

# СИСТЕМЫ ЗАЩИТЫ ОТ ИМПУЛЬСНЫХ ПЕРЕНАПРЯЖЕНИЙ В АППАРАТУРЕ ПЕРЕДАЧИ ДАННЫХ

Федоринов О.В., менеджер продукта Концерна "Энергопром".

*До недавнего времени во-просам электромагнитной совместимости (ЭМС) и проблемам перенапряжения не уделялось достаточного внимания. Такая ситуация была характерна не только для нашей страны, но и для тех стран, где автоматизация процессов как на производстве, так и в остальных сферах деятельности (общественные и правительственные организации, банки, биржи и прочие финансовые институты и т.п.) уже давно стала нормой.*

*Во-первых, насыщенность компьютерной и микропроцессорной техникой стала лавинообразно нарастать только в последние двадцать лет.*

*Во-вторых, зависимость как надежности технологических процессов, так и надежности работы финансовых структур от точности и своевременности передачи данных стала существенно выше, чем до широкомасштабного внедрения компьютеров и электронного обмена данными в режиме реального времени. После серии массовых сбоев в банковских системах, произошедших из-за воздействия помех в середине 80-х и приведших к крупным потерям, к разработке комплекса защитных мер были подключены ведущие мировые разработчики.*

Это и привело к появлению директивы 336ЕС 89, которая обязала страны Европейского сообщества ввести единые стандарты по электромагнитной совместимости и разработать систему сертификации. В настоящий момент проблема достаточно хорошо изучена и выпущено много нормативных документов регламентирующих требования к оборудованию с точки зрения ЭМС. В результате с 1996 года в Европе не допускается продажа технических средств без сертификата соответствия стандартам по электромагнитной совместимости.

В России до начала 2001 года обязательной сертификации по ЭМС подлежало электротехническое и электронное оборудование, включенное в соответствующий реестр. Теперь Россия приблизилась к Европе и ввела свою систему стандартов и сертификации. С введением новых стандартов практически вся электротехническая продукция подпадает под обязательную сертификацию по ЭМС. Базовые стандарты на устойчивость к помехам соответствуют МЭК 61000-4.

Основным документом в России по вопросам ЭМС является федеральный закон "О государственном регулировании в области обеспечения электромагнитной совместимости технических средств" (принят Государственной Думой 1 декабря 1999 года).

Кроме этого выпущены и вступили в силу ГОСТы по ЭМС (по большей части разработанные на основе международных и европейских норм), в том числе и по защите от перенапряжения (серия ГОСТ Р 50571...-2000).

Прежде чем заняться изучением вопроса защиты от импульсов перенапряжения, необходимо разоб- раться с природой их

возникновения и возможными последствиями от их воздействия.

## Последствия

Самыми разрушительными последствиями обладают импульсы перенапряжения, возникающие в результате прямого попадания молнии в защищаемый объект. Причем наличие на здании молниезащиты не спасает аппаратуру, находящуюся в здании, от проблем с перенапряжением.

Амплитуда этих импульсов может достигать десятков и сотен киловольт.

Такая энергия способна разрушить не только чувствительные входные сигнальные цепи оборудования, но и силовые цепи (блоки питания) и даже конструкцию здания (правда, такое возможно только в случае грубых просчетов при проектировании молниезащиты).

При прямом попадании молнии в защищаемое здание (рассматриваем только случаи попадания молнии в систему молниезащиты) основными являются три пути возникновения перенапряжения:

1. Повышение потенциала на потенциаловывравнивающем электроде за счет тока молнии, текущего через сопротивление заземления. Основная идея понятна из рисунка 3, а далее вступает в силу закон Ома. Ток в стволе молнии может достигать 200 кА, для простоты расчета возьмем



