ПОКАЗАТЕЛИ ОЦЕНКИ ДОСТОВЕРНОСТИ (БЕЗОШИБОЧНОСТИ) ПЕРЕДАЧИ ДАННЫХ В СЕТЯХ

Надежность сети связана со способностью передавать достоверно (без ошибок)

данные пользователя из одного ООД в другое ООД. Она включает в себя способность

восстановления после ошибок или потери данных в сети, включая отказы канала,

ООД, АКД или ОКД. Надежность также связана с техническим обслуживанием системы,

которое включает ежедневное тестирование, профилактическое обслуживание,

например замену отказавших или допустивших сбой компонент; диагностирование

неисправности при неполадках. В случае возникновения неполадки с каким-либо

компонентом, сетевая диагностическая система может легко обнаружить ошибку,

локализовать неисправность и, возможно, отключить эту компоненту от сети.

Достоверность передачи данных отражает степень соответствия принятого сообщения

переданному. Оценкой достоверности служит коэффициент ошибок, иначе называемый

ООД - оконечное оборудование данных - обобщенное понятие, используемое для

описания машины конечного пользователя, в качестве которой обычно выступает ЭВМ

или терминал.

АКД - аппаратура окончания канала данных - это аппаратура передачи данных. В ее

функции входит подключение ООД к линии или каналу передачи данных.

ОКД - оборудование коммутации данных. Ее основной функцией является коммутация и

маршрутизация трафика (данных пользователя) в сети к месту назначения.

Иногда достоверность определяется как разность между единицей и коэффициентом P.

Согласно рекомендации МККТТ допустимой нормой для телеграфной связи является, ,

то есть не более трех ошибок на 100000 переданных символов, а для передачи

данных .

Появление ошибок при передаче информации объясняется или посторонними сигналами,

всегда присутствующими в каналах, или помехами, вызванными внешними источниками

и атмосферными явлениями, или другими причинами. В телефонии искажением

считается изменение формы тока в приемном аппарате, а в телеграфии - изменение

длительности принимаемых посылок тока по сравнению с передаваемыми посылками.

Телеграфные искажения называются краевыми, если в результате действия помех один

или несколько элементов кодовой комбинации становятся короче или длиннее по

сравнению с их номинальной длительностью. Другая разновидность искажений -

дробление предполагает внутренние изменения в значащем элементе. Если краевые

искажения и дробления достигают большой величины, то приемник телеграфного

аппарата оказывается не в состоянии правильно определить, переданный элемент,

что свидетельствует о наличии ошибки. Помехи - это электрические возмущения,

возникающие в самой аппаратуре или попадающие в нее извне. Наиболее

распространенными являются флуктуационные ,или случайные помехи (например

тепловые шумы, возникающие в оборудовании). Они представляют собой

последовательность импульсов, имеющих случайную амплитуду и следующих друг за

другом через различные промежутки времени.

Типичными примерами импульсных помех являются атмосферные или индустриальные

помехи. Обычно они имеют вид одиночных импульсов, длительность которых может

быть очень маленькой, а амплитуда очень большой. Возможны также сосредоточенные

помехи в виде синусоидальных колебаний. К таким помехам относятся сигналы от

посторонних радиостанций, излучения генераторов высокой частоты и так далее. На

практике возможны и смешанные помехи.

По своей электрической структуре помехи - это колебания, сходные с сигналами, но

беспорядочные и, конечно, ненужные.В приемнике помехи могут подавить

информационный сигнал, то есть ослабить настолько, что приемник или не обнаружит

его, или воспримет как ложный. В частности, в двоичном канале "единица" может

перейти в "ноль" и наоборот. При равнозначной вероятности появления таких

переходов канал связи считается симметричным, в противном случае -

несимметричным. В реальных условиях каналы связи обычно бывают несимметричными.

Наличие помех в системе связи приводит к большому числу неверно выполняемых

вычислений неправильному чтению командных и управляющих посылок , снижению

эффективности сети.

