АВАРИИ НА ОБЪЕКТАХ СВЯЗИ

причина – опасные электромагнитные влияния

Д.Терентьев

Опасные электромагнитные влияния – основная причина аварий на телекоммуникационных узлах и в системах связи в целом. Стойкость к опасным перенапряжениям и помехам – это важнейший фактор надежности работы как систем передачи информации, так и обслуживаемых ими промышленных и социальных объектов. Длительное времена автор занимался проблемами защиты от перенапряжений и электромагнитной совместимости. В ходе работы приходилось как анализировать причины, приведшие к повреждению оборудования и линий связи и пожарам, так и разрабатывать мероприятия и специальное оборудование для предотвращения аварий и нарушений качества связи из-за воздействия электромагнитных влияний. Накопленный опыт позволил системно исследовать проблему, результаты этой работы и рассматриваются в серии публикаций.

В последние годы интенсивность техногенных катастроф в нашей стране возросла настолько, что известия о падении самолета, пожаре с множеством жертв, крупной аварии на объектах энергетики стали едва ли не привычными. Даже поверхностного изучения информации об этих событиях было достаточно, чтобы увидеть, что между ними много общего, а различаются, в основном, только технические детали. Очевидно, что развитие, функционирование и нарушения в работе сложных технических систем должны подчиняться каким-то общим закономерностям.

Несколько печатных работ [1–3], написанных специалистами из различных областей техники, помогли взглянуть на проблему с системной точки зрения. Ю.П.Петров к своей книге [4] о техногенных катастрофах использовал подзаголовок "научный детектив". Попробуем и мы рассмотреть с такой точки зрения несколько десятков аварий на объектах связи, дать описание их причин, а также помочь техническим специалистам понять, как предотвратить подобные случаи. Вся информация дана с точки зрения инженера, т.е. излагаются только технические факты и не рассматриваются субъективные факторы – экономические причины, уровень подготовки персонала и мотивы людей, действия которых могли послужить причиной аварии. Основной материал собран в результате работы на телекоммуникационных и промышленных объектах, проведения консультаций и экспертиз, а также получен в ходе общения с коллегами.

Вспомним наиболее крупные аварии на объектах связи и энергетики за последние годы.

ЗАМОСКВОРЕЦКИЙ ТЕЛЕФОННЫЙ УЗЕЛ МГТС

Пожар в здании Замоскворецкого телефонного узла (ул. Щепкина, 51) начался вечером 14 февраля 2003 года. В результате уничтожено или повреждено оборудование АТС 281, 284, 288, 971, включая коммутаторы, цифровые системы передачи, кроссы, кабельные вводы, электропитающие установки. В этом же здании находилось немало оборудования других операторов связи – "ГолденЛайн","Комстар", "ИПБ-Интернет", "Корбина-Телеком", "ТелекомБюро", "МТУ-Интел".

В результате остались без телефонной связи несколько десятков тысяч абонентов МГТС и "Комстар", в той или иной степени авария отразилась на работе всей телефонной сети Москвы. Серьезные проблемы с межстанционной связью возникли у абонентов Северо-Восточного округа столицы, обслуживаемых Останкинским телефонным узлом. Множество квартир и предприятий осталось без доступа в Интернет. От эфира были отключены радиостанции, сигналы которых транслировались в Останкино по каналам компании "ГолденЛайн".

По утверждению МГТС, пожар в здании Замоскворецкого теле-

фонного узла произошел по вине ЗАО "Моспромстрой". В исковом заявлении МГТС говорится [5], что причиной пожара стало "попадание высокого напряжения на оборудование абонентских номеров вследствие возгорания кабеля электропитания, проложенного в штаб строительства фирмы "Континент" ЗАО "Моспромстрой" в зоне строительной площадки". В иске указано, что "причина пожара установлена на основании акта, составленного 15.02.03 с представителем фирмы ЗАО "Моспромстрой", объяснений свидетелей, докладных записок работников телефонного узла".

Через два дня после пожара я видел здание узла. Было заметно, что ведется интенсивная работа по его восстановлению, вокруг валялись куски обгоревшего кабеля. Количество пены на стенах не оставляло сомнения в том, что стойки с оборудованием, которое не было повреждено огнем, были при тушении этой пеной залиты.

АТС 21/22 ХАБАРОВСКОЙ ГТС

6 ноября 2008 года в Хабаровске произошел пожар в пятиэтажном здании АТС городской телефонной станции на Волочаевской улице. Очаг возгорания был обнаружен на третьем этаже, огонь распространился на площадь в 40 м^2 и частично перешел на четвертый этаж. Пожар удалось локализовать и ликвидировать приблизительно через час после сообщения о возгорании. Был поврежден коммутационный узел на 23 тысячи номеров, в результате чего отключились телефонные линии, номера которых начинаются на 20, 21, 22, 27, 29, 30, 39.

Компания "Дальсвязь" получила официальное заключение испытательной пожарной лаборатории по Хабаровскому краю о причинах возгорания телефонного кросса (коммутационный узел, связывающий телефонную станцию и линейную кабельную разводку внутри здания). Эксперты установили причину пожара – попадание высокого напряжения со стороннего электрического кабеля на слаботочные линии. По предварительной версии, это могло произойти из-за неправильной эксплуатации электрической сети в одном из соседних многоквартирных домов [6, 7].

ОСТАНКИНСКАЯ ТЕЛЕБАШНЯ

История создания этого выдающегося достижения науки и техники, созданного по проекту Николая Васильевича Никитина, широко известна [8]. Башня построена, как стебель растения – из клеток, вытянутых в волокна, только роль волокон в ней выполняют 149 пучков стальных канатов диаметром 38 см, заложенных в бетон по всему телу башни.

Создатели башни задали ей фантастические пределы прочности: она в состоянии выдержать восьмибалльное землетрясение по шкале Рихтера, ураганный ветер силой до 44 м/с, колебания вершины с амплитудой до 12 м. В башню ежегодно без всяких последствий ударяет 40–50 молний.

Однако строители башни не предвидели то, что случится в воскресенье 27 августа 2000 года, когда из 149 стальных тросов, стягивающих бетонные кольца, в результате пожара неповрежденными остались всего 29. Хотя башня устояла, потребовалась ее полная реконструкция, и среди специалистов нет единодушного мнения, что же следует с ней делать – продолжать эксплуатировать или все-таки, не дожидаясь падения, разобрать – так как высокая температура привела к разрушению связи между металлом и бетоном и образованию трещин, по которым к арматуре попадет влага.

В результате катастрофы погибли три человека (в рухнувшем с двухсотметровой высоты лифте). Полностью разрушено лифтовое хозяйство, повреждены системы электроснабжения, вентиляции, кондиционирования, тепло- и водоснабжения, связи и сигнализации. Было прервано вещание на Москву и Московскую область, нарушена работа систем связи.

Вот краткая хронология пожара. Возгорание началось 27 августа 2000 года около 15 ч на высоте 320–350 м. Вначале из башни показались клубы густого дыма. Затем один за другим стали отключаться телевизионные каналы. К 20.00 становится очевидно, что огонь, несмотря на все усилия пожарных, погасить не удается. Пламя, раздуваемое словно в гигантской печной трубе, опускается все ниже. Пожару присвоена 5-я категория сложности.

В 21.00 уже горят ресторан и смотровая площадка. Пожарные пешком на трехсотметровую высоту заносят огнетушители. В 22.00 из башни начинают вырываться языки пламени. Огонь опускается до отметки 280 м. В 24.00 предпринимается очередная попытка остановить огонь. На высоте 200 м перерубаются кабели, а все пространство заполняется огнеупорными материалами. Безрезультатно: огонь медленно ползет вниз. Все это время продолжают падать скоростные лифты.

Горит Останкинская телебашня

К 4 часам утра 28 августа пожарные работают уже на высоте 150 м. К 6 утра огонь разгорается с новой силой, доходя уже практически до земли – до конического основания высотой 63 м. Пожарные начинают использовать воду. К 12 часам дня пламя удается остановить, а затем и потеснить вверх. К 14 часам тушение идет на высоте 300 м, в 17 часов объявлено, что пожар полностью потушен.

По официальной версии, "причиной возгорания Останкинской башни стало значительное превышение нагрузки на фидеры – кабели, передающие сигнал высокой мощности от аппаратуры к антенне". Начальник управления госу-

дарственной противопожарной службы ГУВД Москвы Л.Коротчик заявил на пресс-конференции 30 августа, что башня была "рассчитана на значительно меньшую нагрузку, чем та, которой она подвергалась в последние годы". В последнее время на башне было дополнительно установлено оборудование около 20 объектов радиотелефонной, пейджинговой и космической связи. Пожарный уверен, что это была "погоня за деньгами", которая привела к пренебрежению правилами противопожарной безопасности.

Интенсивное горение фидерных кабелей, имевших горючие полиэтиленовые оболочки, отмечали все участники тушения. При этом падающие вниз капли полиэтилена создавали на различных высотах вторичные очаги горения. При температуре около 1000°C вниз полетели и горящие фрагменты разрушающихся фидеров. Попытки пожарных поставить преграды на пути этого огненного дождя с помощью асбестовых полотен успеха не имели. Выступающие конструкции оставляли зазоры в полотнах, сквозь которые фрагменты кабелей и расплава продолжали лететь вниз.

Кроме того, после начала пожара электроэнергию не отключали более трех часов, что значительно затрудняло работу пожарных. Башня просто не была оборудована современными системами пожаротушения, а потому подобная катастрофа была едва ли не закономерной. В мае 2000 года на башне в последний раз побывали пожарные инспекторы. Они обнаружили 38 недостатков, которые было предписано устранить в срочном порядке. До момента пожара удалось исправить только 16 из них [8].

ОСТАНКИНСКИЙ ТЕЛЕЦЕНТР

11 апреля 2005 в здании телецентра "Останкино" произошло возгорание в кабельном коллекторе между вторым и третьим этажами здания. Очаг был обнаружен быстро, в противном случае, по мнению пожарных, последствия могли бы быть намного серьезнее. Если бы пожар распространился по кабелям, которые проходят по всему телецентру, "Останкино" был бы причинен значительный ущерб. Открытого горения как такового не было, но помещения площадью около 200 кв. м оказались сильно задымленными. Возгорание произошло из-за "теплового эффекта аварийного пожароопасного режима работы аппарата защиты АП-50-3МТ, что является недостатком конструкции данного электротехнического устройства", – говорится в постановлении ГУ МЧС России по Москве.

МОСКОВСКИЙ "БЛЭК-АУТ"

Московская энергоавария 2005 – это совокупность аварийных событий 23–25 мая 2005 года, вызвавшая массовое отключение потребителей электроэнергии в Москве, Московской, Тульской и Калужской областях. Снижению надёжности электрических сетей поспособствовали начало летнего ремонтного сезона, когда значительная часть оборудования была выведена из работы, и необычно жаркая погода. В течение 23 и 24 мая 2005 года на подстанции "Чагино" на юго-востоке Москвы произошло несколько аварийных событий (взрывы измерительных трансформаторов тока, короткое замыкание на сборных шинах), которые привели к полному погашению этой подстанции и разрыву проходящего через нее московского энергокольца на 500 кВ.

Основной предпосылкой к возникновению этой крупнейшей в истории России энергоаварии явился быстрый рост энергопотребления в Московском регионе на фоне массового износа оборудования электрических сетей. Эта авария подробно описана [9], тем не менее, кратко напомним хронологию событий.

23 мая вечером на подстанции "Чагино" возникло небольшое возгорание в одном из шести трансформаторов, расположенном в одноэтажном кирпичном здании. После отключения напряжения возгорание было ликвидировано применением углекислотной пены. Питание потребителей было переключено на пять оставшихся трансформаторов. 24 мая после 21.00 произошло возгорание уже четырех трансформаторов.

Утром 25 мая аварийно отключилась подстанция "Очаково", в результате чего были отключены высоковольтные линии на 220 кВ. В южной части Москвы в результате этих отключений в сети напряжение упало до 90 кВ (вместо 110 кВ), и была потеряна генерация на ГЭС №1, на семи ТЭЦ и ГРЭС-4. Уже в 10.10, с наступлением пика утреннего потребления, отключились еще четыре из семи московских подстанций. Отключились также пять московских электростанций и еще 15 питающих центров. Энергетическая авария перешла в стадию "цепной реакции", оставив без энергоснабжения Подмосковье, Тульскую, Калужскую и Рязанскую области — были отключены Алексинская ТЭЦ, Новомосковская ГРЭС, Ефремовская ТЭЦ, Щёкинская ГРЭС. В Московской области без света остались 34 района. Образовавшийся дефицит электроэнергии вызвал срабатывание устройств противоаварийной автоматики на отключение потребителей. В результате каскадного развития аварии в Московской энергосистеме была отключена 321 подстанция, несколько линий метрополитена и пригородных железных дорог. Полностью обесточена была и Тула – здесь до вечера не ходил транспорт, не работала связь. Развитие аварии было остановлено в середине дня 25 мая; к вечеру 26 мая последствия аварии были полностью ликвидированы.

Авария привела к коллапсу транспортной системы Москвы, нарушению работы и производственного цикла множества предприятий, банков, бирж, органов управления. В эти дни даже из Санкт-Петербурга было практически невозможно дозвониться куда-либо, кроме регионов Северо-Запада. Большая часть российского сегмента Интернета испытывала серьезные проблемы. Резко упала скорость доступа к российским интернет-ресурсам. Число пользователей Интернета снизилось на 20%, а число просмотренных страниц – на 40%. Из-за аварии отключился основной российский узел обмена интернет-трафиком – M9.

Все крупные операторы мобильной связи признали сбои со связью в результате обесточивания базовых станций в Москве и Московском регионе и перевода на резервные источники питания. Одновременно в сети наблюдались перегрузки из-за резко возросшего уровня использования мобильной связи. В течение дня ситуация постоянно

ухудшалась. По предварительным оценкам, проблемы коснулись до 30% абонентов Московского региона, т.е. примерно 6 млн. человек. В помощь связистам (а также больницам и коммунальным службам) были выделены армейские мобильные дизель-генераторы, которые не смогли доставить на места из-за возникших автомобильных пробок.

Расследование этой крупной энергоаварии выявило такие причины ее возникновения и развития [10], как износ и технические отказы оборудования, недостаточная пропускная способность электросетей, в том числе магистральных; неудачные технические решения (неэффективная автоматика релейной защиты магистральных сетей ОАО "Мосэнерго"). Сыграл роль и дефицит реактивной мощности (после отмены Правил пользования электрической и тепловой энергией большинство крупных потребителей перестали участвовать в управлении реактивной мощностью энергосистемы).

Безусловно, влияние оказали и халатность персонала энергосетей (отключение нескольких высоковольтных линий произошло из-за того, что провисшие вдоль просеки провода касались веток деревьев), и воровство электроэнергии (из-за многочисленных набросов некоторые высоковольтные линии имели пониженную пропускную способность), и безответственность потребителей (Московский нефтеперерабатывающий завод, запитанный через ПС "Чагино", не имел требуемой для его класса надежности схемы резервирования).

Авторы работы [10] – сотрудники НИИЭЭ – полагают, что "изначально энергосистемы имеют высокий уровень как технического, так и инфраструктурного резервирования, поэтому только комбинация множества по отдельности маловероятных фактов может привести к масштабной аварии. С другой стороны, подобная комбинация случайностей, разрывая систему сразу в нескольких местах, вызывает в ней волну разнообразных отказов, способных спровоцировать каскадное развитие аварии с выходом из строя всей энергосистемы или существенной ее части: в этом случае последствия будут поистине катастрофическими."

В данном случае непосредственной причиной стали взрывы изношенных трансформаторов, однако Московская авария 2005 года представляет собой системное нарушение, т.е. неспособность энергосистемы как единого целого противостоять стечению негативных обстоятельств, прежде всего по причине нерасчетных возмущений, ошибок в ее стратегическом развитии, оперативном управлении, регулировании и др.

Мы столь подробно остановились на аварии энергообъекта не только потому, что энергетические аварии значительно влияют на сети связи. Сети электроснабжения и сети связи – это сложные технические системы, в поведении которых при нештатных ситуациях много общего. И при всех технических различиях субъективные причины аварий в различных отраслях и областях техники друг от друга практически не отличаются.

Как будет показано далее, подобные аварии имеют достаточно массовый характер и отличаются только масштабами. Еще более к тяжелым последствиям – вплоть до техногенных катастроф – может привести авария системы управления технологическими процессами. Для их предупреждения необходим системный анализ потенциальных угроз, причем для телекоммуникационных систем особую опасность представляют опасные электромагнитные влияния. Их анализу и будет посвящена следующая публикация.

Продолжение в следующем номере.

ЛИТЕРАТУРА

1. **Рогонский В.А., Воронин В.М.** Строительные катастрофы. – СПб, Стройиздат, 2001.
2. **Мак-Ивли А.Дж.** Анализ аварийных разрушений. – М.: Техносфера, 2010.
3. **Петров Ю.П., Петров Ю.Л.** Неожиданное в математике и его связь с авариями и катастрофами. – СПб.: БХВ-Петербург, 2005.
4. **Петров Ю.П.** Расследование и предупреждение техногенных катастроф. Научный детектив. – СПб.: БХВ-Петербург, 2007.
5. Коммерсантъ, №42 (2645) от 13.03.2003.
6. www.rian.ru
7. Пожар на АТС-21. – www.dsv.net.ru
8. www.obashnya.ru
9. Авария в энергосистеме в Москве. – http://ru.wikipedia.org
10. **БелобровВ.,ЭдельманВ.** Риск-менеджмент в электроэнергетике: цель – надежность электроснабжения. – Энергорынок, 2006, №1.

АВАРИИ НА ОБЪЕКТАХ СВЯЗИ

Причина – опасные электромагнитные влияния

Часть 2*

Д.Терентьев
ic@commeng.ru

Мы продолжаем серию публикаций, посвященных авариям на объектах электросвязи. Длительное временя автор занимался проблемами защиты от перенапряжений и электромагнитной совместимости. В ходе работы приходилось как анализировать причины, приведшие к повреждению оборудования и линий связи и пожарам, так и разрабатывать мероприятия и специальное оборудование для предотвращения аварий и нарушений качества связи из-за воздействия электромагнитных влияний. Накопленный опыт позволил системно исследовать проблему, результаты этой работы и рассматриваются в серии публикаций.

АВАРИЯ НА УЗЛЕ СВЯЗИ БРАТСКОЙ ГЭС КАК ЧАСТЬ КАТАСТРОФЫ НА САЯНО-ШУШЕНСКОЙ ГЭС

Саяно-Шушенская ГЭС (СШГЭС) на реке Енисей – самая мощная в России и одна из крупнейших в мире. Установленная мощность составляет 6400 МВт, среднегодовая выработка – около 22 млрд. кВт·ч. Плотина образует водохранилище полным объемом 30,7 млрд. м^3.

О множестве технических проблем на Саяно-Шушенской ГЭС было известно давно. Подробно они описаны в книге бывшего директора станции В.И.Брызгалова [11], изданной в 1999 году. За 20 лет эксплуатации на СШГЭС произошло 64 нарушения работы гидротурбин и повреждения их узлов, а на втором гидроагрегате за 20 лет работы было обнаружено 17 повреждений.

