3. Концепция информационной безопасности Сетей связи общего пользования Взаимоувязанной сети связи РФ/М.: 2002г.

4. Е.Е. Исаков. Устойчивость военной связи в условиях информационного противоборства / Исаков Е.Е. – Спб.: Изд-во Политехн. ун-та, 2009. – 400с.

5. Рек. МСЭ-Т серии Е.400, М.3000, Х.700, Х.800 Х.1000,Y.2000.

6. ГОСТ Р 53111-2008 Устойчивость функционирования сети связи общего пользования. Требования и методы проверки.

7. ГОСТ Р 53109-2008 Система обеспечения информационной безопасности сети связи общего пользования. Паспорт организации связи по информационной безопасности.

8. ГОСТ Р 52448-2005 Обеспечение безопасности сетей электросвязи.

Карпов М.А., Худайназаров Ю.К.

Военная академия связи имени С.М.Будённого

АНАЛИЗ СРЕДСТВ МОДЕЛИРОВАНИЯ ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

При исследовании процессов управления информационной безопасностью в современных информационных системах требуется обоснованный выбор методов и средств моделирования.

Моделирование представляет собой мощный метод научного познания, при использовании которого исследуемый объект заменяется более простым объектом, называемым моделью. Основными разновидностями процесса моделирования можно считать два его вида - математическое и физическое моделирование. При физическом (натурном) моделировании исследуемая система заменяется соответствующей ей другой материальной системой, которая воспроизводит свойства изучаемой системы с сохранением их физической природы. Примером

этого вида моделирования может служить «пилотная» сеть, с помощью которой изучается принципиальная возможность построения сети на основе тех или иных компьютеров, коммуникационных устройств, операционных систем и приложений.

Возможности физического моделирования довольно ограничены. Оно позволяет решать отдельные задачи при задании небольшого количества сочетаний исследуемых параметров системы. Поэтому, при оптимизации сетей, во многих случаях, предпочтительным оказывается использование математического моделирования. Математическая модель представляет собой совокупность соотношений (формул, уравнений, неравенств, логических условий), определяющих процесс изменения состояния системы в зависимости от ее параметров, входных сигналов, начальных условий и времени [1].

Современные информационные системы представляют собой сложный объект, в котором происходят многочисленные процессы различной сложности. Построение адекватной модели в данном случае с помощью какого-либо одного метода практически невозможно известными средствами моделирования. Для моделирования такого объекта необходимо комплексное использование различных методов.

При моделировании сложные информационные системы разбиваются на составные части, каждая из которых рассматривается отдельно от других. Каждая составная часть является представителем некоторого класса однотипных объектов. В связи с этим, для каждого из уровней архитектуры управления информационной системы необходимо выбрать наиболее оптимальное средство с учетом цели исследования.

Так для моделирования стратегического уровня управления, где преобладают организационные процессы возможно использование методов и средств структурно-логического моделирования, а также математические модели.

Для воспроизведения процессов тактического уровня возможно использование специализированных средств структурно-логического, функционального (IDEF) моделирования и компьютерного имитационного моделирования.

Для процессов операционного уровня возможно использование всего разнообразия указанных выше средств моделирования, включая физическое воспроизведение предполагаемых условий (среды) функционирования, процессов и объектов.

Среди современных средств структурно-логического и функционального моделирования наиболее широко известны и применяемы следующие: ERwin LinkObject API, ERwin Examiner, ModelMart, Paradigm Plus, Rational Rose.

ModelMart – это первая многопользовательская среда моделирования, которая обеспечивает координацию крупномасштабного моделирования. ModelMart позволяет координировать действия руководителя проекта, проектировщиков на ERwin и BPwin и администраторов путем предоставления сервисов, включая разрешение конфликтов, контроль версий, безопасность и стандартизацию.

Paradigm Plus – CASE-средство для проектирования, визуализации информационных систем.