Трудности борьбы с помехами заключаются в беспорядочности, нерегулярности и в

структурном сходстве помех с информационными сигналами. Поэтому защита

информации от ошибок и вредного влияния помех имеет огромное практическое

значение и является одной из важнейших проблем современной теории и техники

связи.

Существует несколько источников возникновения помех. Например, атмосферные

помехи возникают вследствие электрических возмущений в земной атмосфере.

Космические помехи могут прийти с Солнца или других звезд, которые излучают

электромагнитную энергию в очень широком частотном спектре. Помехи можно также

обнаружить в проволоке-проводнике или коаксиальном проводнике вследствие того,

что случайное движение электронов в проводнике приводит к образованию тепловой

энергии.

Чтобы успешно бороться с тепловым шумом (а также с другими видами шумов,

например разрядными помехами флуктуациями мощности и так далее), приемники в

системах связи должны проверять данные и в случаях обнаружения "нарушений"

запрашивать повторную передачу.

"Нарушения" или ошибки можно широко классифицировать как случайные, импульсные и

смешанные. В каналах со случайными ошибками для каждого бита данных существует

вероятность Р неправильного приема и Р-1 правильного приема. Ошибки происходят

случайно в блоках принятых данных. Большинство каналов с вещественными

носителями (а также спутниковые каналы) подвержены случайным ошибкам.

Каналы с импульсными ошибками демонстрируют состояние, свободное от ошибок,

большую часть времени, но иногда появляются групповые или разовые ошибки.

Объектом таких ошибок являются радиосигналы, так же как кабели и провода,

например телефонные каналы из витых проводных пар.

Проблема канального шума обусловлена свойствами самого канала и никогда не может

быть устранена полностью.

АНАЛИЗ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОШИБОЧНОСТИ ПЕРЕДАЧИ ДАННЫХ В СЕТЯХ

Для повышения достоверности и качества работы систем связи применяются групповые

методы защиты от ошибок, избыточное кодирование и системы с обратной связью. На

практике часто используют комбинированное сочетание этих способов.

К групповым методам защиты от ошибок можно отнести давно уже используемый в

телеграфии способ, известный как принцип Вердана:

вся информация (или отдельные кодовые комбинации) передается несколько раз,

обычно не четное число раз (минимум три раза).

Принимаемая информация запоминается специальным устройством и сравнивается.

Суждение о правильности передачи выносится по совпадению большинства из принятой

информации методами "два из трех", "три из пяти" и так далее. Например кодовая

комбинация 01101 при трехразовой передаче была частично искажена помехами,

поэтому

приемник принял следующие комбинации: 10101, 01110, 01001. В результате проверки

каждой позиции отдельно правильной считается комбинация 01101.

Другой метод, также не требующий перекодирования информации, предполагает

передачу информации блоками, состоящими из нескольких кодовых комбинаций. В

конце каждого блока посылается информация, содержащая количественные

характеристики переданного блока, например число единиц или нулей в блоке. На

приемном конце эти характеристики вновь подсчитываются, сравниваются с

переданными по каналу связи, и если они совпадают, то блок считается принятым

правильно. При несовпадении количественных характеристик на передающую сторону

посылается сигнал ошибки.

Среди методов защиты от ошибок наибольшее распространение получило

помехоустойчивое кодирование, позволяющее получить более высокие качественные

показатели работы систем связи. Его основное назначение - принятие всех

возможных мер для того, чтобы вероятность искажений информации была достаточно

малой, несмотря на присутствие помех или сбоев в работе сети.

Помехоустойчивое кодирование предполагает разработку корректирующих

(помехоустойчивых) кодов, обнаруживающих и исправляющих определенного рода

ошибки, а также построение и реализацию кодирующих и декодирующих устройств.