Рис. 1. Разрушения конструкции здания

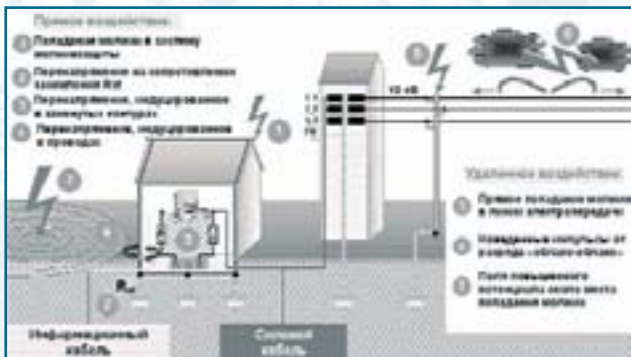


Рис. 2. Возможные способы возникновения импульсов перенапряжения

100 кА, сопротивление заземления возьмем 1 Ом (реально может достигать 30 и выше Ом, следовательно, амплитуда импульса составит 100 кВ (!).

2. Индуцирование импульсов в проводниках, проложенных в непосредственной близости от токопроводящих элементов молниеотвода. Расчеты приводить не будем, сообщим результат - амплитуда импульсов 0,5-2,0 кВ.
3. Индуцирование импульсов в замкнутых контурах, образованных цепями передачи энергии, передачи данных и линиями заземления.

2. Индуцирование импульсов в замкнутых контурах, образованных цепями передачи энергии, передачи данных и линиями заземления.
3. Индуцирование импульсов во всех токопроводящих элементах в защищаемом объ-

екте.

Проведенные исследования показали, что разряд молнии на расстоянии 1 км индуцирует в проводнике длиной 1 м импульс с амплитудой 200 В.

К данной группе можно отнести еще один способ распространения импульсов - перенос перенапряже-

ния от здания, в которое попала молния, к близлежащим зданиям по общим линиям передачи электроэнергии, информации и общим коммуникациям (водопровод, отопление, газопровод, канализация и т.п.).

Не менее опасны последствия импульсов перенапряжения, возникающих в результате коммутационных процессов (включение и выключение мощных потребителей электроэнергии, работа оборудования с большим уровнем помех, передаваемых в питающую сеть и т.п.).

Амплитуда этих импульсов перенапряжения достигает единиц киловольт.

К чему приводит воздействие импульсов перенапряжения? Во-первых, это разрушение входных цепей (как на платах, так и в корпусах микросхем).

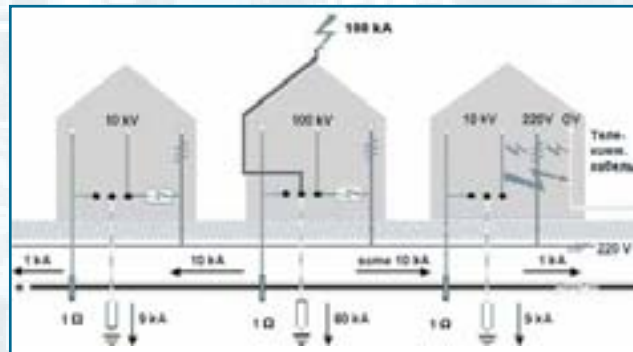


Рис. 4. Перенос импульса перенапряжения между зданиями

Во-вторых, сбои и ложные срабатывания в работе оборудования.

В-третьих, износ полупроводниковых приборов. При прохождении импульса через р-п переход происходит изменение геометрии перехода и перераспределение неосновных носителей. В результате данный полупроводниковый прибор изменяет свои параметры и схема, собранная на этом приборе, работает уже не в том режиме, который планировался при ее разработке. Это, пожалуй, одно из наиболее опасных последствий воздействия импульсов перенапряжения, так как

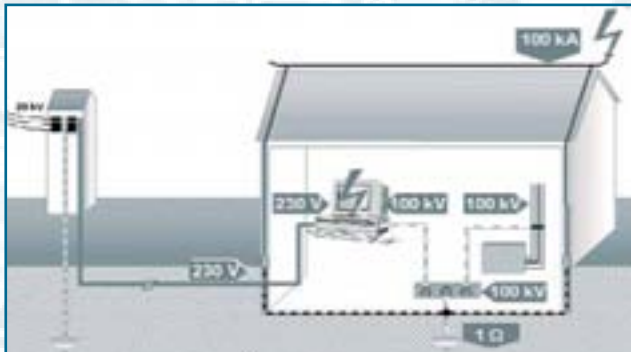


Рис. 3. Повышение потенциала на сопротивлении заземления

Амплитуда импульсов для этого случая также составляет от 0,5 до 2,0 кВ.