17 августа 2009 года на СШГЭС произошла одна из самых значительных в истории мировой гидроэнергетики техногенных катастроф [12, 13]. В результате аварии погибло 75 человек, из 10 работавших на станции гидроагрегатов семь разрушены или получили серьезные повреждения (рис.2). Экономике страны нанесен огромный ущерб, пострадала и экология. По мнению некоторых специалистов, реальная опасность угрожала не только лежащему ниже по течению Абакану, но и Красноярску.

Плотина и горные породы под ней до сих пор находятся в неравновесном состоянии. В книге В.В.Тетельмина [14] подробно рассмотрены пять не учтенных в проекте гидроузла физических процессов, которые определяют загадочное, на первый взгляд, поведение плотины СШГЭС и до сих пор не принимаются во внимание в расчетах плотины на устойчивость. Автор работы выражает надежду, что "17 августа 2009 года станет началом новой истории в развитии безопасной гидроэнергетики России".

Рассмотрим более подробно два аспекта катастрофы на СШГЭС, которые находятся в сфере профессиональных интересов специалистов по телекоммуникациям, электронике и энергетике.

ПОЛНОЕ ОБЕСТОЧИВАНИЕ ВСЕХ СИСТЕМ СШГЭС

В первой части статьи мы описали "Московский блэкаут", вызвавший массовое отключение потребителей

* Продолжение. Начало см. Первая миля, 2011, №1.

энергии в Москве и нескольких областях Центрального региона России, что привело, в частности, к серьезным нарушениям работы систем связи. На СШГЭС все системы, включая аварийные, были полностью обесточены, и если бы не героические и профессиональные действия сотрудников дежурной смены, последствия были бы куда тяжелее и жертв намного больше. Опираясь на источники [12, 15–17], попробуем оценить влияние уничтожения системы электроснабжения и применения резервных источников питания в самые критические часы.

17 августа 2009 года в 8 ч 13 мин по местному времени персонал, находившийся в машинном зале, услышал громкий хлопок в районе гидроагрегата № 2 и увидел выброс столба воды. На центральном пульте управления сработала светозвуковая сигнализация, пропали оперативная связь, электропитание освещения, автоматики, сигнализации, защит и приборов. Автоматические системы, останавливающие гидроагрегаты, сработали только на гидроагрегате № 5. Затворы на водоприемниках других гидроагрегатов оставались открытыми, и вода продолжала поступать на турбины, что привело к разрушению гидроагрегатов № 7 и 9. Потоками воды, поступающими через открытые водоводы, и разлетающимися обломками гидроагрегатов были разрушены стены и перекрытия машинного зала. Все гидроагрегаты ГЭС были затоплены, при этом на работавших гидрогенераторах произошли короткие замыкания.

СШГЭС полностью лишилась электропитания, как следствие – освещения, связи, автоматики, сигнализации. Все оборудование станции, даже не затронутое водой и разрушениями, перестало работать. В связи с потерей энергоснабжения закрыть затворы можно было только вручную, для чего персоналу необходимо было проникнуть в специальное помещение на гребне плотины. Около 8.30 восемь человек оперативного персонала добрались до помещения затворов, после чего связались по сотовому телефону с начальником смены станции, который дал указание опустить затворы, которые были полностью закрыты в 9.20.

Следующей задачей было открыть водосброс (обходной путь для воды через тело плотины), чтобы не допустить перелива воды из водохранилища. Если бы это не было сделано, затопленными могли оказаться населенные пункты ниже по течению Енисея, а также из строя вышла бы и Майнская ГЭС. На гребень плотины была привезена передвижная дизель-генераторная

Рис.2. **Разрушения на Саяно-Шушенской ГЭС**

станция, от которой в 11.32 был запитан козловой кран, расположенный на гребне плотины, и в 11.50 начали открывать затворы водосбросных отверстий. К 13.07 все 11 затворов водосливной плотины были закрыты.

После катастрофы на СШГЭС, а также событий на АЭС "Фукусима-1" стало совершенно очевидно: система резервного электропитания объектов, представляющих повышенную опасность, должна быть рассчитана на работу в условиях крупномасштабной аварии, техногенной и природной катастроф. Эти же требования должны распространяться и на системы связи, обеспечивающие работу таких объектов.

АВАРИЯ НА УЗЛЕ СВЯЗИ БРАТСКОЙ ГЭС

По сведениям ряда информационных источников, авария на Саяно-Шушенской ГЭС была непосредственно связана с пожаром на узле связи Братской ГЭС (БрГЭС). Так, глава Ростехнадзора Н.Кутьин, представивший акт технического расследования причин аварии, отметил: "Нельзя сказать, что Братская ГЭС виновна в аварии на Саяно-Шушенской, это не так, но условия были созданы как раз во время возгорания на Братской" [18]. В то же время пресс-служба ОАО "Иркутскэнерго", дочернее предприятие которого ООО "Иркутскэнергосвязь" занималось обслуживанием узла связи, в своем комментарии от 5 октября 2009 года заявила, что "инцидент, связанный с потерей на 40 мин 16 августа 2009 года связи между Оперативным диспетчерским управлением Сибири

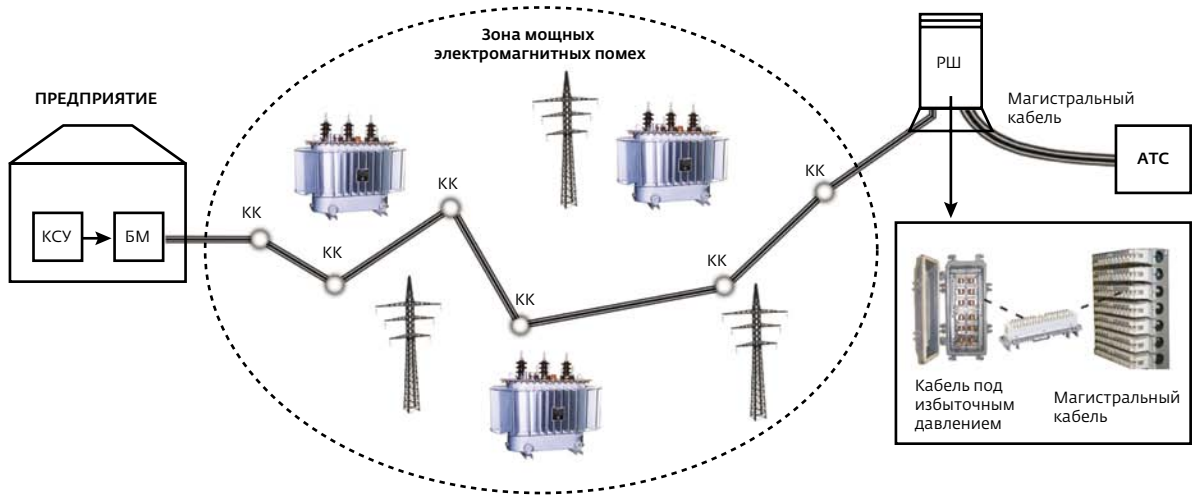


Рис.3. **Кабельная трасса, подверженная влиянию электромагнитных воздействий**

и Братской ГЭС, не является причиной аварии на Саяно-Шушенской ГЭС" [19].

Оставим обсуждение вопроса о связи между аварией на узле связи БрГЭС и катастрофой на СШГЭС специалистам, ограничившись замечанием, что, по всей видимости, такая связь существует. В акте расследования причин аварии [17] в разделе, посвященном описанию работы оперативно-диспетчерского управления (ОДУ) Сибири в Кемерово, которое управляет обеими станциями, значительное место занимает описание аварии системы связи, в результате которой связь БрГЭС с Центром управления ОДУ Сибири оказалась утерянной.

Рассмотрим последовательность событий, отраженную в акте [17]. 16 августа 2009 года в 20 ч 20 мин (время московское) на рабочем месте сменного персонала ССДТУ (службы связи, диспетчерского и технологического управления) БрГЭС сработала пожарная сигнализация цифрового линейного аппаратного зала. На центральном пульте управления БрГЭС сработала сигнализация о неисправности каналов связи, отключились каналы автоматического регулирования частоты и перетоков мощности (АРЧМ), электронно-вычислительные машины, пропала голосовая связь с дежурными диспетчерами оперативно-диспетчерского управления, ОАО "Иркутскэнерго" и ООО "Иркутсэнергосвязь". Сразу же о пожаре сообщили оператору пожарной команды по охране БрГЭС.

В последующие 10 мин в результате пожара поочередно вышли из строя оптические линки между БрГЭС и подстанциями "Покосное" и "Тулун", было повреждено оборудование основных и резервных каналов связи, устройств АРЧМ БрГЭС, устройств телемеханики, прямых голосовых каналов с ОДУ "Сибири" и Иркутским РДУ.

В период с 20.21 до 20.55 принимались все меры по восстановлению связи, используя любые ее виды (междугородная, сотовая, ведомственная и т.д.), а также по передаче сообщений через другие энергообъекты. По данным оперативного журнала БрГЭС, связь по сотовому телефону была восстановлена с дежурным диспетчером ОДУ лишь в 21.00. Таким образом, отсутствие любой связи между БрГЭС и ОДУ Сибири составило 40 мин. 17 августа в 10.03 авария была ликвидирована, связь восстановлена.

Таким образом, практика показала, что системы связи и технологического управления даже таких стратегически важных, опасных и генерирующих мощные финансовые потоки объектов, как Братская и Саяно-Шушенская ГЭС, имели низкую надежность. Нет никаких сомнений, что это не исключение из правил.

Один из важнейших аспектов надежности систем связи – их устойчивость к опасным электромагнитным влияниям. Рассмотрим на реальных примерах различные аспекты этой проблемы, постаравшись сформулировать практические рекомендации и решения. Начнем с АТС, где сосредоточено не только самое массовое, но и самое уязвимое оборудование. Практически любая из многих миллионов жил кабелей телефонной распределительной сети может стать источником перенапряжений различного рода. Нельзя забывать и о низком качестве электропитания, особенно в сельских районах, и об ударах молнии в мачты узлов связи. Однако сначала рассмотрим только опасность, угрожающую оборудованию АТС со стороны абонентских линий.

КАК ГОРЯТ КООРДИНАТНЫЕ АТС

При внедрении координатных АТС решили сэкономить, и на городских АТС кроссы для них (в основном, производства завода "Красная Заря", а также предприятий ЧССР и ГДР) устанавливались практически без защиты. В частности, при монтаже АТСК-У защитные устройства (угольные разрядники и термокатушки ТК-0,25) предусматривались только для воздушных и смешанных линий связи. Кабельные линии связи заводились в рамки с разделительными гнездами 25×5. Оборудование производства ЧССР комплектовалось коммутационными рамками фирмы Tesla. Некоторым станциям достались в наследство от декадно-шаговых АТС громполосы. Вполне допускаю, что такое решение имело техническое и экономическое обоснование. Ведь специалисты научно-исследовательских и проектных институтов не предполагали, что падение техно-

логической дисциплины, несогласованность действий разных организаций, безответственность, а также ужасающее состояние электроустановок жилых зданий в 1990-е и первые годы 21 века станут скорее нормой, чем исключением из правил.

Сельские АТС (АТСК 50/200, АТСК 50/200 М) поставлялись с вводно-коммутационными устройствами, содержащими термокатушки и угольные разрядники, а с АТСК 50/200 М – и газонаполненные разрядники Р-27. Предназначенная для райцентров АТСК 100/2000 по большей части комплектовалась громполосами с термокатушками и угольными разрядниками.

Специалистами МГТС, МТУСИ и МИФИ [21] были проведены исследования АТСК-У с точки зрения стойкости к попаданию постороннего напряжения электросети в абонентские линии. Эту работу продолжило в 2001–2003 годах НПО "Инженеры электросвязи", перед которым одним из операторов была поставлена задача – срочно обеспечить надежную защиту всех координатных АТС и квазиэлектронных АТС "Квант". Прежде всего мы на всех АТС, даже необслуживаемых, установили круглосуточное дежурство. Дежурный персонал несколько раз наблюдал дым и даже открытый огонь в стативах АТС. Немедленно принимались меры по расследованию случившегося, что дало много полезной информации. Причиной такого решения послужили несколько пожаров, произошедших в течение короткого срока.

ПРИМЕР 1.

Во время пожара в жилом доме произошел контакт между оголившимися жилами силового и телефонного кабелей. В результате попадания постороннего напряжения загорелись абонентские комплекты, расположенные в стативе АИ-АВ. Огнем были полностью уничтожены несколько стоек, сгорели кабели, проложенные на кабельростах. Огромный автозал был покрыт толстым слоем сажи.

Районный центр с населением более 30 тыс. человек остался без связи. Вспомним, что 10 лет назад мобильная связь была далеко не у всех, поэтому для вызова аварийных специальных служб в различных точках города были размещены автомобили, оборудованные радиосвязью.

Оператор был вынужден срочно переоборудовать коммутатор, предназначенный для выполнения функций зонового телефонного узла, и еще два года пропускать свой внутренний трафик через междугородный коммутатор другого предприятия связи.

ПРИМЕР 2.

Следующий случай с городской координатной АТС тоже произошел в начале 2000-х годов, было повреждено несколько стативов, много станционного кабеля. Для того чтобы полностью восстановить и настроить АТС силами специалистов, собранных со всех концов области, понадобилось две недели. Расположенная на другом этаже декадно-шаговая АТС заработала в тот же день. Последствия могли быть гораздо хуже, если бы пожар не был в самом начале обнаружен. Правда, их могло бы быть и меньше, если бы сотруднику охраны удалось привести в действие огнетушитель – вполне исправный, как потом выяснилось.

Пример этот интересен обстоятельствами и механизмом опасного воздействия на кабель связи, о других подобных случаях мне неизвестно. Рассмотрим его обстоятельства.

Некое предприятие было связано с городской координатной АТС телефонным кабелем (рис.3). Причем от предприятия кабель проходил до распределительного шкафа (РШ) (вынос АТС), а дальше магистральным кабелем соединялся с АТС. Кабель от предприятия до РШ был проложен в трубах в алюминиевом шланге и частично в свинцовой оболочке, находящийся под избыточным воздушным давлением. Давление поддерживала компрессорно-сигнальная установка (КСУ). В РШ кабель был заведен в магистральный бокс (БМ). С помощью кроссировок через плинты контакты БМ соединялись с магистральным кабелем.

В кабельных колодцах (КК) кабель лежал на металлических консолях, которые соединялись с заземляющими электродами. Трасса проходила по каменистому склону, изгибаясь среди камней и выходов скальной породы. На протяжении порядка 300 м рядом с ней находилось несколько подстанций и сближений с ЛЭП. На этом участке расстояние между колодцами составляло 30–40 м.

Важно отметить, что участок от предприятия до РШ обслуживался одной бригадой, а РШ и магистральный кабель до кросса АТС – другой. Граница ответственности проходила по магистральному боксу в вынесенном РШ.

Кабельная трасса была проложена в незапамятные времена. Позже были построены две подстанции из трех, после чего у бригады, обслуживающей кабельную трассу, начались проблемы. В месте контакта свинцовой оболочки кабеля с консолью колодца в оболочке образовалось отверстие, что было сразу же обнаружено, так

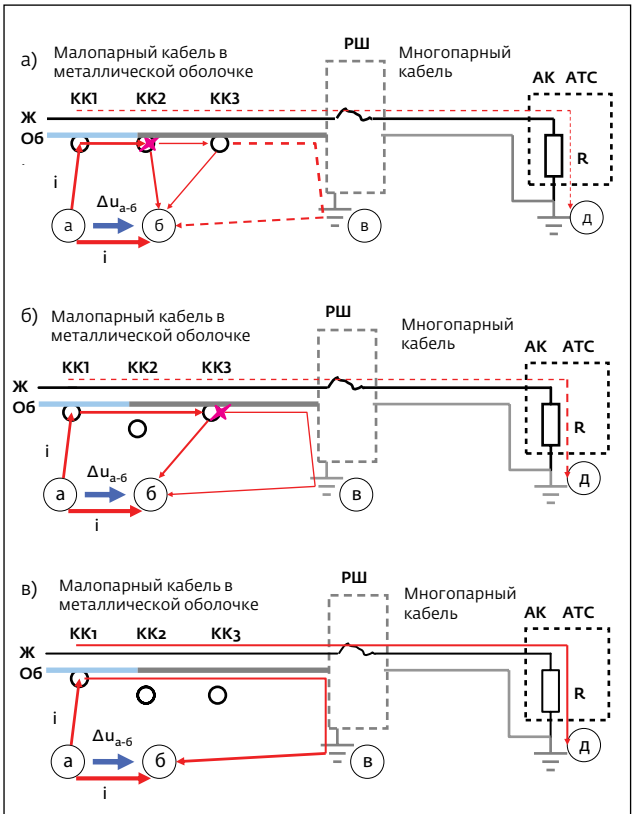


Рис.4. **Упрощенная модель возникновения перенапряжения в жилах кабеля**

как кабель находился под избыточным давлением. Герметичность кабеля была восстановлена, между консолью и оболочкой была проложена изолирующая прокладка. Через некоторое время то же самое произошло в другом колодце. Так продолжалось несколько раз до тех пор, пока на АТС не произошел пожар.

Очевидно, что причиной аварии стало влияние подстанций и ЛЭП, рядом с которыми проходила кабельная трасса. Энергетические объекты – мощный источник помех, которые достигают максимального уровня во время различных коммутаций (переключение линий, отключение и включение нагрузки). При этом в заземляющие устройства электроустановок могут стекать токи в сотни ампер.

После изучения всех обстоятельств и обследования кабельной трассы мною было предложено объяснение причин аварии. Для их понимания рассмотрим механизм возникновения перенапряжения на упрощенной модели (рис.4). Предположим, что в момент коммутации на одной или нескольких подстанциях одновременно между заземляющими устройствами подстанций (точки а, б) возникает разность потенциалов. Под воздействием напряжения $U_{а-б}$ между ними протекает ток. Так как сопротивление скального грунта очень высоко, значительная часть тока протекает по оболочке кабеля (рис.4а). Попадая в оболочку через консоль в колодце КК1, ток стекал через консоли в колодцах КК2 и КК3. Пренебрежимо малая часть тока течет из точки а в точку б через заземляющее устройство распределительного шкафа.

Стекающий через консоль КК2 ток за счет электрохимического и термического воздействий на свинцовую оболочку разрушает ее в зоне контакта. В то же время, в КК1 алюминиевый шланг не был поврежден (муфта расположена между точками контакта с консолями в КК1 и КК2, в каком из колодцев – непринципиально). После устранения повреждения оболочки в КК2 между ней и консолью устанавливается изоляционная прокладка. Следующее повреждение по аналогичной схеме происходит в КК3 (рис. 4б), и опять после ремонта оболочки она изолируется от консоли.