Специалистами доказано, что при использовании помехоустойчивого кодирования

вероятность неверной передачи во много раз снижается. Так, например, с помощью

кода M из N, используемого фирмой IBM в вычислительных сетях, можно обнаружить в

блоке, насчитывающем около тридцати двух тысяч символов, все ошибки, кратные

трем или меньше, или пачки ошибок длиной до шестнадцати символов.

При передаче информации в зависимости от системы счисления коды могут быть

двухпозиционными и многопозиционными. По степени помехозащищенности

двухпозиционные коды делятся на обыкновенные и помехоустойчивые.

Двухпозиционные обыкновенные коды используют для передачи данных все возможные

элементы кодовых комбинаций и бывают равномерными, когда длина всех кодовых

комбинаций одинакова, например пятиэлементный телеграфный код, и неравномерными,

когда кодовые комбинации состоят из разного числа элементов, например код Морзе.

В этом коде точке соответствует одна единица, тире - три единицы. Для отделения

точек и тире друг от друга записывается ноль, а для завершения комбинации - три

нуля. Так, буква А, состоящая из точки и тире, представляется как 10111000, а

буква Б (тире и три точки) - как 111010101000.

В помехоустойчивых кодах, кроме информационных элементов, всегда содержится один

или несколько дополнительных элементов, являющихся проверочными и служащих для

достижения более высокого качества передачи данных. Наличие в кодах избыточной

информации позволяет обнаруживать и исправлять (или только обнаруживать) ошибки.

Основными среди многочисленных характеристик корректирующих кодов являются

значность, корректирующая способность, избыточность и оптимальность кода,

коэффициент обнаружения и исправления ошибки, простота технической реализации

метода и другие. Так, значность кода, или длина кодовой комбинации, включает как

информационные элементы m, так и проверочные (контрольные) k. Как правило,

значность кода n равна m+k.

Оптимальность кода указывает на полноту использования его корректирующих

возможностей.

Выбор корректирующих кодов в определенной степени зависит от требований,

предъявляемых к достоверности передачи. Для правильного его выбора необходимо

иметь статистические данные о закономерностях возникновения ошибок, их

характере, численности и распределении во времени. Так,например, корректирующий

код, исправляющий одиночные ошибки, может быть эффективен лишь при условии, что

ошибки статистически независимы, а вероятность их появления не превышает

некоторой величины. Этот код оказывается совершенно не пригодным, если ошибки

появляются группами (пачками). Рекуррентные коды, исправляющие групповые ошибки,

также могут оказаться неэффективными, если количество ошибок при передаче будет

больше допустимой нормы.

Разработанные различные корректирующие коды подразделяются на непрерывные и

блочные. В непрерывных, или рекуррентных, кодах контрольные элементы

располагаются между информационными. В блочных кодах информация кодируется,

передается и декодируется отдельными группами (блоками) равной длины.

Блочные коды бывают разделимые (все информационные и контрольные элементы

размещаются на строго определенных позициях) и неразделимые (элементы кодовой

комбинации не имеют четкого деления на избыточные и информационные). К

неразделимым относится код с постоянным числом нулей и единиц.

Разделимые коды состоят из систематических и несистематических. В

систематических кодах проверочные символы образуются с помощью различных

линейных комбинаций. Систематические коды - самая обширная и наиболее

применяемая группа корректирующих кодов. Они включают такие коды, как код

Хэмминга, циклические коды, коды Боуза-Чоудхури и другие.

Большие вычислительные системы (Amdal, IBM, Burroughs, ICL) используют очень

сложную методику проверки ошибок при передаче по линиям связи между машинами. В

ПЭВМ обычно применяется более простая техника проверки ошибок.

Одной из простейших форм проверки ошибок является так называемый эхоплекс. В

соответствии с этой методикой каждый символ, посылаемый ПЭВМ по дуплексной линии

связи удаленному абоненту, возвращается обратно к ПЭВМ в виде эха. Если ПЭВМ

принимает тот же символ, что и был послан, подразумевается, что передача символа

прошла правильно. Если нет, значит, при передаче произошла ошибка и необходима

повторная передача этого же символа. Эхоплекс применяется в двунаправленных

дуплексных каналах связи.

