходимо осуществлять «прогон» имитационных моделей, а не «решать» их. Имитационные модели в принципе не способны формировать свое собственное решение, а могут лишь служить в качестве средства для анализа поведения системы в условиях, которые определяются экспериментатором.

2.2. Компьютерная имитационная модель

Построение модели является основным этапом исследования или проектирования любой радиотехнической системы. В настоящее время термины имитационный и компьютерный стали практически синонимами. Компьютерное моделирование - метод решения задачи анализа или синтеза сложной системы (в том числе радиотехнической системы) на основе использования ее компьютерной модели.

В гносеологическом аспекте под моделью будем понимать синтез всех знаний об объекте, о среде распространения и о принципах функционирования системы. Модель эквивалентна формализованным современным научным представлениям об объекте исследования.

Среди функций модели выделим:

- оптимизация характеристик систем связи;
- прогнозирование;
- использование модели в интерпретации экспериментальных результатов.

Д.Вейцен (американский инженер, специалист по радио-коммуникациям) отмечает: «Если инженер хочет изучить различные коммуникационные технологии, то он может применить два подхода. Он может собрать сложную линию, снимать показания приборов год или больше, а затем проанализировать результаты. Даже в этом случае все возможные комбинации конфигурации антенны и параметров системы не могут быть рассмотрены. Лучшим вариантом будет разработка компьютерных программ, которые могут точно смоделировать канал для предсказания работы системы при данном наборе введенных параметров. Например, исследование характеристик системы метеорной связи (СМС) представляет собой достаточно сложную задачу и подходит под тот класс задач, для решения которых становится целесообразным создание компьютерной модели. Информационные характеристики СМС зависят как от большого числа технических характеристик (параметров приемо-передающей аппаратуры и антенных систем), а также имеют значительные вариации, определяющиеся астрономическими факторами, которые зависят от времени и сезона проведения эксперимента. Ввиду сложности и трудоемкости натурного эксперимента вряд ли когда-либо подобные исследования будут проведены в полном объеме в натурном эксперименте. Наиболее перспективным путем развития подобных исследований является имитационное моделирование на математической моде-

ли радиоканала, которая должна быть откалибрована на основе сравнения с экспериментальными данными».

2.2.1. Структура имитационных моделей

Почти каждая модель представляет собой некоторую комбинацию таких составляющих, как

- компоненты,
- переменные,
- функциональные зависимости,
- ограничения,
- целевые функции.

Компоненты - составные части, которые при соответствующем объединении образуют систему. Система определяется как группа, или совокупность объектов, объединенных некоторой формой регулярного взаимодействия или взаимозависимости для выполнения заданной функции. Компоненты суть объекты, образующие изучаемую систему.

Параметры - величины, которые оператор, работающий на модели, может выбирать произвольно, в отличие от переменных, которые могут принимать только значения, определяемые видом заданной функции.

Функциональные зависимости описывают поведение параметров и переменных в пределах компонента или выражают соотношения между компонентами.

Ограничения представляют собой устанавливаемые пределы изменения значений переменных. Они могут вводиться разработчиком модели искусственно (искусственные ограничения) или самой системой вследствие присущих ей свойств (естественные ограничения - обусловлены физической природой системы).

Целевая функция (или функция критерия) – это точное отображение целей и задач системы и необходимых правил их выполнения. Процесс манипулирования с моделью направлен на оптимизацию или удовлетворение заданного критерия.

Контрольные вопросы

1. Перечислите основные преимущества имитационного моделирования.
2. Перечислите основные недостатки имитационного моделирования.
3. Дайте определение компьютерной имитационной модели.
4. Перечислите основные структурные элементы компьютерной имитационной модели.

3.ОБЩИЕ ВОПРОСЫ МЕТОДОЛОГИИ МОДЕЛИРОВАНИЯ

В последнее время среди методов прикладного системного анализа имитационное моделирование, благодаря бурному развитию вычислительной техники, стало одним из мощнейших инструментов исследования сложных систем. Методология разработки компьютерных моделей хорошо представлена в работах Л.А.Бахвалова, Н.П.Бусленко, С.М.Ермакова, Т.Нейлора, Ю.Г.Полляка, Р.Шеннона и др. Бросается в глаза невозможность полного абстрагирования от тематики прикладных проблем. В работах Ю.Г.Полляка достаточно четко просматривается радиотехнический уклон. Направленность исследований Л.А.Бахвалова - проблемы горнодобывающей промышленности. С.М.Ермаков иллюстрирует процесс имитации, моделируя прохождение излучения через вещество. Основа приложений в монографии Т.Нейлора - экономика.

3.1.Основные этапы имитационного моделирования

В принципе модель представляет собой "черный ящик", и довольно трудно определить, в чем причина отличия результатов моделирования от экспериментальных данных и является ли сопоставление с натурным экспериментом единственным и надежным критерием адекватности модели? С другой стороны, возникают вопросы, на каком основании можно ранжировать модели, каким же требованиям должна удовлетворять "хорошая модель"? Удовлетворяет ли этим требованиям разработанная модель? Рассмотрим основные этапы имитации (в соответствии с терминологией, принятой у Р.Шеннона):

1. Определение системы.
2. Абстрагирование.
3. Подготовка данных.
4. Трансляция модели.
5. Оценка адекватности.
6. Стратегическое планирование.
7. Тактическое планирование.
8. Экспериментирование.
9. Интерпретация.
10. Реализация.
11. Документирование.
12. Оптимизация отдельных элементов и всей модели в целом.

Рассмотрим более подробно каждый из этапов.

1-3.Определение системы, абстрагирование, подготовка данных. На первых трех этапах происходит установление границ, в рамках которых будет изу-

чаться система, формулируется целевая функция модели, определяются основные компоненты системы, которые будут включены в модель, определяются параметры и переменные, относящиеся к этим компонентам, определяются функциональные соотношения между компонентами, параметрами и переменными, осуществляется переход от реальной системы к некоторой логической схеме. Особенно важным этапом является подготовка данных. Именно надежная база данных определяет достоверность и точность результатов моделирования.

4. Трансляция модели - описание модели на одном из алгоритмических языков используемого компьютера. Краткое описание языков имитационного моделирования было дано во втором разделе. На этапе трансляции модели приветствуется использование специализированных языков имитационного моделирования. Применение специализированных языков имитационного моделирования позволяет оптимально использовать ресурсы компьютера, значительно повышает скорость моделирования.

Первые четыре этапа характеризуются разработкой и обоснованием алгоритма и заканчиваются созданием программы для ЭВМ. То, что обычно понимается под моделью, является итогом этих этапов имитации.

5. Оценка адекватности. Один из важнейших этапов разработки модели. По существу на этом этапе принимается решение о приемлемости модели и возможности дальнейшего ее использования для изучения и прогнозирования реальной системы. На этом этапе осуществляется проверка структуры модели и проверка модели в целом. Модель должна быть оценена по максимальным пределам изменений величины ее параметров и переменных и проверена на отсутствие нелепых ответов.

6. Стратегическое планирование. Остановимся на стратегическом планировании имитационного эксперимента. В имитационном эксперименте точность и стоимость полученной информации определяются выбором плана эксперимента. Во многом планирование компьютерного эксперимента тождественно планированию натурного эксперимента, но между двумя видами экспериментов имеются различия, учет которых повышает информативность процесса моделирования. Несомненным преимуществом компьютерного эксперимента перед натурным является легкость воспроизведения условий эксперимента. В компьютерном эксперименте более корректно проводится сравнительный анализ альтернативных стратегий. Еще одно преимущество компьютерного моделирования заключается в легкости прерывания и возобновления эксперимента. Д.Клейнен отмечает, что при работе на компьютере можно прервать

процесс моделирования на время, необходимое для анализа результатов и принятия решения об изменении параметров модели или продолжении эксперимента.

7. Тактическое планирование.

Тактическое планирование связано с вопросами эффективности и определением способов проведения испытаний, намеченных планом эксперимента. Тактическое планирование связано с решением задач трех типов:

1) Проблема определения степени надежности результатов моделирования.

2) Определение начальных условий в той мере, в какой они влияют на достижение установившегося режима. Сведение к минимуму влияния переходного процесса, связанного с запуском модели.

3) Проблема уменьшения дисперсии результатов моделирования при одновременном сокращении размеров выборки.

8. Экспериментирование. Прогон модели. Получение информации. Анализ чувствительности, так как многие параметры получены на основании весьма сомнительных данных. Имитационное моделирование идеально подходит для анализа чувствительности, потому что контролируется весь ход эксперимента.

9. Интерпретация результатов. 10. Реализация (практическое использование модели и результатов моделирования). 11. Документирование. 12.Оптимизация отдельных элементов и всей модели в целом.

Пять последних пунктов связаны с использованием модели. По мнению Р.Шеннона распределение времени проектирования модели представляется следующим образом: 25% на постановку задачи, 20% на сбор и анализ данных, 30% на разработку модели и 25% на реализацию.

Опыт работы с компьютерными моделями радиоканала показывает, что все представленные этапы разработки и реализации модели важны.

Контрольные вопросы

1. Перечислите основные этапы имитационного эксперимента.
2. Чем отличаются этапы тактического и стратегического моделирования?
3. Как документирование влияет на надежность результатов моделирования?
4. Как проверяется адекватность модели?

4. СЛУЧАЙНЫЕ ВЕЛИЧИНЫ И ПРОЦЕССЫ, ОСНОВНЫЕ ПОНЯТИЯ И СВОЙСТВА

4.1. Дискретные случайные величины

Дискретной случайной величиной называют случайную величину, которая принимает отдельные, изолированные возможные значения с определенными вероятностями. Число возможных значений дискретной случайной величины может быть конечным или бесконечным.

Законом распределения дискретной случайной величины называют соответствие между возможными значениями и их вероятностями; его можно задать таблично, аналитически и графически.

Рассмотрим следующий пример. Пусть производится n независимых испытаний, в каждом из которых событие A может появиться с вероятность p. Рассмотрим в качестве дискретной случайной величины ξ число появления события A в этих испытаниях. Возможные значения: $\xi: x_1 = 0,\ x_2 = 1,\ x_3 = 2,....,\ x_{n+1} = n.$ Вероятности этих состояний определяются формулой Бернулли, а распределение носит название «биноминальное»:

$$P_n(k) = C_n^k p^k (1-p)^{n-k}, \tag{4.1}$$

где $$C_n^k = \frac{n!}{k!(n-k)!}$$

Пример табличного представления дискретной случайной величины ξ с помощью таблицы вероятностей:

$$\xi \in \begin{matrix} x_i \\ p_i \end{matrix} \rightarrow \begin{cases} x_1, x_2, ..., x_n \\ p_1, p_2, ..., p_n \end{cases} \tag{4.2}$$

x_i - возможные значения дискретной случайной величины;

p_i - соответствующая этому значению вероятность.

События $\xi = x_1,\ \xi = x_2, ...,\ x_n$ составляют полную группу событий и отсюда условие нормировки

$$\sum_{i=1}^{n} p_i = 1 \tag{4.3}$$

Математическое ожидание дискретной случайной величины определяется следующим образом:

$$M(\xi) = \sum_{j=1}^{n} x_j p_j \,. \tag{4.4}$$

Например, вычислим математическое ожидание для биноминального распределения

$$M(\xi)=\sum_{k=0}^{n} k\,\frac{n!}{k!(n-k)!}\,p^{k}(1-p)^{n-k}. \qquad (4.5)$$

Непосредственное вычисление этого выражения весьма затруднительно, но вычисление $M(\xi)$ значительно упрощается с учетом свойств математического ожидания, что и будет показано ниже.

