От авторов

В книге рассмотрены методологические вопросы анализа живучести сетей связи в условиях разрушающих информационных воздействий (РИВ). Дана подробная классификация информационных атак в информационных сетях (ИС) и описаны методы их обнаружения. Большое внимание уделено показателям структурной надежности систем связи, а также ее математическому и компьютерному моделированию.

Учитывая современные тенденции развития телекоммуникационных технологий, в книге также уделено внимание вопросам, связанным с живучестью и надёжностью мобильных систем связи, предложены модели структурной надежности в мобильных сетях передачи данных, а также модель передачи данных абонентами мобильной сети. Рассмотрены алгоритмы обнаружения ошибок в комбинациях группового кодирования, оценки качества приема составных сигналов, определения ненадежности результатов декодирования и определения нумератора весов для циклических кодов.

Приведён обзор систем мониторинга цифровых сетей связи и методов обнаружения РИВ, применяемых с целью защиты информации в реальных ИС. Рассмотрены графические и инструментальные средства поддержки системы моделирования.

В последней главе рассмотрены модели и методы повышения структурной живучести сетей, а так же задачи оптимизации живучести информационных сетей в условиях РИВ. Исследованы стохастические модели сетей с целью определения вероятности и математического ожидания связности структуры транспортных сетей связи. Заканчивается глава описанием модели сети оповещения и экстренных сообщений. В математических моделях и алгоритмах впервые была применена теория S-гиперсетей, которая развивается усилиями авторов этой книги.

Материал книги в основном состоит из результатов, полученных авторами данной монографии, а также сотрудниками секции «Информационные системы» Ученого совета Института вычислительной математики и математической геофизики СО РАН.

Книга рекомендована специалистам в области информационной безопасности, живучести коммуникационных сетей, а также студентам технических вузов, обучающимся по направлениям «Компьютерные сети» и «Сети электросвязи».

Авторы благодарят Генерального директора Национальной строительной корпорации ЭНТЭР Делова Леонида Евгеньевича за помощь в создании книги.

1 Методологические вопросы анализа живучести сетей в условиях разрушающих информационных воздействий

1.1. Проблематика живучести в телекоммуникационных сетях

Концептуальная модель информационной сети

Объектами исследования являются информационные сети, построенные на основе современных информационно-коммуникационных технологий, и происходящие в них процессы преобразования информации, связанные с её сохранением и передачей от источника до получателя.

Информационная сеть есть совокупность информационных средств, предназначенных для реализации следующих операций над информацией: получение, сбор, передача, обработка, хранение, поиск, предоставление, использование и др. [1].

Макроструктура информационной сети представлена на рис. 1.1 и включает три основных компонента: терминальный комплекс, сеть электросвязи, информационную и вычислительную базы.

Все компоненты сети представляют собой совокупность технических и программных средств.

Терминальный комплекс содержит все виды пользовательских устройств, начиная от обычного телефонного аппарата и включая все виды современных абонентских устройств: черно-белый и цветной видеотелефоны, факсимильный аппарат, персональную ЭВМ,

Рис. 1.1. Макроструктура информационной сети

Рис. 1.2. Оконечный узел связи

локальную вычислительную сеть, сигнально-контрольное и специальное оборудование.

Сеть электросвязи по известному определению есть совокупность каналов и трактов, образующих первичную сеть, и построенные на её основе вторичные сети, предназначенные для удовлетворения потребностей пользователей по доставке любой информации, преобразованной в сигналы электросвязи [2].

Первичная сеть предназначена для образования каналов и трактов между узлами (пунктами) связи, используемыми вторичной сетью. В общем случае она состоит из линий связи различной физической природы, систем передачи и системы управления [3].

В качестве линейных средств в первичной сети применяются кабельные, в том числе волоконно-оптические кабели (ВОЛС), радиорелейные, тропосферные и спутниковые системы передачи, а также средства прямой радиосвязи различных диапазонов волн.

Вторичная сеть предназначена для непосредственного обеспечения передачи или обмена сообщениями заданного вида между абонентами и предоставления различных услуг связи пользователям.