Некоторые пользователи ПЭВМ путают эхоплекс с местным эхо. Местное эхо часто

используется при подключении полудуплексного модема к телефонному каналу. В этом

случае данные возвращаются к ПЭВМ не от удаленного окончания, а от местного

(ближнего) модема.

Если устройство не было настроено соответствующим образом, ПЭВМ может выдать на

экран двойные символы. Это случается, если от модема возвращается местное эхо, а

от удаленного окончания удаленное эхо (эхоплекс). Проблема дублирования символов

решается путем подавления местного эха.

Другим часто используемым на практике (и сравнительно простым) методом является

контроль на четность. Его суть заключается в том, что каждой кодовой комбинации

добавляется один разряд, в который записывается единица, если число единиц в

кодовой комбинации нечетное, или ноль, если четное. При декодировании

подсчитывается количество единиц в кодовой комбинации. Если оно оказывается

четным, то поступившая информация считается правильной, если нет, то ошибочной.

Кроме проверки по горизонтали контроль на четность и нечетность может

проводиться и по вертикали. Преимущества контроля на четность заключается в

минимальном значении коэффициента избыточности (для пятиэлементного кода К

=0,17) и в простоте его технической реализации, а недостаток - в том, что

обнаруживаются ошибки, имеющие только нечетную кратность. Однако такая методика

проверки не может обнаружить ошибки в случае двойного переброса (например, две

единицы перебросились в ноль), что может привести к высокому уровню ошибок в

некоторых передачах. Многоуровневая модуляция (когда проверка проверка сигнала

осуществляется по двум или трем битам) требует более сложной техники.

Проверка на четность/нечетность по одному биту также является неприемлемой и для

многих аналоговых линий речевого диапазона из-за группирования ошибок, которое

обычно происходит в линиях связи такого типа.

Двойная проверка на четность/нечетность является усовершенствованием одинарной

проверки. В этой методике вместо бита четности в каждом символе определяется

четность или нечетность целого блока символов. Проверка блока позволяет

обнаруживать ошибки как внутри символа, так и между символами.Эта проверка

называется также двумерным кодом проверки на четность. Она имеет значительное

преимущество по сравнению с одинарной. С помощью такой перекрестной проверки

может быть существенно улучшена надежность работы обычной телефонной лини,

вероятность появления ошибки в которой составляет 10.

Однако как ординарная, так и двойная проверка на четность означают увеличение

накладных расходов и относительное уменьшение выхода информации для

пользователя.

К систематическим кодам также относится и код Хэмминга, который позволяет не

только обнаруживать, но и исправлять ошибки. В этом коде каждая кодовая

комбинация состоит из m информационных а k контрольных элементов. Так, например,

в семиэлементном коде Хэмминга n=7, m=4, k=3 (для всех остальных элементов

существует специальная таблица). Контрольные символы 0 или 1 записываются в

первый, второй и четвертый элементы кодовой комбинации, причем в первый элемент

- в соответствии с контролем на четность для третьего, пятого и седьмого

элементов, во второй - для третьего, шестого и седьмого элементов, и в четвертый

- для пятого - седьмого элементов. В соответствии с этим правилом комбинация

1001 будет представляться вкоде Хэмминга как 0011001, и в этом виде она будет

представляться в канал связи.

При декодировании в начале проверяются на четность первый,третий,пятый и седьмой

элементы, результат проверки записывается в первый элемент контрольного числа.

Далее контролируется четвертый - седьмой элементы - результат проставляется в

младшем элементе контрольного числа. При правильно выполненной передаче

контрольное число состоит из одних нулей, а при неправильной - из комбинаций

нулей и единиц, соответствующей при чтении ее справа налево номеру элемента,

содержащего ошибку.

Для устранения этой ошибки необходимо изменить находящийся в этом элементе

символ на обратный.

