ЗАРЕЧЕНСКИЙ П.А., МОНАХОВ М.Ю

АНАЛИЗ НАДЕЖНОСТИ ФУКЦИОНИРОВАНИЯ СЕТЕЙ

Владимирский государственный университет им. А.Г. Н.Г. Столетовых

На сегодняшний день основная цель моего исследования это определение влияния различных дестабилизирующих факторов на работу сетей, изучение работы сетей, средств мониторинга, восстановления и резервирования сетей. Построение модели функциональной надежности сети, в условиях дестабилизирующих факторов

Для достижения поставленной цели были поставлены следующие задачи:

Определение Сбоя и отказа

Выявление классификационных признаков, достаточных для определения типа отказа;

Составление набора уязвимостей, влияющих на появление отказа

Сегодня в мире бизнеса компьютерная сеть – это больше чем набор соединенных между собой устройств. Для множества видов деятельности предприятий компьютерная сеть – это ресурс, позволяющий сотрудникам собирать, анализировать, организовывать и распространять информацию, являющуюся основой их бизнеса и источником прибыльности всего предприятия. Различные отказы на сети могут приводить, к экономическому ущербу , к отказу в предоставлении услуг.

Поэтому исследования в данной области будут актуальны и востребованы на сегодняшний момент тем, кому необходима стабильность и надежность работы сети.

Сбой - Ненормальная ситуация, которая может привести к снижению или потере способности функционального узла к выполнению предопределенной функции, то есть к отказу

Отказ - Прекращение способности функционального узла к выполнению предопределенной функции. Отказ должен определяться системой, иметь возможность исправления или замены *on-line* без воздействия на функциональность системы как до, так и после восстановления (замены).

В частном случае на практике используют термины

Авария – Нарушение исправного состояния сети МСПД, приведшие к безвозвратным потерям трафика МСПД, в т.ч переключение на резервные каналы

Повреждение – Нарушение исправного состояния сети МСПД, не приведшие к потерям трафика МСПД, подлежит анализу и учету

Аварии и повреждения можно классифицировать по нескольким признакам

1) По месту возникновения:

а) На линейной части

Повреждения линий связи препятствующих функционированию сети. К таким повреждения можно отнести повреждения и обрыв линий связи, повреждение коннекторов и оптических патч-кордов.

б) На стационарном оборудовании

Повреждения и отказы станционного оборудования сети, магистрального оборудования. К таким повреждениям можно отнести отключения питания оборудования, выход из строя элементов оборудования, сбои в программном обеспечении оборудования

2) По степени влияния на пользователей:

а) Глобальный

При возникновении отказа все пользователи не имеют доступа к сети. К таким отказам можно отнести: сбои DNS серверов, повреждения магистрального оборудования, сбои авторизации (работы биллинг серверов), повреждения МСПД. Сбои системного программного обеспечения оборудования.

б) Групповой

При возникновении отказа определенная группа пользователей не имеет доступа к сети .

К таким отказам можно отнести: повреждения и отказы коммутаторов и коммутаторов MetroEthernet, повреждения оптических кабелей внутрирайонных сегментов сети, отказы оборудования медной связи (xDSL) ,отключения электропитания

3) По времени возникновения

а) Случайный отказ оборудования *{Random hardware failure)* - Отказ, проявляющийся в произвольный момент времени, приводящий к запуску одного или более механизмов скачкообразной деградации оборудования. Реальные условия работы оборудования приводят к тому, что элементы системы отказывают по разным механизмам отказа и в произвольные моменты времени. Поэтому оценить можно всего лишь частоту отказов, но не конкретные моменты их появления**.**

б) Систематический отказ *(Systematic failure)* - Отказ, проявляющийся вполне определенным образом по определенной причине, от которой можно избавиться только изменением конструкции, технологических процедур, документации, или других определяющих факторов. Систематические отказы иногда могут быть устранены путем моделирования причин и условий отказа. Однако профилактическое

обслуживание без внесения радикальных изменений, как правило, не устраняет первопричины отказа.