Rational Rose – средство визуального моделирования объектно-ориентированных информационных систем компании Rational Software Corp. Благодаря уникальному языку программирования UML (Universal Modeling Language), Rose применима для решения практически любых задач в проектировании информационных систем: от анализа бизнес-процессов до кодогенерации на определенном языке программирования. Rose позволяет разрабатывать как высокоуровневые, так и низкоуровневые модели, осуществляя тем самым либо абстрактное проектирование, либо логическое.

Особым классом математических моделей являются имитационные модели. Такие модели представляют собой компьютерную программу, которая шаг за шагом воспроизводит события, происходящие в реальной системе. Применительно к вычислительным сетям их имитационные модели воспроизводят процессы генерации сообщений приложениями, разбиение сообщений на пакеты и кадры определенных протоколов, задержки, связанные с обработкой сообщений, пакетов и кадров внутри операционной системы, процесс получения доступа компьютером к разделяемой сетевой среде, процесс обработки поступающих пакетов маршрутизатором и т.д. При имитационном моделировании сети не требуется приобретать дорогостоящее оборудование, так как его работа имитируется программами, достаточно точно воспроизводящими все основные особенности и параметры такого оборудования.

Преимуществом имитационных моделей является возможность подмены процесса смены событий в исследуемой системе в реальном масштабе времени на ускоренный процесс смены событий в темпе работы программы. В результате за несколько минут можно воспроизвести работу сети в течение нескольких дней, что дает возможность прогноза поведения сети в широком диапазоне варьируемых параметров [2].

Результатом работы имитационной модели являются собранные в ходе наблюдения за протекающими событиями статистические данные о наиболее важных характеристиках сети: времени реакции, коэффициентах использования каналов и узлов, вероятности потерь пакетов и т.п.

Существуют специальные языки имитационного моделирования, которые облегчают процесс создания программной модели по сравнению с использованием универсальных языков программирования. Примерами языков имитационного моделирования могут служить SIMULA, GPSS, SIMDIS.

Существуют также системы имитационного моделирования, которые ориентируются на узкий класс изучаемых систем и позволяют строить модели без программирования.

Arena – разработанное компанией Systems Modeling Corporation программное обеспечение для имитационного моделирования позволяет создавать подвижные компьютерные модели [3].

Пакет Opnet Modeler версии 14.5 также является одним из средств, которое предлагает пользователям графическую среду для создания, выполнения и анализа событийного моделирования сетей связи. Данный пакет позволяет анализировать воздействия приложений типа клиент-сервер и новых технологий на работу сети; моделировать иерархические сети, многопротокольные локальные и глобальные сети с учетом алгоритмов маршрутизации; осуществлять оценку и анализ производительности сетей. Также с помощью пакета можно осуществить проверку протокола связи, анализ взаимодействий протокола, оптимизацию и планирование сети, проверку правильности аналитических моделей [4]. Далее рассмотрим некоторые возможности Opnet Modeler, интересные в плане моделирования процессов управления информационной безопасностью.

На начальном этапе моделирования возможен выбор масштаба моделируемой сети: от небольшого офиса до всемирной сети, имеется возможность располагать объекты с привязкой к местности, чтобы ещё точнее учитывать её особенности. При построении сети необходимо учитывать услуги, которые реализуются на базе данной сети.

Каждый из типов трафика предъявляет свои требования к показателям качества обслуживания. Для обеспечения необходимого QoS для всех услуг выбрана следующая трехуровневая топология построения сетей класса Metro: уровень ядра, уровень агрегации (уровень распределения), уровень доступа.

На уровне доступа осуществляется концентрация абонентских линий, организуется разделение абонентов с использованием виртуальных сетей, обеспечивается ограничение скорости передачи данных на входе в сеть и реализуются базовые функции безопасности.

