УДК 621.39

Аварийное планирование при обработке данных в электротехнических системах

Т.С. Аббасова, А.Г. Никифоров

Рассмотрены наиболее актуальные на современном этапе развития средств вычислительной техники вопросы планирования системы климатизации для охлаждения оборудования, осуществления резервного питания и обеспечения электромагнитной совместимости в соответствии с требованиями стандарта TIA/EIA-942.

The most topical questions about climate systems for equipment cooling, power backup implementation, and electromagnetic compatibility implementation according with TIA/EIA-942 standard requirements are considered.

Развитие элементной базы электротехнических систем происходит в направлении снижения уровня питающих напряжений и информационных сигналов. Информационные сигналы могут переносить собственно информационные данные, данные аварийной сигнализации, данные, полученные в результате сбора статистики о состоянии сетевого оборудования и пр. В связи с этим может возникнуть опасность ложного срабатывания аппаратуры под воздействием различного рода помех, уровень которых соизмерим с уровнем информационного сигнала, что может привести к сбоям, отказам и даже катастрофам. Наряду с термином «отказоустойчивость» в современных исследованиях на эту тему вводится термин «катастрофоустойчивость».

Постановка задачи

Требуется обеспечить непрерывность аварийного планирования, свести к минимуму фактор внезапности воздействия на информационную систему, несущего угрозу всему предприятию.

При планировании действий персонала в критических ситуациях важно помнить главное правило: что бы ни угрожало работе предприятия или функционированию информационной системы, сохранение жизни и здоровья сотрудников – главная задача.

Для решения поставленных задач необходим комплексный подход, что нашло отражение в принятом в июле 2004 г. стандарте TIA/EIA-942 (от англ. Telecommunications Infrastructure Standard for Data Centers), где значительное внимание уделяется инженерным системам – электрике, кондиционированию, кабельным каналам [1].

Влияние архитектуры информационной системы на безопасность функционирования

Современные информационные системы (ИС) берут свое начало от тех систем, архитектура которых предполагала централизацию основных вычислительных мощностей.

Модель с централизацией основных вычислительных мощностей представлена на рис. 1, файл-серверная обработка данных – на рис. 2, клиент-серверная обработка данных – на рис. 3.

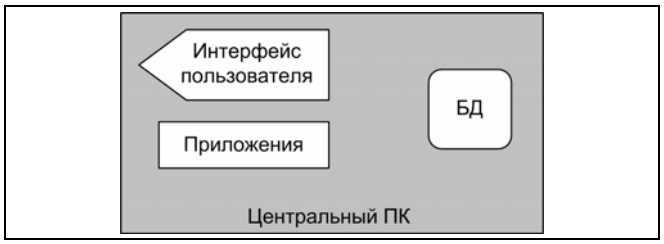

Рис. 1. Централизованная модель вычисления

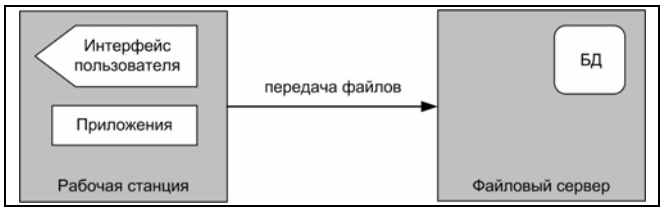

Рис. 2. Файл-серверная обработка данных

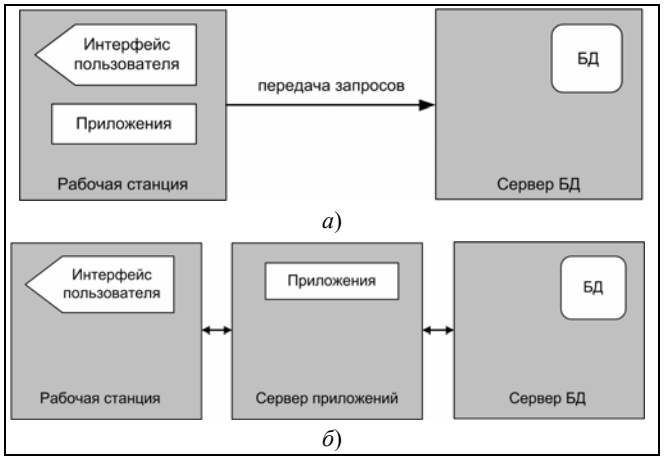

Рис. 3. Клиент-серверная обработка данных: *а* – двухуровневая; *б* – трехуровневая

При централизованной обработке данных все средства обработки установлены и функционируют на одном персональном компьютере (ПК). При файл-серверной распределенной обработке данных на сервере хранятся файлы базы данных (БД), идет извлечение файлов из БД с нужной информацией.