Вторая крупная группа причин возникновения перенапряжения - это разряд молнии на некотором удалении от защищаемого объекта. Здесь также можно рассмотреть три основных пути распространения импульсов перенапряжения:

1. Прямое попадание молнии в линии электропередач (передачи данных) или наведение импульса на этих линиях за счет близкого разряда молнии. Здесь нужно иметь в виду, что, несмотря на наличие на пути

ния от здания, в которое попала молния, к близлежащим зданиям по общим линиям передачи электроэнергии, информации и общим коммуникациям (водопровод, отопление, газопровод, канализация и т.п.).

Не менее опасны последствия импульсов перенапряжения, возник-

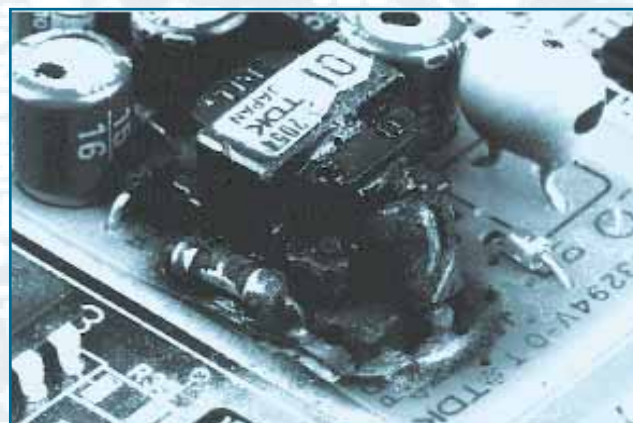


Рис. 5. Разрушения на плате

может проявляться через длительное время после воздействия импульса и очень трудно определить истинную причину сбоя или поломки.

## Способы защиты

До недавнего времени основным способом защиты от импульсов перенапряжения было использование в защищаемой цепи фильтров низкой частоты (ФНЧ). Этот способ имеет два основных недостатка: во-первых, ФНЧ представляет собой дифференцирующую цепочку и, соответственно, уменьшая по амплитуде импульс, он увеличивает его длительность, тем самым энергия импульса остается без изменения; во-вторых, данное решение невозможно использовать в цепях передачи данных из-за искажения формы сигнала.

Современные системы защиты от импульсов перенапряжения построены на различных разрядниках, именуемых в зависимости от их предназначения или гродозащитными разрядниками (ГЗР) или устройствами защиты от перенапряжения (УЗП).

В основу системы положены два главных принципа - это разбиение защищаемого объекта на гродозащитные зоны (ГЗЗ) и принцип выравнивания потенциалов.

Для определения места установки защитных устройств защищаемый объект делится на ГЗЗ. Различают четыре ГЗЗ.

**ГЗЗ 0** - это пространство, окружающее защищаемый объект. В этой зоне возможно прямое попадание молнии и все проводники, находящиеся в ней, не защищены конструкцией здания от наведенных импульсов. Различают два подвида этой зоны: ГЗЗ 0а и ГЗЗ 0б. Различие заключается в том, что в ГЗЗ 0б вероятность прямого попадания молнии практически равна нулю (зона, защищенная молниеотводом).

**ГЗЗ 1** - все внутреннее пространство защищаемого объекта. В этой зоне прямое попадание молнии невозможно и электромаг-



Рис. 6. Разрушения в микросхеме

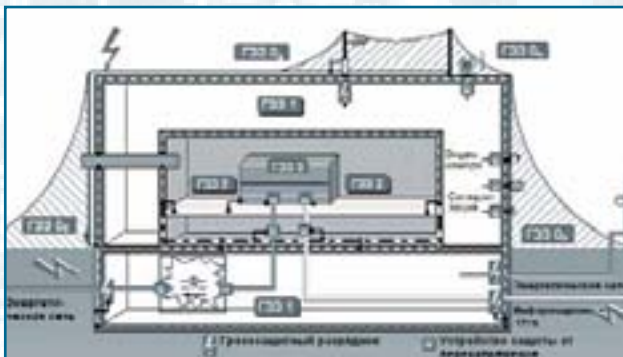


Рис. 7. Принцип разбиения на гродозащитные зоны

нитные поля, вызванные разрядом молнии, существенно ослаблены конструкцией здания.