На уровне распределения моделируются виртуальные сети доступа с использованием протокола IP, что позволяет имитировать обмен трафиком между различными узлами уровня распределения. Домен распределения предоставляет доступ к оборудованию сервисов, осуществляет функции обеспечения безопасности и управления качеством обслуживания на сети [5]. Возможность моделирования совокупности узлов уровня распределения, объединенных в единую физическую структуру (домен распределения), позволяет планировать и исследовать процессы обеспечения информационной безопасности на сетевом уровне.

Система OpNet позволяет использовать в работе дискретное, гибридное и аналитическое моделирование. Тип моделирования можно выбрать в пункте меню Simulation Kernel. Логику поведения процессора и модулей очередности определяет модель процесса, которую пользователь может создавать и изменять в пределах редактора процесса. В редакторе процесса пользователь может определить модель процесса через комбинацию алгоритма работы конечного автомата (finite-state machine – FSM) и операторов языка программирования C/C++. Вызов события модели процесса в течение моделирования управляется возбуждением прерывания, а каждое прерывание соответствует событию, которое должно быть обработано моделью процесса.

Несколько основных моделей процесса входят в базовую комплектацию пакета, моделируя популярные протоколы работы с сетями, протокол шлюза границы (border gateway protocol – BGP), протокола контроля передачи, интернет протокол (TCP/IP), ретрансляции кадров (frame relay), Ethernet, асинхронного режима передачи (asynchronous

transfer mode – ATM), и WFQ (weighted fair queuing). Базовые модели полезны для быстрого развития сложных имитационных моделей для общих архитектур сети, а также для изучения точного функционального описания протокола.

После построения модели сети её необходимо верифицировать, т.е. проверить топологию сети. Если сеть построена неправильно, OpNet обозначит некорректные соединения, которые необходимо исправить.

Необходимо отметить, что предлагаемая в комплекте база моделей оборудования актуальна на 2008 год, поэтому для моделирования новых объектов или условий необходимо использовать комбинированные шаблоны, добавляя имеющемуся оборудованию новые свойства.

После того как настройка оборудования завершена, необходимо указать тип собираемой статистики. Для этого на исследуемом оборудовании или соединительной линии нажать правой кнопкой мыши и выбрать графу Choose Individual Statistics. Далее для каждого сетевого элемента предлагаются на выбор варианты сбора данных и формирования результатов моделирования.

В настоящее время во многих организациях существует два реальных центра управления: администратор сети и администратор безопасности. Естественно, что такая ситуация приводит к рассогласованности действий. Для крупномасштабной распределенной информационной системы данный факт становится особенно важным. Системы, к которым предъявлены высокие требования готовности актуальным является вопрос об управлении безопасностью с минимальным нарушением нормального процесса работы системы. А для этого необходим продукт, позволяющий собирать статистические данные о системном трафике за определенный период времени (направленность, приложение, протокол, распределение во времени и т.д.), а затем производить их анализ на модели. Система OpNet позволяет выполнить гибкий многовариантный анализ и предвидеть

проблемы до их реального возникновения. Это является исключительно важным достоинством моделирования, существенно повышающим надежность и безопасность информационной системы с минимальными расходами на эксперименты.

Таким образом, система OpNet может использоваться для исследования процессов информационной безопасности на технологическом уровне управления, в частности для моделирования мониторинга состояния безопасности системы [6], обмена безопасности, т.е. информационного обмена, который осуществляется в рамках обеспечения безопасности системы.

Литература:

1.Моделирование сетей ЭВМ: М.М. Бутаев, Н.Н. Конов – Пенза: Изд-во Пенз. гос. ун-та, 2007.

2.Введение в исследование операций: Хемди А. Таха – М.: «Вильямс», 2007

3.Чувиков С.В. Метрология и сертификация программного обеспечения: Учеб. пособие /РГЭУ. – Ростов н/Д., 2004. –с.88

4.Учимся моделировать: Т. Стернс – www.osp.ru

5.Моделирование и анализ корпоративных информационных систем: М. Васильев, И. Хомков, С. Кравченко, С. Шаповаленко – www.pcweek.ru

6.Рекомендации МСЭ-Т X.802, X.803.