Вторичная сеть состоит из каналов первичной сети, используемых данной сетью, аппаратуры преобразования, обработки и ввода в канал связи сообщений данного вида информации, устройств коммутации сообщений или каналов, а также системы управления [3].

Важным элементом структуры вторичных сетей являются оконечные узлы связи (рис. 1.2). Оконечный узел предоставляет абоненту все виды услуг обеспечиваемых данной вторичной сетью.

Основными структурными элементами оконечного узла могут быть пункт или станция каналообразования (кросс-каналы, системы передачи), пункт управления, оборудование коммутации и маршру-

тизации, радиоцентры, оборудование абонентского доступа и абонентская сеть, системы электропитания и др.

Информационная и вычислительная базы представляют собой распределённые по территории системы банков данных и систему компьютеров большой производительности, обеспечивающих вычислительную поддержку терминальных комплексов.

Сеть электросвязи предназначена для доставки любой информации между терминальными комплексами и банками данных в заданном сочетании [3]. Под термином «доставка» понимается передача информации по каналам связи, коммутация, хранение информации на узлах коммутации в процессе её передачи и коммутации, а также хранение как самостоятельная функция с различной длительностью, в том числе оперативное, длительное и архивное хранение.

Для облегчения разработки методов оценки живучести множество сетей связи условно разбиваются на два класса — двухполюсные и многополюсные. При наличии в системе связи только двух оконечных узлов — система двухполюсная, если количество узлов более двух — многополюсная [3]. Понятие двухполюсной сети целесообразно использовать в случае необходимости оценки живучести связи на том или ином информационном направлении, т. е. между определённой парой полюсов многополюсной системы связи.

Таким образом, система доставки информации включает в себя множество связанных между собой элементов, отказ или повреждение каждого из которых оказывает влияние различной степени на работоспособность системы в целом.

Понятия надёжности и живучести, их различия

Оба понятия связаны с работоспособностью системы связи во времени, т. е. с выполнением заданных функций в установленном объёме на требуемом уровне качества в течение определённого периода эксплуатации или в произвольный момент. Различия этих понятий обусловлены прежде всего различиями причин или факторов, нарушающих нормальное функционирование системы, и характером нарушений.

Надёжность системы связи обусловлена её свойством обеспечивать связь, сохраняя во времени значения установленных показателей качества в заданных условиях эксплуатации. Она отражает влияние на работоспособность системы главным образом внутрисистемных факторов — случайных отказов техники, вызываемых физико-химическими процессами старения аппаратуры, дефектами технологии её изготовления или ошибками обслуживающего персонала.

Живучесть [4] характеризует устойчивость системы связи против действия причин, лежащих вне системы и приводящих к разрушениям, значительным повреждениям или временной потере работоспособности всей сети или некоторой части её элементов — узлов, пунктов, станций и линий связи. Все причины можно разделить на два класса: случайные (или стихийные) и преднамеренные. К стихийным (случайным) факторам относятся такие, как гроза, землетрясение, оползни, разливы рек, ошибки персонала, пользователей и т. п., а к преднамеренным — огневые (в том числе и ракетно-ядерные) удары противника в условиях войны, использование высокоточных видов вооружений, диверсионных и информационных разрушающих воздействий.

Различия в причинах нарушения связи обусловливают существенные отличия в их проявлении, характере и масштабности нарушений связи, их продолжительности, путях и способах их устранения и повышения устойчивости системы. Если поток случайных отказов техники приводит к нарушению лишь отдельных связей и обладает свойством ординарности (вероятность одновременного отказа нескольких связей мала), то нарушения работы системы указанными выше факторами живучести обладают существенно иными свойствами. Особенно это характерно для преднамеренного поражения системы, когда одновременно может выводиться из строя значительная часть или даже вся система связи. Интервалы между воздействиями факторов живучести на систему связи не подчиняются экспоненциальному закону, что характерно для случайных отказов аппаратуры, а преднамеренные воздействия противника, кроме того, не являются случайными. Нарушения работы отдельных связей из-за случайных отказов или ошибок обслуживающего персонала обычно кратковременны, так как они в большинстве случаев быстро устраняются, что же касается нарушений связи из-за разрушения отдельных её элементов — узлов, линий, то они несравненно более продолжительны. Если первые исчисляются обычно минутами или десятками минут, то вторые часами и сутками, поскольку это связано с большим объёмом восстановительных работ.

