

В последнее время в связи с большим распространением электронного оборудования, бурным развитием сетевых технологий, электронной коммерции и ежегодному росту денежного оборота в этой сфере, все большее число компаний на рынке признают, что финансовые и имидживые потери от сбоев в работе компьютерного оборудования становятся настолько ощутимыми и что вопрос обеспечения их безаварийной работы становится одним из наиболее приоритетных.

Возникает резонный вопрос, а что именно необходимо предпринять и какие технические решения воплотить в жизнь, чтобы обеспечить должный уровень работоспособности и помехоустойчивости устройств. В нашей стране, из-за стремительного внедрения информационных технологий практически во все сферы бизнеса, персонал обслуживающий инженерные системы зданий оказался не готов к столь быстрому изменению ситуации, поэтому довольно быстро были найдены «простые решения» возникающих проблем. Происходит повсеместное внедрение **источников бесперебойного питания (UPS)**

, кроме того выполняются работы по разработке и монтажу «чистой системы заземления» для компьютерного и сетевого оборудования. К сожалению, подобные технические мероприятия не только не решают возложенные на них задачи, но в большинстве случаев приводят к обратному эффекту. Иными словами, позаимствованные российскими специалистами у зарубежных коллег технические решения, являются необходимыми, но далеко не достаточными, и поэтому зачастую оказываются не только ошибочными, с точки зрения безаварийной работы, но и опасными (с точки зрения обеспечения электро- и пожаробезопасности).

## Мифы об UPS

Основное заблуждение по поводу установки **источников бесперебойного питания** сводится к концепции, которую проповедуют большинство российских компаний, предлагающих подобные и смежные им устройства на рынке. В целом эта концепция сводится к утверждению, что UPS «спасает» от всех существующих и возможных будущих проблем в системе электроснабжения. В связи с этим необходимо напомнить, что несмотря на постоянное техническое совершенствование выпускаемых устройств,

основная функция источников бесперебойного питания заключается в защите оборудования от длительных перерывов в электроснабжении. В тоже время, основная задача, которая ставится перед системами бесперебойного питания – это результирующая надежность, которая подразумевает: гарантию сохранности данных, сохранности оборудования, а также гарантию защиты от простоев в работе.

Практика обследования систем бесперебойного электропитания ряда офисных зданий, а также международные стандарты и нормативная документация по этой тематике (IEEE, ANSI, IEC) показывают, что для воплощения всех поставленных задач необходимо провести полномасштабное обследование системы электроснабжения здания. Кроме обязательных стандартных проверок: сопротивления изоляции, сопротивления петли фаза-ноль, проверки работоспособности автоматических выключателей, необходимо обследовать электроустановку здания на предмет наличия ошибок в выполнении системы заземления (что приводит к возникновению токов утечки), а также выполнить длительный мониторинг напряжений и токов, проанализировать существующую систему молниезащиты и систему защиты от грозовых и коммутационных перенапряжений.

Для чего это нужно? Во-первых, наличие токов утечки в системе электроснабжения здания приводит к искажению изображения на видеомониторах компьютеров, сбоям в работе оборудования и потере информации при передаче данных по сети. Во-вторых, неправильно выполненная система молниезащиты и система защиты от перенапряжений при определенном стечении обстоятельств (в результате прямого и/или удаленного удара молнии) почти гарантированно приведет к физическому выходу из строя электронного оборудования.

В нашей практике имел место случай, когда источник бесперебойного питания, установленный в офисном здании и питающий группу ответственных электропотребителей часто и необоснованно переходил на питание от аккумуляторных батарей. Длительный мониторинг питающего UPS напряжения не показал каких-либо значительных отклонений от нормы. Кроме того, было проведено обследование систем защитного зануления и заземления.

В ходе проверки были выявлены грубые ошибки в выполнении вышеуказанных систем, после их устранения и приведения в соответствие с требованиями отечественной и международной нормативной документации количество частых переключений источников бесперебойного питания на аккумуляторные батареи резко снизилось. Исходя из этого, можно сделать вывод о высокой чувствительности современных UPS средней и большой мощности к повышенному и изменяющемуся напряжению между системами рабочего и защитного заземления.

Поскольку все вышеизложенные факторы прямо или косвенно влияют на предъявляемую ко всем электронным системам и оборудованию надежность, можно утверждать, что только после выполнения всего комплекса технических мероприятий целесообразно разрабатывать систему бесперебойного питания и принимать решение об установке тех или иных типов UPS в зависимости от характера и мощности установленных нагрузок здания, а также в соответствии с обеспечением необходимого

уровня надежности.

### Мифы о заземлении

В отличие от систем бесперебойного электропитания, применение которых является дополнительным средством обеспечения надежности, заземление прежде всего выполняет функции защиты людей от поражения электрическим током, а также обеспечивает пожаробезопасность зданий и сооружений. Сейчас все чаще выдвигаются предположения, что для нормального функционирования компьютерной техники, информационных сетей и систем связи необходимо применять отдельное, «чистое» заземление, изолированное от общей системы защитного заземления здания. Однако реализация этих решений является не только ошибочной и приводящей к выходу из строя электронных устройств, но в ряде случаев и опасной для здоровья и жизни людей.