Возникшая снова высокая разность потенциалов между точками а и б теперь привела к тому, что значительная часть тока попадала в точку б через заземление РШ (точка в). Ток в металлической оболочке кабеля $I_{об}$ создает ЭДС $E_{ж-об}$ в цепи "жила-оболочка", которая совпадает по фазе с током и ЭДС в цепи "жила-земля" $E_{ж-з}$, величина которых прямо пропорциональна $I_{об}$. Механизм экранирования и взаимосвязь ЭДС и токов в оболочке и жилах подробно рассмотрен в [22]. Реальный случай гораздо сложнее модели – в частности, оболочка в нескольких местах соединена с землей, основной ток помехи протекает по оболочке, кроме того, присутствуют и индуктивные наводки от ЛЭП. Кроме того, ток в оболочке изменяется по сложному закону, включает множество гармоник и может протекать достаточно длительное время.

Тем не менее очевидно, что за счет взаимной индуктивности между оболочкой и жилами кабеля в последних протекает ток, величина которого зависит от характеристик тока в оболочке, коэффициента взаимоиндукции М между жилами и оболочкой, и длины участка, на котором происходит влияние внешних помех. Длина участка, на котором происходили индуктивные наводки на жилы кабеля, постоянно увеличивалась работниками линейной бригады при изоляции кабелей от консолей, что и привело к увеличению наведенной ЭДС в жилах кабеля. Индуцированный ток, проходя через несколько абонентских комплектов, вызвал в них возгорание.

Таким образом, можно выделить три непосредственных причины аварии. Во-первых, линия, эксплуатируемая без проблем много лет, после строительства ЛЭП и подстанций стала источником повышенной опасности. Обслуживающий персонал не сделал правильных выводов из нескольких случаев, предшествующих пожару. Более того, действия линейных электромонтеров были ошибочны. Квалифицированные инженеры, которые могли бы правильно оценить ситуацию, к решению проблемы привлечены не были. В данном случае (до замены кабеля на кабель в полиэтиленовой оболочке) следовало бы обеспечить хороший электрический контакт оболочки с консолями, что исключило бы ее прогорание и уменьшило наводки на жилы кабеля.

Вторая причина – в плинте, через который контакт бокса БМ был соединен с плинтом магистрального кабеля (см. рис.3), был установлен модуль защиты по напряжению, однако его заземляющий контакт не был подключен. Так как этот плинт находился на границе раздела ответственности двух линейных бригад, никто не поинтересовался, правильно ли установлены модули защиты. В этот плинт, а еще лучше – в бокс БМ, необходимо было установить модули комплексной защиты, в идеальном случае – с пониженным током срабатывания. Третья причина возгорания – в кроссе АТС модули защиты отсутствовали и были установлены только после пожара.

ТЕХНИЧЕСКИЕ ПРИЧИНЫ ВОЗГОРАНИЙ НА КООРДИНАТНЫХ АТС

В двух публикациях мы рассмотрели четыре случая возгорания городских координатных АТС. Так сегодня эксплуатируется достаточно много таких станций, разберемся, каким образом на них воздействует постороннее напряжение.

Рассмотрим схему абонентского комплекта АТСК-У (рис.5) [23]. Результат попадания постороннего напряжения в абонентскую линию зависит от множества факторов – не только от источника перенапряжения, пути его

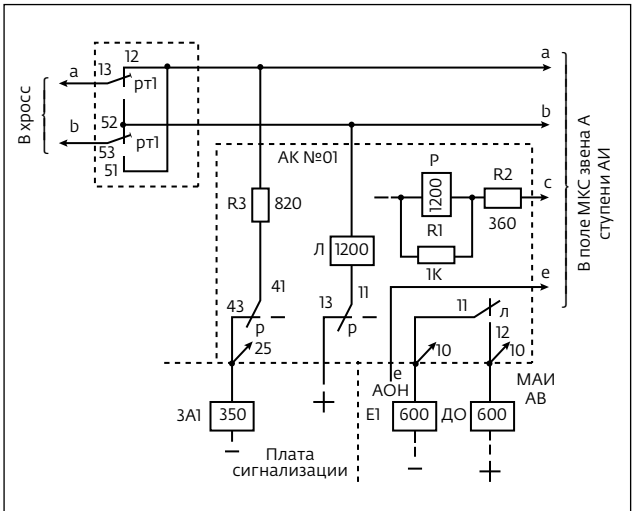


Рис.5. **Абонентский комплект усовершенствованной системы АТСК-У**

попадания в линию и параметров линии, но и от особенностей оборудования (например, текстолитовая или гетинаксовая плата) и даже от нагрузки на приборы АТС.

При попадании постороннего напряжения в провод b срабатывает линейное реле Л и к линии подключаются исходящий шнуровой комплект (ИШК) и другое станционное оборудование, эти приборы могут быть повреждены. В том случае, если ИШК не подключается к абонентскому комплекту при отсутствии промежуточных путей на ступени АВ, отсутствии свободных ИШК или неуверенного срабатывания реле Л (пульсации), весь ток протекает через обмотку реле Л, что приводит к его разогреванию и снижению сопротивления обмотки. Возгорание обмотки реле возможно, но маловероятно.

Однако наиболее опасным является протекание тока через резистор R3 мощностью 2 Вт. При токе порядка 100 мА и выше он может стать источником открытого огня. При частичном разрушении таких резисторов они могут стать источниками устойчивой электрической дуги, которая воспламеняет все вокруг. Старая изоляция проводов в жгутах, залитые лаком платы могут быстро загореться (см. пример 2).

Сделаем выводы, которые касаются не только АТСК и АТСК-У, но и сельских координатных АТС. АТС координатной системы имеют высокую стойкость к импульсным помехам. На кабельных подземных и коротких подвесных линиях они не требуют защиты по напряжению. На воздушных и смешанных линиях связи в грозоопасных районах такая защита необходима. Ее не обязательно устанавливать в кроссе – можно и в кабельных ящиках, которые соединены с кроссом АТС кабелями в канализации. Для защиты можно использовать газонаполненные разрядники и, в ряде случаев, варисторы. Защита по току необходима, так как при попадании постороннего напряжения может произойти возгорание АТС.

Токовая защита должна срабатывать при минимально возможном токе, который ограничен снизу уровнем броска тока при снятии трубки во время посылки вызова и током на линиях с низкоомным шлейфом (зона прямого питания, телефонный аппарат с низким сопротивлением). Таким образом, термокатушка ТК-0,25 не может обеспечить надежную защиту АТС. Как показывает опыт, предохранители имеют большой разброс параметров и могут перегорать при снятии трубки во время посылки вызова.

Единственным экономически и технически обоснованным вариантом токовой защиты является применение резисторов с положительным температурным коэффициентом – полимерных или керамических позисторов с гарантированным током срабатывания не более 100 мА и гарантированным током несрабатывания не менее 70 мА.

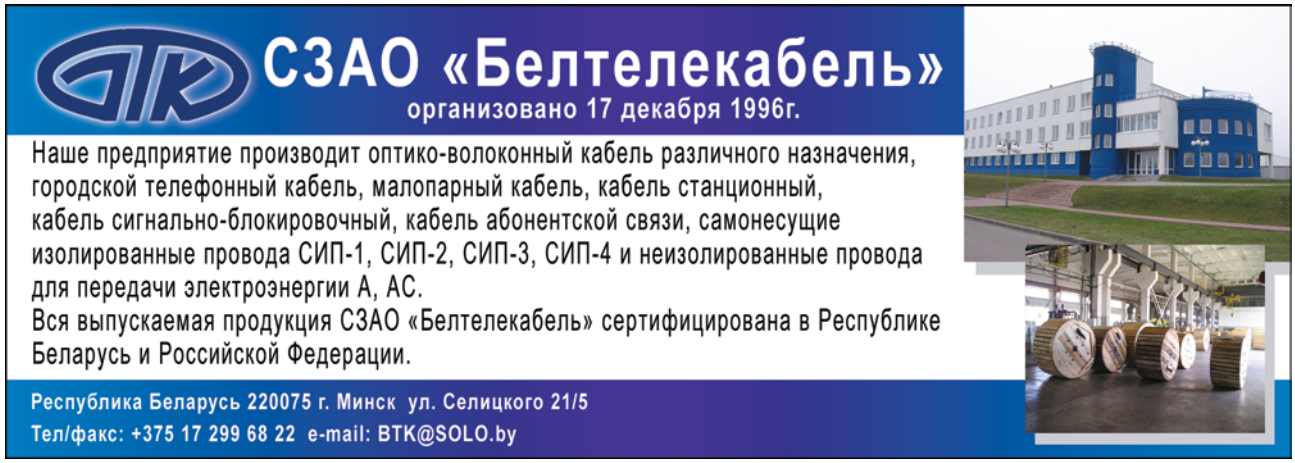
* * *

В заключение отметим, что каждый тип АТС горит по-своему. Воздействия, критичные для координатных АТС, безопасны для декадно-шаговых или электронных станций. Поэтому при анализе опасности электромагнитных воздействий нужно учитывать специфику каждого типа АТС, чем мы и займемся в последующих публикациях.

Продолжение следует

ЛИТЕРАТУРА

11. **Брызгалов В.И.** Из опыта создания и освоения Красноярской и Саяно-Шушенской гидроэлектростанций. – Красноярск: Сибирский ИД "Суриков", 1999.
12. Авария на Саяно-Шушенской ГЭС. – http://ru.wikipedia.org
13. http://www.plotina.net/
14. **Тетельмин В.В.** Плотина Саяно-Шушенской ГЭС: Состояние, процессы, прогноз. – М.: Книжный дом "Либроком", 2010.
15. **Беляков Е.** Саяно-Шушенскую ГЭС спас инженер. – Комсомольская правда в Красноярске, 3 сентября 2009.
16. Вестник РусГидро, №9, 2009.
17. Акт технического расследования причин аварии, произошедшей 17 августа 2009 года в филиале ОАО "РусГидро" – "Саяно-Шушенская ГЭС им.П.С. Непорожнего". – ru.wikisource.org/wiki
18. Новости России, 3 октября 2009. – www.newsru.com
19. http://www.irkutskenergo.ru
20. Материалы заочного научно-практического семинара "Защита оборудования связи от опасных токов и напряжений. Подготовка к грозовому сезону. – НПО "Инженеры электросвязи", 1999. – www.commeng.ru
21. **Евстигнеев Ю.Г., Пшеничников А.П. и др.** Токовая защита координатных АТС на Московской городской телефонной сети элементами ЭЗТ-100К. В сборнике [20]. – www.commeng.ru
22. **Михайлов М.И., Разумов Л.Д., Соколов С.А.** Защита сооружений связи от опасных и мешающих влияний. – М.: Связь, 1978.
23. **Корнышев Ю.Н., Маркович А.Я., Пискер М.Н., Романцов В.М.** Станционные сооружения городских телефонных сетей. – М.: Радио и связь, 1989.



АВАРИИ НА ОБЪЕКТАХ СВЯЗИ

Причина – опасные электромагнитные влияния

Часть 3

Д.Терентьев
ic@commeng.ru

В предыдущих частях статьи* мы рассмотрели наиболее известные аварии последнего десятилетия, которые тем или иным образом связаны с телекоммуникациями. В части 3 предложена наглядная модель возникновения аварий и проанализирована на ряде примеров. Рассмотрено заземляющее устройство, как причина появления перенапряжений. Кроме того, продолжен разговор о системах коммутации – на этот раз квазиэлектронных и электронных АТС.

ПИРАМИДА АВАРИЙ

От устойчивости объекта связи к опасным электромагнитным влияниям непосредственно зависит его надежность – свойство сохранять в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и в требуемых условиях применения. Количественно надежность оборудования – это величина, обратная интенсивности отказов на заданном интервале времени [24].

Так же, как и для расчета надежности, для оценки устойчивости к опасным электромагнитным влияниям применяются статистические методы, например, описанные в рекомендации ITU-T K.39 [25]. Все инструкции по молниезащите содержат методики расчета вероятности удара молнии и других параметров, например, вероятного числа повреждений оптических кабелей [26]. Накоплен большой объем инструкций, методик, статистических данных, создан развитой математический аппарат, которые могут быть применены для расчета вероятности аварий на объектах связи. Тем не менее, мне не известны случаи, когда подобные расчеты делались в комплексе для всех систем объектов связи, а тем более для сетей в целом.

Предлагаю использовать для понимания проблемы электромагнитной безопасности простую и наглядную модель "пирамида аварий" (рис.6) [27]. В соответствии с моделью, множество опасных условий и ненадежных процессов порождает сотни небольших аварий и ситуаций, чреватых сбоями. Если на них не обращать внимания, результатом могут стать десятки случаев имущественного ущерба и травматизма персонала. Следующая ступень пирамиды – серьезные аварии, несчастные слу-

* Часть 1 и 2 см. Первая миля, 2011, №1 и 2, а также на сайте www.commeng.ru в разделе "Публикации".

чаи. Если в масштабах крупного предприятия, отрасли ничего не предпринимается, то рано или поздно произойдет крупная авария с тяжелыми последствиями, а если рассматриваются промышленные, энергетические или транспортные объекты с повышенным уровнем опасности, то и катастрофа.

Для снижения вероятности аварий и предотвращения катастроф нужно уменьшать площадь пирамиды, что можно сделать двумя путями:

- сокращением числа опасных технических решений, процессов и оборудования на уровне 2 (будем считать, что на внешние источники перенапряжений влиять мы не можем);
- уменьшением угла при основании пирамиды: предпринимаются дополнительные меры, чтобы не допустить развития аварии. Например, эту функцию на некоторых опасных производственных объектах выполняют пожарные или горноспасательные части.

Рассмотрим пирамиду аварий применительно к теме аварий на объектах связи. Первопричиной аварий (первый уровень) служат опасные электромагнитные влияния природного и промышленного характера (гроза, помехи от ЛЭП, низкое качество электроэнергии). Применение ошибочных технических решений, недостаточно устойчивого к помехам оборудования, нарушение технологической дисциплины приводят к сбоям и мелким авариям. Кроме того, второй уровень пирамиды может сам стать источником опасных или мешающих влияний. Например, источником помех может стать собственная электроустановка объекта.

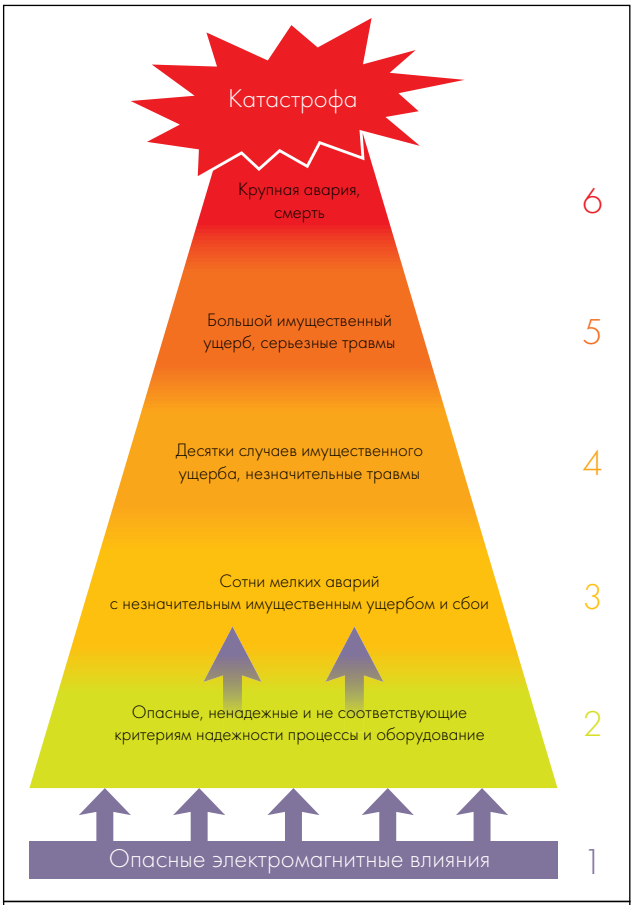


Рис.6. **Пирамида аварий**

Множество незначительных событий предвещает более крупные неприятности. Например, многократное повторение незначительных повреждений кабеля стало предвестником крупного пожара на АТС, который произошел, когда определенным образом совпали ряд факторов (см. пример 2, часть 2). Каждая ступень пирамиды служит основанием для следующего уровня, и на самой ее вершине – крупная авария или катастрофа. Применительно к телекоммуникациям крупная авария – происшествие на Замоскворецком телефонном узле 14 февраля 2003 года, а авария на грани катастрофы – это пожар на Останкинской телебашне 27 августа 2000 года (оба случая описаны в части 1).

К сожалению, если систематизированные данные о всех уровнях пирамиды аварийности у крупных отечественных операторов связи и имеются (в чем я сомневаюсь), то они в любом случае недоступны. Однако технические системы подчиняются общим закономерностям и поэтому можно обратиться к опыту других отраслей. Так как попытки найти какую-либо информацию по России оказались безрезультатными, будем использовать данные по промышленности США в целом.

Так, в США на каждые 300 аварий без травм приходится приблизительно 30 аварий, сопровождающихся незначительными травмами, и одна крупная авария, влекущая тяжелые травмы или смертельный исход. По итогам анализа 1,7 млн. аварий и несчастных случаев, сведения о которых были предоставлены 297 организациями, на каждые 600 аварий без ущерба или травм приходится около 30 аварий, сопровождающихся имущественным ущербом, 10 аварий с незначительными травмами и одно увечье, приводящее к потере работоспособности [27]. Наблюдается устойчивая закономерность – множество мелких несчастных случаев предвещает более крупные, что позволяет ориентировочно оценить вероятность крупных аварий.

ЗАЗЕМЛЯЮЩЕЕ УСТРОЙСТВО КАК ПУТЬ ДЛЯ ОПАСНЫХ ВЛИЯНИЙ

Основание пирамиды аварий может быть сложено из множества "кирпичиков", но зачастую бывает и так, что фундаментом ее служит крупная ошибка, заложенная при проектировании технической системы, и без ее исправления крупные и мелкие неприятности будут периодически повторяться. Это правило действует как для отдельно взятого объекта, так и для технологических решений, тиражируемых в серийном оборудовании. Показателен пример потенциальной аварийности, заложенной на этапе разработки оборудования АТСКЭ "Квант" и ЦАТС МТ 20/25. К ним мы вернемся чуть позже, а пока рассмотрим три случая из моей практики, когда причиной повреждений и аварий стало... заземляющее устройство.

Во многих источниках, рекламирующих "грозозащиту", популярно объясняется, что: 1. Без хорошего заземления защита от перенапряжений невозможна (на самом деле, нередко приходится обеспечивать защиту не просто при "плохом" заземлении, но и при полном его отсутствии). 2. Помехи "сливаются" на "землю".

В целом, это почти соответствует истине, хотя очень важно понять, что же такое "земля" и "хорошее" зазем-

ление. Сегодня такое понимание у многих специалистов присутствует, а вот лет 10–15 назад, когда внедрение современного оборудования резко повысило требования к ЭМС, "земля" стала terra incognita (земля неизведанная, лат.) до тех пор, пока не накопились и не стали доступными информация и опыт. Статьи [28–30] написаны уже давно, но и сегодня могут быть полезны, так как в них проблемы заземления и уравнивания потенциалов рассматриваются с точки зрения инженера-связиста.