В силу небольших перерывов связи из-за случайных отказов многие связи могут обходиться без резервирования. С учётом же аспекта живучести без резерва не обойтись, так как обслуживаемые процессы управления, как правило, не допускают столь длительного отсутствия связи.

Случайные отказы характерны для отдельных устройств, линий или каналов связи. При этом отказ одного аппарата на узле связи обычно не вызывает отказов других комплектов аппаратуры, а тем

более целого элемента или всего узла связи. Исключение составляют общие коммутаторы и агрегаты электропитания. Поэтому при расчёте надёжности системы или сети связи отказы её структурных элементов, не имеющих общих устройств, считаются взаимонезависимыми.

Поражающие факторы могут выводить из строя одновременно несколько элементов узла и даже системы. Так, если воздействию подвергается узел связи, то могут оставаться непораженными лишь его вынесенные пункты и станции. Поскольку аппаратура систем передачи обычно размещается в составе ядра узла связи, при поражении узла с большой вероятностью выходят из строя подходящие к нему кабельные линии связи. Соответственно, могут быть нарушены все связи, осуществляемые данным узлом. В период массированного ядерного удара противника взаимная зависимость событий-поражений распространяется на все элементы системы. Естественно, что эти особенности нельзя не учитывать при расчёте живучести систем и сетей связи.

Следует иметь в виду и неодинаковую степень погрешности исходных данных для оценки надёжности и живучести систем. По эксплуатационно-техническим отказам техники и линий связи имеется обширный статистический материал. И хотя достоверность исходных данных по надёжности техники связи представляет пока что известную проблему, достигнутая их точность несравненно выше точности исходных данных для анализа живучести системы связи. К примеру, не существует пока еще достаточных научных основ прогнозирования землетрясений. Естественно не может быть сколько-нибудь необходимой для расчётов живучести вероятности того, что в течение определённого периода в интересующем районе землетрясения не будет, нельзя достоверно описать его параметры. Весьма проблематично также и прогнозирование поражающего воздействия противника.

Из этого факта следует, что в настоящее время и в обозримом будущем оценка живучести сети (системы) связи может быть лишь грубо приближённой, ориентировочной. Поэтому и методы её расчёта могут быть приближенными, лишь бы вносимая ими погрешность не превышала неточности исходных данных.

Методика расчёта показателей надёжности, к которым обычно предъявляются высокие требования по точности, в некоторых случаях могут использоваться для расчёта оценки живучести системы связи, однако для сокращения трудоёмкости расчётов, исходя из изложенного выше, они могут быть существенно упрощены. Если же для анализа и синтеза живучести системы связи разрабатываются

специальные методы, то излишнее их усложнение во имя повышения точности было бы неоправданно.

Неодинаковы также и критерии отказов связи между полюсами системы. Если при оценке надёжности связь между парой полюсов может считаться отказавшей при наличии $k < n$ заданных связей ($n = 1, 2, \ldots$), то при оценке живучести критерием отказа связи между двумя полюсами обычно является полное отсутствие связи любого вида.

Таким образом, надёжность и живучесть — различные понятия и самостоятельные проблемы, требующие своих решений при разработке и совершенствовании систем и сетей связи.

Понятия устойчивости и живучести

Под устойчивостью будем понимать свойство системы связи, заключающееся в ее способности осуществлять своевременную передачу информации в необходимом объеме и с качеством не хуже заданного при определенных условиях. Живучесть — устойчивость системы связи к повреждению (полному или частичному) элементов стихийными факторами и преднамеренными воздействиями противника [4].

Живучесть сети связи включает в себя два основных свойства, каждое из которых разбивается на два частичных (рис. 1.3).

Структурная живучесть — живучесть (выживаемость) системы связи в течение некоторого времени при пассивном противодействии повреждениям (случайным или целенаправленным) элементов сети.