Среднее значение случайной величины ξ по выборке размером *p*:

$$\bar{\xi}=\frac{1}{p}\sum_{j=1}^{p}\xi_j\,. \qquad (4.6)$$

Дисперсией дискретной случайной величины называют математическое ожидание квадрата отклонения случайной величины от ее математического ожидания

$$D(\xi)=M\left[\xi-M(\xi)\right]^2. \qquad (4.7)$$

4.2. Свойства характеристик дискретной случайной величины

Свойство 1. Математическое ожидание постоянной величины равно самой постоянной:

$$M(c)=c\,. \qquad (4.8)$$

Доказательство. Рассмотрим *c* как дискретную случайную величину, принимающую одно значение $x_1=c$ с вероятностью $p_1=1$. Тогда $M(c)=\sum_{i=1}^{\infty}p_i x_i=1\cdot c=c\,.$

Свойство 2. Постоянный множитель можно выносить за знак математического ожидания:

$$M(c\xi)=cM(\xi). \qquad (4.9)$$

Свойство 3. Математическое ожидание произведения двух независимых случайных величин равно произведению их математических ожиданий. Случайные величины называют независимыми, если закон распределения одной из них не зависит от того, какие возможные значения приняла другая величина. Произведение независимых случайных величин ξ и η определим как случайную величину ξ·η, возможные значения которой равны произведениям каждого возможного значения ξ на каждое возможное значение η; вероятности возможных значений произведения ξ·η равны произведениям вероятностей возможных значений сомножителей:

$$M(\xi\eta) = M(\xi)M(\eta). \qquad (4.10)$$

Свойство 4. Математическое ожидание суммы двух случайных величин равно сумме математических ожиданий слагаемых:

$$M(\xi + \eta) = M(\xi) + M(\eta). \qquad (4.11)$$

Теперь, используя свойство 4, вычислим математическое ожидание для биномиального распределения.

Теорема. Математическое ожидание числа появления события A в n независимых испытаниях равно произведению числа испытаний на вероятность p появления события в каждом испытании:

$$M(\xi) = np. \qquad (4.12)$$

Доказательство. Будем рассматривать в качестве случайной величины ξ - число наступлений события A в n независимых испытаниях. Очевидно, число ξ появлений события A в этих испытаниях складывается из чисел появления события в отдельных испытаниях. Поэтому, если ξ_1 - число появлений событий в первом испытании (в данном примере любое ξ_i может принимать случайным образом только два значения: 0 или 1), ξ_2 - во втором, ξ_n в n-м, то общее число появления события А будет равно $\xi = \xi_1 + \xi_2 + ... + \xi_n$. Согласно четвертому свойству математического ожидания имеем

$$M(\xi) = M(\xi_1 + \xi_2 + ... + \xi_n) = M(\xi_1) + M(\xi_2) + ... + M(\xi_n). \qquad (4.13)$$

Каждое из слагаемых правой части есть математическое ожидание числа появлений событий в одном испытании, а математическое ожидание числа появлений события в одном испытании равно вероятности появления p. Подставляя в правую часть выражения (4.13) вместо каждого слагаемого p, получим искомое выражение $M(\xi) = np$.

Свойство 5. Дисперсия постоянной величины равна нулю:

$$D(c) = 0. \qquad (4.14)$$

Доказательство: $D(c) = M\left[c - M(c)\right]^2 = M\left[c - c\right]^2 = 0$.

Свойство 6. Постоянный множитель можно вынести за знак дисперсии, возведя его в квадрат:

$$D(c\xi) = c^2 D(\xi). \qquad (4.15)$$

Доказательство:

$$D(c\xi) = M\left[c\xi - M(c\xi)\right]^2 = M\left[c\xi - cM(\xi)\right]^2 = M\left[c^2(\xi - M(\xi))^2\right] = c^2 D(\xi).$$

Преобразуем формулу (4.14) следующим образом:

$$D(\xi)=M(\xi-M(\xi))^2=M\left[\xi^2-2\xi\cdot M(\xi)+M^2(\xi)\right]$$
$$=M(\xi^2)-M\left[2M(\xi)\cdot\xi\right]+M\left[M^2(\xi)\right]=M(\xi^2)-2M^2(\xi)+M^2(\xi)$$

В результате получим, что

$$D(\xi)=M(\xi^2)-M^2(\xi). \tag{4.16}$$

Это выражение позволяет на практике вычислять дисперсию результатов в одном цикле без предварительного вычисления среднего значения, как разность между средним квадратов случайной величины и квадратом среднего значения

$$\sigma_\xi^2=\bar{\xi}^2-\bar{\xi}^2. \tag{4.17}$$

Свойство 7. Дисперсия суммы двух независимых случайных величин равна сумме дисперсий этих величин.

$$D(\xi+\eta)=D(\xi)+D(\eta). \tag{4.18}$$

Для доказательства используем формулу (4.16):

$$D(\xi+\eta)=M\left[(\xi+\eta)^2\right]-\left[M(\xi+\eta)\right]^2=M(\xi^2+2\xi\eta+\eta^2)-\left[M(\xi)+M(\eta)\right]^2=$$
$$M(\xi^2)+2M(\xi\eta)+M(\eta^2)-M^2(\xi)-2M(\xi)M(\eta)-M^2(\eta)=$$
$$M(\xi^2)-M^2(\xi)+M(\eta^2)-M^2(\eta)+2M(\xi\eta)-2M(\xi)M(\eta)=D(\xi)+D(\eta)$$

4.3. Непрерывные случайные величины

Случайную величину ξ будем называть **непрерывной случайной величиной**, если она может принимать любое значение на интервале (*a,b*). В общем случае на интервале $(-\infty,+\infty)$.

Пусть x - действительное число на интервале (*a,b*). **Интегральной функцией распределения** вероятностей случайной величины называют функцию $F(x)$, определяющую для каждого значения x вероятность события, что случайная величина ξ примет значение, меньшее x, т.е.

$$F(x)=P(\xi<x) \tag{4.19}$$

Геометрически это равенство можно истолковать так: $F(x)$ есть вероятность того, что случайная величина примет значение, которое изображается на числовой оси точкой, лежащей левее x.

Рассмотрим основные свойства интегральной функции.

Свойство 1. Значения интегральной функции принадлежат отрезку (0,1): $0\le F(x)\le 1$.

Свойство 2. $F(x)$ - неубывающая функция.

Свойство 3. Вероятность того, что случайная величина примет значение, заключенное в интервале (α, β), равна приращению интегральной функции на этом интервале:

$$P(\alpha \le \xi \le \beta) = F(\beta) - F(\alpha). \quad (4.20)$$

Дифференциальной функцией распределения (плотностью вероятностей) называют первую производную от интегральной функции: $f(x) = \frac{dF(x)}{dx}$.

Из приведенного определения следует, что интегральная функция является первообразной для дифференциальной функции. Зная дифференциальную функцию, можно вычислить вероятность того, что непрерывная случайная величина примет значение, принадлежащее заданному интервалу (α, β):

$$P(\alpha \le \xi \le \beta) = \int_{\alpha}^{\beta} f(x)dx. \quad (4.21)$$

Условие нормировки для непрерывной случайной величины:

$$\int_{-\infty}^{\infty} f(x)dx = 1. \quad (4.22)$$

Математическое ожидание непрерывной случайной величины определяется в соответствие со следующим выражением

$$M(\xi) = \int_{-\infty}^{\infty} x \cdot f(x)dx. \quad (4.23)$$

Дисперсией непрерывной случайной величины называют математическое ожидание квадрата ее отклонения:

$$D(\xi) = \int_{-\infty}^{\infty} [x - M(\xi)]^2 f(x). \quad (4.24)$$

Корреляционным моментом $\mu_{\xi,\eta}$ двух случайных величин ξ и η называют математическое ожидание произведения отклонении от математического ожидания этих величин:

$$\mu_{\xi,\eta} = M[(\xi - M(\xi))(\eta - M(\eta))]. \quad (4.25)$$

При интерпретации результатов моделирования большое значение играют следствия из следующей теоремы.

Теорема. Корреляционный момент двух независимых случайных величин равен нулю. Доказательство заключается в том, что если ξ и η независимые

случайные величины, то и их отклонения от математического ожидания также независимы.

$$\mu_{\xi,\eta} = M\left[\left(\xi - M(\xi)\right)\left(\eta - M(\eta)\right)\right] = M\left(\xi - M(\xi)\right)M\left(\eta - M(\eta)\right) =$$
$$= \left(M(\xi) - M(\xi)\right)\left(M(\eta) - M(\eta)\right) = 0$$

Коэффициентом корреляции двух случайных величин является величиной безразмерной:

$$r_{\xi,\eta} = \frac{\mu_{\xi,\eta}}{\sqrt{D(\xi)D(\eta)}} \ . \qquad (4.26)$$

4.4. Статистическая проверка гипотез

Часто необходимо знать закон распределения генеральной совокупности. Если закон распределения неизвестен, но имеются основания предположить, что он имеет определенный вид (назовем его *A*), выдвигают гипотезу: генеральная совокупность распределена по закону *A*. Возможен случай, когда закон распределения известен, а его параметры неизвестны. Если есть основания предположить, что неизвестный параметр θ равен определенному значению θ_0, выдвигают гипотезу: $\theta = \theta_0$. Таким образом, в этой гипотезе речь идет о предполагаемой величине параметра.

Возможны и другие гипотезы: о равенстве параметров двух или нескольких распределений, о независимости выборок и многое другое.

Статистической называют гипотезу о виде неизвестного распределения, или о параметрах известных распределений. Наряду с выдвинутой гипотезой рассматривают и противоречащую ей гипотезу. Если выдвинутая гипотеза будет отвергнута, то имеет место противоречащая гипотеза.

Нулевой (основной) называют выдвинутую гипотезу *Ho*.

Конкурирующей (альтернативной) называют гипотезу H_1, которая противоречит нулевой.

Выдвинутая гипотеза может быть правильной или неправильной, поэтому возникает необходимость ее проверки. Поскольку проверку производят статистическими методами, ее называют **статистической проверкой**. В результате статистической проверки могут быть допущены ошибки двух родов.

Ошибка первого рода состоит в том, что будет отвергнута правильная гипотеза. Вероятность совершить ошибку первого рода принято обозначать через α, и ее называют уровнем значимости. Наиболее часто уровень значимости принимают равным 0.05 или 0.01.

Ошибка второго рода состоит в том, что будет принята неправильная гипотеза. Вероятность совершить ошибку второго рода принято обозначать через β. Величина 1-β называется мощностью критерия.

Статистическим критерием называют случайную величину *K*, которая служит для проверки нулевой гипотезы. После выбора определенного критерия, множество всех его возможных значений разбивают на два непересекающихся подмножества: одно из них содержит значения критерия, при которых нулевая гипотеза отвергается, а другое – при которых она принимается.

Критической областью называют совокупность значений критерия, при которых нулевую гипотезу отвергают.

Областью принятия гипотезы называют совокупность значений критерия, при которых гипотезу принимают.

Основной принцип проверки статистических гипотез можно сформулировать так: если наблюдаемое значение критерия принадлежит критической области - гипотезу отвергают, если наблюдаемое значение критерия принадлежит области принятия гипотезы - гипотезу принимают.

Контрольные вопросы

1. Как осуществляется статистическая проверка гипотез?
2. Что такое область принятия гипотезы?
3. Чем отличаются ошибки первого и второго рода?
4. Что такое статистический критерий?

5. ЭМПИРИЧЕСКАЯ ПРОВЕРКА КАЧЕСТВА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

При построении статистической имитационной модели необходимо уметь генерировать величины и процессы с наперед заданными статистическими свойствами. Основу метода статистических испытаний составляет генератор псевдослучайных чисел (ГПСЧ), равномерно распределенных на интервале (0,1) - ГПСЧР. Далее будет показано, что используя ГПСЧР можно построить схему реализации любого процесса с заданными свойствами. Датой рождения метода статистических испытаний (метода Монте-Карло) принято считать 1949 год, когда вышла в свет статья Дж.Неймана «The Monte-Carlo method», посвященная проблемам экранирования мощных источников радиоактивного излучения.