ПРИМЕР 3

Электрифицированная железная дорога – мощный источник помех, особенно если она работает на переменном токе [22]. И если операторы связи прокладывают или подвешивают свои кабели рядом с ней лишь по необходимости, то связистам-железнодорожникам и специалистам службы СЦБ (сигнализация, централизация и блокировка) приходится обеспечивать работу систем связи и автоматики на объектах, которые сами являются источником опасных воздействий (вдобавок к молниям, которые часто ударяют в контактные опоры и провода).

В середине 1990-х годов я принимал участие в строительстве крупной железнодорожной станции – наша фирма занималась монтажом и наладкой систем технологической связи, позднее нам передали монтаж линейно-аппаратных залов волоконно-оптической связи. Профильный железнодорожный институт (Гипротранссигналсвязь) к проектированию привлечен не был, раздел проекта "связь" напоминал многократно переписанный студентами-двоечниками курсовик, изначальный вариант которого был сдан много лет назад. Длины многочисленных кабелей были указаны с точностью до полуметра, приведены их марки, но многие квадратики, обозначавшие оборудование, идентификации не поддавались, причем часть оборудования к тому времени просто перестала выпускаться.

Сегодня кажется невероятным, но тогда практически за месяц удалось совместными усилиями найти правильные решения, выбрать оборудование, договориться с поставщиками. В итоге связь заработала почти вовремя, даже системы уплотнения, которые мы не успели заменить (правда, пришлось собирать одну рабочую стойку из двух-трех, полученных с завода и хранения).

Приближался срок сдачи объекта, но к заземляющим устройствам даже не приступали. Оказывается, их не было не только в проекте, но и в смете на строительство. Недели за две до приезда приемочной комиссии работу по заземлению все-таки начали. С одной стороны здания станции был перрон и железнодорожные пути, с другой, в нескольких десятках метров, – заболоченный лес. Казалось бы, именно с противоположной стороны – подальше от железнодорожных путей – и нужно монтировать заземляющие устройства. Но позади станции были разбиты альпийские горки, посажены цветы и проложены дорожки. Вероятно, кто-то распорядился не портить всю эту красоту, иного объяснения тому, что произошло, я не вижу. Буквально в трех метрах от насыпи были забиты швеллеры, к ним приварили широкую толстую железную полосу, которую завели в здание и подключили к главной заземляющей шине. Все попытки объяснить порочность и опасность такого решения привели лишь к тому, что когда на объект приехала комиссия, мне настоятельно рекомендовали находиться в выделенном для нас вагоне.

Объект был принят. Но в том же году оператор, оптический кабель которого был подвешен на опорах контактной сети, обратился к нам с проблемой: периодически выходили из строя платы выделения каналов из магистральной линии. С учетом того, что платы были очень дорогими, арендаторов каналов было довольно много, а для замены платы надо было потратить целый рабочий день, для оператора это стало неприятной неожиданностью. Выяснилось, что выход из строя плат происходил в момент переключения тяговых подстанций, и проблему решили установкой защитных устройств.

Все эти неприятности были лишь предвестниками серьезной аварии. И она произошла. Высокое напряже-

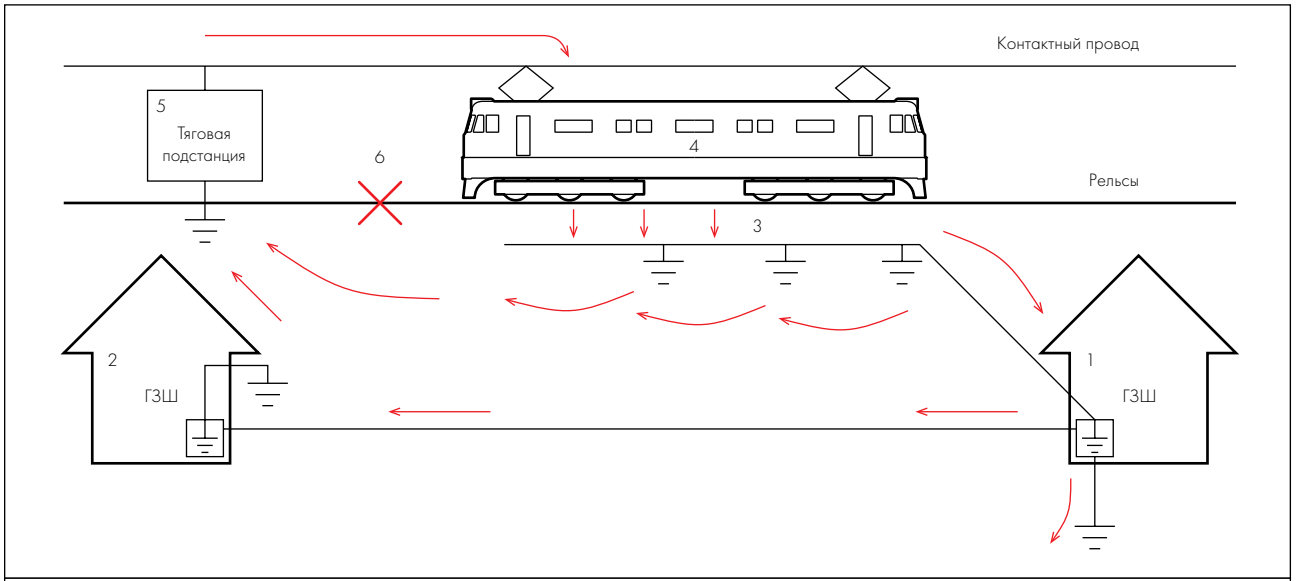


Рис.7. **Протекание части тягового тока через заземляющее устройство**

ние попало на станционную аппаратуру, в результате было повреждено оборудование связи и СЦБ, загорелся уличный шкаф с оборудованием. Причиной аварии стал тяговый ток, часть которого какое-то время протекала через заземляющее устройство. Когда развеялся дым в линейно-аппаратном зале (ЛАЗ), оказалось, что в кроссе АТС варисторы так нагрелись, что потекла пластмасса корпусов модулей защиты. Это значит, что напряжение на заземляющем устройстве превысило 500 В (классификационное напряжение варисторов составляло 470 В). В итоге потребовалась замена значительной части оборудования АТС, были повреждены устройства питания, технологической связи, СЦБ. Если бы корпуса модулей защиты были выполнены из горючего пластика, вряд ли бы обошлось без пожара.

Что послужило непосредственной причиной аварии? Рассмотрим ее возможный механизм (рис.7). Как выяснилось, в момент возникновения аварии рядом со станцией проехал электровоз, причем путь впереди движения ремонтировался. К главной заземляющей шине (ГЗШ) здания 1 подключено заземляющее устройство 3, представляющее собой электроды, вбитые рядом с железнодорожными путями и соединенные между собой и ГЗШ стальной полосой. Электровоз, проезжающий мимо, питается от тяговой подстанции напряжением переменного тока 27,5 кВ. Вторичные обмотки подстанции соединены треугольником, фаза С заземляется и соединяется с рельсами железной дороги. В контактную сеть пути подается напряжение одной из двух других фаз (А или В). Так как в точке 6 рельсы разобраны, ток, потребляемый электровозом, течет к заземлению подстанции через землю, другие рельсы и другие проводники, в числе которых и заземляющее устройство АТС (3). Часть тока затекает в систему уравнивания потенциалов здания, растекается по различным металлоконструкциям, оболочкам кабелей (в том числе к будке 2) и возвращается таким путем к тяговой подстанции. При этом напряжение на корпусах оборудования и других токоведущих частях превысило 500 В.

Применив к этому примеру "пирамиду аварий", увидим, что причиной аварии стало ошибочное инженерное решение, которое было реализовано из-за низкого качества проекта, плохой организации строительно-монтажных работ и безответственности должностных лиц, отдавших распоряжения вопреки законам физики и здравому смыслу. Можно считать, что причины перенапряжений в данном случае находятся на втором уровне (уровне технических решений и процессов), так как их источником служит заземляющее устройство объекта связи. Крупной аварии предшествовало несколько небольших повреждений и периодические сбои в работе систем связи, вызванные помехами. Если бы модули кроссовой защиты были выполнены из горючего пластика (применительно к "пирамиде аварий" – это потенциально опасное оборудование на уровне 2), в ЛАЗ мог возникнуть пожар. Авария произошла на железной дороге, являющейся источником повышенной опасности, была нарушена работа систем связи и СЦБ. При стечении определенных обстоятельств подобная ситуация может привести к крушению поезда с пассажирами или опасными грузами, то есть к катастрофе.

ПРИМЕР 4

Совершенно загадочная история произошла несколькими годами позже. Маленький, закрытый до недавнего времени город, рядом с ним – предприятие. Цех связи обслуживает и производство, и население. Устанавливают новое цифровое оборудование, и тут же оно регулярно начинает выходить из строя. Более того, вылетают типовые элементы замены (ТЭЗ) даже АТСКЭ и систем передачи, которые раньше работали без особых проблем. Связисты в отчаянии – без всякой видимой причины за одну смену может выйти из строя практически вся связь (как-то за смену было убито порядка 40–50 ТЭЗов).

Разгадка лежала на поверхности: при установке нового оборудования было построено новое заземляющее устройство, причем в непосредственной близости от проходившего рядом газопровода. Когда начался массовый выход аппаратуры из строя, решили сделать заземление еще лучше – еще больше электродов, дополнительные шины. Не помогло. Причиной опасности служил газопровод, в непосредственной близости от которого находились мощные источники помех (на производственных и испытательных площадках), а сама металлическая труба была приемником и проводником для них. Причем получить информацию об источниках помех и точном времени их возникновения, чтобы сопоставить

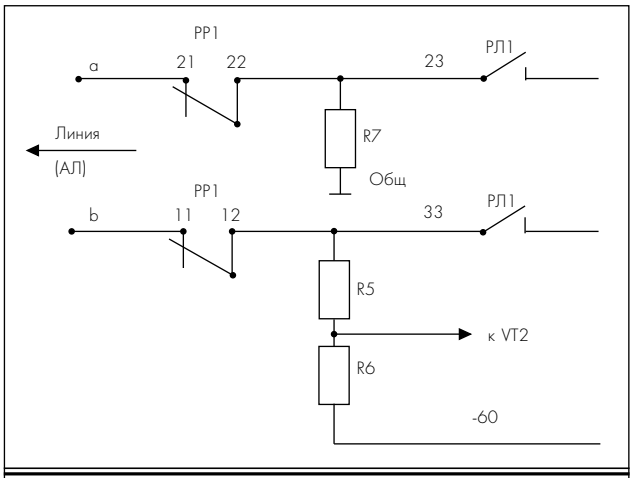


Рис.8. **Схема подключения комплекта АКР к абонентской линии**

со сбоями в работе связи, было, естественно, невозможно. Грунт – песчаный, поэтому часть тока, наведенного в трубе газопровода, текла в заземляющие устройства узла связи.

Итак, в этом примере приемником внешних помех тоже послужило заземляющее устройство, выбор места для которого производился без учета наличия такого вторичного источника перенапряжений, как газопровод. Последовательное "улучшение" заземления приводило все к более худшим результатам (это напоминает случай, описанный в примере 2 части 2).

ПРИМЕР 5

Еще через пару лет группа наших специалистов столкнулась с похожей проблемой – в коттеджном поселке при грозе повреждалась АТС, хотя линии связи были короткими, в хорошем состоянии, а в кроссе стояла защита. Наш инженер предположил, что заземление закопано рядом с трубой газопровода, чем заработал себе у коллег непререкаемый авторитет. Перенос заземляющего устройства от газопровода дал положительный результат. Очевидно, при ударе молнии поблизости от трассы газопровода большая часть тока молнии текла по его металлической трубе. Грунт был песчаный, т.е. с высоким удельным сопротивлением, поэтому существенная часть тока попадала в заземление АТС.

КВАЗИЭЛЕКТРОННЫЕ АТС

Очевидно, что АТСКЭ "Квант" в массе своей будут сняты с эксплуатации раньше, чем координатные АТС. И вряд ли будут вкладываться средства для продления срока их эксплуатации. Тем не менее, остановимся на них подробнее – уж очень показательный пример. Являясь электромеханической системой с программным управлением, АТСКЭ "Квант" с точки зрения защиты от перенапряжений похожа как на координатные, так и на цифровые АТС. Как и цифровые АТС (ЦАТС), "Квант" подвержена воздействию импульсных помех, в результате которого выходят из строя полупроводниковые приборы в различных блоках станции. Аналогично координатным АТС, в АТС "Квант" возможно подключение различных устройств (шнуровых комплектов, регистров, приемников тонального набора) через коммутационное поле к абонентской линии, на которой может присутствовать постороннее напряжение. В результате из строя могут выходить не только абонентские комплекты, но и другие приборы.

Таким образом, АТСКЭ "Квант" значительно более уязвима, чем координатная или цифровая станции практически любого типа. Следует отметить, что "Квант" разрабатывалась как учрежденческо-производственная АТС, а в качестве сельской стала применяться из-за отсутствия в 1980-х годах современного оборудования. Казалось бы, этого уже достаточно, но есть у станции "Квант" серьезная проблема, которая приводила к неоднократным возгораниям, иногда заканчивающимся большим пожаром на узле связи. Мне достоверно известно о трех случаях, два из них произошли в 2001 и 2002 годах, последний – два года назад (на самом деле их было значительно больше).

Рассмотрим одну из уязвимостей этой АТС. "Квант" имеет несколько типов абонентских комплектов, из них наиболее чувствителен к перенапряжениям комплект АКР-4. Почему так часто горит АКР-4? Как видно из его схемы (рис.8), если не установлено соединение, абонентская линия отключена от коммутационного поля АТС и приборов контактами реле РЛ1. К точке между R5 и R6 подключена база транзистора, который опрашивается процессором для детектирования поднятия трубки и определения цифр при импульсном наборе номера. При попадании в абонентскую линию постороннего напряжения 220 В/50 Гц повреждается резистор R7, а в определенных случаях – и R5. Резистор обугливается, появляется дым, а порой и открытый огонь. Этого бывает достаточно, чтобы поджечь печатную плату, особенно если постороннее напряжение попало на несколько абонентских линий.

Резисторы имеют сопротивление 2,7 кОм, допустимую мощность рассеивания 2 Вт. Быстрое возгорание наблюдалось при токе порядка 30 мА. Очевидно, что эта величина соответствует разговорному току, поэтому если бы даже и имелись элементы токовой защиты с такими характеристиками, применить их было бы невозможно.

После двух аварий, одна из которых закончилась большим пожаром, была создана рабочая группа в составе специалистов ЛОНИИС, оператора и НПО "Инженеры электросвязи". В результате были подготовлены рекомендации по защите АТСКЭ "Квант" [31]. Мы предложили эффективное решение, вполне доступное и в конце 1970-х годов, когда разрабатывалась "Квант". По всей видимости, тогда испытания комплекта АКР-4 на стойкость к перенапряжениям не проводились, поскольку пройти их он в принципе не мог.

ПЕРВЫЕ МАССОВЫЕ ЦИФРОВЫЕ АТС: DX-200 И МТ 20/25

Массовое внедрение цифровых АТС на отечественных сетях началось во второй половине 1980-х годов. Первая АТС DX-200 концерна Telenokia была установлена трестом "Лентелефонстрой" в 1984 году. До 1991 года в Ленинграде было введено в эксплуатацию 34 электронных АТС типа DX-200 общей емкостью 230 тыс. номеров. С этой АТС не было серьезных проблем как при сопря-

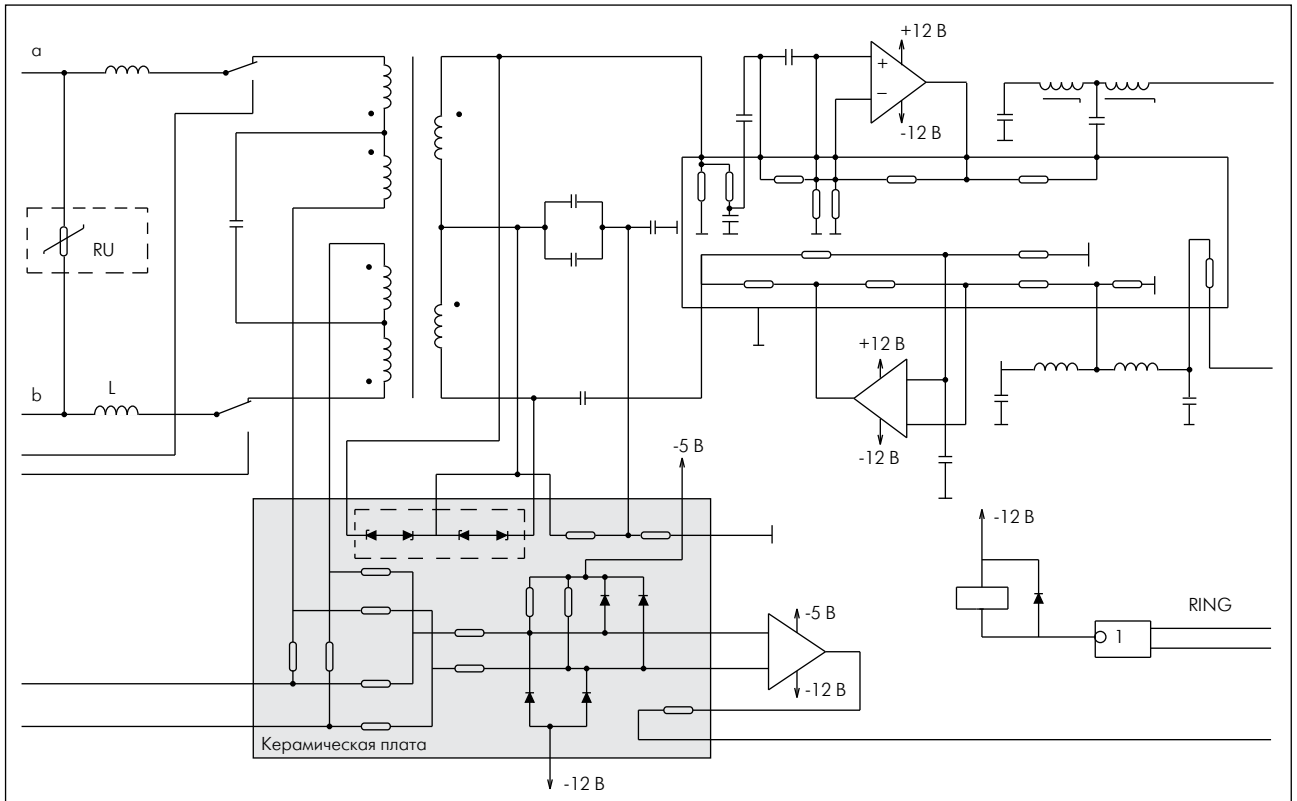


Рис.9. **Абонентский комплекс электронной АТС 4-го поколения**

жении с сетью, так и при дальнейшей эксплуатации. Более того, технические решения, заложенные в станции, позволяли модернизировать ее путем замены программного обеспечения с уровня R3/R4 до уровня L4,5, что позволило реализовать ОКС №7, СОРМ, тарификацию местных соединений и другие требования к современным системам коммутации [32].