Пассивное противодействие осуществляется при нормальном режиме работы системы связи за счёт защищённости элементов, вклю-

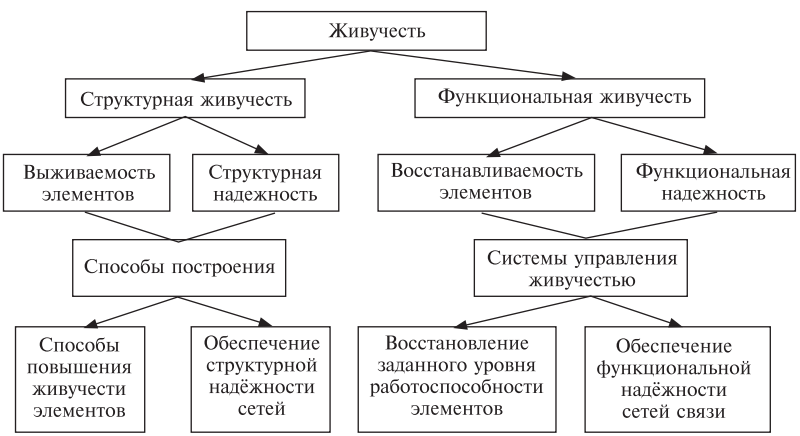

Рис. 1.3. Основные свойства живучести систем связи

ченного резерва, структурной организации и принятого алгоритма управления маршрутизацией. Таким образом, данное понятие включает живучесть как элементов, так и сети связи в целом.

Выживаемость элементов — структурная живучесть элементов системы связи.

Структурная надёжность — структурная живучесть системы связи при заданном алгоритме (процессе) разрушения элементов.

Функциональная живучесть — живучесть (выживаемость) системы связи в течение некоторого времени при активном противодействии повреждениям (случайным или целенаправленным) элементов сети.

Активное противодействие в основном осуществляется во время действия разрушающих факторов и определяется системами восстановления элементов и управления на сетях связи.

Таким образом, при исследовании функциональной живучести сеть моделируется динамическими объектами.

Восстанавливаемость элементов — функциональная живучесть элементов системы связи.

Функциональная надёжность — функциональная живучесть системы связи при заданном алгоритме (процессе) разрушения элементов сети.

Критерии живучести

Работоспособность сети (элемента) — сеть (элемент) работоспособна, если она способна выполнять все или заданную часть функций в полном или частичном объёме.

Критерий выживаемости элемента — время, при котором элемент остаётся работоспособным с начала его разрушения заданными способами и средствами или количественная мера определённых средств разрушения, не нарушающих работоспособность элемента.

Критерий восстанавливаемости элементов — время, за которое может быть восстановлена работоспособность элемента при заданном уровне резервирования и системы техобслуживания, или количественная мера определённых ресурсов, восстанавливающих работоспособность элементов при заданной степени разрушения.

К ресурсам восстановления можно отнести:

- резервы элементов сети в целом, отдельных блоков аппаратуры связи для ремонта элементов;
- количество людей, работающих над восстановлением;
- наличие предприятий, изготовляющих новые элементы, и т. д.

В качестве показателей живучести элементов можно принять:

- вероятность отказа или количество ресурса разрушения;

- среднее время восстановления или количество ресурса восстановления.

Критерий структурной надёжности — число отказавших элементов, не нарушающих работоспособность сети связи, при условии, что заданная часть абонентов сети из выделенных пунктов связи (или всех) будет соединена связующей системой (коммуникацией) при отказе любых k элементов сети связи.

Под коммуникацией будем понимать некоторую двухполюсную сеть с необходимыми ограничениями (расстояние между полюсами, связность, пропускная способность). Поэтому необходимо определить множество работоспособных коммуникаций и типы отказов элементов. Например, пункты x и y сети связи соединены коммуникацией тогда и только тогда, когда между x и y существует не менее T независимых цепей, длина которых превосходит d, а суммарная пропускная способность не меньше заданной величины.

Критерий функциональной надёжности — время активного сохранения работоспособности сети связи при заданной интенсивности отказов её элементов.