Существует огромное число подходов в реализации ГПСЧ. И если библиография, выпущенная в США в 1972 году, насчитывала 491 ссылку на литературу по генераторам псевдослучайных чисел, то в настоящее время такой список не поддается оценке. Основой любого метода генерации псевдослучайных чисел является итерационная схема $x_i = \Phi\left(x_{i-1}, x_{i-2,}.....\right)$. В генераторах, построенных на основе целочисленной математики, x - как правило, целое число. В генераторе должен быть предусмотрен алгоритм вычисления псевдослучайного числа r_i, равномерно распределенного на интервале (0,1).

Генератор псевдослучайных чисел должен удовлетворять требованиям, предъявляемым к «хорошим генераторам». Решение проблемы проверки качества случайности в принципе неслучайной числовой последовательности осуществляется на основе использования различных тестов. Кроме того, генератор должен иметь максимально большой период (периодом ГПСЧР называется повторяющийся цикл чисел).

Основная задача ГПСЧР - получение последовательностей, которые похожи на случайные. Статистическая теория дает нам некоторые качественные и количественные критерии случайности, которые на практике реализуются в виде статистических тестов. Рассмотрим основные эмпирические тесты. Тесты применяются к последовательностям:

- x_i (целые числа);
- $r_i \in 0,1$;

- $u_i = \lfloor d \cdot r_i \rfloor$ - вспомогательная последовательность, в которой целые числа u_i равномерно распределены на интервале (0, $d-1$). Здесь знаком $\lfloor y \rfloor$ обозначено ближайшее целое к произвольному положительному числу y.

5.1. Частотный тест (проверка равномерности)

Первое требование, предъявляемое к ГПСЧР, заключается в том, чтобы числа r_i были действительно равномерно распределены между нулем и единицей. Проверить равномерность можно по следующему алгоритму.

1. Интервал (0,1) разбиваем на k частей (отрезков) длиной $\frac{1}{k}$.

2. Проводим имитационный эксперимент, в котором генерируем N чисел вида r_i.

3. Для каждого отрезка подсчитываем число попаданий случайной величины r в этот отрезок - $N_{э,i}$ (экспериментальная частота).

4. Для каждого отрезка подсчитываем теоретическую частоту $N_{T,i}$. Для равномерного распределения $N_{T,i} = \frac{N}{k}$.

5. В качестве статистического критерия используем критерий χ^2 с числом степеней свободы, равным $k-1$.

$$\chi^2 = \sum_{j=1}^{k} \frac{\left(N_{э,j} - N_{T,j}\right)^2}{N_{T,j}}. \qquad (5.1)$$

В работе Д. Кнута показано, что для **частотного** теста не только при больших отклонениях результатов моделирования от теоретических результатов, но и при очень хорошем совпадении качество генератора считается неудовлетворительным. Рассмотрим статистику

$$P\left[\chi^2 > \chi^2_{kp}(\alpha;k)\right] = \alpha. \qquad (5.2.)$$

При уровне значимости $\alpha < 0.01$ и $\alpha > 0.99$ генератор считается неудовлетворительным, при $\alpha < 0.05$ и $\alpha > 0.95$ генератор считается подозрительным. Считается, что ГПСЧР удовлетворяет частотному тесту, если $0.1 < \alpha < 0.9$. Область принятия гипотезы «данный ГПСЧР удовлетворяет частотному тесту» определяется неравенством

$$\chi^2_{кр}(\alpha = 0.1) < \chi^2 < \chi^2_{кр}(\alpha = 0.9). \qquad (5.3)$$

5.2. Сериальный тест

В сериальном тесте проверяется равномерность и независимость пар (троек, четверок и т. д) следующих друг за другом случайных чисел. Статисти-

ческая оценка осуществляется на основе критерия χ^2. Рассмотрим применение сериального теста для проверки равномерности и независимости пар следующих друг за другом случайных чисел.

Сериальный тест проводится со вспомогательной последовательностью $u_i = \lfloor d \cdot r_i \rfloor$. Например, выбираем $d = 10$, тогда u_i - целое число, равномерно распределенное на интервале (0,9). Разбиваем весь ряд чисел u_i на $\frac{N}{2}$ пар, а каждую пару рассматриваем как двухзначное число z, лежащее в интервале $0 \le z \le 99$. Проверку на равномерность псевдослучайной величины z проводим на основе критерия χ^2. В данном случае число степеней свободы равно 99, а $N_{T,i} = \frac{N}{2 \cdot 100}$.

5.3. Покер – тест

Тестируется возможность появления различных комбинаций случайных чисел. В покер-тесте анализируется вспомогательная последовательность $u_i = \lfloor d \cdot r_i \rfloor$. Разобьем весь ряд псевдослучайных чисел на $\frac{N}{5}$ пятерок. Возможны семь классов пятерок, отличающихся различным содержанием цифр (порядок появления цифр не играет значения):

1. a,b,c,d,e - все цифры различны, например 67834;
2. a,a,b,c,d - две цифры совпадают, остальные различны, например 55490;
3. a,a,b,b,c - совпадают две пары, например 55499;
4. a,a,a,b,c - три цифры одинаковы, остальные две различны, например 77743;
5. a,a,a,b,b - совпадают три цифры и две других, например 55599;
6. a,a,a,a,b - совпадают четыре цифры, например 88882;
7. a,a,a,a,a - совпадают все пять цифр, например 77777.

Теоретические вероятности каждой комбинации (для $d > 5$) вычисляются следующим образом:

$$P_1 = \frac{(d-1)(d-2)(d-3)(d-4)}{d^4}, \quad (5.4)$$

$$P_2 = 10\frac{(d-1)(d-2)(d-3)}{d^4}, \quad (5.5)$$

$$P_3 = 15\frac{(d-1)(d-2)}{d^4}, \quad (5.6)$$

$$P_4 = 10\frac{(d-1)(d-2)}{d^4}, \tag{5.7}$$

$$P_5 = 10\frac{(d-1)}{d^4}, \tag{5.8}$$

$$P_6 = 5\frac{(d-1)}{d^4}, \tag{5.9}$$

$$P_7 = \frac{1}{d^4}. \tag{5.10}$$

В имитационном эксперименте определяется экспериментальное число появления каждой комбинации. Далее, как и в предыдущих случаях, статистическая оценка осуществляется на основе критерия χ^2.

5.4. Проверка на монотонность

С помощью этого теста производится анализ длин монотонных подпоследовательностей исходной последовательности. В качестве примера рассмотрим следующую последовательность:

$$|1,2,9,|8,|5,|3,6,7,|0,4|$$

В ней выделены интервалы монотонного возрастания. Длина этих интервалов соответственно равна: 3,1,1,3,2.

При проверке на монотонность нельзя применять статистку χ^2 в чистом виде, так как данные не являются независимыми. После длинного отрезка, как правило, следует короткий, и наоборот.

В этом тесте используется статистика

$$V = \frac{1}{N}\sum_{i=1}^{6}\sum_{j=1}^{6}(\omega[i] - N\cdot b_i)(\omega[j] - N\cdot b_j)\cdot a_{ij} \tag{5.11}$$

N - длина последовательности,

i - длина интервала монотонности,

$\omega[i]$ - число таких интервалов,

$\omega[6]$ - число интервалов длиной 6 и более.

Коэффициенты a_{ij} и b_i таковы:

$a_{ij} = a_{ji}$,

$$a_{ij} = \begin{bmatrix} 4529{,}4 & 9044{,}9 & 13568 & 18091 & 22615 & 27892 \\ & 18097 & 27139 & 36187 & 45234 & 55789 \\ & & 40721 & 54281 & 67852 & 83685 \\ & & & 72414 & 90470 & 111580 \\ & & & & 113262 & 139476 \\ & & & & & 172860 \end{bmatrix},$$

$$b_i = \left(\frac{1}{6}, \frac{5}{24}, \frac{11}{120}, \frac{19}{720}, \frac{29}{5040}, \frac{1}{840} \right).$$

Статистика V соответствует статистике χ^2 с шестью степенями свободы. Длина последовательности N должна быть больше 4000. Аналогичный тест применяется для не возрастающих отрезков.

5.5. Корреляционный тест

Тест проверки корреляционных свойств заключается в расчете коэффициента корреляции R между членами последовательностей x_i и y_i и в частном случае коэффициента последовательной автокорреляции R_1 (в этом случае $y_i = x_{i+1}$).

$$R = \frac{N\sum_i^N x_i y_i - \sum_i^N x_i \sum_i^N y_i}{\sqrt{\left[N\sum_{i=1}^N x_i^2 - \left(\sum_{i=1}^N x_i \right)^2 \right] \left[N\sum_{i=1}^N y_i^2 - \left(\sum_{i=1}^N y_i \right)^2 \right]}} . \qquad (5.12)$$

Для 5%-ного уровня значимости (α=0.05) значение R должно лежать в пределах

$$-\frac{1}{N-1} - \frac{2}{N-1}\sqrt{\frac{N(N-3)}{N+1}} \le R \le \frac{1}{N-1} + \frac{2}{N-1}\sqrt{\frac{N(N-3)}{N+1}} .$$

Определение длины периода непосредственно не является процедурой тестирования. С другой стороны, длина периода является одной из важнейших характеристик генератора, и вопросы качества генератора имеет смысл рассматривать при реализации генератора, имеющего максимальный период.

Выше представлен далеко не полный список статистических тестов. Здесь рассмотрены только основные тесты, отражающие какие-то определенные свойства случайности в псевдослучайной последовательности. При тестирова-

нии нужно придерживаться двух эмпирических правил, регламентирующих практическую проверку ГПСЧР.

Правило 1. Качественный ГПСЧР должен иметь как можно больший период и отвечать требованиям эмпирических тестов.

Правило 2. Если генератор не удовлетворяет некоторому эмпирическому тесту, то он плох. Если генератор удовлетворяет некоторому эмпирическому тесту, то его желательно проверить на другой тест.

Сравнение среднего значения случайной величины с математическим ожиданием также является хорошим тестом для псевдослучайной последовательности. Этот вопрос рассмотрен в разделе, посвященном тактическому планированию.

6. ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ

Один из первых ГПСЧР реализован на основе «метода серединных квадратов». Рассмотрим алгоритм реализации этого метода.

1. Берем произвольное четырехзначное целое число;

2. Возводим его в квадрат, если нужно добавляем слева нули, чтобы получить восьмизначное число;

3. Берем 4 цифры из середины и идем на выполнение второго пункта.

Рассмотрим пример такой псевдослучайной последовательности:

$$x_0 = 2152 \qquad x_0^2 = 04631104$$
$$x_1 = 6311 \qquad x_1^2 = 39828721$$
$$x_2 = 8287 \qquad x_2^2 = 68674369$$

и т.д.…

В данном случае очевидно, что равномерно распределенное на интервале (0,1) число $r_i = \frac{x_i}{10000}$.

Основным недостатком генераторов данного типа является очень короткий период. Последовательность очень быстро (после нескольких итераций) вырождается, и получить практически необходимое число псевдослучайных чисел невозможно. В своей монографии Д.Кнут выдвинул аргументированное утверждение о принципиальной невозможности вырабатывать псевдослучайные числа с помощью случайного алгоритма. По его мнению, для создания качественного генератора ПСЧР должна использоваться итерационная схема, позволяющая получать априорную информацию о качестве генератора ПСЧР.

В компьютерном моделировании, при реализации генераторов псевдослучайных чисел, упор сделан на использовании методов, позволяющих максимально использовать априорную информацию о характеристиках псевдослучайных чисел. В плане сокращения непроизводительных затрат машинного времени несомненное предпочтение заслуживает метод вычетов, основанный на хорошо разработанных положениях целочисленной математики. Также достаточно исследованы характеристики генераторов, основанных на использовании алгебраических свойств периодических псевдослучайных бинарных последовательностей a_i максимальной длины (М-последовательностей), генерируемых регистром сдвига с цепью обратной связи.