В абонентском комплекте станции DX-200 (рис.9) защита реализована следующим образом. Между проводами a и b включен варистор с классификационным напряжением 150 В, далее дроссель в каждый провод. Как показала практика, в условиях ГТС Ленинграда (Санкт-Петербурга), когда практически весь кабель лежит в канализации, а вероятность удара молнии в линейные сооружения ничтожна, этого вполне достаточно. Если линии связи подвержены импульсным помехам (смешанные линии, подвесные кабели), то дополнительно в кроссе должны устанавливаться разрядники.

При попадании постороннего напряжения в один или два провода вызванный им ток протекает через резисторы, выполненные по пленочной технологии на керамической плате (выделена серым прямоугольником). При этом резисторы перегорают или же плата в месте нагрева трескается, разрывая цепь. Как правило, все этим и ограничивается – впоследствии требуется небольшой ремонт. Стабилитроны, включенные на выходе дифсистемы, служат скорее для устранения помех, чем для защиты от выхода кодека из строя. Причем повреждение печатной платы и элементов на ней возможно и при

токах, недостаточных для разрушения защитного сопротивления. В эксплуатации наблюдались случаи обугливания участков платы [33], что не вызывало возгорания благодаря высокой термоустойчивости применяемых материалов.

Поскольку к началу 1980-х годов попытки создать отечественную цифровую коммутационную систему не увенчались успехом, было принято решение приобрести лицензию, конструкторско-технологическую документацию и оборудование для производства таких АТС у французской фирмы Thomson CSF Telephone, впоследствии вошедшей в состав Alkatel. Для выпуска АТС МТ 20/25 был создан Уфимский завод коммутационной аппаратуры (УЗКА).

В 1985 году была выпущена первая АТС МТ 20/25 на импортной комплектации и основных конструкционных материалах, в 1987 году – на смешанной комплектации. С 1988 года промышленность приступила к выпуску АТС на отечественных компонентах и материалах [34]. Работы по изменению МТ 20/25 для производства промышленностью СССР (так называемая "советизация") проводились на "Красной Заре".

Можно предположить, что по согласованию с администрацией связи Франции фирма Thomson посчитала возможным снизить требования к стойкости от перенапряжений (что допускается рекомендацией K.20 МККТТ). В составе абонентской платы присутствуют только стабилитроны, включенные примерно так же, как и в DX-200. Защита от попадания постороннего напряжения в линию связи в абонентском комплекте не предусматривалась. Однако ее при необходимости всегда можно установить в кроссе. При подаче напряжения 220 В на вход абонентского комплекта последний выходил из строя, однако не горел.

Французскими специалистами для СССР были разработаны специальные сборки с металлическим креплением, на которых устанавливались стеклянные разрядники (типа отечественных Р-27) с напряжением срабатывания 250 В. Такое решение нельзя назвать удачным. Однако при освоении системы на УЗКА было найдено еще более неудачное [33].

Так, в отличие от решения Thomson разрядники были размещены не отдельно, а в общем пакете плат, заполняющих статив концентратора. Для этой цели была разработана плата PRO. Разрядники устанавливались в закрепленных на плате держателях из легковоспламеняющейся пластмассы. Кроме того, были введены элементы токовой защиты – позисторы (терморезисторы), увеличивающие сопротивления при протекании сверхтока. Они ставились в цепи после разрядников. Поскольку статическое напряжение пробоя разрядников составляло 250 В, то при попадании переменного напряжения 220 В разрядники пробивались (так как амплитудное значение составляло 310 В). При этом терморезисторы не срабатывают – ведь разрядники стоят перед ними и функцию свою выполняют. В разряднике, к которому постоянно приложено напряжение пробоя, тепловыделение настолько велико, что через несколько минут загораются пластмассовые держатели, затем изоляционные материалы платы (видимо, при "советизации" рационализаторы поработали и над платой). Таким образом, плата защиты оказалась основным источником опасности для АТС.

Испытания ЛОНИИС были проведены уже после того, как в 1989 году произошли возгорание плат PRO и пожар на узле связи в одном из городов Украины. Несколько подобных случаев было в 1990-х годах и в России. Чтобы оборудование перестало гореть, оказалось достаточным просто снять разрядники с платы PRO и, при необходимости, установить защиту в кроссе. Соответствующие рекомендации были разработаны по заказу Министерства связи, однако в начале 2000-х годов я еще видел установленные в платах PRO разрядники. Их не снимали даже после случаев обугливания и расплавления пластмассовых держателей.

Необходимо добавить, что на сетях России и Украины эксплуатируется немало АТС МТ 20/25 общей емкостью более миллиона номеров. До сих пор происходит модернизация как программного обеспечения, так и "железа" МТ 20/25, чем занимается несколько предприятий. Это говорит о том, что в целом система оказалась жизнеспособной, с потенциалом для развития. Все проблемы, связанные с перенапряжениями, были вызваны только тем, что на этапе разработки не были привлечены компетентные специалисты.

Продолжение следует

ЛИТЕРАТУРА

24. ГОСТ 27.002-89. Надежность в технике. Основные понятия, требования и определения.
25. Оценка риска повреждений, возникших вследствие разряда молнии. Рекомендация K.39. ITU-T, 1996.
26. Руководство по защите оптических кабелей от ударов молнии. – М.: ЦНИИС, 1996.
27. **Шеффи Й.** Жизнестойкое предприятие. – М.: АЛЬПИНА БИЗНЕС БУКС, 2006.
28. **Терентьев Д.Е.** Заземляющие устройства объектов связи: проблемы и пути их решения./ В сб. I Всероссийской конференции по заземляющим устройствам. – Новосибирск, 2002, www.commeng.ru.
29. **Терентьев Д.Е.** Высокочастотные свойства заземляющих проводников. – Электросвязь, 2004, №11, www.commeng.ru.
30. **Терентьев Д.Е.** Минимизация и стабилизация сопротивления разъемных контактов в системах уравнивания потенциалов и заземляющих устройствах./ В сб. VI всероссийской конференции "Состояние и перспективы энергетики связи". – СПб., 2004, www.commeng.ru.
31. Рекомендации по защите комплектов АКР в АТСКЭ "Квант" от перенапряжений и избыточных токов. – СПб.: ЛОНИИС, 2002, www.commeng.ru.
32. **Гольдштейн Б.С.** Модернизация станций DX-200: концепция и результаты. – Вестник связи, 1999 №11.
33. Средства защиты абонентских комплектов ЭАТС от перенапряжений и избыточных токов. Совершенствование средств защиты для ЭАТС МТ-20/25. – СПб.: ЛОНИИС, 1992.
34. **Шарипов Ю.К., Кобляков В.К., Сухих Е.А.** и др. Электронная автоматическая станция МТ 20/25./Под ред. Ю.К.Шарипова. – М.: Радио и связь, 1992.

АВАРИИ НА ОБЪЕКТАХ СВЯЗИ

Причина – опасные электромагнитные влияния

Часть 4*

Д.Терентьев
ic@commeng.ru

Защита от перенапряжений, как область техники, имеет очень интересную особенность. Многие специалисты с электротехническим образованием считают, что ничего сложного здесь нет – ведь значительная часть терминологии, физических моделей и математического аппарата основаны на институтских курсах физики и электротехники. С другой стороны, возникновение и характер электромагнитных помех, а также реакция технических систем на их воздействия могут зависеть от множества факторов, которые часто трудно или даже невозможно определить. Именно поэтому при решении задач по молниезащите, защите от помех и электромагнитной совместимости часто возникают ситуации, которым, как может показаться, нет рационального объяснения (пример 4 в части 3).

Мир молний полон неразгаданных тайн. Достаточно сказать, что существуют около 200 теорий, объясняющих природу шаровой молнии, но ни одна из них не получила абсолютного признания. Мы используем в качестве надежного инструмента методы теории вероятности и математической статистики, но иногда происходят и невероятные события. Так, американский лесничий Рой Кливленд Салливан в период с 1942 по 1977 годы был семь раз поражен молнией [35]. В связи с этим он получил прозвище "человек-громоотвод" и был занесен в Книгу рекордов Гиннеса.

- В 1942 году молния ударила Роя в ногу, когда он находился на пожарной башне, при этом оторвался ноготь на большом пальце;

*Продолжение. Начало см. Первая миля, 2011, №1, 2 и 5

- в 1969 году в результате удара молнии во время езды по горной дороге Рой остался без бровей и потерял сознание;
- в 1970 году очередной удар молнии привел к травме левого плеча, руку при этом парализовало. Это произошло на лужайке его собственного дома;
- в 1972 году из-за удара молнии на территории административного здания лесничества загорелись волосы Салливана. После этого случая он всегда возил с собой емкость с водой;
- 7 августа 1973 года молния ударила в голову Роя, когда он ехал в машине по территории вверенного ему леса. От удара снова загорелись волосы, лесника выкинуло из машины и с ног сорвало обувь;
- 5 июня 1976 года шестой удар молнии привел к сильной травме лодыжки на территории палаточного лагеря;
- 25 июня в 1977 года молния отправила Роя Салливана на больничную койку с ожогами грудной клетки и живота. Рой всего лишь хотел порыбачить.

Досталось и его жене, которая тоже получила удар молнией, когда развешивала белье. Люди стали избегать Салливана из-за страха быть пораженными молнией заодно с ним. И все-таки погиб он не от молнии, а покончил с собой в возрасте 71 года выстрелом в живот – как сообщается, из-за неразделенной любви.

Согласно статистике, вероятность поражения человека молнией в течение жизни составляет 1:3000. Таким образом, математическая вероятность произошедшего с Салливаном составляет $1:3000^7$, то есть примерно $5 \cdot 10^{-26}$. Конечно, род занятий Салливана, связанный с постоянным пребыванием на природе, делал поражение молнией несколько более вероятным.

Есть и другие необъяснимые с сугубо материалистической точки зрения факты, которые даже заставляют некоторых исследователей предполагать у некоторых электромагнитных явлений наличие интеллекта. Однако вернемся от загадочных явлений к тем, для понимания сути которых достаточно знания законов физики.

КАКИЕ ГРОЗЫ ПОМНИТ ЛИНЕЙНЫЙ ИНЖЕНЕР?

Весной 1996 года в Гатчинском РУС Ленинградской области на большей части регенераторов ЦСП ИКМ-30 и ИКМ-15 были установлены модули защиты. В результате число отказов аппаратуры существенно снизилось. Казалось бы, все очевидно. Но польза от применения устройств защиты еще какое-то время была сомнительной для ряда руководителей – просто "Гатчинский район стали обходить грозы". Конечно, грозы все-таки были, но как крестьянину гроза запоминается гораздо лучше, если у него сгорел стог сена, так и связисту – если вышло из строя оборудование и был перерыв связи. Связь работала – значит, гроз не было.

Рис.10. Воздействие межоблачного разряда на проводник, проложенный в земле

Понадобилось несколько лет, чтобы польза средств защиты стала очевидной. Только в начале 2000 года началась массовая установка устройств защиты типа МЗСП-Е1 (модуль защиты систем передачи Е1) на зоновой сети в Ленинградской и Новосибирской областях. В результате число повреждений регенераторов из-за воздействия молний и коммутационных помех от высоковольтных ЛЭП снизилась в ОАО "Ленсвязь" в 10 раз, в ОАО "Электросвязь" Новосибирской области – в 7 раз [36].

Меня однажды попросили объяснить, почему десяток сильных гроз в районе прокладки кабельной линии никак на нее не повлияли, а в сентябре несколько раз громыхнуло, и линия встала – вышли из строя сразу три регенератора. Попробую дать ответ.

Рассмотрим простой случай – межоблачный разряд над участком, где в грунте проложен изолированный проводник (рис.10). В соответствии с законом электромагнитной индукции, ЭДС, индуцируемая в проводнике током i, протекающем в другом проводнике, прямо пропорциональна изменению силы тока:

$$\varepsilon = - M \cdot di/dt,$$

где M – коэффициент взаимоиндукции, определяющий взаимную индуктивность проводников.

От чего зависит эта ЭДС? Пусть разряд молнии параллелен поверхности земли и проходит по прямой линии, трасса кабеля также прямолинейна (см. рис.10). Тогда коэффициент взаимоиндукции M определяется такими величинами, как длина трассы прокладки проводника, на которую воздействует удар молнии (L); расстояние от канала молнии до поверхности земли (H); угол между проекцией канала молнии и трассой прокладки (α), при изменении которого от 0 до 90° M изменяется от максимального значения до нуля. Даже если и принять эту крайне упрощенную модель, то придется учесть конструкцию кабеля, удельное сопротивление грунта, сопротивление заземляющих устройств регенераторов. Амплитуда тока молнии может изменяться от единиц до сотен килоампер, время разряда находиться в пределах 5–100 мкс, в одном канале может быть несколько повторных разрядов и т.п. Причем модель описывает случай, когда воздействие происходит через электростатическую и электромагнитную индукцию. Гораздо опаснее удары молнии в землю рядом с кабелем, и модель их влияния еще сложнее.

Вывод: субъективная оценка опасных влияний (например, число и яркости молний, гром, личные впечатления) не должна приниматься в качестве основного критерия при оценке причин повреждений и электромагнитной безопасности. Безусловно, корреляция между впечатлением и реальным положением дел присутствует и возрастает с ростом квалификации наблюдателя – но тогда субъективная оценка становится мнением эксперта.

ЗАЩИТА ОТ ПЕРЕНАПРЯЖЕНИЙ: ПРИНЦИПЫ

Какая цель ставится при проведении мероприятий по защите? Чтобы получить руководство к действию, надо представить мероприятия по защите как некий оператор, преобразующий электромагнитные воздействия по определенному правилу. Под мероприятиями по защите понимается не только установка защитных устройств, но и создание системы уравнивания потенциалов, правильный монтаж, методы эксплуатации и т.п.

Мероприятия по защите снижают опасные влияния до допустимого уровня (рис.11). При этом допустимые уровни заранее известны и обычно зависят от стойкости оборудования, которая определяется стандартами, оговаривается в технических условиях и проверяется при сертификационных испытаниях. Значит, следует определить множество опасных влияний, от которых необходима защита. Таким образом, мероприятия по защите являются функцией множества ожидаемых опасных воздействий и уровней воздействий, безопасных для оборудования. На практике обязательно также учитываются вероятностные характеристики опасных влияний, стоимость мероприятий по защите и требования к надежности функционирования оборудования.

В качестве примера приведем защиту цепей питания оборудования связи переменным током. В соответствии со стандартом [37], оборудование проводной связи должно выдерживать воздействие импульсов с фронтом 1 мкс и длительностью 50 мкс и с амплитудой в цепях электропитания по схеме "провод-земля" – до 2 кВ, в цепях электропитания по схеме "провод-провод" – до 1 кВ. В зависимости от ожидаемого уровня воздействий необходимо применить разные решения: при защите от коммутационных помех или наводок от ударов молнии установить устройства защиты от импульсных помех (УЗИП) только III класса. Если вероятны прямые удары молнии в антенно-мачтовые сооружения или при силовом вводе воздушной ЛЭП может потребоваться полный комплекс мероприятий по защите в соответствии с зоновой концепцией защиты [38, 39].

Опасные влияния на системы связи можно разделить на две группы: импульсные помехи и сверхтоки. Встречаются (к счастью – не часто) помехи, которым одновременно присущи и высокое напряжение, и длительное воздействие. Такое крайне опасное сочетание возникнет, если провод высоковольтной ЛЭП под напряжением соединится с проводами линий связи – например, при грубых нарушениях правил строительства и эксплуатации линий связи. Но они редки и более характерны для крупных энергетических объектов. Обычно связисты сталкиваются со значительно более мягким вариантом такого "смешанного" типа влияний, когда кабель связи проложен прямо под опорами высоковольтной ЛЭП (эти случаи мы рассмотрим в последующих публикациях).

ЗАЩИТА ОТ СВЕРХТОКОВ

Источником сверхтоков обычно служат электроустановки и электрифицированные железные дороги. При значительно меньшем уровне напряжения их воздействие дольше: попросту говоря, если в кабель связи попало постороннее

напряжение – это надолго. Именно воздействие сверхтоков привело к пожарам, которые были описаны в предыдущих частях статьи.

Сосредоточимся на борьбе со сверхтоками только в линиях связи. В отличие от импульсных помех, уровень опасных токов обычно близок к максимальным рабочим токам оборудования. Например, ток порядка 110–120 мА, протекающий через абонентский комплект цифровой АТС, может привести к повреждению. Рабочий же ток в зоне прямого питания (если телефон установлен в соседнем с АТС здании) может достигать 45–50 мА.

Для линий связи устройства защиты от сверхтоков работают по тепловому принципу – при протекании тока происходит нагрев элемента, благодаря чему плавится припой и освобождается пружина в термокатушке, перегорает предохранитель, переходит в высокоомное состояние позистор и т.п. Позисторы постоянно совершенствуются и являются основными элементами токовой защиты в системах проводной связи. Но даже позистор, перед тем как сработать, должен нагреться – на что нужно время. Для быстрого срабатывания позистора ток, протекающий через него, должен значительно превышать максимально допустимый рабочий ток. Поэтому приходится балансировать на тонкой грани между эффективностью защиты и возможностью срабатывания позистора от рабочего тока.

ПРИМЕР 6

Заказчик поставил задачу обеспечить максимально эффективную защиту новой цифровой АТС от сверхтоков, для чего в модули кроссовой защиты были установлены керамические позисторы с максимально допустимым рабочим током 50 мА. Защита была установлена в кросс 7 марта. Через несколько дней в бюро ремонта стали поступать заявки о повреждении: по словам абонентов, сначала был слышан треск, слышимость ухудшалась, затем соединение прерывалось. Так как заявка делалась обычно с "неисправного телефона", контрольное соединение и измерения повреждения не выявляли – повреждения как бы и не было. Особо настойчивым абонентам задавался вопрос: "а телефон у вас сертифицирован"?

Примерно через месяц руководство районного узла связи поняло, что проблема реально существует и обратилось к фирме, поставившей защиту – т.е. к нам. Выявилась странная закономерность: жалобы поступали от небольшой

Рис.11. Воздействие межоблачного разряда на проводник, проложенный в земле

группы абонентов, объединенной тремя общими признаками:

- все они жили рядом с зданием узла связи;
- они приобрели недавно завезенные в город дешевые китайские телефоны;
- все пострадавшие абоненты любили долго разговаривать по телефону, нарушения связи наступали через 10, 20 или даже 30 минут разговора.

Выяснилось, что сопротивление этих телефонов при снятой трубке было очень мало (порядка 100 Ом). В результате позистор находился в граничном режиме, постепенно увеличивал сопротивление и затем переходил в непроводящее состояние. Проблему решили заменой модулей защиты с позисторами на 80 мА на небольшой части плинтов. Та же самая проблема, но в значительно меньшей степени, присутствует и у полимерных позисторов, поэтому в своей линейке кроссовой защиты мы применяем в качестве стандартного варианта элементы с максимальным током 55 мА, и 80 мА – по заказу. Более детально вопросы элементной базы для защиты рассмотрены в работах [40–42] – они не только интересно и грамотно написаны, но и доступны в сети.