Для рассмотрения различных факторов ,влияющих на работу сети, составим перечень уязвимостей. Уязвимости можно разделить на несколько основных групп:

Надежность и качество ПО

Проблемы электропитания. Отсутствие резервирования

Плохие условия Физической среды ВЦ

Человеческий фактор

Надежность и качество ПО

Для обеспечения надежности программных средств необходимы разработка и применение эффективных методов и средств, предупреждающих и выявляющих дефекты, а также удостоверяющих надежность программ и оперативно защищающих функционирование ПС при их проявлениях. Для систематической, координированной борьбы с угрозами надежности должны проводиться исследования конкретных факторов, влияющих на качество функционирования и безопасность применения программ со стороны реально существующих и потенциально возможных дефектов в создаваемых комплексах программ. В каждом проекте должен целенаправленно разрабатываться скоординированный комплекс методов и средств обеспечения заданной надежности функционирования ПС при реально достижимом снижении уровня дефектов и ошибок разработки. Учет факторов, влияющих на затраты ресурсов при создании конкретного ПС, должен позволять рационализировать их использование и добиваться заданной надежности функционирования ПС при минимальных или допустимых затратах.

Проблемы электропитания. Отсутствие резервирования

Часто возникающая проблема при работе оборудования. Поэтому стоить рассмотреть данную уязвимость поподробнее

Перебой электропитания определяется как полное отсутствие напряжения в сети или тока через нагрузку. Различают перебои:

малой длительности 0,5-30 периодов;

средней длительности от 30 периодов до 2 секунд;

большой длительности от 2 секунд до 2 минут;

продолжительные более 2 минут.

Причины перебоев могут быть различны, но обычно речь идет о повреждении электросети того или иного рода, включая удар молнии, попадание в провода животных, падение деревьев, дорожно-транспортные происшествия, неблагоприятные погодные явления (сильный ветер, налипание снега и льда на провода ЛЭП и т.п.), отказе оборудования или срабатывании предохранителей. Хотя в инфраструктуре электросетей предусматриваются меры автоматического реагирования в подобных ситуациях, абсолютной защиты они не обеспечивают.

Один из наиболее частых источников перебоев питания в коммерческой электросети — защитное оборудование, такое как автоматы повторного включения. Они определяют продолжительность большинства перебоев питания, в зависимости от характера неисправности. Автоматы повторного включения осуществляют мониторинг силы тока и при ее возрастании из-за короткого замыкания отключают напряжение. Спустя заданное время напряжение снова включается — с тем, чтобы попытаться выжечь замыкающий проводник (которым нередко оказывается ветка дерева или небольшое животное, оказавшееся в проводах).

Перебой электропитания, будь то малой, средней, большой длительности или продолжительный, способен повлечь за собой нарушения работы, повреждения и простои, не важно, идет ли речь о бытовом

потребителе или промышленном. Пользователь домашнего компьютера или небольшое предприятие может утратить при обесточивании оборудования ценные данные.

В крупных предприятиях существует достаточно распределенная сетевая инфраструктура где, персонал ведет свою работу по сети с удаленными подразделениями, с различными серверами. Отказ в работе оборудования сети по причине отключения электропитания оборудования на каком-либо участке может привести, как к потере данных, так и к экономическому ущербу и простою в работе.

Плохие условия Физической среды ВЦ

Окружающие условия в которых находится оборудование непосредственно влияют на его работу. Поэтому окружающую среду необходимо рассматривать как целое и заблаговременно выявлять потенциальные угрозы и вторжения. влияющие на физическую среду. В число таких угроз входит повышенная температура воздуха, используемого для охлаждения серверов, утечки воды, неавторизованный доступ посторонних в помещения ВЦ или некорректные действия персонала

Удаленные узлы сети, включая офисы филиалов, хранилища данных и контрольно-кассовые терминалы, где отсутствует персонал, способный надежно контролировать температуру и влажность, особенно нуждаются в автоматизированном мониторинге. С подключением к сетям удаленных объектов, присутствие на которых персонала вообще не предполагается, для получения сведений оттуда оказываются необходимы надежные автоматические средства.