6.1. Генератор псевдослучайных чисел, основанный на использовании алгебраических свойств М-последовательностей

Предлагаемый вариант ГПСЧ первоначально ориентировался на использование в аппаратуре, построенной на элементах цифровой техники: регистрах сдвига и вентилях (логических элементах «исключающее или»). Получение в ГПСЧ псевдослучайных двоичных чисел с равномерным законом распределения основано на использовании алгебраических свойств периодических псевдослучайных бинарных последовательностей максимальной длины (М-последовательностей), генерируемых регистром сдвига с цепью обратной связи (рис.6.1).

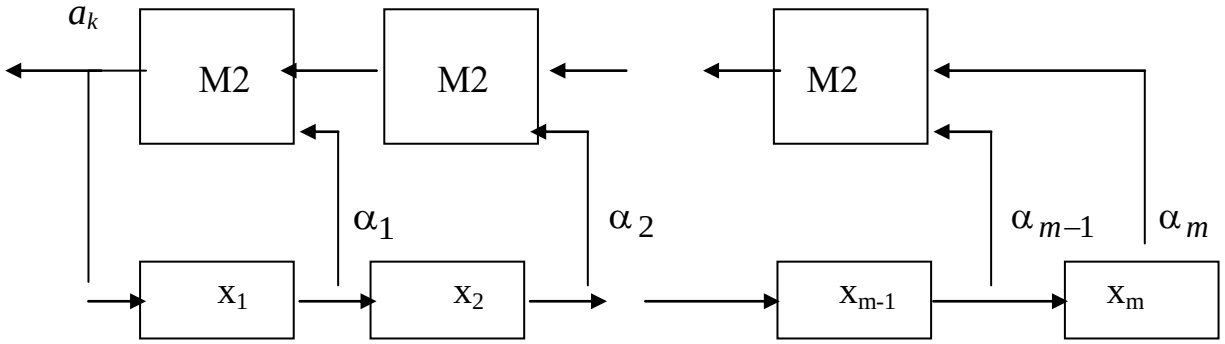

Рис.6.1. Генератор псевдослучайных чисел на основе регистра сдвига с линейной обратной связью

М2 – логические элементы «исключающее или»;

$x_1, x_2, ..., x_m$ - состояние разрядов регистров;

$\alpha_1, \alpha_2, ..., \alpha_m$ - коэффициенты, определяющие функцию обратной связи;

a_k - выходная М-последовательность, $a_k = 0$ *или* 1.

Отметим основные свойства таких генераторов:

- Критерий случайности. Серии следующих друг за другом одинаковых символов (0 или 1, 00 или 11, 000 или 111 и т.д.) появляются в $\{a_k\}$ с такой же частотой, как и в случайных последовательностях равномерных бинарных символов.
- Свойство «идеальной автокорреляции М-последовательности». Нормированная автокорреляционная функция М-последовательности

$$R(\tau) = \frac{\sum_{k=0}^{M-1} a_k a_{k+\tau}}{\sum_{k=0}^{M-1} a_k^2} = \begin{cases} 1 & при \quad \tau = 0 (\mathrm{mod}\, M) \\ -\frac{1}{M} & при \quad \tau \neq 0 (\mathrm{mod}\, M) \end{cases}. \qquad (6.1)$$

Для получения псевдослучайной последовательности, имеющей максимально возможный период $T = 2^m - 1$, необходимо, чтобы характеристический полином схемы $f(x) = \alpha_m x^m + \alpha_{m-1} x^{m-1} + \alpha_{m-2} x^{m-2} + ... + \alpha_1 x + 1$, определяющий структуру цепи обратной связи ($\alpha_i = 1$ при наличии связи от *i*-го разряда, $\alpha_i = 0$ при ее отсутствии), был примитивным.

На практике среди множества полиномов одинаковой степени m выбирают такие, которые позволяют получить наиболее простую структуру обратной связи, при которой суммируют выходы только двух разрядов регистра сдвига *l* и *m*.

В качестве иллюстрации на рис.6.2. приведена структурная схема регистра сдвига, отвечающая примитивному полиному $\varphi(x) = x^5 + x^2 + 1$. Получаемая при этом на выходе цепи обратной связи *M*-последовательность имеет вид: 00101011101100011111100110…

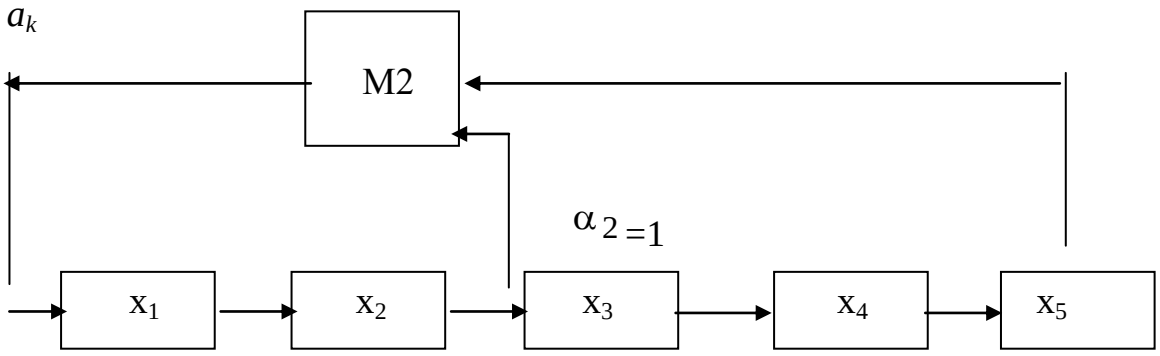

Рис.6.2. Структурная схема регистра сдвига, отвечающая примитивному полиному $\varphi(x) = x^5 + x^2 + 1$

Для практического использования могут быть рекомендованы генераторы, соответствующие характеристическому полиному $x^m + x^\ell + 1$:

$m = 127, \quad \ell = 15$

$m = 151, \quad \ell = 15$

$n = 175, \quad \ell = 16$

6.2. Генератор псевдослучайных чисел, основанный на методе вычетов

Рассмотрим генератор псевдослучайных чисел, построенный по следующей итерационной схеме (метод вычетов):

$$x_i = (a \cdot x_{i-1} + c) \bmod m \qquad (6.2)$$

где:

x_0 - начальное значение;

a - множитель;

c - приращение;

m- модуль; $\bmod m$ - операция целочисленного деления по модулю m.

Например, при $x_0 = a = c = 7, m = 10$ псевдослучайная последовательность выглядит так: 7,6,9,0,7,6,9,0,7,……..

При работе с генератором, построенным по методу вычетов, есть возможность получить априорную информацию о периоде генератора и коэффициенте последовательной автокорреляции. Под качественным генератором будем понимать генератор псевдослучайных чисел, имеющий максимальный период и возможно наименьший коэффициент автокорреляции.

Величину периода генератора, построенного по методу вычетов, можно оценить на основе выводов теоремы 1.

Теорема 1. Длина периода генератора, основанного на методе вычетов, равна m тогда и только тогда, когда

- c и m взаимно простые числа,
- a-1 кратно p для любого простого p, являющегося делителем m,
- $a-1$ кратно 4, если m кратно 4.

Коэффициент последовательной автокорреляции определим на основе выводов теоремы 2.

Теорема 2. Коэффициент последовательной автокорреляции для последовательности с максимальным периодом определяется следующим выражением:

$$R_1 \cong \frac{1}{a}\left(1 - 6\frac{c}{m} + 6\frac{c^2}{m^2}\right) + \Delta \ , \qquad (6.3)$$

поправка Δ не превосходит:

$$\Delta < \frac{a-6}{m}$$

Соотношение (6.3) помогает при выборе значения *c*. Числа *c*, кроме того, что они взаимно простые, должны удовлетворять условию:

$$\frac{c}{m} \approx 0.211$$

Из соотношения (6.3) также следует, что нужно избегать малых значений *a*. С другой стороны, большие значения *a* еще не гарантируют того, что корреляция будет мала, так как в этом случае возрастает величина поправки. Если $a \approx \sqrt{m}$, то значение коэффициента последовательной корреляции ограничено величиной $\frac{2}{\sqrt{m}}$.

7. ТЕХНИКА ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

7.1. Моделирование непрерывной случайной величины

7.1.1. Метод обратного преобразования

Для решения задачи моделирования непрерывной случайной величины ξ на основе использования ГПСЧР необходимо найти вид функционала Φ, однозначно связывающего ξ и равномерно распределенную на интервале (0,1) случайную величину r. Рассмотрим случайную величину ξ, у которой определена дифференциальная функция распределения вероятностей (плотность вероятностей) $f(x)$ и интегральная функция распределения вероятностей $F(x)$. Случайную величину, удовлетворяющую этим свойствам, моделируют на основе метода обратного преобразования.

Теорема. Если $F(x)$- интегральная функция распределения вероятностей случайной величины, а r - случайная величина с равномерным распределением на интервале (0,1), то случайная величина, равная

$$\xi = F^{-1}(r), \tag{7.1}$$

имеет функцию распределения $F(x)$. Здесь F^{-1} - функция, обратная по отношению к F. Этот алгоритм носит название «метод обратного преобразования».

Докажем теорему: по определению

$$F(\xi) = P(\xi \le x); \tag{7.2}$$

подставим в (7.2) значение ξ из (7.1):

$$F(\xi) = P(F^{-1}(r) \le x); \tag{7.3}$$

тождественно преобразуем выражение в скобках:

$$F(\xi) = P(r \le F(x)) = \int_0^{F(x)} f(r)dr, \tag{7.4}$$

и с учетом того, что $f(r)=1$, получим

$$\int_0^{F(x)} f(r)dr = F(x). \tag{7.5}$$

Отсюда следует $F(\xi) = F(x)$, что и требовалось доказать.

Рассмотрим следующий пример. Необходимо промоделировать случайную величину τ : интервал времени между последовательными случайными событиями (например, поступление пакетов на узел коммутации). Средний интервал $\bar{\tau} = \frac{1}{\lambda}$, где λ - интенсивность поступления пакетов.

Как правило, интервалы между случайными событиями распределены по экспоненциальному закону:

$$f(x) = c_1 \exp(-c_2 x). \tag{7.6}$$

Константы c_1 и c_2 найдем из условия нормировки:

$$\int_0^\infty f(x)dx = 1, \tag{7.7}$$

и с учетом того, средний интервал $\bar{\tau} = \frac{1}{\lambda}$,

$$\int_0^\infty x f(x)dx = \frac{1}{\lambda}, \tag{7.7}$$

получаем, что $c_1 = c_2 = \lambda$, находим интегральную функцию

$$F(x) = \int_0^x \lambda \cdot \exp(-\lambda y)dy = 1 - \exp(-\lambda x). \tag{7.9}$$

Применим метод обратного преобразования:

$$1 - \exp(-\lambda\tau) = r, \tag{7.10}$$

отсюда

$$\tau = -\frac{1}{\lambda}\ln(1-r), \tag{7.11}$$

и учитывая, что случайная величина $1-r$ равномерно распределена на интервале (0,1), заменим $1-r$ на r:

$$\tau = -\frac{1}{\lambda}\ln r. \tag{7.12}$$

7.2. Моделирование псевдослучайной величины, распределенной по нормальному закону

Нормально распределенные случайные величины широко распространены на практике и в частности при моделировании радиотехнических систем. Объяснение этого факта дано М.А.Ляпуновым в центральной предельной теореме теории вероятности. Рассмотрим следствие из центральной предельной теоремы теории вероятности: *если случайная величина* Ω *представляет собой сумму очень большого числа взаимно независимых случайных величин, влияние каждой из которых на всю сумму ничтожно мало, то* Ω *имеет распределение, близкое к нормальному.*

Пример нормального распределения в радиотехнике: нормальный (гауссов) шум.