Код Хэмминга имеет существенный недостаток: при обнаружении любого числа ошибок

он исправляет лишь одиночные ошибки. Избыточность семиэлементного кода Хэмминга

равна 0,43. При увеличении значности кодовых комбинаций увеличивается число

проверок, но уменьшается избыточность кода. К тому же код Хэмминга не позволяет

обнаружить групповые ошибки, сконцентрированные в пакетах. Длина пакета ошибок

представляет собой увеличенную на единицу разность между именами старшего и

младшего ошибочных элементов.

Распространенным кодом, но не относящимся к группе неразделенных, является код с

постоянным числом нулей или единиц или код M из N. Так, семиэлементный код имеет

соотношение единиц и нулей, равное 3:4. Кодирование и декодирование выполняются

заменой одной кодовой группой другой. Например, комбинация 01110 посылается в

канал связи в виде 0101010. На приемном конце она вновь декодируется в 01110.

Фирма IMB использует восьмиэлементный код, содержащий четыре единицы и четыре

нуля.

Еще одной формой проверки ошибок служит подсчет контрольных сумм. Это несложный

способ, который обычно применяется вместе с контролем ошибок с помощью эхоплекса

или проверки на четность/нечетность. Сущность его состоит в том, что передающая

ПЭВМ суммирует численные значения всех передаваемых символов.

Шестнадцать младших разрядов суммы помещаются в шестнадцатиразрядный счетчик

контрольной суммы, который вместе с информацией пользователей передается

принимающей ПЭВМ. Принимающая ПЭВМ выполняет такие же вычисления и сравнивает

полученную контрольную сумму с переданной. Если эти суммы совпадают,

подразумевается, что блок передан без ошибок. При этом имеется незначительная

вероятность того, что в результате такой проверки ошибочный блок может быть не

обнаружен, но опыт показывает, что это случается не чаще одного раза но тысячу

сеансов передач. Сколько же при этом может быть передано безошибочных блоков,

прежде чем встретится один ошибочный? Если передача производится по

высококачественной линии, то - несколько тысяч. В обычной конфигурации

необнаруженный ошибочный блок может возникнуть не более одного раза в течение

нескольких месяцев работы.

Последним словом в области контроля ошибок в сфере ПЭВМ является циклическая

проверка с избыточным кодом (CRC - cyclic redunduncy check). Она широко

используется в протоколах HDLC, SDLC, но в индустрии ПЭВМ появилась сравнительно

недавно.

Поле контроля ошибок включается в кадр передающим узлом. Его значение получается

как некоторая функция от содержимого всех других полей. В принимающем узле

производятся идентичные вычисления еще одного поля контроля ошибок. Эти поля

затем сравниваются; если они совпадают, велика вероятность того, что пакет был

передан без ошибок. Этот процесс, как уже было упомянуто, называется циклическим

контролем по избыточности (CRC), а поле называется контрольной

последовательностью кадра (КПК). В случае несовпадения, возможно, имела место

ошибка передачи, и принимающая станция посылает сигнал, означающий, что

необходимо повторить передачу кадра.

При вычислении КПК используется производящий полином 16+12+5+1.

Вычисление и использование кода CRC производится в соответствии со следующими

правилами:

-) К содержимому кадра добавляется набор нулей, количество которых равно длине

поля КПК.

-) Образованное таким образом число делится на производящий полином, который

содержит на один разряд больше, чем КПК, и который в качестве старшего и

младшего разрядов имеет единицы.

-) Остаток от деления помещается в поле КПК и передается в приемник.

-) Приемник выполняет деление содержимого кадра и поля КПК на полином.

-) Если результат равен некоторому определенному числу, считается, что передача

выполнена без ошибок.

Метод CRC позволяет обнаруживать всевозможные кортежи ошибок длиной не более

шестнадцати разрядов, вызываемых одиночной ошибкой, а также 99,9984%

всевозможных более длинных кортежей ошибок.