Кроме элементов защиты, принцип действия которых основан на пробое газового промежутка (разрядники), тепловом пробое pn-переходов (варисторы, тиристоры, стабилитроны и т.п.), изменении характеристик материала при нагревании (позисторы), существуют элементы защиты, принцип действия которых – размыкание линии связи полупроводниковым ключом. Реализация такого принципа стала возможной с появлением транзисторов со стабильными характеристиками, низким сопротивлением в открытом состоянии и стойкостью к высокому (сотни вольт) приложенному напряжению – в закрытом. Такие транзисторы стали доступны только 10–15 лет тому назад. Первый элемент на подобном

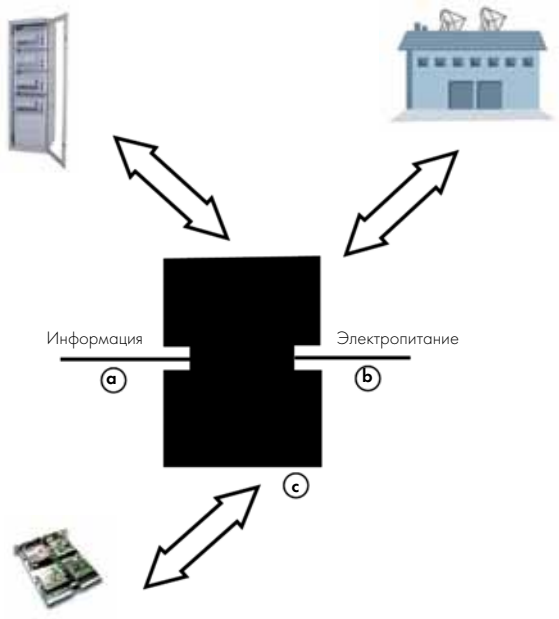


Рис.12. Система связи в виде "черного ящика"

принципе ЭТЗ (элемент токовой защиты) был разработан группой специалистов из Орла и Санкт-Петербурга и производился фирмой "Синтэк" [43–46]. Второй – через несколько лет после этого фирмой Bourns (США) [47], элемент получил название TBU и серийно выпускается. ЭТЗ разрабатывался как моментально действующий элемент для защиты от сверхтоков, принцип работы TBU основан на размыкании линии при прохождении по ней импульсной помехи.

К сожалению, сейчас ЭТЗ не производится, так как российский рынок имеет слишком низкую емкость для того, чтобы организовать крупносерийный выпуск этих микросхем, а условия для производства и экспорта высокотехнологичной продукции в России несравнимы с любой экономически развитой страной.

Нельзя не упомянуть о том, что устройства защиты не должны оказывать влияния на режимы работы систем связи и электропитания. Поэтому при разработке, производстве и выборе устройств защиты должны учитываться не только параметры ожидаемой помехи, но и рабочие токи и напряжения, спектр передаваемых в линии сигналов. С ростом скорости передачи в линиях связи измерения электрических параметров стало недостаточно. Так, в НПО "Инженеры электросвязи" при разработке устройств защиты для современных систем цифровой передачи (в том числе – Ethernet) проводятся измерения их влияния на скоростной потенциал линии [48].

ЗАЩИТА ОТ ИМПУЛЬСНЫХ ПОМЕХ

Импульсные помехи имеют высокую амплитуду и короткую продолжительность. Их причиной служат наводки от ударов молнии, переключений на высоковольтных ЛЭП, резкие изменения нагрузки в электросетях. Наиболее мощной импульсной помехой является прямой удар молнии. Обращаю внимание на два важных момента, справедливых как для цепей передачи информации, так и электропитания:

- энергия импульсных помех (за исключением прямых ударов молнии) относительно невелика;
- задачу защиты от импульсных помех значительно облегчает тот факт, что рабочее напряжение и максимальное безопасное для оборудования напряжение значительно различаются, а такие устройства защиты, как разрядники, варисторы, полупроводниковые элементы достаточно резко переходят в проводящее состояние при превышении порога срабатывания.

Устройства защиты от импульсных помех – это часть системы уравнивания потенциалов. Такой вывод можно сделать, если внимательно изучить литературу по технике защиты от перенапряжений, хотя подобная формулировка нигде не встречается. Мне понадобилось семь лет работы в этой области, прежде чем я смог сформулировать для себя этот принцип [49]. В результате пути решения многих проблем стали очевидны, удалось просто объяснить решения, найденные интуитивным путем.

Представим различные защищаемые объекты – плату ТЭЗ, статив, объект связи в целом – в виде "черного ящика" (рис.12). К нему подключается по крайней мере одна линия передачи информации, одна линия электропитания и токопроводящие элементы, имеющие нулевой электрический потенциал. Элементы с нулевым потенциалом на плате – это дорожки и контакты разъемов, в стативе к ним добавляются металлоконструкции (корпус). На объекте связи элементы с нулевым потенциалом – это система уравнивания потенциалов, к которой подключены остальные элементы, вплоть до дорожек "земли" на плате.

Для простоты представим, что данные и электропитание передаются по однопроводным линиям (a и b, соответственно), система также имеет "общую точку" (c) – металлический конструктив ТЭЗ, металлический статив, систему уравнивания потенциалов узла связи.

Пусть имеется набор импульсных перенапряжений с определенными значениями амплитуды, длительностями и формами импульсов, которые могут привести к выходу системы из строя. То есть мы можем любой технической системе поставить в соответствие набор значений напряжений U_{a-b}, U_{b-c}, U_{c-b}, при воздействии которых она выходит из строя.

Чтобы защитить техническую систему от импульсных помех, необходимо уровнять потенциалы всех токоведущих частей, для чего их необходимо соединить. К системе уравнивания потенциалов здания мы подключаем водопроводные трубы, оболочки кабелей, короба вентиляции, корпуса оборудования и т.д. Но нельзя напрямую соединить с ней провода кабелей связи и электропитания. Для этого применяются устройства защиты от импульсных помех (УЗИП), которые, не нарушая режимов передачи информации и электроэнергии, при определенном уровне разности потенциалов начинают пропускать через себя ток уравнивания потенциалов. Отсюда вывод: устройства защиты от импульсных помех являются частью системы уравнивания потенциалов. Два следствия из него:

- УЗИП бесполезны (не эффективны), если система уравнивания потенциалов отсутствует или не обеспечивает низкого сопротивления на высоких частотах между точками подключения к ней;
- УЗИП бесполезны, если они не подключены к системе уравнивания потенциалов или подключены неправильно.

ЗАЗЕМЛЕНИЕ ИЛИ УРАВНИВАНИЕ ПОТЕНЦИАЛОВ?

До сих пор в этой части статьи мы ни разу не использовали слово "заземление". А может ли быть защита от перенапряжений, вплоть до ударов молнии, без защитного заземления? Да, может. Представим себе узел связи, у которого нет не только заземления, но и вообще

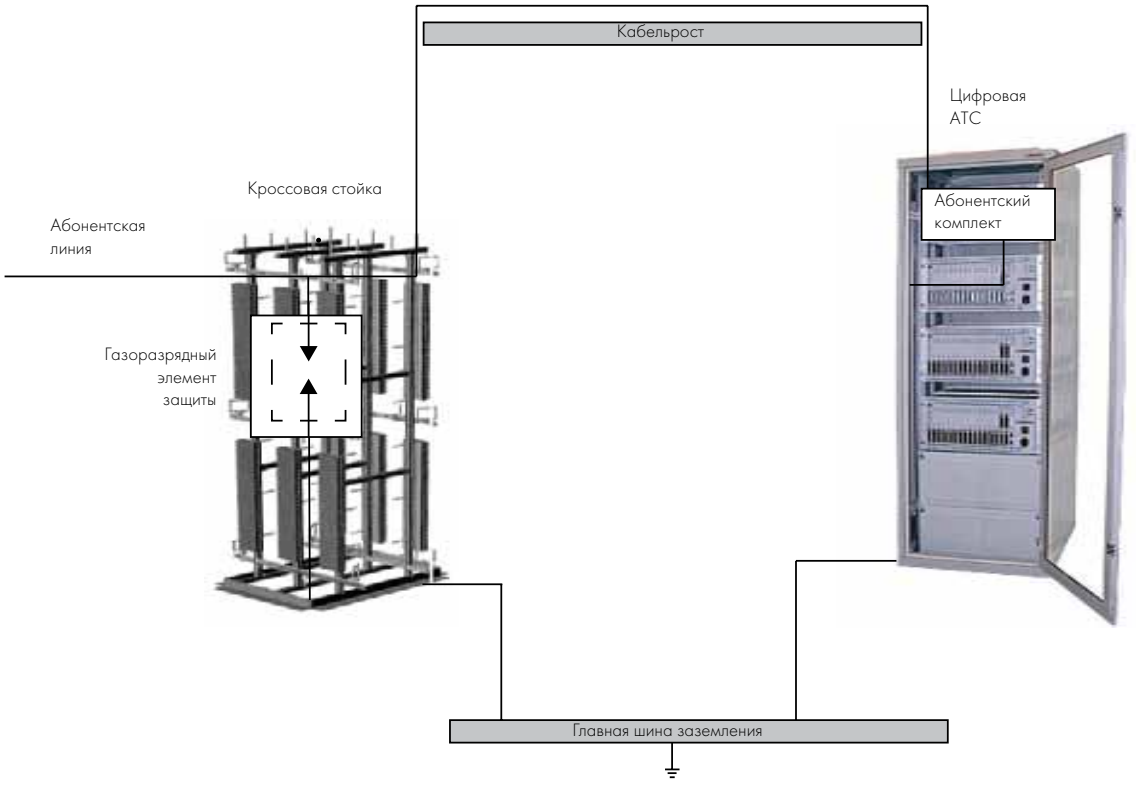


Рис.13. Сопротивление между заземляющим контактом разрядника и корпусом статива АТС может оказаться слишком большим

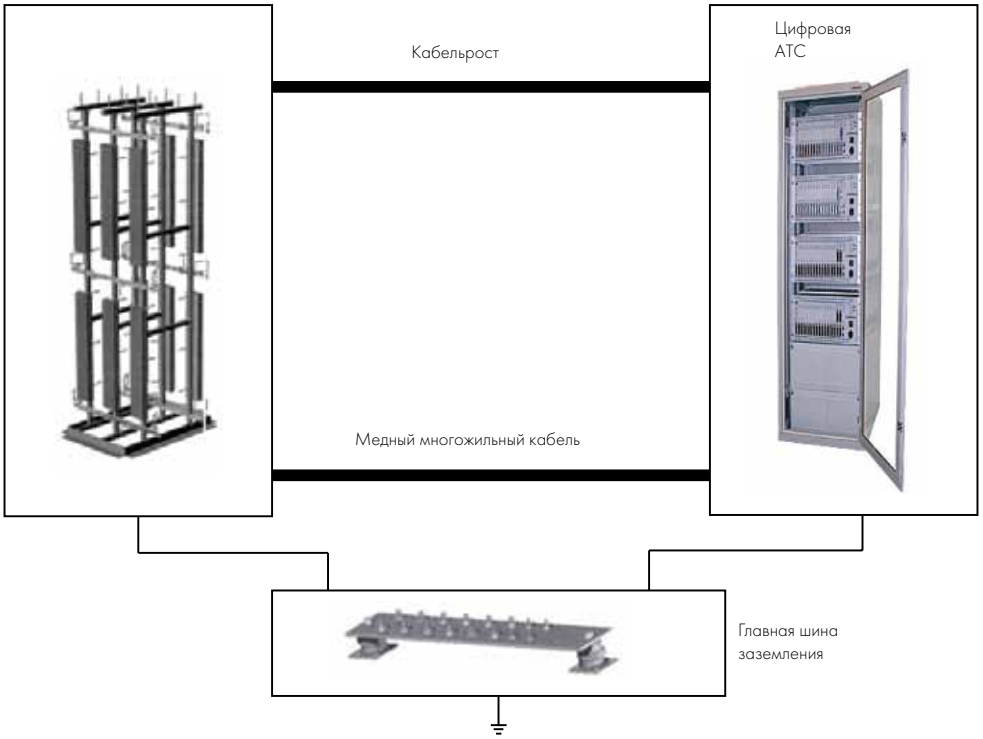


Рис.14. Уравнивание потенциалов. Необходимо дополнительно соединить контакты заземления кросса и статива АТС медным многожильным кабелем, проложив его по кратчайшему пути

контакта с землей – например, дирижабль или самолет с ретранслятором. Удары молнии в летательные объекты – обычное дело, там есть и устройства защиты, и система уравнивания потенциалов, в качестве которой используется металлическая оболочка. Однако при приземлении самолета его подключают к заземляющему устройству. То есть в самом общем случае заземляющее устройство служит для уравнивания потенциалов земли и системы уравнивания потенциалов объекта.

Ни в коей мере не отрицая важность заземляющих устройств для электробезопасности, защиты от перенапряжений и ЭМС в целом, отметим, что иногда приходится решать вопросы защиты при невозможности подключения к заземлению (если организована изолированная система уравнивания потенциалов [28]), или просто при его отсутствии.

УСТРОЙСТВА ЗАЩИТЫ КАК ЧАСТЬ СИСТЕМЫ УРАВНИВАНИЯ ПОТЕНЦИАЛОВ

Рассмотрим достаточно распространенный пример построения системы защиты на АТС (рис.13). Абонентские линии входят в кросс, где к ним параллельно подключаются газоразрядные элементы, установленные в кассетах в кроссовой стойке. Далее кабель абонентской линии по кабельросту (несущий кабельный лоток из стали) проходит до стойки цифровой АТС. Конструктив кросса соединен с главной шиной заземления (ГШЗ). Кроме того, к нему присоединен (механически, как правило – прикручен) кабельрост, который другим концом прикреплен к стативу цифровой АТС. Статитв АТС также соединен кабелем с ГШЗ. Для нас принципиально, что газоразрядные элементы защиты подключены к шине заземления по схеме: контакт заземления кассеты – монтажная скоба – металлический конструктив кросса – кабель заземления – ГШЗ. В свою очередь, общая точка (земля) аппаратуры абонентского комплекта АТС соединена с главной шиной заземления по схеме: статив АТС – кабель заземления – ГШЗ. Кроме того, каркас кросса и статив АТС связаны между собой кабельростом.

Возможны два варианта воздействия импульсной помехи на абонентский комплект АТС: бросок "потенциала земли" и помеха в линии связи. Хотя механизмы их возникновения и воздействия различны, для пони-

мания достаточно ограничиться последним, причем рассмотрим только один провод линии связи.

При попадании высокого напряжения задача системы защиты – обеспечить низкую разность потенциалов между входом абонентского комплекта и его общей точкой. Когда импульс высокого напряжения поступает в провод абонентской линии, в газоразряднике загорается дуга, через него течет ток уравнивания потенциалов между линией и стативом АТС по следующей цепи: провод линии связи – разрядник – контакт заземления кассеты – монтажная скоба – металлический конструктив кросса. Далее ток распространяется по двум основным цепям:

- кабель заземления кросса – ГШЗ – кабель заземления АТС – статив АТС;
- кабельрост – статив АТС.

В теории сопротивление всех этих цепей должно быть близким к нулю. Тогда при попадании на абонентскую линию высоковольтной помехи разность потенциалов на входе абонентского комплекта и на стативе АТС будет определяться падением напряжения в газоразряднике и не превысит предельно допустимый уровень (токи выравнивания потенциалов не приведут к дополнительным падениям напряжения на различных участках этой цепи). Но на практике ситуация совсем иная.

Разность потенциалов между проводом абонентской линии и общей точкой абонентского комплекта АТС (с точки зрения цепи выравнивания потенциалов) будет определяться суммой падения напряжений на дуге в разряднике (порядка 10–30 В, в зависимости от тока, при установившемся режиме), в конструктиве кросса и на элементах цепи от конструктива кросса до статива АТС.

Уже из описания цепей выравнивания потенциалов на рис.13 видно, что они составлены из различных элементов и различных материалов (кабели, элементы конструктива, кабельросты в качестве проводников и т.п). Если пройти по цепочке соединений от разрядника до болта заземления кросса, то при непрофессиональном монтаже с применением подручных материалов весьма вероятно, что где-то контакт будет плохим (если не рассматривать случай, что его вовсе нет). Уже один этот факт способен привести к существенному падению напряжения в зонах плохих контактов, т.е. никакого выравнивания потенциалов не произойдет.

Кроме того, при анализе импульсных помех нельзя забывать о реактивной составляющей сопротивления цепей, т.е. по крайней мере о собственной индуктивности проводников. Она зависит от материала и конструкции проводника – в частности, индуктивность проводника из меди или алюминия (не ферромагнетики) на три порядка ниже, чем стального. Только по этой причине кабельрост едва ли эффективен как проводник в цепи уравнивания потенциалов. Подробно этот вопрос рассмотрен в работе [50], отметим лишь, что если подключение кросса к системе уравнивания потенциалов выполнено так, как показано на рис.13, индуктивное сопротивление цепи выравнивания потенциалов может оказаться значительно большим, чем сопротивление проводов абоненткой линии от плинта до абонентского комплекта АТС.

Таким образом, чтобы защитить аппаратуру АТС от воздействия импульсной помехи, необходимо, чтобы сопротивление цепи протекания тока уравнивания потенциалов от разрядника и до статива АТС было сопоставимо с сопротивлением жилы кабеля абонентской линии (лежащего на кабельросте). Чтобы этого достичь, достаточно соединить кросс со стативом АТС медным проводником по кратчайшему пути (рис.14). Именно такой способ монтажа описывается в инструкциях по монтажу рядя типов АТС (например, EWSD фирмы Siemens).

ПРИМЕР 7

В 2004 году к нам поступила рекламация на устройства защиты: после их установки повреждаемость оборудования АТС практически не снизилась по сравнению с прошлым годом и составила к середине июля более 10 ТЭЗ абонентских комплектов при общей емкости порядка 6 тыс. портов. Для выяснения причин пришлось срочно выехать на место.

Как обычно, выявилось довольно много причин для отказов. И грозовая активность в месте установки оборудования была в три раза выше, чем в расположенном в двух часах езды центре региона, и линейные сооружения связи находились в ужасном состоянии, какая-либо защита в кабельных ящиках отсутствовала. При этом большинство линий было выполнено проводами на изоляторах или подвесными кабелями, как часто бывает в южных районах при малоэтажной застройке. Но как всегда, была и основная причина.

Монтаж кросса был выполнен, как показано на рис. 13. При этом нас уверяли, что кабельрост обеспечивает хорошее электрическое соединение между кроссом и стативом АТС. Он был собран из окрашенных секций и просто лежал на окрашенном стативе АТС. Чтобы померить сопротивление, соскребли немного краски на кабельросте и на корпусе АТС, подключили тестер. Расстояние между точками подключения – сантиметров 20. Измерить сопротивление не удалось, вместо него измерили напряжение – 3,5 В! Его источник мы искать не стали, но было абсолютно ясно, что при мощных импульсных помехах разность потенциалов достигает величины, достаточной для повреждения оборудования. Проблема была решена соединением кросса и статива АТС медным кабелем, как показано на рис.14. Поставленный диагноз и выбор метода лечения оказались точными – в течение трех последующих лет отказов не было.