Под активным сохранением понимается возможность противостоять разрушениям с помощью системы управления живучестью сети связи, в частности, за счёт восстановления структуры и функций первичной и вторичной сетей, систем управления потоками, нагрузкой и маршрутизацией. При этом для определения функциональной надёжности необходимо определить процесс отказов элементов сети.

В том случае, когда процесс отказов детерминирован, критерий функциональной надёжности можно видоизменить следующим образом: это число восстановленных коммуникаций между выделенными абонентами сети в определённый отрезок времени и при фиксированном процессе отказов. Легко понять, что эти два критерия эквивалентны, так как для любой сети из одного критерия следует второй.

Показатели живучести — количественная характеристика одного или нескольких свойств, составляющих живучесть систем связи и её элементов.

Из этого определения непосредственно следуют несколько признаков, по которым можно классифицировать показатели живучести как показатели живучести элементов или системы связи в целом:

- единичный (комплексный) показатель живучести относится к одному (нескольким) из свойств, составляющих живучесть системы связи;

- однозначный (многозначный) показатель живучести выражается одним числом (вектором или функцией);
- непосредственный показатель живучести соответствует выбранному критерию живучести, а опосредованный показатель функционально связан с непосредственным показателем и оценивает последний сверху или снизу;
- детерминированный (стохастический) показатель живучести характеризует свойства живучести в детерминированных (стохастических) сетях связи; детерминированные показатели живучести можно разбить на прямые и обратные;
- стохастические показатели живучести также разбиваются на два подтипа: вероятностные — характеризуют вероятность появления некоторого события; числовые — математическое ожидание некоторой случайной величины (время, число элементов, коммуникаций и т. д.).

Так как в любом критерии живучести рассматриваются два фактора, то, зафиксировав один, по другому проводят оптимизацию.

Очевидно, что число показателей резко возрастет, если учесть разнообразие сетей связи, типы отказов и структуру абонентов связи, т. е. система показателей определяется еще и классификацией теоретических моделей сетей связи.

Показатели функциональной надёжности системы связи

Для детерминированных сетей связи, прежде всего, интересны показатели, характеризующие возможности систем управления по поддержанию работоспособности сети в заданных пределах на определённый отрезок времени. Здесь возможны два подхода к формированию показателей.

Первый подход заключается в оценке возможности системы управления восстановить максимальное число необходимых связей с заданной пропускной способностью за счёт фиксированных средств обеспечения функциональной надёжности сети. Таким образом, при этом подходе фиксируется разрушение и ресурс восстановления (необходимость восстановить определённые связи в течение некоторого времени), например число восстановленных связей за счёт управления структурой вторичной сети при заданных резервах и характере разрушения элементов сети, оценка возможности системы управления оптимально перестраивать структуру вторичной сети с целью повышения работоспособности.

Второй подход заключается в оценке возможности системы управления восстановить работоспособность на необходимом уровне за счёт минимально возможного резерва.

Из-за сложности определения оптимального разрушения сети для заданного обеспечения живучести более широкое распространение получили стохастические показатели:

- вероятность того, что сеть будет в работоспособном состоянии в случае воздействия на нее поражающих факторов, а также прогнозируемая длительность восстановления связи;
- среднее значение вероятности выживания связи между одной парой узлов;
- математическое ожидание времени восстановления работоспособности;
- математическое ожидание времени перестройки вторичной сети;
- математическое ожидание времени передачи сообщения при воздействии разрушающих факторов.

Необходимо также рассматривать показатели, связанные непосредственно с сообщениями, передаваемыми по сети. В качестве таких показателей можно рассмотреть следующие:

- $\gamma_{\text{п}} = 1 - M/N$ — коэффициент потерь сообщений, где N — число всех сообщений, а M — число полученных сообщений;
- вероятность прихода исходного сообщения в заданный интервал времени;
- вероятность того, что сообщение не будет изменено;
- математическое ожидание времени нахождения сообщения (пакета) в сети;
- вероятность передачи и приема сообщения не по заданному адресу;
- вероятность перехвата и прочтения сообщения посторонними лицами.