При клиент-серверной двухуровневой обработке данных на сервере БД хранятся файлы БД и система управления базами данных (СУБД). Рабочие станции (РС) посылают серверу запросы на интересующие их данные, сервер выполняет извлечение и предварительную обработку данных. Уменьшается трафик сети и обеспечивается прозрачность доступа всех приложений к файлам БД.

При клиент-серверной многоуровневой обработке данных сервер выполняет всю содержательную обработку данных, в качестве РС используются сетевые ПК. Эта архитектура с точки зрения безопасности функционирования признается сейчас наиболее перспективной [2].

Аппаратное обеспечение СУБД составляет один или несколько мощных серверов, а технический персонал уделяет им повышенное внимание с момента их запуска. Остановка основного сервера, даже на непродолжительное время, может вызвать серьезные последствия.

В этих условиях технической архитектурой должно предусматриваться наличие резерва – кластера серверов высокой надежности. Важно отметить, что в большинстве случаев резервный сервер находится в том же здании, а порой и в той же серверной комнате. С точки зрения обеспечения надежности выполняемых приложений и работы бизнес-процессов такое решение до настоящего времени считалось само собой разумеющимся. Однако является ли оно отказоустойчивым (катастрофоустойчивым)?

В условиях централизации вычислительных мощностей невозможно получить действительно отказоустойчивое (катастрофоустойчивое) решение, если защита оборудования от сбоев осуществляется в пределах одной площадки. В особенности это касается предприятия, имеющего разветвленную сеть филиалов. Решение, где предусматривается единственная возможность резервирования данных путем копирования на резервную систему хранения, обладает существенным недостатком – отсутствием гарантии их восстановления. С точки зрения непрерывности работы предприятия подобная система резервирования должна рассматриваться лишь в качестве вспомогательной.

Очевидно, что координатор работ по аварийному планированию должен учитывать как одиночные отказы оборудования внутри ИС, так и выход из строя всего комплекса оборудования, размещенного на основной площадке.

Таким образом, централизованная техническая архитектура ИС является наиболее уязвимой и наименее приспособленной для обеспечения непрерывности бизнес-процессов крупного предприятия [3].

Для осуществления непрерывности аварийного планирования и снижения риска катастрофических последствий следует предусмотреть ряд систем:

контроля затопления помещений;

контроля задымления, наличия в воздухе различных газов;

контроля открытого огня и пожаротушения;

бесперебойного электропитания;

кондиционирования;

резервирования данных;

безопасности локальной вычислительной сети (ЛВС) и вычислительной техники (ВТ);

видеонаблюдения и контроля доступа;

оповещения.

Наиболее актуальны на современном этапе развития средств вычислительной техники вопросы планирования системы климатизации для охлаждения оборудования, осуществления резервного питания, решения вопросов электромагнитной совместимости для обеспечения безопасности ЛВС и ВТ.

При планировании системы климатизации следует учитывать, что быстродействующие серверы и большая плотность размещения превращают серверные шкафы в электронагреватели. В настоящее время существуют следующие способы охлаждения оборудования.

1. При помощи направленных вентиляторов, посредством которых поток воздуха может подаваться чуть ли не за угол, удается добиться мощности охлаждения в 3 кВт – заметное преимущество по сравнению с традиционными 1,5…2 кВт, поскольку традиционные концепции охлаждения оказываются несостоятельными. Однако современное оборудование выделяет гораздо больше тепла: типовой сервер (ультраплоский сервер высотой 4,5 см) вырабатывает уже около 350 Вт тепла, а модульный – еще больше. На небольшой площади серверного помещения можно получить тепловыделение до 15…25 кВт на каждый шкаф.

2. При встраивании в дверь вентиляторов большой мощности можно отводить от 7 до 16 кВт

тепла в зависимости от модели, а шкафы с жидкостным охлаждением справляются с тепловыделением в 25 кВт и более. Но любая жидкость – это дополнительный риск для вычислительного центра. Для снижения этого риска приходится устанавливать датчики влажности, системы мониторинга и даже ванны.

3. Необходимо планировать системы управления микроклиматом, учитывающие не только серверные шкафы, но и освещение, и число сотрудников – ведь человек выделяет в среднем до 100 Вт тепла.