Распределение вероятностей непрерывной случайной величины описывается дифференциальной функцией

$$f(x)=\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right), \tag{7.13}$$

где μ - математическое ожидание, σ^2 - дисперсия.

Важным свойством нормального распределения является «правило трех сигм»: $P(|\Omega-\mu|)<3\sigma=0.997$.

Интегральная функция распределения нормально распределенной случайной величины $F(x)=\int_{-\infty}^{x} f(z)dz=\Phi(x)$ представляет собой спецфункцию, которая задается табличным образом. В этом случае нельзя использовать метод «обратного преобразования».

При моделировании нормально распределенной случайной величины с произвольными параметрами μ,σ удобно перейти к случайной величине ξ с $\mu=0,\sigma=1$ и дифференциальной функцией распределения

$$f(x)=\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{x^2}{2}\right). \tag{7.14}$$

Связь между Ω и ξ определяется следующим выражением:

$$\Omega=\sigma\xi+\eta. \tag{7.15}$$

Рассмотрим основные методы моделирования нормально распределенной случайной величины.

7.2.1. Метод, основанный на центральной предельной теореме

Этот метод непосредственно формализует следствия предельной теоремы: распределение суммы независимых случайных величин $U_i, i=1,2,...,n$ приближается к нормальному при неограниченном увеличении n, если выполняются следующие условия:

- все величины имеют конечные математическое ожидание и дисперсию;
- ни одна из величин не является превалирующей.

Представим ξ в виде

$$\xi = \frac{\sum_{i=1}^{n} r_i - \frac{n}{2}}{\sqrt{\frac{n}{12}}}, \qquad (7.16)$$

где r - псевдослучайная величина, равномерно распределенная на интервале (0,1).

Ограничим $n = 12$, тогда

$$\xi = \sum_{i=1}^{12} r_i - 6 \qquad (7.17)$$

Найдем математическое ожидание и дисперсию случайной величины ξ:

$$M(\xi) = M\left(\sum_{i=1}^{12} r_i - 6\right) = \sum_{i=1}^{12} M(r_i) - M(6) = 12 \cdot 0{,}5 - 6 = 0, \qquad (7.17)$$

$$\sigma^2(\xi) = D\left(\sum_{i=1}^{12} r_i - 6\right) = \sum_{i=1}^{12} D(r_i) - D(6) = 12 \cdot \frac{1}{12} - 0 = 1. \qquad (7.19)$$

Данный метод моделирования нормально распределенной величины реализуется двумя способами:

- параллельно работают 12 различных генераторов ПСЧР;
- работает 1 генератор ПСЧР, 12 последовательных членов генератора ПСЧР дают одно нормально распределенное число.

Недостатки данного метода заключаются в следующем:

- в зависимости от способа реализации необходимо обеспечить 12 некоррелированных генераторов ПСЧР или низкий коэффициент последовательной корреляции вплоть до R_{11} во втором случае;
- диапазон изменения случайной величины ξ (-6,6) ограничен, в то время как нормально распределенная случайная величина может принимать любые значения на интервале $(-\infty, \infty)$. С учетом «правила трех сигм» этот недостаток не является существенным.

7.2.2. Аппроксимация Зелинского

Так как интегральную функцию нельзя представить в элементарных функциях, для положительных значений аргумента предложена аппроксимация с ошибкой аппроксимации, не превышающей 10%.

$$\sqrt{\frac{1}{2\pi}} \exp\left(-\frac{x^2}{2}\right) \approx \frac{k \cdot \exp(-kx)}{(1 + \exp(-kx))^2}, \qquad x > 0, \qquad k = \sqrt{\frac{8}{\pi}} \qquad (7.20)$$

Теперь интегральную функцию $F(x)$ легко представить в элементарных функциях:

$$F(x)=\int_{o}^{x}\frac{k\cdot\exp(-ky)}{(1+\exp(-ky))^2}dy=\frac{2}{1+\exp(-kx)}-1 \tag{7.21}$$

Применяем метод «обратного преобразования»

$$\frac{2}{1+\exp(-k\xi)}-1=r \tag{7.22}$$

и получаем искомое выражение:

$$\xi=\frac{1}{k}\ln\frac{1+r}{1-r}. \tag{7.23}$$

Для того чтобы была возможность моделировать случайную величину на всем интервале $(-\infty,\infty)$, нужно реализовать еще один генератор ПСЧР - $r2$, отвечающий за знак, который будет случайным образом генерировать знак случайной величины ξ:

- если $r2_i<0{,}5$, то ξ_i берем со знаком (-);
- если $r2_i\geq 0{,}5$, то ξ_i берем со знаком (+).

7.2.3. Метод Брокса-Маллера

Введем еще одну независимую случайную величину η, распределенную по нормальному закону:

$$f(y)=\frac{1}{\sqrt{2\pi}}\exp\left(-\frac{y^2}{2}\right) \tag{7.24}$$

Ввиду того, что ξ и η – независимые случайные величины, то их совместную плотность вероятности $f(x,y)$ можно представить в виде произведения

$$f(x,y)=f(x)f(y)=\frac{1}{2\pi}\exp\left(-\frac{x^2+y^2}{2}\right). \tag{7.25}$$

ξ и η можно рассматривать как случайные координаты в декартовой системе координат. Перейдем к полярной системе координат, в которой случайными координатами будут радиус–вектор ρ и угол β (относительно оси ξ),

$$\xi=\rho\cos\beta,\quad \eta=\rho\sin\beta. \tag{7.26}$$

Якобиан перехода в полярную систему координат равен ρ. Тогда совместная плотность вероятности будет равна

$$f(\rho,\beta)=\frac{\rho}{2\pi}\exp\left(-\frac{\rho^2}{2}\right). \qquad (7.27)$$

Покажем, что совместную плотность вероятности можно представить в виде произведения: $f(\rho)f(\beta)=f(\rho,\beta)$, что будет означать статистическую независимость случайных величин ρ и β:

$$f(\rho)=\int_0^{2\pi} f(\rho,\beta)d\beta=2\pi\frac{\rho}{2\pi}\exp\left(-\frac{\rho^2}{2}\right)=\rho\exp\left(-\frac{\rho^2}{2}\right). \qquad (7.27)$$

$f(\beta)=\int_0^{\infty} f(\rho,\beta)d\beta$ найдем из условия нормировки:

$$\int_0^{2\pi}\int_0^{\infty} f(\rho,\beta)=1 \quad \Rightarrow \quad 2\pi\int_0^{\infty} f(\rho,\beta)d\rho=2\pi f(\beta)\ , \qquad (7.29)$$

отсюда $f(\beta)=\frac{1}{2\pi}$ и $f(\rho)f(\beta)=f(\rho,\beta)$.

Статистическая независимость случайных величин ρ и β доказана.

К случайным величинам ρ и β применим «метод обратного преобразования».

$$\beta\Rightarrow \quad f(\beta)=\frac{1}{2\pi}\Rightarrow \quad F(\beta)=\int_0^{\beta}\frac{1}{2\pi}dx=\frac{\beta}{2\pi}\Rightarrow \quad \frac{\beta}{2\pi}=r1,$$

отсюда

$\beta=2\pi r1$

$$\rho\Rightarrow \quad f(\rho)=\rho\cdot\exp\left(-\frac{\rho^2}{2}\right)\Rightarrow \quad F(\rho)=\int_0^{\rho} x\cdot\exp\left(-\frac{x^2}{2}\right)=1-\exp\left(-\frac{x^2}{2}\right)\ \ 1-\exp\left(-\frac{x^2}{2}\right)=r2$$

отсюда

$\rho=\sqrt{-2\ln r2}$,

$r1$ и $r2$ - статистически независимые ГПСЧР.

Подставляя β и ρ в (7.26), получим:

$$\begin{aligned}\xi&=\cos 2\pi r1\cdot\sqrt{-2\ln r2}\\ \eta&=\sin 2\pi r1\cdot\sqrt{-2\ln r2}\end{aligned} \qquad (7.30)$$

В методе Брокса-Маллера генерируется две статистически независимых последовательности, распределенных по нормальному закону.

Анализ методов моделирования нормально распределенных псевдослучайных величин. Первый метод, основанный на предельной теореме, требует использования 12 статистически независимых ГПСЧР, что очень сложно реали-

зовать на практике. Недостатком метода Зелинского является то, что события с низкой теоретической вероятностью генерируются значительно чаще. Наиболее корректным является метод Брокса-Маллера. В этом методе необходима реализация только двух статистически независимых ГПСЧР.

7.3. Моделирование дискретных случайных величин

Сначала рассмотрим, как моделируются случайные события с известным распределением вероятностей. Предположим, что заданы численные значения вероятностей $P_1, P_2, \ldots\ldots P_n$ для независимых событий $A_1, A_2, \ldots\ldots, A_n$, составляющих полную группу событий. Разобьем отрезок (0,1) на n отрезков так, чтобы длина i-го отрезка равнялась P_i. Генерируя псевдослучайное число r, будем определять, на какой отрезок попадает число r. Попадание случайного числа на j-ый участок фиксируется как факт совершения события A_j.

Очевидно, что при достаточно большом числе испытаний количество попаданий на i-ый участок будет пропорционально его длине (т.е. значению P_i), а это означает, что случайные события воспроизводятся в соответствии с заданным распределением вероятностей. Таким образом, процесс сводится к генерации псевдослучайных чисел r и последовательной проверке условия

$$\sum_{i=1}^{j-1} P_i < r \le \sum_{i=1}^{j} P_i . \qquad (7.31)$$

Для конкретного r неравенство (7.31) выполняется лишь при каком-то одном значении j ($j=1,2, \ldots ,n$). Это значение j и определяет номер события A.

7.3.1. Моделирование распределения Пуассона

Этот тип распределения находит очень широкое применение в теории массового обслуживания и в теории телетрафика. Дискретное распределение Пуассона имеет вид

$$P(\xi = m) = \frac{\lambda^m \cdot \exp(-\lambda)}{m!}, \qquad (7.32)$$

где $P(\xi = m)$ - вероятность того, что случайная величина ξ примет значение, равное m, а параметр $\lambda = M(\xi)$.

Из множества способов генерации случайной величины, удовлетворяющей закону Пуассона, рассмотрим два основных.

Первый способ основан на использовании итерационной схемы, представленной выражением (7.31), где в качестве P_i используется конкретное для данного распределения выражение (7.32). Аналогичным образом можно моделировать любое дискретное распределение.

Второй способ основан на том, что в пуассоновском процессе величина интервала между событиями является случайной величиной, которая подчиняется экспоненциальному закону.

Допустим, задана интенсивность процесса λ, имеющая размерность: число событий в единицу времени (1/сек). Тогда средний интервал времени между событиями $\bar{\tau} = \frac{1}{\lambda}$. Далее, генерируя случайную величину τ – интервал времени между событиями в соответствии с выражением (7.12), получим последовательность событий, которая подчиняется закону Пуассона.

8. ПЛАНИРОВАНИЕ ИМИТАЦИОННОГО ЭКСПЕРИМЕНТА

8.1. СТРАТЕГИЧЕСКОЕ ПЛАНИРОВАНИЕ

План имитационного эксперимента представляет собой методологию получения с помощью эксперимента необходимой информации, стоимость которой зависит от способа сбора и обработки данных. Эффективность моделирования существенным образом зависит от выбора плана эксперимента. Имитационный эксперимент требует затрат труда и времени экспериментатора и использования соответствующего компьютера. Чем больше средств вложено экспериментатором в данное исследование, тем меньше их остается на остальные исследования, и поэтому необходимо иметь план, позволяющий извлекать из каждого эксперимента максимально возможное количество информации.

Планирование эксперимента выгодно в двух отношениях:

- оно позволяет уменьшить число необходимых испытаний и тем самым повысить экономичность имитационного эксперимента;
- служит структурной основой процесса исследований.

