# Классификация сетевых отказов телекоммуникационных сетей

М.С. Манукян,
аспирант кафедры АПП

Традиционная техника и модели, используемые для определения показателей надежности и отказов телекоммуникационных сетей, основаны на классических моделях отказов, таких как прогнозирование Среднего Времени Между Отказами (СВМО) и Среднего Времени Между Перерывами в Обслуживании (СВМПО). Сетевые отказы происходят по многим различным причинам и во многих различных формах. Данные классические модели только лишь предполагают, что отказы вызваны аппаратным компонентом сети. В связи с широким использованием интернет-технологий необходимо исследовать другие факторы, вызывающие отказы в коммуникационных сетях или способствующие им [1]. Были установлены и определены две дополнительные модели отказов, помимо уже существующих и исследованных моделей отказов, отказ по причине атаки системы с целью нарушения нормального обслуживания пользователей и отказ вследствие катастрофических событий.

Стандартная мера надежности оценки электронного оборудования и систем основана на анализе среднего времени в часах, необходимого для отказа электронных компонентов, называемого средним временем между отказами (СВМО). Было использовано несколько стандартов, а также множество модификаций и производных, чтобы предсказать поведение коммуникационного оборудования, находящегося в настоящий момент в производстве. Исследование показало, что чрезмерно оптимистическое прогнозирование отказов происходит в результате неправильного понимания и неправильного применения оценки СВМО.

Несмотря на неправильное понимание и неправильное употребление данных прогнозов, коммуникационная промышленность все

еще значительно сфокусирована на их использовании. Изучение технической документации у ведущих изготовителей телекоммуникационного оборудования (Cisco и Juniper Networks) показывает, что имеется обширная документация по прогнозированию отказов, основанная на стандартах СВМО и СВМПО, но мало сказано о других причинах сетевых отказов. Такой коллективный взгляд на данную проблему наблюдается во всей коммуникационной промышленности, где можно найти множество информации относительно использования прогнозирования СВМО, но при этом мало информации относительно других категорий сетевых отказов.

Нужно выделить пять категорий ошибок, которые могут привести к общему системному отказу в системах обработки данных и которые выходят за рамки прогнозирования отказов СВМО. К ним относятся:

1) ошибка оператора;
2) проблемы массовой памяти;
3) проблемы аппаратного обеспечения компьютера;
4) проблемы программного обеспечения;
5) сетевые проблемы.

Данное исследование рассматривает пять категорий, предложенных с целью определения того, являются ли необходимыми дополнительные категории или есть ли возможность описать общую модель прогнозирования отказов [1].

### Категории сетевых отказов

#### Категория 1: Проблемы аппаратного обеспечения

Поставщики коммуникационного оборудования сосредоточились на категории проблем аппаратного обеспечения, как главном предсказателе показателей сетевых отказов. Приблизительно 25% всех отказов происходят в результате проблем аппаратного обеспечения, таких как компьютерные отказы. Чтобы усилить общую надежность телекоммуникационного оборудования, поставщики предлагают большой выбор продукции. Сетевой проектировщик может выбрать и использовать оборудование с широким диапазоном выбора, начиная от отсутствия и до полного дублирования оборудования и связей. В наше время общепринято использование индивидуальных аппаратных компонентов коммуникационного оборудования, СВМО которого варьируется от 80 000 часов до нескольких сотен тысяч часов.

В процессе фактической эксплуатации сетей различия наблюдаются не только, когда речь идет о выборе аппаратных компонентов. Данные вариации включают качество оборудования, качество сетевого планирования и проекта, сложность выполнения, взаимодействие и совместимость компонентов.

Сети, созданные для решения критически важных, ответственных задач, проектируются таким образом, чтобы иметь 99% при-

годности и соответствовать рабочим характеристикам, основанных на оценке CBMO. Однако существуют еще четыре важные категории отказов, включающие оставшиеся 75% сетевых отказов, которые нельзя определить с помощью CBMO-анализа проблем аппаратного обеспечения. Необходимо рассмотреть эти другие причины сетевых отказов или пригодности для того, чтобы точно оценить и предсказать сетевую пригодность. Для трех из данных категорий анализ CBMO не подходит.

**Категория 2: Ошибка оператора**

Ошибки оператора определяются как отказы, вызванные непосредственно действиями человека. Далее ошибки оператора подразделяются на намеренные и непреднамеренные ошибки, которые причиняют или не причиняют ущерб. Ошибки оператора влекут за собой свыше 3–5% всех системных отказов. Эта цифра обычно варьируется от предприятия к предприятию в зависимости от уровня квалификации и других факторов, таких как корпоративная культура и процедуры.