АНАЛИЗ СРЕДСТВ ОБЕСПЕЧЕНИЯ БЕЗОШИБОЧНОСТИ ПЕРЕДАЧИ ДАННЫХ В СЕТЯХ

В соответствие с особенностями корректирующих кодов выбираются кодирующие и

декодирующие устройства. Один из методов построения кодирующих устройств

предполагает применение логических схем, на выходах которых при каждом такте

кодирования образуются контрольные элементы. Такие устройства более

целесообразны при малых значениях информационных и контрольных символов. Другой

способ требует наличия запоминающего устройства в котором контрольные символы

хранятся и извлекаются лишь при появлении на входном регистре информационных

символов.

Наиболее сложным построением декодирующих устройств является метод сравнения,

который требует запоминающих устройств большой емкости. При пользовании более

простым методом контрольных чисел декодирующее устройство по принятым

информационным символам вновь образует контрольные символы, которые и сравнивает

с полученными по каналу связи. Метод коррекции предполагает корректировку

информационных символов в зависимости от проверок, осуществляемых по элементам,

отстающим друг от друга на какой-то определенный шаг.

Информационные элементы из информационного регистра поступают в сумматоры, число

которых равняется количеству контрольных символов. Образовавшиеся на выходах

сумматоров контрольные символы записываются в ячейки проверочного регистра.

Формирование элементов кодовой комбинации и ее выдача в канал связи выполняются

под воздействием управляющих импульсов через переключатель П.

При декодировании каждая кодовая комбинация фиксируется в приемном регистре и

проверяется на четность в сумматорах. При правильной передаче на выходах

сумматоров отмечаются только нули, и информационные элементы через переключатель

П выдаются получателю.

Если же передача произошла неверно составляется ненулевое контрольное число, в

зависимости от которого дешифратор формирует семиэлементную комбинацию,

состоящую из семи нулей и одной единицы в том элементе, где произошла ошибка.

При сложении этой комбинации с принятой кодовой комбинацией образуется

правильное число, информационные элементы которого через переключатель П будут

отправлены получателю.

Кодирующие и особенно декодирующие устройства, применяемые для кодов с

исправлением ошибок, являются более сложными, поскольку схемы их построения

содержат целый ряд дополнительных устройств.

Разработаны два варианта упрощенной технической реализации таких декодирующих

устройств:

-) Вероятностный, при котором высоковероятные малоискаженные кодовые комбинации

декодируются без проверки, а маловероятные, сильноискаженные - с проверкой и

исправлениями.

-) Алгебраический, при котором используется неоптимальный алгоритм

декодирования, имеющий более простую схему построения.

В вычислительных системах корректирующие коды в основном используются для

обнаружения ошибок, исправление которых осуществляется путем повторной передачи

искаженной информации. С этой целью почти все сети используют системы передачи с

обратной связью. Кроме того, наличие между абонентами двусторонней связи

облегчает применение таких систем.

Системы передачи с обратной связью подразделяются на:

-) системы с решающей обратной связью

-) системы с информационной обратной связью

В первом случае решение о повторной передаче информации выносит приемник, а во

втором случае аналогичное решение принимает передатчик.

Особенностью системы с решающей связью (или, как их иначе называют, систем с

автоматическим запросом ошибок, или систем с перезапросом) является обязательное

применение помехоустойчивого кодирования, с помощью которого на приемной станции

осуществляется проверка принимаемой информации. Канал обратной связи

используется для посылки на передающую сторону или сигнала переспроса, который

свидетельствует о наличии ошибки и необходимости повторной передачи, или сигнала

подтверждении правильности приема, автоматически определяющего начало следующей

передачи.

В целях повышения скорости передачи передающая аппаратура обычно не ожидает

сигнала с приемной стороны, а работает непрерывно. При появлении ошибки и приеме

сигнала переспроса она повторяет всю информацию, начиная с неверно принятой.Это

несколько усложняет всю систему в целом, так как требуется дополнительное ЗУ.