Для того, чтобы развеять этот миф, рассмотрим простую ситуацию. Допустим что для заземления компьютерной техники в каком-либо помещении была выполнена «чистая» система заземления, т.е. все металлические корпуса компьютерной техники, сетевых и прочих устройств присоединены к выделенному контуру заземления не связанному с системой защитного заземления здания.

Путь тока при коротком замыкании (КЗ) между фазным проводником, питающим компьютер и его корпусом, возникающее вследствие пробоя конденсатора в сетевом фильтре на входе в устройство. Обратный путь тока КЗ будет проходить через два контура: общий контур защитного заземления здания (ТП) и «компьютерное заземление». Сопротивление контура заземления трансформаторной подстанции (ТП) обычно составляет не более 4 Ом, сопротивление «чистого» заземления составляет порядка 10 Ом.

Тока будет не достаточно для срабатывания автоматического выключателя, установленного на поврежденной линии. Если на линии установлен автоматический выключатель с номинальным током 16 А, то для быстрого отключения тока короткого замыкания должен сработать электромагнитный расцепитель, величина уставки которого находится в пределах от 45 до 100 А и более.

Следовательно, при протекании тока величиной 15,7 А устройство защиты просто «не поймет», что протекающий по нему ток является результатом аварийной ситуации в системе электроснабжения и не отключит поврежденную линию. При прикосновении к

корпусу такого электрооборудования люди попадают под напряжение, кроме того небольшие по сечению соединительные провода и интерфейсные элементы оборудования будут интенсивно нагреваться. Нагрев происходит из-за разности потенциалов между корпусом и экранами сетевых кабелей, таким образом по ним будет протекать ток, что может привести к выходу их из строя и возгоранию.

Поражение электрическим током зависит от множества факторов (состояние нервной системы, состояние кожи и т.д.), тем не менее очевидно, что при неотпускающем токе 20-30мА, протекающий через тело человека ток в 155мА – смертелен.

В то же время, существуют методы выполнения заземления, которые соответствуют всем нормам, являются безопасными и уменьшают разности потенциалов между корпусами электронного оборудования и близко расположенными заземленными объектами, а также обеспечивают стабильную работу оборудования. Главная идея заключается в том, что все заземляемые части оборудования, нулевые защитные проводники, металлические трубопроводы коммуникаций, металлические части каркаса здания, металлические части централизованных систем вентиляции и кондиционирования, заземляющие устройства системы молниезащиты, заземляющие проводники рабочего заземления, металлические оболочки телекоммуникационных и сетевых кабелей должны быть объединены в основную систему уравнивания потенциалов.

Для соединения с основной системой уравнивания потенциалов все указанные части должны быть присоединены к главной заземляющей шине.

### **Безопасная система заземления**

Это соглашение минимизирует помехи, возникающие от протекания токов по системе заземления в аварийных режимах, обеспечивая тем самым надежное функционирование оборудования и безопасность людей. В этом случае по поврежденной линии будет протекать существенно больший ток (определяемый сопротивлением петли фаза-нуль), что позволит электромагнитному расцепителю автоматического выключателя быстро отключить поврежденную линию, а ток, протекающий это короткое время по системе заземления, равномерно растечется и не вызовет появления помех благодаря наличию системы уравнивания потенциалов.

Необходимо напомнить, что по системе заземления в нормальном режиме работы не должно протекать никаких токов. Тем не менее, имеются несколько источников вероятного появления помех в системе заземления, это перенапряжения, вызванные прямыми и/или удаленными ударами молнии, а также коммутациями в системе

электроснабжения, кроме того могут возникать повреждения в измерительных цепях и цепях релейной защиты и автоматики. Не стоит также недооценивать токи утечки на металлоконструкции и трубопроводы здания.

Если компьютер находится в помещении, по стенам, за потолком или под полом которого проходят кабельные линии с токами утечки, вызывающие повышенный уровень магнитного поля, то изображение на мониторе может заметно искажаться («плыть» или «дрожать»). Известны случаи, когда картинка покрывается цветными пятнами различных оттенков, а иногда изображение полностью или частично пропадает на несколько секунд, и появляется вновь. Естественно, работать за таким монитором невозможно и вредно.

Протекание токов по системе РЕ здания, а значит и по защитным экранам интерфейсных и сетевых кабелей компьютеров может вызывать сбои и «зависания» компьютерных сетей и невозможность нормальной работы другого офисного и электронного оборудования. Подобные проблемы возникают из-за изменения потенциала в системе защитного заземления, которая в свою очередь является системой опорного потенциала для компьютерной техники. Кроме того, перенапряжения, вызванные прямыми и/или удаленными ударами молний, а также коммутациями в системе электроснабжения, могут инициировать помехи протекающие по системе опорного потенциала здания, эти помехи имеют разную частоту (от единиц Гц до десятков МГц) и в связи с этим в системе заземления, выполненной по одноточечному принципу могут протекать значительные помехи, вызванные резонансными явлениями в защитных проводниках.

Для подавления высокочастотных помех основную систему защитного заземления можно дополнять установкой рабочего (функционального) заземления. Однако необходимо помнить, что функциональное заземление служит только для обеспечения работы оборудования, но ни в коем случае не для обеспечения электробезопасности. Поэтому использовать рабочее заземление в качестве единственной системы заземления категорически запрещается.

Автор: Петухов В.С., Соколов В.А., Красилов И.А.  
Источник: Tesla.ru