Несмотря на то, что цели компьютерного моделирования и проведения физического эксперимента, по существу, совпадают, между этими видами экспериментов существуют и различия. При этом наиболее важное значение имеют следующие факторы, присущие имитационному моделированию:

- Легкость повторения и воспроизведения условий проведения эксперимента.
- Легкость прерывания и возобновления эксперимента.
- Наличие или отсутствие корреляции между последовательными выборочными точками.
- Управление условиями проведения имитационного эксперимента. В физическом эксперименте стохастические условия не зависят от экспериментатора. В компьютерном эксперименте эти условия определяются экспериментатором.

Одним из основных преимуществ компьютерного эксперимента является легкость воспроизведения условий эксперимента. При проведении сравнения двух альтернатив, можно сравнить их при одинаковых условиях (при одинаковой последовательности событий). Это достигается путем использования одной и той же последовательности случайных чисел для каждой из альтернатив, в результате чего уменьшается разностная вариация усредненных характеристик альтернатив, что позволяет осуществлять статистически значимое различие этих характеристик при значительно меньших размерах выборки.

Еще одно преимущество компьютерного эксперимента перед натурным (физическим) состоит в легкости прерывания и возобновления эксперимента. Это позволяет применять в компьютерном эксперименте последовательные или эвристические методы, которые могут оказаться нереализуемыми в натурном эксперименте. При работе с компьютерной моделью всегда можно прервать эксперимент на время, необходимое для анализов результатов и принятия решения об изменении параметров модели или продолжении эксперимента при тех же значениях параметров.

Основным недостатком компьютерного эксперимента является автокорреляция выходных данных. Автокорреляция означает, что наблюдения в выходных последовательностях не являются независимыми (независимость - одно из основных предположений многих методов планирования эксперимента). При этом значения наблюдаемого выхода зависят от одного или нескольких предыдущих наблюдений и поэтому содержат меньше информации, чем в случае независимых наблюдений. Так как в большинстве существующих методов планирования эксперимента предполагается независимость наблюдений, то многие обычные статистические методы нельзя непосредственно применять в случае наличия автокорреляции.

В зависимости от конкретных целей эксперимента для анализа его результатов могут потребоваться различные методы. Наиболее широко распространены следующие типы экспериментов:

1. Сравнение средних и дисперсий различных альтернатив.

2. Определение влияния на целевую функцию переменных и ограничений, наложенных на эти переменные.

3. Отыскание оптимальных значений на некотором множестве возможных значений переменных.

Эксперименты первого типа обычно являются так называемыми однофакторными экспериментами. Они довольно просты, и основные вопросы, встающие перед экспериментатором при их проведении, это вопросы о размере выборки, начальных условиях и наличии или отсутствии корреляции. В разделе 8.2. рассмотрено большинство этих вопросов.

Экспериментам второго типа посвящено большинство книг по планированию экспериментов и анализу их результатов. Основными методами истолкования результатов этих экспериментов являются дисперсионный и регрессионный анализ.

Третий тип экспериментов предполагает использование последовательных или поисковых методов построения экспериментов с использованием аппарата факторного анализа.

8.2. Тактическое планирование имитационного эксперимента

Так как флуктуации присущи всем стохастическим имитационным моделям, то для достижения заданной точности результатов имитационного эксперимента необходимо повторять эксперимент, каждый раз меняя значения входящих в модель случайных факторов.

Время одного прогона сложного модельного эксперимента может быть большим. Поэтому становится актуальной проблема минимизации затрат компьютерного времени.

С другой стороны, экспериментатор должен проводить эксперимент таким образом, чтобы не только получить результаты, но и оценить их точность, т.е. степень доверия к тем выводам, которые будут сделаны.

В случае проверки совпадения двух режимов экспериментатор должен задать допустимые величины рисков ошибочных выводов, которые он может сделать, если:

- придет к выводу, что режимы различны, тогда как на самом деле они совпадают (ошибка первого рода);
- придет к выводу, что режимы совпадают, тогда как на самом деле они различны (ошибка второго рода).

Рассмотренные понятия составляют основу аппарата математической статистики и являются достаточно универсальными.

8.2.1. Определение объема выборки

Как много испытаний нужно сделать (сколько получить выборочных значений), чтобы обеспечить достаточную статистическую значимость результатов моделирования? На этапе тактического планирования имитационного эксперимента определяется размер выборки, который позволяет обеспечить желаемый уровень точности и в то же время минимальную стоимость моделирования.

Размер выборки можно определить одним из двух путей:

- априорно (т.е. независимо от работы модели);
- в процессе работы модели на основе полученных с помощью модели результатов.

8.2.2. Априорное определение объема выборки. Определение объема выборки по оценке среднего значения.

В условиях применения центральной предельной теоремы и отсутствия автокорреляции для определения необходимого объема выборки можно использовать метод доверительных интервалов.

Моделируем случайную величину с известным математическим ожиданием и дисперсией: $\xi\left(M(\xi),\sigma_\xi^2\right)$, и вычисляем выборочное среднее $\bar{\xi}=\frac{1}{n}\sum_{j=1}^{n}\xi_j$ по *n* реализациям.

Рассмотрим статистику:

$$P\left\{M-d\le\bar{\xi}\le M+d\right\}=1-\alpha \qquad (8.1)$$

1-α - вероятность попадания среднего значения, вычисленного по *n* реализациям, в интервал $M\pm d$.

Задача состоит в определении необходимого для выполнения условия (8.1) объема выборки. При заданном уровне значимости α нужно определить величину *n*.

Если закон распределения случайной величины γ не известен, воспользуемся неравенством Чебышева:

$$P\left(\left|\gamma-M(\gamma)>k\sigma_\gamma\right|\right)\le\frac{1}{k^2}. \qquad (8.2)$$

Преобразуем (8.1)

$$P\left\{-d\le\bar{\xi}-M(\xi)\le d\right\}=1-\alpha. \qquad (8.3)$$

Тогда вероятность непопадания в интервал $\left[M(\xi)\pm d\right]$ будет

$$P\left\{\left|\xi-M(\xi)\right|>d\right\}=\alpha, \qquad (8.4)$$

$$P\left\{\left|\frac{\xi_1+\xi_2+\ldots+\xi_n}{n}-M(\xi)\right|>d\right\}=\alpha. \qquad (8.5)$$

Введем случайную величину $\gamma=\xi_1+\xi_2+\ldots+\xi_n$, и преобразуем выражение (8.5).

$$P\left\{\left|\gamma-M(\xi)n\right|>dn\right\}=\alpha. \qquad (8.6)$$

Учтем, что

$M(\xi)=M(\xi_1)+M(\xi_2)=\ldots=M(\xi_n)=M(\xi),$

$M(\gamma)=nM(\xi),$

$\sigma_{\xi_1}^2=\sigma_{\xi_2}^2=\ldots.=\sigma_{\xi_n}^2=\sigma_{\xi_1}^2,$

$\sigma_\gamma^2 = n\sigma_\xi^2$, и тогда:

$$P\{|\gamma - M(\gamma)| > dn\} = \alpha . \quad (8.7)$$

Сделаем следующее допущение: преобразуем неравенство Чебышева в равенство:

$$P(|\gamma - M(\gamma) > k\sigma_\gamma|) = \frac{1}{k^2} \quad (8.8)$$

Сопоставив два последних выражения, получим:

$k\sigma_\gamma = k\sqrt{n}\sigma_\xi = dn$ и $\alpha = \frac{1}{k^2}$, а из этих выражений получим:

$$n = \frac{\sigma_\xi^2}{d^2} \cdot \frac{1}{\alpha} . \quad (8.9)$$

Рассмотрим различные приложения, в которых используется данная формула.

1. Задаем уровень значимости α и величину доверительного интервала d. По формуле (8.9) определяем число испытаний, в соответствии с которым выборочное среднее попадает в доверительный интервал с заданным уровнем значимости.

2. Задаем уровень значимости α и число испытаний n. В имитационном эксперименте вычисляем $d_э = |\bar{\xi} - M(\xi)|$, а по формуле $d = \frac{\sigma}{\sqrt{n\alpha}}$ вычисляем критическую точку $d_{кр}$. Если $d_э \le d_{кр}$, то принимаем гипотезу $\bar{\xi} = M(\xi)$. В противном случае эта гипотеза должна быть отвергнута.

Случайная величина ξ распределена по нормальному закону. Построим следующую статистику:

$$P\{M(\xi) - d \le \bar{\xi} \le M(\xi) + d\} = 1 - \alpha . \quad (8.10)$$

Преобразуем выражение (8.10):

$$P\{-d \le \bar{\xi} - M(\xi) \le d\} = 1 - \alpha , \quad (8.11)$$

$$P\left\{-d \le \frac{\xi_1 + \xi_2 + ... + \xi_n}{n} - M(\xi) \le d\right\} = 1 - \alpha , \quad (8.12)$$

$$P\{-dn \le \xi_1 + \xi_2 + ... + \xi_n - nM(\xi) \le nd\} = 1 - \alpha . \quad (8.13)$$

Рассмотрим новую случайную величину $\gamma = \xi_1 + \xi_2 + ... + \xi_n$, у которой $M(\gamma) = nM(\xi)$ и $\sigma_\gamma^2 = n\sigma_\xi^2$, тогда выражение (8.13) перепишем в виде:

$$P\{-dn \le \gamma - M(\gamma) \le dn\} = 1-\alpha\,. \qquad (8.14)$$

Перейдем к «стандартной» случайной нормальной величине μ с $M(\mu)=1,\quad \sigma_\mu = 1.$ Связь между μ и γ осуществляется по формуле $\gamma = \sigma_\gamma \mu + M(\gamma)$. Теперь выражение (8.14) перепишем в виде:

$$P\left\{-\frac{dn}{\sigma_\gamma} \le \mu \le \frac{dn}{\sigma_\gamma}\right\} = 1-\alpha\,, \qquad (8.15)$$

$$P\left\{-\frac{dn}{\sigma_\gamma} \le \mu \le \frac{dn}{\sigma_\gamma}\right\} = 1+\Phi\left(\frac{dn}{\sigma_\gamma}\right) - \left[1+\Phi\left(-\frac{dn}{\sigma_\gamma}\right)\right] == 2\Phi\left(\frac{dn}{\sigma_\gamma}\right), \qquad (8.16)$$

Φ(z) - функция Лапласа.

С учетом (8.14) получим

$$\Phi\left(\frac{dn}{\sigma_\gamma}\right) = \frac{1-\alpha}{2}\,. \qquad (8.17)$$

Введем обозначение $x = \frac{dn}{\sigma_\gamma}$. Учитывая, что $\sigma_\gamma = \sqrt{n}\sigma_\xi$, получим

$$n = \frac{\sigma_\xi^2 \cdot x^2}{d^2}, \qquad (8.18)$$

где x – корень уравнения $\Phi(x) = \frac{1-\alpha}{2}$.

В таблице 8.1 приведены значения x при наиболее часто используемых значениях уровня значимости α.

Таблица 8.1

α	x	x^2
0,1	1,65	2,72
0,05	1,96	3,84
0,05	2,58	6,66

9. ПРОБЛЕМА АДЕКВАТНОСТИ МОДЕЛИ

Модель строится для достижения конкретных целей, связанных с функционированием реальной системы. Мы хотим построить модель таким образом, чтобы она обладала характеристиками, близкими к характеристикам изучаемой реальной системы. Оценить качество модели означает оценить уровень нашей уверенности в том, что выводы, сделанные с помощью модели, применимы к реальной системе.

Понятие адекватной модели не является бинарным: да или нет. Адекватность (точность) модели можно представить в виде некоторого числа от 0 до 1, где 0 означает абсолютно неточную модель, а 1 означает абсолютно точную модель.