В системах с решающей обратной связью ошибки могут возникнуть и при передаче

сигналов по обратному каналу. Так, если сигнал переспроса не достигнет

передатчика, то передатчик не осуществит повторной посылки сообщения, которое

было принято неверно. В результате сообщение к абоненту не поступит. Такое

явление называется аннигиляцией сообщения. Если же вместо сигнала подтверждения

по каналу обратной связи будет принят сигнал переспроса, то у абонента появится

лишняя информация (ложные повторы). В практической работе для уменьшения

вероятности ошибок подобного рода сигнал подтверждения кодируется нулями, а

сигнал переспроса - единицами.

Различают системы с ограниченным и неограниченным числом повторений передач. В

первом случае заранее устанавливается максимальное число повторений, при

достижении которого передатчик прекращает отвечать на переспросы, а приемник

решает, какое из нескольких полученных сообщений считать правильными. Во втором

случае посылка нового сообщения начинается лишь после прекращения всех

переспросов.

В системах с информационной обратной связью передача информации осуществляется

без помехоустойчивого кодирования. По каналу обратной связи приемник передает

всю ту информацию, которая была им принята по прямому каналу и записана в его

ЗУ. Передатчик сравнивает хранящуюся у него информацию с принятой по каналу

обратной связи и при правильной передаче посылает сигнал подтверждения. В

противном случая происходит повторная передача всей информации.

Системы с информационной и решающей обратной связью могут иметь адресное и

безадресное повторение. Преимущество систем с адресным повторением заключается в

том, что при обнаружении ошибок повторно передается не вся информация, как в

системах с безадресным повторением, а только ошибочная информация. Однако

использование системы с адресным повторением связано со значительным усложнением

схем построения приемопередающей аппаратуры.

Системы с решающей и информационной обратной связью обеспечивают одинаковую

достоверность. При возникновении ошибок, которые группируются в пакеты,

предпочтительнее системы с информационной обратной связью, поскольку передача

сообщений по обратному каналу происходит в более благоприятные интервалы

времени, чем по прямому каналу.

Однако системы с информационной обратной связью имеют более сложное техническое

оборудование, а используемые в них каналы связи характеризуются меньшей

пропускной способностью. Поэтому в действующих сетях чаще применяются системы с

решающей обратной связью в сочетании с контролем на четность или циклическим

кодированием.

ОЦЕНКА ЗАВИСИМОСТИ ПОКАЗАТЕЛЕЙ ЭФФЕКТИВНОСТИ МЕТОДОВ ОБЕСПЕЧЕНИЯ БЕЗОШИБОЧНОСТИ

ПЕРЕДАЧИ ДАННЫХ ОТ РАЗЛИЧНЫХ ПАРАМЕТРОВ

Как же влияет избыточность (а точнее количество контрольных элементов,

содержащихся вместе с информационными в кодах) на эффективность работы кода и

системы в целом?

С одной стороны, чем больше избыточность кода, тем выше его помехоустойчивость

и, соответственно, тем достовернее будет передаваться информация, то есть

вероятность необнаружения ошибки будет ниже (коэффициент обнаружения и

исправления ошибок.

С другой же стороны, чем выше содержание контрольных элементов в коде (или его

избыточность), тем выше будет его значность, а следовательно возрастет возрастет

время передачи данных по каналу, пропускная способность которого уменьшится.

Это, безусловно, сделает систему менее привлекательной для пользователя и

эффективность ее упадет.

В связи с этим более предпочтительными считаются коды с меньшей избыточностью,

так как избыточность напрямую связана с эффективностью сети. Также следует

учитывать и то, что чем выше избыточность кода, тем сложнее и дороже должны быть

кодирующие и декодирующие устройства, что является не менее важным фактором, чем

допустим пропускная способность канала связи, поскольку стоимость оборудования

должна соответствовать ее необходимости, то есть должна окупаться сравнительно

быстро.