В таблице 1 сведена информация о распределенных физических угрозах, об их значении для ВЦ

Таблица 1 – Распределенные физические угрозы

Угроза	Определение	Опасность для ВЦ	Типы датчиков
Температура воздуха	Температура воздуха в помещениях, стойках и внутри корпусов устройств.	Выход из строя и сокращение срока службы оборудования вследствие превышения температуры над расчетной и / или резких колебаний этого	Температурные датчики.
Влажность	Относительная влажность в помещениях и стойках при определенных температурах.	Выход из строя оборудования из-за разрядов статического электричества, накапливающегося в условиях пониженной влажности. Осаждение конденсата в условиях повышенной влажности.	Датчики влажности.
Протечки жидкостей	Протечки воды или охлаждающей жидкости.	Намокание полов, кабелей и оборудования. Признак неисправности аппаратуры кондиционирования	Линейные датчики протечки. Точечные датчики
Человеческие ошибки и доступ персонала	Непреднамеренное причинение вреда персоналом. Злонамеренное неавторизованное и / или силовое проникновение в вычислительный центр.	Повреждение оборудования и потеря данных. Простои оборудования. Хищение оборудования и саботаж.	Цифровые видеокамеры. Датчики движения. Датчики открывания на дверцах стоек. Датчики открывания на дверях комнат. Датчики
Задымление / пламя	Электрические замыкания или возгорание различных	Отказ оборудования. Утрата материальных активов и данных.	Дополнительные датчики задымления.
Опасные примеси в атмосфере	Распространяющиеся по воздуху химические вещества, такие как водород, выделяющийся из аккумуляторов, и твердые частицы, такие как пыль.	Опасность для здоровья персонала и / или для надежного функционирования ИБП из-за выделения водорода. Отказы оборудования из-за накопления статического электричества и засорение фильтров / вентиляторов.	Датчики водорода / других химических загрязнений. Датчики запыленности.

Человеческий фактор

Возможность принятия человеком ошибочных или алогичных решений в конкретных ситуациях приводящих к отказу в работе сети

Любому человеку свойственны ограничения возможностей или ошибки. Не всегда психологические и психофизиологические характеристики человека соответствуют уровню сложности решаемых задач или проблем.

Характеристики, возникающие при взаимодействии человека и технических систем, часто называют «человеческий фактор». Ошибки, называемые проявлением человеческого фактора, как правило, непреднамеренны: человек выполняет ошибочные действия, расценивая их как верные или наиболее подходящие.

Причины, способствующие ошибочным действиям человека, можно объединить в несколько групп:

недостатки информационного обеспечения, отсутствие учёта человеческого фактора;

ошибки, вызванные внешними факторами;

ошибки, вызванные физическим и психологическим состоянием и свойствами человека;

ограниченность ресурсов поддержки и исполнения принятого решения.

Ошибки человека также могут привести к отказу в работе оборудования или повреждению линейных каналов связи, поэтому работа с персоналом и информирование людей тоже необходимое условие для обеспечения надежности сети.

Рассмотрев все факторы влияющие на работу оборудования и каналов связи, можно отметить что дестабилизирующих факторов достаточно много.

Для построения надежной сети необходимо изначально просчитать все возможные сбои, их вероятность и частоту проявления. При необходимости внедрять в сеть избыточность, использовать средства резервирования питания.

Литература

1. ОАО Ростелеком., Регламент взаимодействия тех. служб по вопросам эксплуатации. и устранения повреждений МСПД. Владимир 2008
2. Fluke Networks. Руководство по обнаружению сбоев в компьютерных сетях 2009
3. Стандарт IEC 61508 «Функциональная безопасность электрических / электронных / программируемых электронных систем безопасности".
4 ГОСТ 27.002-89 Надежность в технике. Основные понятия
5. *Christian Cowan*. American Power Conversion. Информационные статьи 2006
6. *Josef Seymus*. APC Schneider Electric. Информационная статья №18 2006

Сведения об авторах

Монахов Михаил Юрьевич, Владимирский государственный университет, заведующий кафедрой ИЗИ, д.т.н.,профессор monakh@izi.vlsu.ru
Зареченский Павел Александрович, Владимирский государственный университет, , аспирант кафедры ИЗИ, инженер Владимирского ф-ла компании ОАО Ростелеком pavel-z@inbox.ru