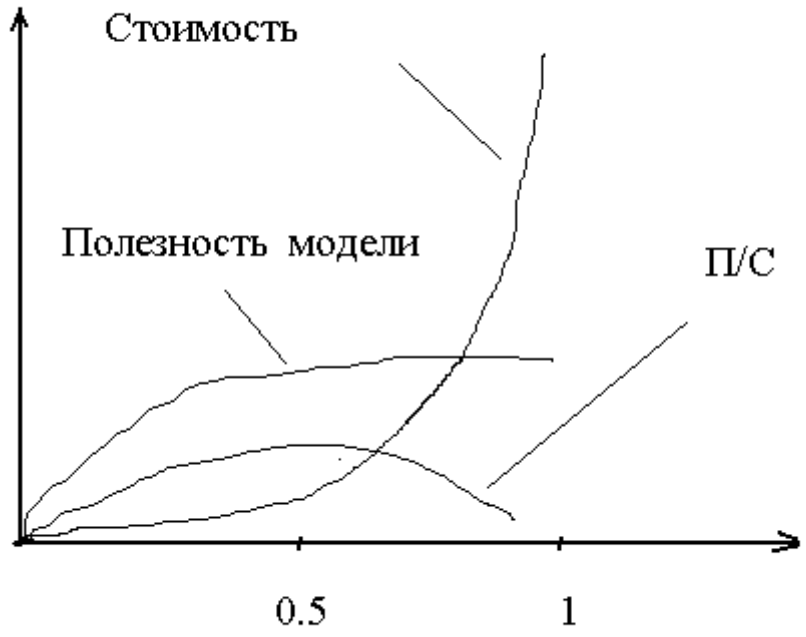

Рис.9.1. Зависимости полезности и стоимости модели от точности

Рассмотрим графики, представленные на рис. 9.1. На этих графиках приведены типичные зависимости стоимости и полезности модели от точности модели. С ростом точности модели возрастает ее стоимость и ее полезность для исследователей. Но стоимость растет значительно быстрее, чем полезность. Таким образом, отношение полезность/стоимость будет достигать максимума в точке, которая лежит ближе к началу координат, чем точка, соответствующая наиболее обоснованной модели, которую можно построить не щадя средств.

На первой стадии моделирование сводится к построению внутренней структуры модели на основе априорной информации, прошлых исследований и существующих теорий. Любая сложная имитационная модель состоит из большого числа простых моделей. Имитируемые этими простыми моделями процессы обычно хорошо определены и понятны. Однако при объединении их в сложную совокупность большое число вариантов возможных взаимодействий делает понимание поведения всей системы затруднительным.

При использовании имитационного моделирования для изучения сложных систем возникают различного рода ошибки, которые могут привести к неверным выводам. Ошибки возникают:

- при построении модели;
- при программировании;
- в используемых данных;
- в интерпретации результатов.

В процессе построения и применения модели разработчик модели должны помнить о возможности появления таких ошибок и делать все возможное, чтобы избежать их.

В большинстве имитационных экспериментов используются случайные числа. Модель содержит последовательности случайных событий, сложным образом взаимодействующих друг с другом. В разделе «тактическое планирование» показано, что при достаточно большом числе испытаний результаты моделирования можно сделать сколь угодно точными.

Проблема состоит в том, что эти «точные результаты» точны только в том случае, если идентичны процессы, происходящие в модели и в реальной системе. Если же между этими процессами есть расхождения, то результатам моделирования присуща неточность, которую нельзя устранить увеличением числа испытаний.

Можно выделить три основные проблемы оценки адекватности модели:

1.Проверка внутренней состоятельности модели. Здесь можно отметить: а) проверку наличия ошибок чисто программистских; б) проверку наличия нелепых результатов; в) отладку отдельных модулей программы.

2. Соответствие реальной системе. Оценка точности соответствия поведения модели поведению реальной системы.

3. Проблемный анализ. Анализ и интерпретация данных, полученных в имитационном эксперименте.

Проблему оценки точности соответствия поведения модели поведению реальной системы рассмотрим более детально. Введем понятие «изоморфизм».

Сходство модели с объектом, который она отображает, называется степенью изоморфизма. Для того чтобы быть изоморфной, модель должна удовлетворять двум условиям:

- должно существовать однозначное соответствие между элементами модели и элементами представляемого объекта;
- должны быть сохранены точные соотношения или взаимодействия между элементами.

Степень изоморфизма модели относительна, и большинство моделей скорей гомоморфны, чем изоморфны. Под гомоморфизмом понимают сходство по форме при различии основных структур, причем имеет место лишь поверхностное подобие между различными группами элементов модели и объекта. Гомоморфные модели являются результатом процессов упрощения.

Теперь проблему адекватности можно представить следующими вопросами:

1. Насколько изоморфными должны быть модель и реальная система?

2. Если модель достаточно точно предсказывает результаты работы системы, то насколько важным является изоморфизм модели и реальной системы?

3. Может ли модель быть существенно гомоморфной и тем не менее достаточно точной?

Начнем с последнего пункта. Классическим примером достаточно точной гомоморфной модели является геоцентрическая модель вселенной. Другой пример представляет экономическая модель Элмагреби. Им разработана модель для предсказания (прогнозирования) экономических циклов, основанная на высокой коррелированности этих циклов с количеством пятен на Солнце. В этом случае можно встать на точку зрения, что важна только полезность модели независимо от соответствия ее структуры моделируемому явлению.

Проблемы построения и тестирования модели имеют очень много общего с методами познания. Проблема обоснования применимости имитационной модели ничем не отличается от проблемы обоснования применимости теории или гипотезы в любой отрасли науки.

Рассмотрим три основных направления в теории познания: рационализм, эмпиризм и прагматизм, в контексте, связанном с имитационным моделированием.

Представители рационализма и эмпиризма считают, что построение модели начинается с наблюдения за моделируемой системой. На этом ограничивается общее между двумя подходами. Рационалисты постулируют способы

взаимодействия элементов системы (от общего к частному!). Эмпирики рассматривают только те взаимодействия, которые можно проверить экспериментально.

Приверженцы рационализма считают, что модель есть совокупность правил логической дедукции, которые ведут от предпосылок к объективным выводам. Сами предпосылки могут поддаваться (или не поддаваться) эмпирической проверке. В чистом виде рационализм основан на том, что Кант называл синтетическими априорными предпосылками. Примером модели, основанной на философии рационализма, является модель города, предложенная Форрестером. Основу модели составляют 5 основных тезисов (или постулатов), типа: «Если условия в данном городе более благоприятны, чем вне его, то люди и промышленность будут стремиться в него, естественно правильно и обратное». Согласиться с правильностью такой модели - значит согласиться с основными предпосылками и логикой, которой они между собой связаны.

В отличие от рационалистов, которые считают, что достаточно показать основные тенденции в функционировании системы, представители эмпиризма требуют опоры на доказанные или проверяемые факты и отказа от всяких непроверенных предположений. Эмпирик этот раздел модели города сформулировал бы на основе статистических выкладок.

Мы можем рассматривать имитационную модель как черный ящик, преобразующий входные переменные в выходные. Рационалист и эмпирик занимаются выявлением структуры черного ящика. Абсолютного прагматика не интересует структура черного ящика. Главным мерилом адекватности модели является соответствие результатов моделирования эксперименту. При таком подходе экономическая модель Элмагреби имеет право на существование, несмотря на абсурдность ее основ.

Утилитарный подход. Большинство моделей используют все три подхода. Подход к обоснованию модели, включающий в какой-то мере точки зрения рационалистов, эмпириков и абсолютных прагматиков, можно назвать утилитарным подходом.

Процесс построения имитационной модели и ее проверки состоит из трех перемежающихся стадий:

- построение гипотез о взаимодействии элементов системы, основанных на имеющейся информации (которая включает в себя наблюдения, теории и интуитивные представления; в общем случае являющиеся атрибутами рационального подхода);
- проверка принятых допущений и гипотез (атрибуты эмпиризма);

- сравнение соотношений входов и выходов модели и реальной системы (прагматизм).

Что же все-таки можно назвать адекватной моделью? Для определения адекватности нет простых тестов. Выполнение всех 12 этапов имитации, которые представлены в разделе 4, повышает степень адекватности модели. Большинство этапов моделирования и их влияние на модель подробно рассмотрены. Покажем, как такой этап как документирование повышает достоверность модели. Проблема проверки модели носит на первый взгляд только объективный характер. На самом деле вопрос значительно сложнее. Во-первых, при сопоставлении имитации с экспериментом невозможно охватить весь объем сопоставимого материала. А во-вторых, что является, наверное, самым главным, сопоставление носит все-таки субъективный характер, и разработчик модели волен сам подбирать сопоставляемый материал. После того как работа прошла этап документирования и представлена в виде статьи, диссертации, действующего программного комплекса и т.п. и т.д., она попадает в руки независимых экспертов, что значительно расширяет рамки сопоставления имитации и модели и уточняет степень достоверности модели.

10.ИМИТАЦИОННАЯ МОДЕЛЬ МЕТЕОРНОЙ КРИПТОГРАФИИ

В качестве примера имитационной модели рассмотрим модель метеорной криптографической системы на основе компьютерной имитационной модели метеорного радиоканала «КАМЕТ». Для начала кратко опишем способ генерации и распределения ключей между абонентами метеорной радиолинии.

Метеорные частицы представляют собой небольшие частицы космического мусора массой 10^{-5}-10^{-2}г, которые непрерывно влетают в атмосферу Земли со скоростями 12-72 км/с. После пролета такой частицы в атмосфере Земли на высотах 70-110 км образуется ионизированный столб шириной примерно 1 м и длиной от 5 до 15 км, обладающий свойством зеркального отражения радиоволн. Уникальными свойствами метеорного радиоканала является его высокая взаимность для двух пунктов связи и стабильность во времени.

На рис.10.1. представлена схема метеорной связи между двумя законными пользователями А и В, которые по метеорному каналу производят двусторонний обмен радиосигналами. При приёме метеорных радиоотражений на каждом пункте измеряют время их распространения (или фазовую задержку), которые, в силу принципа взаимности, оказываются одинаковыми на обоих концах радиолинии. Путём наблюдения за некоторым множеством метеорных следов происходит накопление двух идентичных экземпляров последовательности случайных чисел. Далее на каждом пункте связи накопленный набор измерений используется для генерации одного (из двух) экземпляра секретного ключа шифрования. Существенно то, что секретный ключ создаётся непосредственно в пунктах связи, и фактически не требуется физическая передача ключа от одного абонента другому.

Вследствие зеркального отражения радиоволн (на рис.10.1 показана зеркальная точка M_{AB} для законных пользователей) от метеорного следа существует лишь ограниченная область, прилегающая к пункту связи, где возможна корреляция характеристик сигнала. Для любого третьего пункта связи С, располагающегося в окрестности одного из легальных пунктов (например, пункта В), на метеорном следе образуется другая отражающая точка M_{AC}, что приводит к другому пути распространения сигнала и отсутствию корреляции измерений третьих лиц с измерениями легальных пользователей. Это физически исключает возможность перехвата ключевой информации.

Таким путем организуется автоматическое распределение ключей между участниками информационного обмена и исключается возможность доступа посторонних лиц к секретным ключам шифрования/расшифрования информа-

ции. Проведение натурных экспериментов по метеорной генерации и распределению ключей шифрования («метеорной криптографии») требует наличия полностью отлаженной системы синхронизации, и чем точнее система метеорной синхронизации, тем выше скорость генерации ключевой последовательности.

Основные тактико-технические характеристики рассматриваемой системы:

Дальность связи до 1800 км. Теоретически дальность связи ограничивается плоскостью местного горизонта обоих пунктов связи, но на практике ограничения связаны с технически труднореализуемой задачей обеспечения необходимой высоты подвеса антенн. Известны эксперименты на метеорных радиолиниях до 1800 км.

Частотный диапазон. Метеорная связь, как правило, реализуется на частотах 40 -70 МГц. С ростом частоты производительность системы метеорной криптографии будет уменьшаться.