Система управления микроклиматом контролирует параметры воздуха в серверных и аппаратных, строится на основе распределенных сетей управления при наличии центральной станции мониторинга и управления, обеспечивающей дополнительные сервисные функции. Исполнительные контроллеры системы, как правило, размещаются вблизи управляемых устройств и датчиков. По сети они обмениваются информацией с автоматизированным рабочим местом (АРМ) оператора. В случае потери связи с «центром» они могут работать в автономном режиме в соответствии с алгоритмом ранее загруженных программ [4].

В состав системы гарантированного бесперебойного электроснабжения входят источники бесперебойного питания (ИБП), которые поддерживают работу серверов и коммутаторов по крайней мере до тех пор, пока не будут сохранены все данные и корректно остановлены все серверы.

Стратегия защиты питающей сети включает в себя следующие этапы [5].

1. Установка одного (нескольких) ИБП, мощности которых достаточно для питания всего оборудования в текущей конфигурации с учетом перспектив развития сети. Этот ИБП отрабатывает все входные возмущения и пропадание питания. Для бытовых нужд прокладывается отдельная питающая сеть. Капитальные затраты в этом случае высоки.

2. Индивидуальная защита критичных элементов сети локальными ИБП. Капитальные затраты могут быть растянуты во времени, новые ИБП могут приобретаться по мере необходимости. Если индивидуально будут защищены все устройства, то суммарные затраты могут оказаться выше, чем при централизованном варианте.

3. В особо ответственных случаях применяют двухступенчатые схемы: от общего ИБП питается локальный ИБП, нагруженный серверами или коммуникационным оборудованием.

Во всех перечисленных вариантах общую сеть желательно защитить по входу высокочастотным фильтром и ограничителем перенапряжений.

Главный вопрос: где поставить ИБП – в серверном помещении или в отдельной комнате? Если бы в вычислительном центре все оборудование устанавливалось рядом, тогда и мониторинг всех систем, и их защиту было бы осуществлять намного удобнее. Но ИБП также выделяет тепло, которое следует принять в расчет при определении параметров системы климатизации. Если по причинам надежности и отказоустойчивости вычислительного центра система охлаждения подключается к источнику бесперебойного питания, то, чтобы сервер во время длительного отказа не перегревался, ее мощность (а это немалая величина) необходимо учитывать при выборе ИБП.

Систему гарантированного бесперебойного электроснабжения необходимо дополнить *системой удаленного мониторинга и управления электроснабжением.* Система предназначена для защиты информации, хранящейся на серверах и рабочих станциях. В случае длительного пропадания электропитания во входной сети вначале корректно закрываются приложения, работающие на станциях, затем – на серверах. Таким образом, сеть закрывается без сбоев и потерь информации.

Оценка электромагнитной обстановки

В стандарте TIA/EIA-942 значительное внимание уделяется электрике. На смену канала с тремя разъемами пришла модель с четырьмя разъемами. Усложнена топология магистралей. Допускается комбинация централизованной и иерархической архитектуры. Определены четыре уровня электромагнитной совместимости. Исключены системы с волновым сопротивлением 150 Ом и альтернативные типы среды передачи. Кабели и разъемы с волновым сопротивлением 120 Ом предусмотрены только для систем класса С и ниже.

Одной из основных проблем при внедрении современной цифровой аппаратуры, входящей в состав высокоскоростных систем передачи, является обеспечение электромагнитной совместимости аппаратуры с электромагнитной обстановкой (ЭМО) на самом объекте. Подавляющее большинство технических объектов проектировалось задолго до массового распространения цифровой аппаратуры и, следовательно, без должной проработки вопросов ЭМС.

На функционирование цифрового оборудования влияют следующие факторы:

нахождение на небольшом расстоянии от цифрового оборудования аппаратов и конструкций, способных нести значительные токи и потенциалы, а также создавать электромагнитные поля высокой напряженности;

отклонение от проекта в ходе его реализации;

старение заземляющего устройства (ЗУ), различных металлических конструкций и т. п.;

проведенные модернизации предприятия и т. п.

Если оборудование располагается в офисных помещениях или в обычных отдельно стоящих зданиях, где уровни помех значительно ниже, чем непосредственно на самих предприятиях, то даже в этом случае отдельные виды помех могут достигать очень больших значений:

«грозовые» импульсы, амплитуда которых в обычной сети питания может достигать нескольких киловольт;

силовые питающие линии метрополитена;

подземные кабельные коммуникации;

работа радиостанций;

электростатические разряды;

помехи, вызванные работой строительных инструментов, лифтовых и других электродвигателей, нагревательных приборов, мощной копировальной техники.