**ГЗЗ 2** - специально выделенная область внутри здания с повышенными требованиями надежности защиты (например, компьютерный зал).

**ГЗЗ 3** - собственно защищаемый прибор (например, сервер).

На границах этих зон устанавливаются соответствующие ГЗР (граница зон 0 и 1) и УЗП (границы зон 1 и 2 и зон 2 и 3).

Такое разбиение позволяет, во-первых, четко определить количество и места установки УЗП, во-вторых, подобрать УЗП соответствующие возможному уровню перенапряжений в данной зоне, в-третьих, распределить систему по всему объекту и тем самым обеспечить защиту от импульсов, возникающих внутри самого объекта.

Другой основной принцип - принцип выравнивания потенциалов. Разрушения от импульсов перенапряжения происходят от возникновения опасных разностей потенциалов между различными токоведущими элементами оборудования и здания. Если обеспечить равенство потенциалов ВСЕХ (!) токоведущих элементов здания (в идеале приравнять его к нулю относительно заземления), то не будет и разрушений.

Для систем заземления, элементов конструкции здания, систем водопровода, канализации и т.п. эта задача решается относительно просто - **все токоведущие элементы должны иметь надежную гальваническую связь с потенциаловыравнивающей шиной.**

Для линий передачи электроэнергии и линий передачи информации такой подход неприемлем. Для этих линий применяют соединение с потенциаловыравнивающей шиной через вентильные устройства (ГЗР и УЗП). В штатном режиме эти устройства не оказывают никакого влияния на передаваемый сигнал. В случае превышения определенного порога срабатывания (возникновение импульса перенапряжения) сопротивление УЗП резко снижается и обеспечивает выравнивание потенциала.