Однако в моей практике было несколько случаев, когда после всех описанных действий повреждения случались значительно реже, но продолжали происходить, причем их характер менялся.

ПРИМЕР 8

АТС обслуживала коттеджный поселок, в котором малопарные кабели были подвешены на столбах и стойках. Выход из строя абонентских комплектов во время гроз очень беспокоил оператора, по его просьбе для определения причин мы командировали туда специалиста. Причина была аналогична описанной выше. После проверки контактов и соединения кросса и АТС кабелем напрямую повреждаемость резко сократилась, однако изменился характер повреждений: стали выходить из строя источники вторичного электропитания на ТЭЗ АК, а также элементы, к которым подключались цепи питания.

Вспомним наш "черный ящик" (см. рис.12): мы уменьшили разность потенциалов между проводами линий связи и стативом АТС ниже опасного уровня, одновременно увеличив разность потенциалов между стативом АТС и проводами ЭПУ постоянного тока. Для того чтобы уменьшить ее, оказалось достаточно установить УЗИП на входах электропитания АТС, после чего повреждения прекратились.

Продолжение следует

ЛИТЕРАТУРА

35. **Салливан, Рой.** – www.ru.wikpedia.org.
36. **Терентьев Д.Е., Шорин О.В., Краснопольский Н.И.** Защита оборудования линейного тракта систем передачи. – Вестник связи, 2001, №4, www.commeng.ru.
37. ГОСТ Р 50932-96. Устойчивость оборудования проводной связи к электромагнитным помехам. Требования и методы испытаний.
38. IEC-1024-1 (1990-03). Защита сооружений от удара молний. Часть 1. Общие принципы.
39. IEC-1312-1 (1995-02). Защита от электромагнитного импульса молнии. Часть 1. Общие принципы".
40. **Курышев К.Н.** Элементы защиты по току и напряжению Raychem Circuit Protection в телекоммуникационных цепях. – Компоненты и технологии, 2005, №4, www.konkurel.ru
41. **Курышев К.Н.** Все, что вы хотели узнать о PolySwitch, но боялись спросить. Компоненты и технологии, 2006, №3, www.konkurel.ru.
42. **Родионов М.Г.** Введение в технику защиты от перенапряжений/В сборнике [20]. – www.commeng.ru
43. Свидетельство на полезную модель №18031, Зарегистрировано 10.05.2001. Устройство токовой защиты. Авторы: Терентьев Д.Е., Цейтин А.Г.
44. Заявка № 2005106970/09 от 10.03.2005. Устройство защиты от токовых перегрузок. Авторы: Барановский Д.М., Терентьев Д.Е., Федосов В.С.
45. **Пашкевич А.Ю., Сергеев А.В., Федосов В.С., Барановский Д.М.** Совместная разработка производителей оборудования связи и компонентов. – Техника связи, 2006, №3, www.commeng.ru.
46. **Барановский Д.М.** Интегральные микросхемы токовой защиты К294ХП1. – Компоненты и технологии, 2007, №1.
47. www.bourns.com
48. **Терентьев Д.Е.** Метрологическое обеспечение разработки, производства и эксплуатации устройств защиты проводной связи/ Сб. трудов конференции "Кабели и линии связи" в г.Анапа, 2007 г. – www.commeng.ru
49. **Терентьев Д.Е.** Устройства защиты от импульсных помех, как часть системы уравнивания потенциалов объекта связи. – Техника связи, 2006, №1, www.commeng.ru
50. **Терентьев Д.Е.** Высокочастотные свойства эквипотенциальных проводников. – Электрическое питание, 2004, № 3–4.

АВАРИИ НА ОБЪЕКТАХ СВЯЗИ

Причина – опасные электромагнитные влияния

Часть 5*

Д.Терентьев
ic@commeng.ru

Инженеры и не инженеры видят окружающие нас вещи и явления по-разному – видимо, потому, что первые всегда имеют дело с реальными системами и устройствами при их реальной эксплуатации. Именно им приходится расхлебывать многочисленные проблемы, обусловленные не чисто техническими или чисто субъективными факторами, а их сложной смесью. Одну из самых известных проблем такого рода описал в 1949 году капитан ВВС США Эдвард Мерфи, в то время – инженер исследовательского проекта MX981, сформулировав "Закон Мерфи": "Если какая-нибудь неприятность может произойти, она случится". Заметим, сам Мерфи формулировал свой закон и ряд следствий из него совершенно серьезно. Многочисленные последователи развили законы Мерфи, многие из них собраны в книжке "Законы Мерфи" [52].

В полной мере "законы Мерфи" применимы и к различным элементам систем связи, в том числе – к системам их защиты. Ведь эти законы – отражение типичных человеческих ошибок при работе с техническими системами. Проанализируем наиболее типичные проявления этих законов в области устройств защиты, сосредоточив внимание на особенностях технических решений в этой сфере.

Может ли один удар молнии стоить миллиард долларов?

Предоставленные самим себе, события имеют тенденцию развиваться от плохого к худшему.

В конце 1990-х годов значительную часть мобильных телефонов производили две скандинавские компании – Nokia (27% мирового производства) и Ericsson(12%). Обе фирмы являлись технологическими лидерами, конкурировали между собой и никто не собирался уступать. Но уже в конце 2000 года их рыночные доли составляли соответственно 30 и 9%. Ericsson сообщила об убытках подразделения по производству мобильных телефонов в размере 2,34 млрд. долл., в январе 2001 года объявила о своем намерении уйти с рынка мобильных телефонов. В апреле 2001 года было подписано соглашение с корпорацией Sony

*Продолжение. Начало см. Первая миля, 2011, №1, 2, 5 и 6.

о создании совместного предприятия. Что же оказало столь сильное влияние как на Nokia и Ericsson, так и на телекоммуникационный рынок в целом [27]?

Около 20 ч 17 марта 2000 года в здание полупроводникового завода компании Royal Philips Electronics (Philips N.V.), расположенное в Альбукерке (штат Нью-Мексико, США), ударила молния, после чего возник пожар [27, 51]. Сработала автоматическая система пожаротушения, огонь был потушен в течение 10 мин силами персонала. Прибывшим на место пожарным осталось только удостовериться, что все в порядке, и оформить документы. На первый взгляд, ничего страшного не произошло – повреждения были очень локальными, реально пострадали несколько кассет с полупроводниковыми пластинами (комплектующие для нескольких тысяч телефонов).

Но подлинная драма, отразившаяся на нескольких корпорациях и судьбах тысяч людей, была впереди. Дым, распространившийся по всему зданию, обувь пожарных, обошедших с инспекцией помещения, оставили грязные следы, нарушили чистоту гермозон – особо чистых помещений для производства полупроводниковых приборов. В результате оказались испорченными пластины, находившиеся на различных стадиях производства, которых хватило бы на выпуск микросхем для миллионов аппаратов. Тем не менее, руководство завода полагало, что восстановить чистые помещения и запустить производственный цикл удастся в течение недели. Об этом оно и решило сообщить своим потребителям, в первую очередь Nokia и Ericsson, что и было сделано в понедельник, 20 марта. Дальнейший ход событий был определен различной корпоративной культурой этих компаний и их реакцией на сообщение поставщика.

Nokia не очень встревожило сообщение о недельной задержке, которую можно было компенсировать запасом комплектации на складе. Однако ситуация немедленно была взята под особый контроль, и когда стало ясно, что запуск производства займет несколько недель, а восстановление графика поставок – несколько месяцев, план действий уже был готов. Nokia провела анализ возможностей производителей и разместила заказы на их заводах в различных регионах мира. Так как несколько позиций могла изготавливать только Philips, Nokia выдвинула жесткие требования и настояла на перераспределении и максимальном использовании производственных возможностей поставщика. В результате ее конвейер не остановился и потребители могли получать телефоны самых последних модификаций.

Сотрудники Ericsson спокойно отреагировали на сообщение о недельной задержке и не сообщили об этом происшествии руководству, даже когда стало ясно, что поставка комплектующих задерживается существенно. Когда проблема стала очевидной, было уже поздно: резервные мощности не только Philips, но и других производителей были уже заняты заказами Nokia.

В результате пожара потери продаж полупроводниковых приборов Philips составили менее 1%, прямой ущерб заводу был покрыт страховкой. Значительно более сильный удар был нанесен по Nokia, сумевшей справиться с ситуацией и даже обратить ее в свою пользу. А Ericsson в итоге потеряла целое направление бизнеса.

Так что удар молнии может стоить существенно дороже миллиарда долларов, если к нему не относиться во всей серьезностью. Приведенный пример стал классикой в литературе по управлению предприятиями [27]. В области телекоммуникаций проблемы аварий могут быть – и в ряде случаев оказываются – не менее значительными. Кроме прямых потерь из-за выхода из строя оборудования и снижения трафика за время, прошедшее от начала аварии до устранения ее последствий, оператор может снизить свою долю на конкурентном рынке. Сегодня последствия крупных пожаров на узлах связи начала 2000-х годов, которые описаны в предыдущих частях статьи, были бы еще тяжелее – пострадавшие операторы неминуемо потеряли бы часть абонентов. Это осознают многие, однако технические решения, и поныне применяемые как в кроссовой защите на узлах связи, так и в самих средствах защиты, не вселяют уверенность в их надежности. Почему это происходит?

Может быть, дело в том, что ошибки при разработке и производстве устройств защиты средств связи кажутся менее опасными, чем при разработке аналогичных систем для электроустановок? Действительно, в области энергетики подобные ошибки выявляются заказчиками быстрее и обходятся производителям дороже. Вероятно, поэтому далеко не все, кто хотел бы заняться производством средств защиты для электроустановок, решаются на это, а те, кто решился, вынужденно тратят больше усилий на преодоление "законов Мерфи".

Техническое мифотворчество

Технические параметры приборов, заявляемые фирмой-изготовителем, надо умножить на коэффициент 0,5.

Технические параметры устройств защиты определяет используемая в них элементная база – во многом, но не во всем. Об этом зачастую забывают многие производители, попросту переписывая параметры элементов защиты (разрядников, позисторов, полупроводниковых приборов) в технические описания своей продукции. Далее на эти технические описания ориентируются покупатели, иногда эти параметры даже записываются в тендерную документацию. Беда в том, что порой не только заказчик, но и сам производитель не понимает, что значит тот или иной параметр. В результате в документации приводятся такие характеристики устройства, которые иначе как плодом фантазии не назовешь.

Типичный случай – производитель на основании параметров используемого разрядника заявляет, что модуль кроссовой защиты рассчитан на максимальный импульс тока 10 кА 8/20 мкс (8 мкс – фронт импульса, 20 мкс – время спада до половины). Предположим, что производитель разрядника указал верные значения, и при таком импульсе сам разрядник не выйдет из строя. Но значит ли это, что именно от таких импульсов этот разрядник защитит аппаратуру? Допустим, что конструкция модуля, контакты плинта, жилы кабеля выдержат такой импульс тока (что маловероятно). Однако к защищаемому оборудованию будет приложено напряжение, амплитуду которого можно оценить, умножив максимальное значение тока на сопротивление дуги газового разряда. Если принять это сопротивление равным даже 0,5 Ом (на самом деле может быть значительно больше), то 5 кВ для выхода из строя оборудования будет вполне достаточно.

На самом же деле амплитуда импульса тока, протекающего через разрядник, установленный в кроссе, вряд ли превысит 100–200, максимум 300 А при самых мощных наводках – если, конечно, не будет прямого удара молнии в кабель.

ПРИМЕР 9

Несколько лет назад мне позвонил инженер из дилерской фирмы, в обязанности которого входила техническая поддержка при продаже нашего оборудования. Его беспокоило, что устройства кроссовой защиты нашего производства якобы имели очень большие недостатки, которые подробно описывались в распространяемом в Интернете материале, озаглавленном примерно так "О некоторых ошибках при производстве модулей грозозащиты". Наша "ошибка", с точки зрения этого материала, была действительно серьезной – в модуле кроссовой защиты на печатной плате входные цепи были выполнены в виде тонких дорожек проводников. Напомню, модуль включается в разрыв линии между входным кабелем и станционным оборудованием. Упомянутые токопроводящие дорожки соединяют вход кросса и абонентский комплект, разрядник в самом модуле подключается параллельно этому оборудованию. Процитируем аргументы, которые произвели такое большое впечатление на очень грамотного и способного, но в то время еще недавно закончившего вуз специалиста:

- толщина токопроводящей дорожки явно недостаточна для пропускания больших токов, а именно для защиты от воздействия грозовых перенапряжений, при которых создаются импульсы в 5–30 кА;
- проведенные испытания показали, что при подаче переменного напряжения 220 В с током, не превышающим 4 А, токопроводящие медные дорожки перегорают;
- известно, что при подаче кратковременного импульсного перенапряжения токопроводящие дорожки могут выдержать ток, в пять раз превышающий постоянно действующий. Однако импульсный ток 20 А возникает только при слабых перенапряжениях, вызванных электрифицированным транспортом и промышленными установками. Поэтому защитить оборудование от импульсов тока, которые возникают при коммутациях в ЛЭП и тем более при грозовых разрядах, данное устройство не в состоянии.

Вывод: данный модуль кроссовой защиты не может выполнить свою главную функцию – защитить телекоммуникационное оборудование от больших токов и перенапряжений, поскольку перегорают дорожки и разрядник не успевает сработать.

Не останавливаясь на анализе несостоятельности подобных "аргументов", отмечу лишь, что в нашем модуле защиты дорожки сделаны тонкими специально, чтобы перегореть в случае мощных импульсных сверхтоков, попадания постороннего напряжения в линию или замыкания в защищаемом оборудовании. Причем мне известен только один случай перегорания дорожки в нашем модуле – и хорошо, что это случилось, иначе бы вступил в действие "закон Клипштейна в приложении к производству" [52]: "Прибор, защищаемый быстродействующим плавким

предохранителем, сумеет защитить этот предохранитель, перегорев первым".

А самое главное, приведенный в материале в качестве примера "правильный" модуль защиты имел толстые дорожки совсем по иной причине. В нем использовалось достаточно редкое техническое решение – термоконтакты на входе линии (это решение, рис.19в, мы рассмотрим ниже и по другому поводу). Очевидно, чтобы припаять к дорожке толстую пружину термоконтакта, она (дорожка на плате) должна быть максимально широкой и толстой – это вопрос технологии устройства, ток тут ни при чем.

Старый друг лучше новых двух

Ошибка выявится только после завершения окончательной проверки прибора.

Как известно, одной из причин аварии межпланетной станции "Фобос-Грунт" стала элементная база системы управления, не соответствующая требованиям к компонентам категории space. Контрафактная низкокачественная элементная база – серьезная проблема для производителей электроники. Наивно полагать, что с элементами защиты дело обстоит иначе. Например, малогабаритные газонаполненные разрядники – массово применяемые и относительно дорогие компоненты. Однако таких проблем с качеством нам не доставляла ни одна другая группа комплектации (не только средства защиты, но и разнообразные микросхемы, реле, разъемы, пассивные элементы и т.п.).

В конце 1990-х и начале 2000-х годов мы использовали отечественные разрядники, и серьезных претензий к их качеству у нас не было. Однако узкий ассортимент, неудобные условия поставки и абсолютное безразличие к нам как к покупателю заставило искать других поставщиков. В течение последних 10 лет мы закупаем разрядники, как и значительную часть другой элементной базы для защитных устройств, у известной компании, недавно вошедшей в состав крупнейшего мирового концерна, и проблем не испытываем. В то же время наша компания, как и любой производитель, стремится иметь несколько поставщиков. Однако два случая заставили нас относиться к их выбору с крайней осторожностью и принять поговорку "старый друг лучше новых двух" как руководство к действию.

ПРИМЕР 10

Российские представители зарубежной компании N в течение нескольких лет посылали нам на испытания разрядники, которые тут же тестировались – с неизменно отрицательным результатом. Однажды, когда у нашего поставщика не оказалось на складе разрядников нужного типа, мы все-таки решились взять 500 приборов этой компании. После входного неразрушающего контроля [53] отсеялось порядка 10% разрядников. Проверка разрядников в составе уже готовой продукции показала, что у части из них после первой проверки (при воздействии тока в несколько микроампер за время менее секунды!) изменились параметры, а у некоторых дуга в заявленном диапазоне перестала зажигаться совсем. Вся партия модулей не прошла наш ОТК, однако поставщик разрядники у нас обратно не взял под тем предлогом, что они были со следами пайки.

ПРИМЕР 11

Вряд ли мы когда-нибудь произведем больше устройств защиты для модемов и регенераторов, чем в 2007 году – ведь такого массового спроса на системы, работающие по медному кабелю, уже не будет. Участники "интернетизации" помнят, какие были проблемы со сроками поставки оборудования. Нужны были десятки тысяч разрядников на складе, потребовался второй поставщик.

Фирма, предложившая свою продукцию, не вызывала никаких сомнений, условия поставки выглядели привлекательно. Нашим разработчикам очень импонировало сочетание небольших размеров разрядников и высокой стойкости к воздействию помех. Некоторое сомнение вызывали заявленные параметры: ведь очевидно, что чем меньше площадь электрода, тем ниже допустимый ток, чем меньше физический объем, тем меньшая энергия в нем может быть рассеяна. Ответ о том, что применяются электроды, изготовленные по особой технологии, нас удовлетворил – тем более, что один из крупнейших мировых производителей сообщал о применении таких технологий (хотя столь впечатляющих результатов соотношения размеры/максимально допустимый импульсный ток этот производитель не достиг).

Входной контроль показал несоответствие напряжения пробоя у менее чем 0,5% приборов (что позволяло перенести выявление брака разрядников на финальную стадию проверки), и закупленные несколько десятков тысяч разрядников тут же начали использоваться в производстве. Однако несколько разрядников отдали на полноценное испытание, и результат ошеломил. Можно было ожидать, что максимально допустимый

ток будет вдвое ниже заявленного (что, в общем-то, было приемлемо), но разрядник "умирал" при импульсе тока с амплитудой, в 7–8 раз ниже указанной в спецификации. Пришлось останавливать производство, отзывать уже отгруженную продукцию и решать все проблемы со сроками, финансированием закупки новых комплектующих и разговорами с покупателями. Хотя разрядники все-таки можно было использовать для других применений, это не очень утешало – общие потери предприятия без всяких сомнений значительно превысили стоимость всей партии.

Отметим, что обычно производители, заботящиеся о качестве, обеспечивают реальные показатели надежности, энергопотребления, срока службы своих изделий выше, чем указанные в технической документации. В этом случае даже при небольших нарушениях производственного процесса параметры изделия не выйдут за допустимые пределы. Например, используемые нами разрядники при проверке выдерживают максимальный импульсный ток в 1,5–2 раза выше, чем заявленный.

Надежность стоит денег

В поиски повышения надежности будут вкладываться средства до тех пор, пока они не превысят величину убытков от неизбежных ошибок или пока кто-нибудь не потребует, чтобы была сделана какая-то полезная работа.