В результате уровни помех на многих объектах часто превосходят уровни устойчивости аппаратуры. Оценка ЭМО на действующих объектах производится обычно путем проведения натурных испытаний и измерений, которые включают в себя следующее:

100%-ный контроль сопротивлений оснований электрооборудования и конструкций, присоединенных к ЗУ;

измерение сопротивления растеканию ЗУ в целом;

расчетно-экспериментальную оценку потенциалов на элементах ЗУ и помех во вторичных кабелях при коротких замыканиях и грозовых разрядах;

измерение помех во вторичных цепях при коммутационных операциях;

оценку уровней импульсных и постоянно действующих полей в широком диапазоне частот.

По результатам оценки производится разработка и реализация комплекса защитных мероприятий, направленных на приведение ЭМО в соответствие с требованиями цифровой аппаратуры. Эти мероприятия включают в себя:

улучшение состояния ЗУ путем прокладки дополнительных заземлителей и восстановление нарушенных связей;

защита цепей вторичных кабелей путем экранирования;

изменение схем заземления элементов грозозащиты;

прокладка «барьерных» заземлителей;

изменение способа и трасс прокладки на отдельных участках и т.п.;

оптимальное (по условиям ЭМС) размещение микропроцессорной аппаратуры, рабочих мест обслуживающего персонала и кабелей межмашинного обмена; правильную организацию заземления и питания цифровой аппаратуры.

Стандартизация при внедрении информационных систем

Одна из основных задач информационной системы – обработка данных. Стандарт ANSI/EIA/TIA-942 обобщает многолетний опыт создания центров обработки данных. Следование его рекомендациям позволяет максимально приблизиться к уровню надежности с пятью девятками – 99,999%. На рис. 4 показана базовая топология информационной системы для обработки данных.

Распределение оборудования по нескольким модулям позволяет повысить его физическую защищенность, а, следовательно, и надежность предоставляемого сервиса. Модульный подход способствует экономичному использованию ресурсов электроснабжения, кондиционирования, климат-контроля, позволяет сократить вложения в дорогостоящие антистатические фальшполы, а также обеспечивает масштабируемость инфраструктуры ИС без значительных начальных вложений в инфраструктуру.

При участии координатора в управлении ИС необходимо учитывать факторы, влияющие на эффективность, качество, точность, скорость, надежность действий координатора, а также проанализировать процессы переработки информации человеком, ее хранения и принятия решения, психологических механизмов регуляции деятельности координатора. Информация о состоянии системы должна быть представлена в удобной форме. Например, информацию об отказе некоторого элемента сети можно представить в световой или/и звуковой форме. Работы, направленные на устранение отказа, могут быть различной степени сложности, а начало восстановительных работ может быть для различных отказов неодинаково. Также необходимо продумать сигнализацию о предотказовом состоянии элемента системы [6].