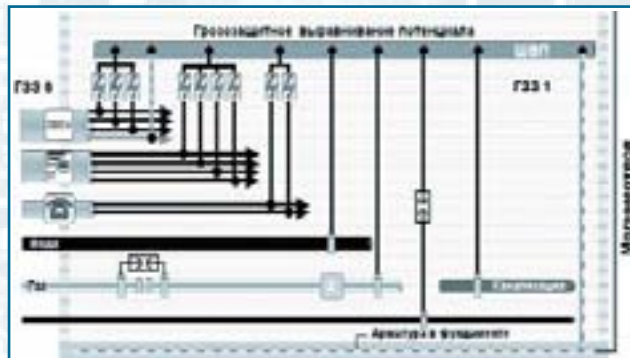


Рис. 8. Принцип выравнивания потенциала

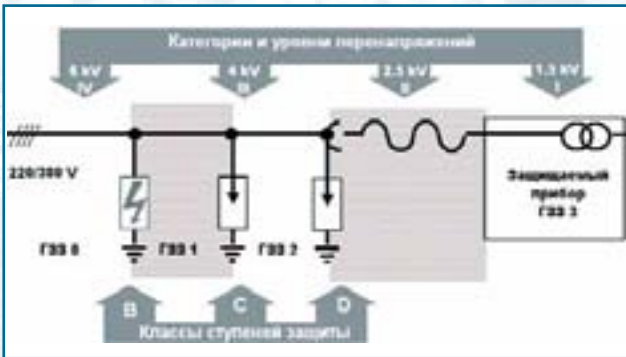


Рис. 9. Принцип выравнивания потенциала

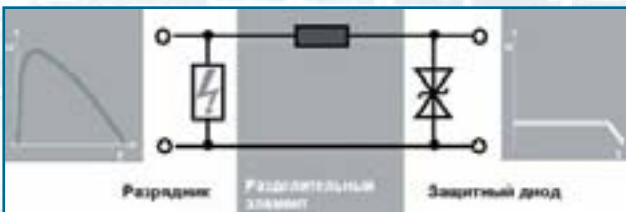


Рис. 10. Типичная схема УЗП для информационных цепей

### Построение системы защиты от перенапряжения в силовых цепях

Для силовых цепей используется трехступенчатая система защиты. На границах зон 0, 1, 2 и 3 устанавливаются соответственно разрядники классов В, С и D (разрядник класса А предназначен для установки в высоковольтной части линии передачи электроэнергии). Практически это обычно выглядит следующим образом: в вводной щит устанавливается ГЗР (класс В), во вторичный



Рис. 11. УЗП BLITZDUCTOR® фирмы DEHN

щит (распределительный) - УЗП класса С, в непосредственной близости от защищаемого прибора - УЗП класса D.

Все ГЗР и УЗП включаются параллельно нагрузке и поэтому не требуют внесения радикальных изменений в существующую схему разводки щитов. Кроме того, так как данные устройства подключены параллельно, то они не зависят от тока (не зависят от потребляемой мощности).

Построение системы защиты от

перенапряжения в информационных цепях.

Основные принципы как для силовых, так и для информационных цепей остаются одинаковыми. Единственное различие - чаще всего в информационных цепях устанавливают два УЗП - на границе ГЗЗ 0 и 1 и на границе ГЗЗ 2 и 3, но сами эти УЗП имеют в своем составе две ступени.

Учитывая большое количество различных интерфейсов и способов передачи данных, ассортимент УЗП для информационных цепей очень разнообразен. Есть, конечно, унифицированные УЗП (например, BLITZDUCTOR® фирмы DEHN), но большинство УЗП все же разрабатываются и подбираются для конкретных применений.

Защитные элементы в УЗП включаются параллельно нагрузке и поэтому не оказывают никакого влияния на передаваемый сигнал (затухание, вносимое УЗП, в большинстве случаев равно нулю либо не превышает 0,2 dB).

### Оптимизация системы защиты от импульсов перенапряжения

Для построения оптимальной для данного объекта системы защиты необходимо провести комплексное исследование на предмет возможных путей растекания токов молнии и возможных взаимовлияний проводников. Но, используя основные принципы построения системы защиты, можно выстроить достаточно надежный комплекс.

В первую очередь необходимо помнить, что в защите информационных цепей одним из наиболее важных вопросов остается защита силовой цепи питания прибора. Это связано с тем, что, при возникновении перенапряжения в силовой части, разрушения обязательно коснутся информационных входов (если общий потенциал прибора повысится на несколько киловольт, то произойдет пробой именно в информа-

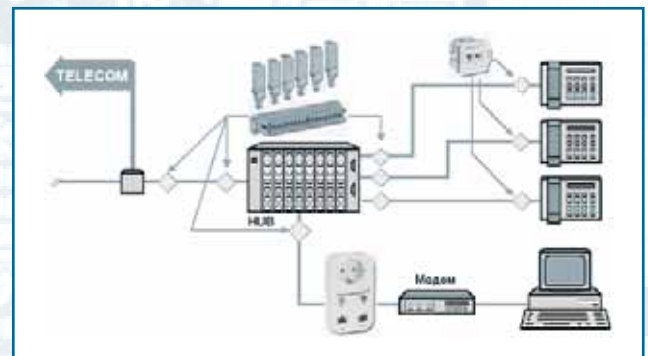


Рис. 12. Пример защиты офисной АТС

ционных входных цепях).

К сожалению, рамки журнальной статьи не позволяют подробно рассмотреть особенности защиты каждого вида интерфейса, но общий подход для всех систем остается одинаковым.

При построении полной и комплексной системы защиты обеспечивается высокая помехозащищенность и надежность работы оборудования. Стоимость такой комплексной системы получается достаточно высокой, но соотносить ее нужно не со стоимостью защищаемого оборудования, а со стоимостью тех процессов, которыми это оборудование управляет. В таком случае необходимость и целесообразность таких систем становится очевидной.