Данный вид ошибок полезен в исследовании возможных видов сетевых системных отказов. Ошибка оператора, воздействующая на надежность сети, может явиться результатом взаимодействия людей с сетевым оборудованием, физическими кабелями и соединителями, а также результатом неполадок с другими ИТ-устройствами, вызванными действиями пользователей. Другие ИТ-устройства, такие как серверы базы данных, серверы электронной почты и т. д., могут производить «широковещательные штормы» и дублировать сетевые адреса вследствие действий индивидуумов, работающих с различными устройствами внутри сети.

**Категория 3: Массовые запоминающие устройства**

Эта категория определяется как отказы, связанные с массовыми запоминающими устройствами. Отказы данных устройств изучаются как различными изготовителями, так и пользователями этих устройств. Хотя высококачественные жесткие диски могут достигать исключительно высоких показателей CBMO до 10 в 6 степени часов (почти 114 года), многие организации, использующие банки жестких дисков, часто сталкиваются с более высоким уровнем отказов просто из-за большого количества используемых дисков.

К тому же, внешние воздействующие факторы, такие как изменение температуры, физическое обращение или неправильное обращение в сочетании с частотой определенных операций диска, таких как операция непрерывного поиска, повлияет как на CBMO, так и на его статистическое распределение. Анализ отказов может учитывать данные факторы в процессе планирования надежности сети.

Хотя отказы данных устройств сами по себе не считаются сетевыми отказами, значительно возросло использование Сетей Хране-

ния Данных (СХД), в которых огромное количество массовых запоминающих устройств непосредственно соединяются с сетью с помощью мощных каналов. СХД действительно относят к сетевым устройствам, поскольку они являются сетецентрическими. С позиции аппаратного обеспечения компьютера, традиционные оценки СВМО подходят для этих устройств [3].

**Категория 4: Проблемы программного обеспечения**

В настоящее время корпоративные сети соединяют большое количество серверов, поддерживающих большое количество пользователей, использующих очень большое количество приложений программного обеспечения. Широко распространенные системы обычны в предприятиях, которые территориально рассредоточены. Сеть полностью обеспечивает возможность связи между различными компьютерными платформами и клиентами. В системах такой сложности даже при тщательном планировании, мониторинге и оценивании трудно предсказать сервисные требования к сети. Отказы могут явиться результатом недостаточной мощности, чрезмерных задержек во время пиковой нагрузки, также как катастрофические отказы являются результатом потери необходимого компонента или ресурса.

Сетевые программные ошибки могут быть вызваны неисправностью драйверов устройства, незначительными отличиями в выполнении и обработке протокола, ошибками и дефектами операционной системы. Проблемы программного обеспечения несут ответственность за приблизительно такое же число отказов, что и проблемы аппаратного обеспечения примерно 25%, и являются важными для любых значимых анализов надежности.

**Категория 5: Сетевые проблемы**

К данной категории относятся проблемы аппаратного и программного обеспечения, которые непосредственно связаны с сетью. Они отвечают за более одной трети ИТ (информационно-технологических) отказов. Для лучшего понимания распространения и природы данных видов отказов целесообразно рассмотреть их в контексте модели взаимодействия открытых систем. Диаграмма (рис. 1) показывает распространение ошибок среди уровней модели взаимодействия открытых систем в локальных компьютерных сетях.

Причинами отказов на нижних уровнях модели часто являются неисправные сетевые адаптеры, неисправные кабели и соединения, повреждения в интерфейсных картах, мостах, маршрутизаторах и коммутаторах, сигнальный отказ кольцевой сети с маркерным доступом, ошибки в контрольной сумме и ошибки в размерах пакета. Так как со временем интернет-технологии улучшились, количество отказов на нижних уровнях модели взаимодействия открытых систем сократилось, но возросло коли-

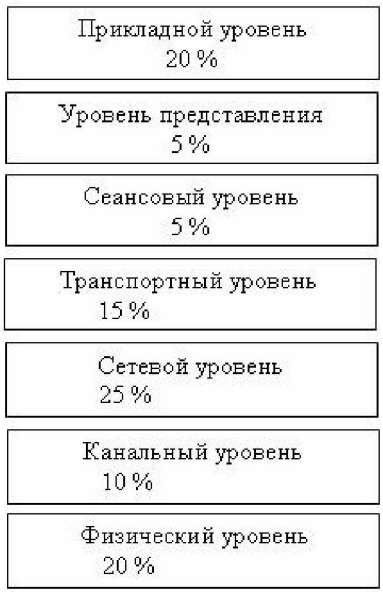


Рис. 1. Частота ошибок локальной сети на уровнях модели взаимодействия открытых систем

чество отказов на прикладном уровне, поскольку сложность программного обеспечения продолжает значительно увеличиваться.