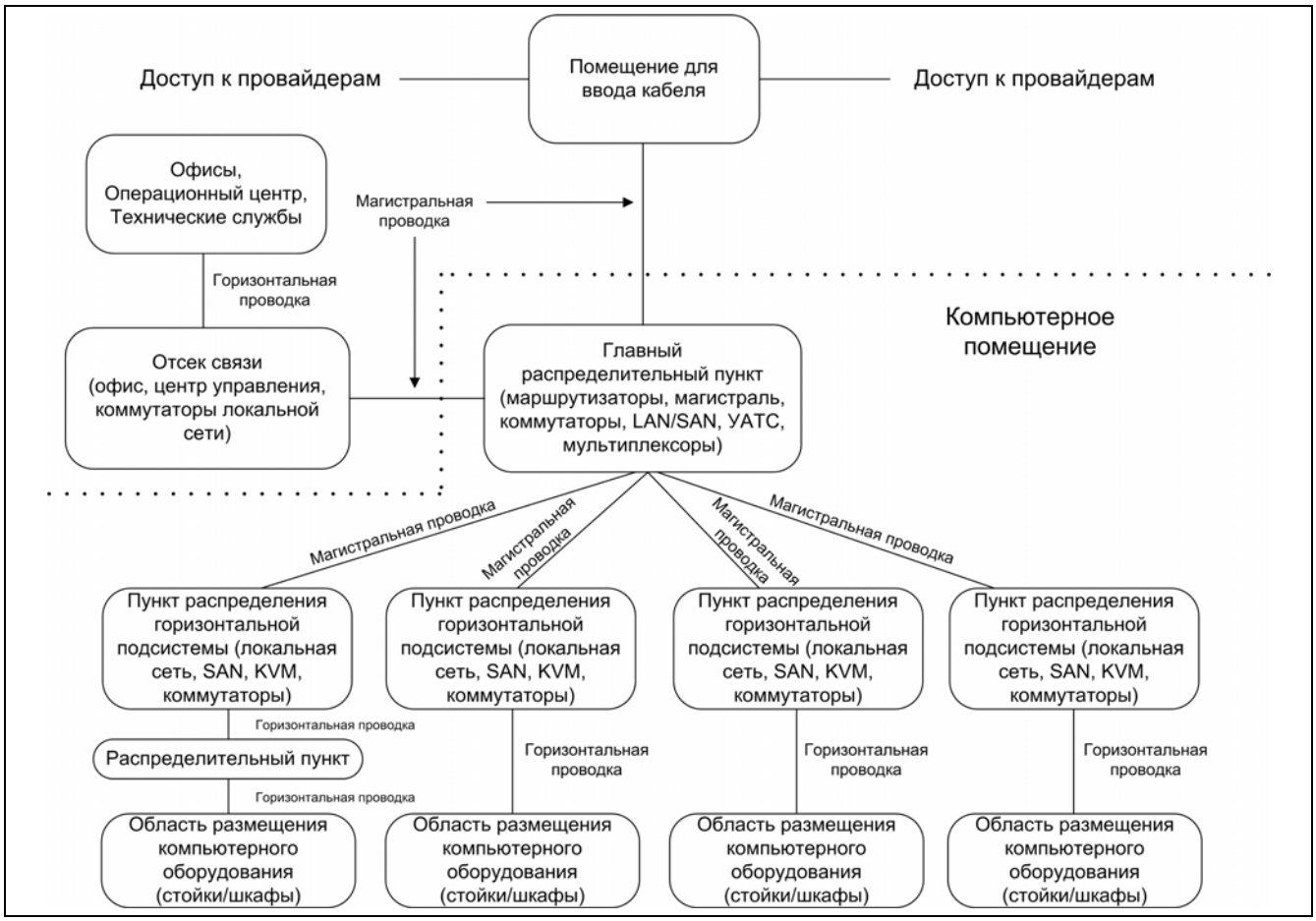

Рис. 4. Базовая топология информационных систем для обработки данных

Таким образом, для обеспечения непрерывности аварийного планирования должны быть проведены следующие мероприятия:

проектирование и монтаж кабельных систем для электротехнических комплексов должно осуществляться в соответствии с требованиями международных организаций по стандартизации;

децентрализация и резервирование функций центральных элементов управления;

переход к многоуровневой распределенной клиент-серверной обработке данных;

разработка плана аварийного восстановления;

планирование системы климатизации для охлаждения оборудования в аппаратных помещениях;

обеспечение бесперебойного электропитания;

решение вопросов электромагнитной совместимости цифрового оборудования;

распределение оборудования по нескольким модулям;

учет влияния человеческого фактора при определении надежности любой системы, разработка удобных средств пользовательского интерфейса измерительных и диагностических приборов, позволяющих повысить надежность действий человека-координатора.

ЛИТЕРАТУРА

1. Telecommunications Infrastructure Standard for Data Centers TIA/EIA-942 – http://zeus.sai.msu.ru
2. *Бройдо В.Л.* Вычислительные системы, сети и телекоммуникации. М. – СПб.: ПИТЕР, 2003.
3. Аварийное планирование в центрах данных. – LAN, 2006, №7, с. 42–48.
4. *Артюшенко В.М., Шелуин Д.О.* Повышение энергоэффективности инженерных систем интеллектуальных зданий // XI-я Междунар. научн.-практ. конф. Секция «Применение информационных технологий в электротехнических комплексах и системах». – М.: МГУС, 2006, с. 30–36.
5. *Гук М.* Аппаратные средства локальных сетей. Энциклопедия. – СПб.: ПИТЕР, 2002.
6. *Аббасова Т.С.* Оптимальная стратегия восстановления каналов связи территориально-распределенных систем управления // XI-я Международная научн.-практ. конф. Секция «Применение информационных технологий в электротехнических комплексах и системах». – М.: МГУС, 2006, с. 74 –79.

Поступила 10. 05. 2007