Точность синхронизации, которая была обеспечена в натурных экспериментах, лучше 1 наносекунды.

Скорость генерации ключевой последовательности (по результатам моделирования) 0,23 бит/с. Для создания ключа шифрования длиной 1024 бит потребуется 74 минуты. Иными словами, появляется возможность 19 раз в сутки непредсказуемо изменять ключ шифрования.

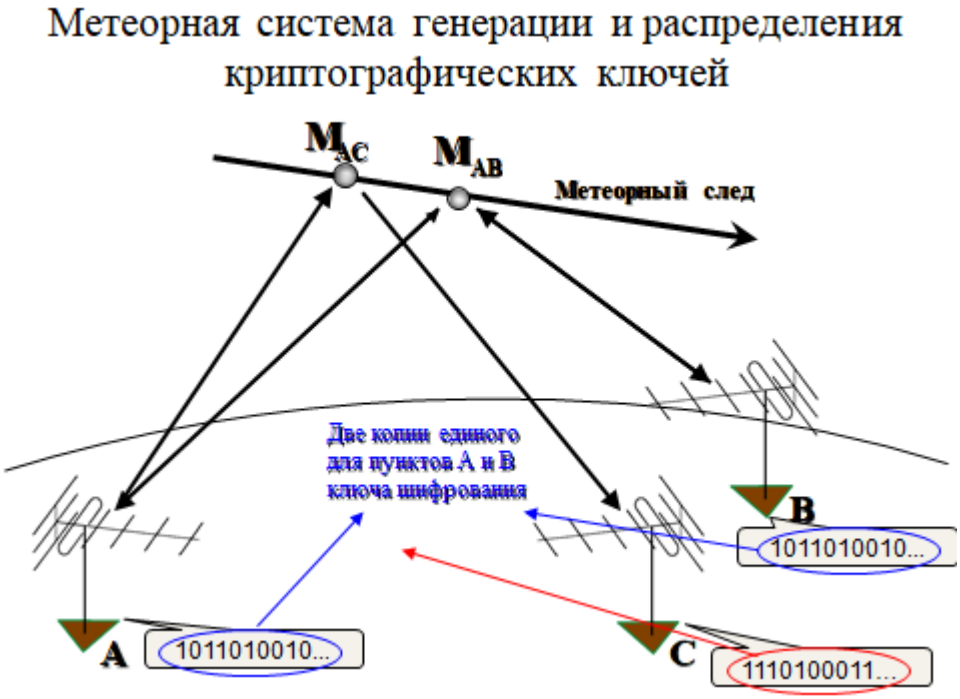

Рис. 10.1. Система метеорной криптографии.

Проведем обзор основных этапов моделирования метеорного радиоканала по Шеннону.

1. Определение системы и абстрагирование. Система метеорной криптографии является одной из практических реализаций использования уникальных свойств метеорного радиоканала для генерации ключевых последовательностей, необходимых для решения задач криптографии. Следовательно, создаваемая модель метеорного радиоканала должна быть в первую очередь ориентирована на решение задач генерации ключей, аутентификации абонентов на двух концах линии и проверки сгенерированных ключей на предмет наличия ошибок. Основные этапы функционирования модели: 1) генерация метеорных следов и отражающих точек на них, 2) измерение времени распространения τ_p от передатчика к приемнику через конкретную отражающую точку на следе, 3) формирование последовательности бит из значения τ_p; 4) проверку наличия/отсутствия ошибок при измерении τ_p; 5) формирование ключевой последовательности.

2. Подготовка данных. Выделим основные подсистемы модели метеорной криптографии:

1.Астрономическая;

2. Физика атмосферы и метеора;

3. Взаимодействие электромагнитных волн с плазмой метеорного следа (электродинамическая);

4. Радиоканал (параметры оборудования и антенных систем);

5. Элементы криптографии.

Выделим основные данные, которые будут обрабатываться моделью. Во-первых, это данные, необходимые для имитации распределения распространения метеорного вещества на небесной сфере, а также физических параметров и характеристик этих метеоров. Так как количество регистрируемых радиометеоров меняется в зависимости от времени и местонахождения пунктов связи, то для корректного моделирования астрономической компоненты необходимо знать: 1) час, день и месяц предполагаемого эксперимента; 2) географические координаты пунктов, в которых находятся абоненты. Для корректного моделирования аппаратуры приемника и передатчика необходимо знать: 1) мощность передатчика; 2) несущую частоту; 3) вид модуляции; 4) порог чувствительности приемника; 5) полосу пропускания. Для антенной системы необходимо знать: 1) поляризацию антенн на двух пунктах; 2) число вибраторов, составляющих антенны; 3) число рядов антенн; 4) число этажей антенн; 5) расстояние между рядами в антеннах; 6) расстояние между этажами в антеннах; 7) сдвиг фазы

между рядами в антеннах; 8) сдвиг фазы между этажами в антеннах; 9) поворот антенн; 10) высота подвеса антенн; 12) вид подстилающей поверхности антенн. Выходными данными или результатами имитации будут 1) количество бит ключа; 2) ключ шифрования.

3. Трансляция модели.

Первоначально составляется блок-схема с кратким описанием переменных и функций будущей модели метеорной криптографии. На основе этой схемы формируются подпрограммы для работы с указанными выше подсистемами и их взаимосвязи. Трансляция осуществляется при помощи объектно-ориентированного языка программирования С++. Результатом является компьютерная программа для моделирования генерации ключей шифрования через метеорный радиоканал.

4. Оценка адекватности модели. Оценка адекватности модели метеорной криптографии осуществляется получением значения хэш-функции младших разрядов битовой ключевой последовательности, полученной на каждом метеоре. Если для большинства метеоров значение хэш-функции для битового значения t_p от первого абонента к второму равно битовому значению t_p, полученному при распространении радиоволн от второго абонента к первому, то модель можно считать корректной, т.к. выполняются условия взаимности и стабильности метеорного радиоканала.

После создания и проверки корректности результатов моделирования можно приступать к планированию имитационных экспериментов.

5. Стратегическое планирование. На этом этапе определяется план эксперимента. В него входят: 1) определение радиотрассы, на которой планируется защищенная связь; 2) определение времени и даты предполагаемого сеанса связи; 3) определение характеристик используемой аппаратуры и антенной системы. На этом этапе необходимо четко представлять, где, когда и как будет проводиться генерация ключей по метеорному радиоканалу.

6. Тактическое планирование. На этапе тактического планирования определяются условия для надежности результатов моделирования и дальнейшего применения их в практике. Для модели криптографической системы это насущный вопрос, так как он тесно связан с вопросом криптоанализа способа генерации ключей. Для применения модели необходимо знать возможный радиус перехвата ключа, а также влияние фазовых ошибок и помех на полученную ключевую последовательность для получения оптимального порога, при котором генерация будет наиболее эффективной.

7. Экспериментирование. Прогон модели на различных радиотрассах и с различной используемой приемной и передающей аппаратурой с целью проверки и выявления зависимостей количества бит ключевой последовательности от времени, места и используемых аппаратных средств.

8. Интерпретация полученных результатов. Проверка качества ключа при помощи различных тестов (например, тестов NIST) и оценка помехозащищенности и защищенности системы от воздействия криптоаналитика.

9. Реализация (практическое использование модели и результатов моделирования).

10. Документирование. Создание руководств пользователя и программиста для криптографической модели.

11. Оптимизация отдельных элементов и всей модели в целом. Изменение модели для более детального исследования каких-либо частных случаев генерации ключей на основе свойств метеорного радиоканала.

ЗАДАНИЯ

Целью практических заданий является создание программного комплекса, с помощью которого можно реализовать и протестировать компьютерную имитационную модель. Программный комплекс должен быть выполнен по модульному принципу, определенных требований к языку программирования нет.

Задания:

1. Генераторы псевдослучайных чисел (раздел 6).

1.1. Написать программу генератора, построенного по методу серединных квадратов.

1.1.1. Написать программу, определяющую период (в данном случае число членов последовательности до момента вырождения).

1.1.2. Среди начальных чисел, лежащих в интервале (1, 9999), определить числа, обеспечивающие максимальный период.

1.1.3. Построить распределение длины периода генератора.

1.2. Написать программу генератора, построенного по методу вычетов.

1.2.1. Написать программу определения периода псевдослучайной последовательности.

1.2.2. На конкретных примерах проанализировать влияния соотношений между параметрами генератора (теорема 1, стр.48) на длину периода.

1.3. Написать программу генератора, основанного на использовании алгебраических свойств М-последовательностей.

1.3.1. Написать программу определения периода псевдослучайной последовательности.

1.3.2. На конкретных примерах проанализировать влияния параметров характеристического полинома генератора на длину периода.

2. Эмпирические тесты

Написать программы соответствующих генераторов и протестировать генераторы псевдослучайных чисел: а) генератор по методу вычетов; б) генератор на основе М-последовательности; в) генератр Random.

2.1. Частотный тест

2.2. Сериальный тест.

2.3. Покер тест.

2.4. Проверка на монотонность.

2.5. Корреляционный тест.

2.6. Интервальный тест.

3. Моделирование случайных величин с заданным законом распределения.

3.1. Написать программы для моделирования соответствующих распределений:

а) Экспоненциальное распределение $f(x)=\lambda \exp(-\lambda x)$.

б) Распределение Парето $f(x)\sim x^{-c-1}$.

В) Распределение Вейбулла $f(x)=\left(\frac{cx^{c-1}}{b^c}\right)\exp\left[-\left(\frac{x}{b}\right)^c\right]$

3.2. Организовать вывод на экран результатов моделирования и график теоретического распределения.

3.3. Протестировать результаты моделирования с использованием:

3.3.1. Частотного теста.

3.3.2. Корреляционного теста.

3.3.3. Интервального теста.

4. Моделирование нормальной случайной величины.

4.1. Написать программы для моделирования нормального распределения:

а) По методу, основанному на центральной предельной теоремы теории вероятности.

б) По методу Зелинского.

В) По методу Брокса-Маллера.

4.2. Организовать вывод на экран результатов моделирования и график теоретического распределения.

4.3. Протестировать результаты моделирования с использованием:

4.3.1. Частотного теста

4.3.2. Корреляционного теста.

4.3.3. Интервального теста.

ЛИТЕРАТУРА

1 Клейнен Д. Статистические методы в имитационном моделировании, вып. 1: Перевод с англ.- М.: Статистика,1978.- 222с.

2. Шеннон Р. Имитационное моделирование систем - искусство и наука: Перевод с англ.- М.: Мир, 1978. - 418с.
3. Бахвалов Л.А. Компьютерное моделирование: долгий путь к сияющим вершинам? // Компьютерра.- 1997.- №40(217).- С.26-36.
4. Кнут Д. Искусство программирования для ЭВМ. Т.2, получисленные алгоритмы. М. Мир. 1977. 723с.
5. Быков В.В. Цифровое моделирование в статистической радиотехнике. М. Сов.радио, 1971.- 326 с.
6. Лоскутов А. Ю., Михайлов А. С. Основы теории сложных систем. М.-Ижевск: НИЦ "Регулярная и стохастическая динамика", 2007. - 620 с.
7. Сирота А.А. Компьютерное моделирование и оценка эффективности сложных систем. М. Техносфера, 2006. – 280с.
8. Карпов А.В. Современные программные средства структурно-функционального и схемотехнического моделирования. Учебно-методическое пособие для магистрантов и студентов старших курсов. А.В. Карпов, С.А. Калабанов, Р.И. Шагиев / http://radiosys.ksu.ru/?p=478 / 2013. - 36С.
9. Карпов А.В. Современные программные средства проектирования и моделирования печатных плат радиотехнических систем и СВЧ-устройств. Учебно-методическое пособие для магистрантов и сту-дентов старших курсов. А.В. Карпов, С.А. Калабанов, Р.И. Шпгиев / http://radiosys.ksu.ru/?p=514/ 2014. – 30 С.