Многие из описанных здесь ошибок и отказов часто ограничены определенным участком, обычно одним компьютером или пользователем и не являются катастрофическими по своей природе. Для понимания вклада локального отказа в надежность сети важно учитывать масштаб и размер отказов, вызванных индивидуальными сетевыми компонентами. Например, неисправность сетевого адаптера едва ли приведет к единичному отказу корпоративной сети. Однако отказ магистрального маршрутизатора без соответствующей избыточности и распределительных устройств может нарушить работоспособность всей сети [2].

### Дополнительные отказы

К дополнительным отказам можно отнести следующие дополнительные категории отказов сети: отказы по причине атаки системы с целью нарушения нормального обслуживания пользователей («черви», «вирусы», «троянские кони» и вредоносные программы).

### Категория 6: Атака системы с целью нарушения нормального обслуживания пользователей

Атаки системы с целью нарушения нормального обслуживания пользователей являются главным источником сетевых отказов, начиная с 2000 года. В настоящее время они происходят несколько раз в

год, приводя к нарушению сервисного обслуживания по всему миру. Частота данных сетевых отказов возрастает в тревожащем темпе. Только частные, строго контролируемые сети, не имеющие доступа к Интернету, невосприимчивы к такой форме атаки, используя воздушные зазоры в сети. Воздушные зазоры это физическая брешь без возможности соединения, в которой данные вручную переносятся между узлами. Такой подход не является практичным для преимущественного большинства сетей, полагающихся на интернет-связь.

Примером воздействия Атак-системы с целью нарушения нормального обслуживания пользователей служат вирус Code Red (кодовый «красный» вирус) и более поздняя вариация, «червь Slammer», нарушившие работу миллионов компьютеров, запустив хорошо слаженную, распространенную атаку системы с целью нарушения нормального обслуживания пользователей. Увеличение частоты осуществления или угрозы атаки и воздействие данного типа сетевых отказов на нарушение работы значительны, и поэтому категория атаки системы с целью нарушения нормального обслуживания пользователей должна быть включена в любую действующую модель анализа отказов корпоративной сети, подключенной к Интернету.

Сложно спрогнозировать процент сетевых отказов, вызванных этим видом ошибки, поскольку это явление происходит хаотично и случайно. Однако потенциальное воздействие этого отказа огромно и широко распространено, и не должно быть недооценено.

Всестороннее развитие методологии отказов заключается в представлении нескольких категорий, определяющих возможную причину и типы отказов телекоммуникационных сетей. В некоторых случаях оценка вероятности и природы отказа предсказуемы, а во многих других любая оценка была бы только догадкой и, таким образом, была бы неточна.

Можно оценить каждую из этих шести категорий и осуществить количественные и гипотетические прогнозы. Этому можно уделить первостепенное внимание и использовать как входные данные при оценке степени риска для телекоммуникационной инфраструктуры. Этот подход может обеспечить методологию, в соответствии с которой можно оценить и ответить на широкий диапазон отказов в сети. Однако можно использовать также альтернативный, менее гипотетический подход — теорию динамических систем [3].

Теория динамических систем, впервые предложенная Томом, описывает катастрофы как раздвоения различных видов равновесия или фиксированных точек притяжения. Она используется для характеристики большого количества естественных и синтетических явлений, начиная от популяций насекомых и заканчивая опрокидыванием кораблей в море. Определенные типы отказов в телекоммуникационных

системах, очевидно, могут быть описаны с помощью этой теории. Такие сетевые отказы, как колебание маршрута являются наиболее подходящими объектами для описания с помощью данного подхода с целью моделирования отказа.

В настоящее время остаются открытыми вопросы возможности применения теории случайных процессов и теории динамических систем к вышеперечисленным категориям сетевых отказов и сравнения результатов с существующими моделями, использующими в качестве предсказателей СВМО и СВМПО.

**Библиографический список**

1. http://www.knijki.net/faq_manual_154.html (Базовые технологии локальных сетей).

2. http://book.itep.ru/4/45/network_r.htm (Сетевая надежность).

3. http://www.cta.ru/ (Аппаратное резервирование в промышленной автоматизации).

4. Анализ деятельности сети МГУП.