Перечисленные показатели не могут быть вычислены непосредственно по модели сети, так как они существенно зависят от средств воздействия на сеть. Разумеется, структура и система управления сетью также существенно влияют на эти показатели. Поэтому данные показатели могут быть найдены только с помощью имитационных моделей.

К комплексным показателям живучести относятся:

- вероятность того, что система связи окажется в работоспособном состоянии в произвольный момент времени;
- вероятность того, что все вызовы будут реализованы в заданный период времени;
- коэффициент технического использования — отношение математического ожидания времени пребывания системы связи в рабочем состоянии за некоторый период эксплуатации к продолжительности этого периода;

- коэффициент обеспеченности вызовов — математическое ожидание отношения потерь к общему числу вызовов, поступивших за тот же период времени;
- вероятность того, что все сообщения будут доставлены своевременно;
- вероятность того, что между выделенными узлами будет обслужен поток с качеством, не хуже заданного в заданный период времени;
- вероятность сохранения заданного числа каналов между выделенными узлами сети до определённого момента времени.

Однако самыми эффективными показателями живучести являются характеристики сетей, связанные с потоками в сетях, например такие показатели:

- математическое ожидание максимального потока между узлами s и t (s-t потока);
- коэффициент обеспеченности пропускной способности — отношение математического ожидания максимального s-t потока к величине максимального s-t потока в неатакованной сети;
- вероятность того, что текущий максимальный s-t поток не меньше заданной величины;
- математическое ожидание максимального s-t потока в мобильной сети передачи данных на заданных маршрутах абонентов $A(s)$ и $A(t)$ в определенный период времени Δt.

Разумеется, этими показателями не исчерпываются интегральные потоковые показатели. Рассматриваются и другие полезные показатели, соответствующие различным критериям живучести.

Факторы внешнего и внутреннего воздействия на сети связи

Внешние воздействия разрушительного свойства различаются масштабом и характером. Характер разрушений определяется видами основных факторов. Разрушения могут иметь целенаправленный (стохастический) либо случайный (детерминированный) характер. При целенаправленном характере разрушения сети учитывается возможности максимального повреждения и разрушения элементов сети при минимальных затратах, т. е. достижение противником максимальной цели минимальными средствами.

Степень разрушительного воздействия на элементы сети связи определяет степень неработоспособности элемента и зависит от следующих факторов [5]:

- вид воздействия;
- мощность воздействия;

- масштаб воздействия;
- точность воздействия.

Виды воздействия могут быть следующими:

- ударное воздействие, в основном в результате взрыва условного боеприпаса установленной мощности;
- электромагнитное воздействие в результате взрыва специального боеприпаса;
- тепловое воздействие;
- радиационное воздействие;
- информационное разрушающее воздействие;
- воздействие природной стихии. Это может быть, например, шторм, наводнение, землетрясение и др.

Исчисление мощности воздействия:

- при ударном воздействии — в тротиловом эквиваленте;
- при электромагнитном воздействии — в напряжённости электрического поля;
- при тепловом воздействии — в градусах по шкале Кельвина;
- при радиационном воздействии — в уровне радиоактивного излучения;
- при программном воздействии мощность воздействия можно определить характером возможного подключения к системе и областью воздействия на нее и условно обозначить через масштаб возможного повреждения системы при подключении к определённой точке сети;
- при воздействии сил природной стихии мощность воздействия каждого вида можно исчислять в общепринятых единицах исчисления, т. е. в баллах, а для вычисления совокупного воздействия привести к единым условным единицам воздействия по отношению к элементам сети.

Масштаб воздействия определяется целями и задачами, которые ставит перед собой противник, а также видами и мощностью применяемых средств разрушения сети. Основной целью противника будем считать максимально возможное разрушение сети, т. е. полную или частичную потерю работоспособности такого количества элементов сети, при котором будет существенно затруднена или невозможна передача информации пользователя сети.

Масштаб событий условно можно разделить на следующие виды:

- локальный военный конфликт;
- глобальный военный конфликт;
- скрытый конфликт при отсутствии открытых военных действий.