Качество и надежность работы изделий обеспечивают различные механизмы. В НПО "Инженеры электросвязи" разработан стандарт предприятия "Классификация изделий по группам ответственности" (см. таблицу), который позволяет более точно определить требования к изделиям уже на первом этапе разработки, начиная с технического задания. Стандарт помогает оптимизировать номенклатуру изделий, предложив потребителям устройства одинакового назначения, но разного класса ответственности, облегчить задачу проектировщикам и разработчикам систем и объектов по выбору оборудования [55].

Практически все выпускаемые нами устройства защиты относятся к группам 4 и 3.

Стандарт предприятия НПО "Инженеры электросвязи" "Классификация изделий по группам ответственности"

Группа ответственности	Краткая характеристика группы
Группа 1 Наивысший уровень	Изделия для применения в некоторых инженерных системах и на объектах с повышенными требованиями надежности, работающих в особо сложных условиях, выход из строя которых может привести к прекращению выполнения системой своей функции, ее уничтожению или иным тяжким последствиям
Группа 2 ВЫСОКИЙ УРОВЕНЬ	Изделия для применения в некоторых инженерных системах и на объектах с повышенными требованиями надежности, в том числе: • на потенциально опасных объектах; • в системах оборонного назначения; • на особо важных объектах жизнеобеспечения и государственного управления. Группа включает изделия, выход из строя которых приводит к нарушению функционирования объекта, техногенной катастрофе, опасности для жизни и здоровья людей
Группа 3 Повышенный уровень	Возможные последствия при выходе изделий из строя: • повреждение инженерных систем; • перерывы в связи и нарушение технологических процессов; • приостановка работы народнохозяйственных и социальных объектов. Выход из строя изделий этой группы влечет за собой значительный экономический ущерб, незначительную опасность для жизни и здоровья людей и экологической обстановки
Группа 4 Средний уровень	Возможные последствия при выходе изделий из строя: • нарушение и снижение качества связи; • нарушение технологических процессов; • повреждение оборудования или технической системы, в составе которой работает изделие. Выход из строя изделий этой группы приводит к незначительному экономическому ущербу и не представляет опасности для жизни и здоровья людей и экологической обстановки
Группа 5 Обычный уровень	Возможные последствия при выходе изделий из строя: • нарушения и снижение качества связи; • сбои в работе технической системы, в составе которой работает изделие. Выход из строя изделий этой группы приводит к минимальному экономическому ущербу и не представляет опасности для жизни и здоровья людей и экологической обстановки

Как показывает практика, не все заказчики адекватно реагируют на наличие такого стандарта. Некоторых он может даже испугать. Зачем покупать устройство защиты с какой-то непонятной 4-й группой ответственности, в описании которой заложены ограничения по надежности и применению? Ведь за ту же цену можно купить что-то подобное, и продавец уверит в 200%-ной супернадежности. Не все, как ни странно, понимают, что надежность всегда меньше 100%, она составляет 99,999..%, и за каждую девятку после запятой приходится очень дорого платить. Весь вопрос – насколько соразмерны риски аварии и стоимость средств защиты.

ПРИМЕР 12

Через несколько месяцев после событий на Саяно-Шушенской ГЭС к нам поступил запрос на устройства защиты от импульсных помех от предприятия, обеспечивающего связь на объектах энергетики. Как выяснилось, этот запрос был связан с аварией на узле связи Братской ГЭС, который был одной из составляющих крупнейшей промышленной катастрофы (см. часть 2 статьи).

Хотя из акта технического расследования [17] не было понятно, почему загорелся узел связи Братской ГЭС, некоторые выводы сделать я мог. С большой степенью вероятности можно предположить, что причиной возгорания оборудования стал сверхток в кабелях связи. Высокую опасность для систем связи на электростанциях представляют не только мощные коммутационные помехи, но и множество силовых кабелей, которые прокладываются в непосредственной близости от слаботочных.

Учитывая характер ожидаемых помех, условия эксплуатации и потенциальную опасность аварии, заказчику было настоятельно рекомендовано приобрести устройства защиты от сверхтоков и уровнем ответственности группы 3. Однако рекомендация эта затерялась где-то между техническими службами и снабженцами, в итоге заказ был повторен. В результате были приобретены устройства, которые не могли выполнить задачи, для которых они покупались.

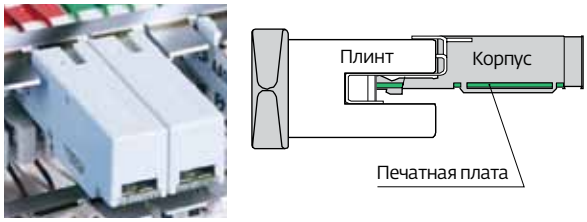


Рис.15. В модуле ComProtect токоведущие части изолированы от прикосновения

Конструктивные особенности

Если какая-нибудь неприятность
может случиться, она случается.

По внешнему виду далеко не всегда можно определить качество устройства. Совсем не обязательно, что из двух образцов следует выбрать более красивый: возможно, пластик его корпуса горит как свечка или же имеет низкую прочность. Но иногда достаточно одного взгляда, чтобы составить однозначное мнение.

ПРИМЕР 13

При общении с коллегами в различных компаниях электросвязи несколько раз повторялась одинаковая ситуация – из коробки доставали модуль кроссовой защиты и спрашивали: "Что ты можешь об этом сказать"? Видимо, что- то в этом устройстве вызывало сомнение. Конструкция модуля была такой же, как у штекеров ComProtect фирмы ADC-KRONE. Качество пластмассы и печатной платы было заметно хуже, чем у оригинала, но дело было не в этом. Проблема состояла в том, что элементы защиты в ComProtect установлены по технологии поверхностного монтажа. Токоведущие части платы, доступные для прикосновения, закрыты маской и таким образом изолированы (рис.15).

В демонстрируемых модулях кроссовой защиты элементы были установлены в отверстия, причем их выводы торчали из платы наружу. Чтобы вытащить модуль, установленный в ряду других, его необходимо зажать пальцами (рис.16) (хотя инструмент для вынимания модулей защиты существует, но я никогда не видел, чтобы им пользовались). При выводном монтаже элементов в таком модуле неизбежен электрический контакт кожи и выводов элементов, соединенных как с линией, так и с оборудованием. Если вынимать модуль в момент посылки вызова, можно почувствовать неприятные ощущения, что заставит отдернуть руку.

Но не это самое неприятное. Устанавливая токовую защиту, мы предполагаем, что возможно попадание в линию связи постороннего напряжения – как правило, при контакте с кабелями низковольтных установок электро-

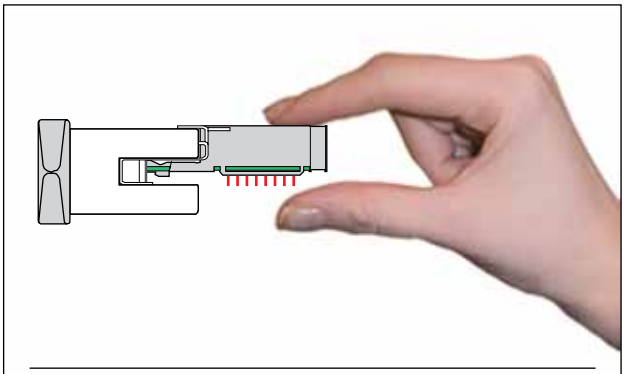


Рис.16. Возможный контакт человека с токонесущими элементами при монтаже в отверстия

питания (многочисленные случаи описаны в предыдущих частях статьи). Что произойдет, если на одном или обоих проводах линии связи окажется высокое напряжение силовой сети ("фаза"), при этом человек коснется одной рукой выводов элементов (как показано на рис.16), а другой – заземленных металлоконструкций кросса? Как применение таких устройств защиты согласуется с правилами техники безопасности?

Природа ошибок в схемотехнических решениях

Система обеспечения надежности выведет из строя другие системы.

Лет 15 назад в Санкт-Петербурге проводил семинар по защите специалист из США – он рассказывал о продукции фирмы, которую представлял. Мой вопрос о том, почему в их абонентском защитном устройстве для телефонных линий нет токовой защиты, вызвал удивление. По его словам, попадание постороннего напряжения в линию связи – событие крайне маловероятное, хотя в то время в США в районах малоэтажной застройки было много не только воздушных ЛЭП, но и воздушных линий связи. Видимо, их качество было таково, что исключало попадание в линии связи посторонних напряжений. К тому же в США основное напряжение сети электропитания – 120 В (для запитки мощных потребителей используются две цепи в противофазе). Поэтому там вероятность тяжелых последствий в случае контакта с линиями связи ниже. Кроме того, при таком контакте не происходит пробоя разрядника со статическим напряжением 230 В,

Рис.17. Кросс после пожара. Фотография предоставлена блоггером dkphoto http://dkphoto.livejournal.com/

так как амплитудное напряжение в сети составляет порядка 170 В. Мы живем и работаем в других условиях, поэтому многим приходилось видеть почерневшие и обугленные кассеты с разрядниками, а некоторым – и выгоревшие кроссы (рис. 17).

О потенциальной опасности применения схем защиты АТС с замыканием сверхтоков на защитное заземление достаточно подробно рассказано в отчете [33] и статьях [56, 57]. Посмотрим на проблему возгорания АТС разных типов (которая уже затронута в частях 3 и 4) под другим углом: почему в течение многих лет применяется опасное техническое решение.

В начале 1990-х в Россию в составе кроссового оборудования стали поступать магазины защиты с разрядниками со статическим напряжением пробоя 230–250 В. Поставки этих решений не прекратились и по результатам работы, проведенной ЛОНИИС по заказу Министерства связи в 1991–1992 годах. Неприятность подстерегала в тех случаях, когда амплитудное напряжение вызывного сигнала, наложенное на постоянное напряжение, подаваемое в линию, превышало напряжение пробоя – происходило ложное срабатывание разрядника. С учетом разброса параметров разрядников для этого было достаточно вызывного сигнала порядка 95–100 В (действующее значение) и напряжения питания АТС 60 В.

Кроме того, поставщики должны были объяснять покупателям, почему поставляются разрядники с номиналом 230 и 250 В. И ответ был найден – при напряжении питания АТС 48 В надо использовать разрядники на 230 В, при напряжении 60 В – разрядники с напряжением пробоя 250 В. До сих пор такие рекомендации можно найти на сайтах поставщиков "магазинов грозозащиты". На самом же деле значения 230 и 250 В указывались производителями разрядников совсем по иной причине. В силу специфики производственного процесса всегда присутствовал технологический разброс параметров разрядников от партии к партии и даже внутри нее. Поэтому напряжение пробоя, которым маркировался разрядник, определялось после его изготовления. Сейчас ситуация иная, но 15 лет назад было именно так.

С точки же зрения техники защиты от импульсных помех, никакой существенной разницы между разрядниками на 230 и 250 В нет. Сравним осциллограммы срабатывания разрядников со статическим напряжением пробоя 230 и 400 В (рис.18). Амплитуда импульса помехи составляет 1,5 кВ, передний фронт – 10 мкс, длительность импульса – 700 мкс. Разрядник с номиналом 230 В (см. рис.18а) пробивается на меньшем напряжении и примерно на 0,2 мкс раньше, чем разрядник на 400 В (см. рис.18б). После пробоя остаточное напряжение на разряднике (в данном случае) составляет порядка 20–30 В – эта величина зависит от мощности помехи, т.е. от тока, протекающего через разрядник. Энергия помехи, поступившей на входные цепи защищаемого оборудования, пропорциональна площади под кривой напряжения импульса на разряднике (плюс площади под кривой самого импульса помехи до срабатывания разрядника). Легко заметить, что эта энергия составляет лишь малую часть от энергии

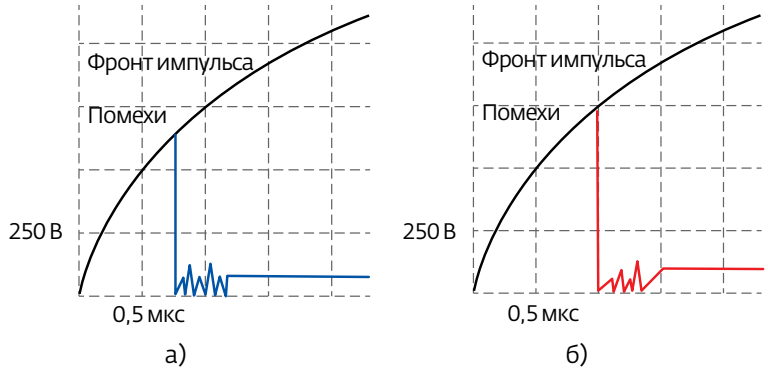


Рис.18. Осциллограммы напряжения на разрядниках со статическим напряжением пробоя 230 В (а) и 400 В (б) при воздействии импульса 10/700 мкс

импульса – на графике виден только его передний фронт. Поэтому во многих случаях разница между напряжением пробоя 230 и 400 В непринципиальна. А разница между напряжением пробоя 230 и 250 В с точки зрения энергии помехи, воздействующей на защищаемое оборудование, непринципиальна практически всегда.

Тем не менее, разрядники с номиналом 230–250 В настолько прочно вошли на отечественных сетях связи в схемы устройств кроссовой защиты, что можно проследить их эволюционную последовательность (рис.19). Причем если в природе крупные катастрофы приводили к вымиранию целых видов животных, в телекоммуникационной технике то ли катастрофы были не слишком сильными, то ли плохо работают механизмы естественного отбора. Так, описанные ниже технические решения (кроме варианта на рис.19а, уже практически не встречающегося) занимают гораздо большую экологическую нишу, чем это может быть оправданно. Например, за пару часов до написания этих строк пришел запрос на несколько тысяч портов защиты по схеме на рис.19б.

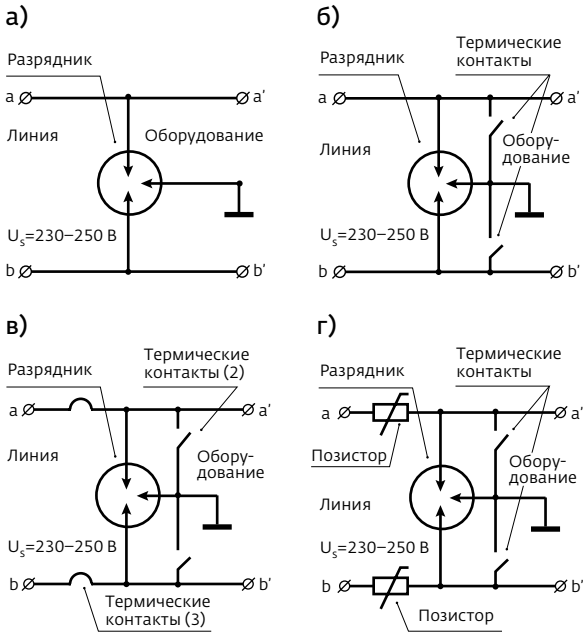


Рис.19. Эволюция схем защиты с замыканием опасного тока "на землю" при использовании разрядника с номиналом 230–250 В: а) базовый вариант; б) шунтирование разрядника через дополнительные термоконтакты; в) дополнительные термоконтакты на входе линии; г) позисторы на входе линии

Эволюция плохих решений

Всякое решение
плодит новые проблемы.

Этап 1 (рис.19а). В 10-парные кассеты установлены разрядники со статическим напряжением пробоя 230–250 В. Вариант был вполне приемлем для США или Японии, где действующее напряжение в сети составляет 120 и 100 В, соответственно. В меньшей степени он подходил для Западной Европы, где напряжение электросети составляет 230 В, но распределительные низковольтные сети уже давно строятся по системе TN-S и находятся в нормальном состоянии. Другое дело – страны бывшего СССР, где в свое время сэкономили, объединив возвратный и защитный проводники, не говоря о том, что состояние электроустановок многих зданий крайне неудовлетворительно. Сейчас положение улучшается, но в 1990-х годах попадание постороннего напряжения в линию связи наблюдалось нередко. В этом случае разрядник пробивался амплитудным напряжением порядка 300 В и если не разлетался, то нагревался докрасна. Дальше все зависело от множества факторов: в сколько жил кабеля попало постороннее напряжение и каким образом; продолжительность воздействия; состав

пластика, из которой сделана кассета защиты. Результат может быть самый разнообразный: изменивший цвет и параметры разрядник, обугленная кассета или возгорание на кроссе – если тепла выделилось достаточно, чтобы поджечь трудногорючий пластик. Операторам такие последствия очень не понравились, и производители предложили другой вариант.

Этап 2 (рис.19б). Чтобы разрядники не нагревались при попадании в линию постороннего переменного напряжения 220 В, надо поднять статическое напряжение пробоя до 350–400 В (с учетом возможности повышения напряжения в сети). Есть и другой путь – как только разрядник начнет нагреваться, подключить провода абонентской линии к заземляющему устройству. Реализовано это с помощью контактов в виде плоских пружин, движение которых ограничено упором, деформируемым при нагреве (легкоплавкий припой, пластик).

Механические контакты в устройствах защиты, которые переключаются при нагреве – это далеко не лучшее решение из-за ненадежности в эксплуатации и применяемых производственных технологий. Подробнее обсудим эту проблему позднее, здесь же ограничимся замечанием, что термоконтакты увеличивают стоимость разрядника и не всегда срабатывают как нужно (например, припой может без нагрева деформироваться под воздействием пружины – тогда обеспечено ложное срабатывание защиты и замыкание линии "на землю").

Итак, что будет, если постороннее напряжение попадет в абонентскую линию – взвесим плюсы и минусы схемы на рис. 19б. Аргументы за:

- после срабатывания термоконтаков опасный ток замкнется "на землю" и постороннее напряжение на входные цепи защищаемого оборудования поступать не будет;
- обеспечение электробезопасности за счет того, что провод с опасным напряжением заземляется (аргумент выглядит несколько сомнительным).

Аргументы против:

- устройство защиты необходимо после срабатывания термоконтактов заменять;
- при замыкании "на землю" в проводах потечет большой ток, который может привести к подгоранию контактов (особенно страдали от этого скрутки), оплавлению изоляции жил кабеля или кроссировки – т.е. обрыв или короткое замыкание может возникнуть в любом месте;
- термоконтакты увеличивают стоимость устройств защиты и делают их менее надежными.

Абсолютно уверен, что аргументы против такого решения многократно перевешивают аргументы за него.

Тупиковая ветвь (рис. 19в). Несколько модулей защиты, выполненные по этой схеме, мы испытали лет 10 назад, результат не впечатлил. Во всяком случае, для кроссовой защиты это тупиковая ветвь. В отличие от схемы на рис.19б, в устройство на входе линии добавлены термические контакты (3). После попадания постороннего напряжения 220 В разрядник пробивается, под воздействием нагрева разрядника срабатывают термоконтакты (2) и замыкают провода линии связи (a, b) на контакт защитного заземления. Резко увеличившийся ток, в свою очередь, приводит к нагреву припоя и размыканию контактов (3). Отметим, что термические контакты – это тоже плоские пружины, один конец которых запаян в отверстие платы обычным припоем, потом пружина наклоняется и другой конец припаивается к дорожке платы легкоплавким припоем.

Стоимость такого устройства, в силу его очевидной нетехнологичности, будет достаточно велика. Поэтому в России такие устройства появились чуть ли не в единичных экземплярах.

Этап 3 (рис.19г). Гораздо проще вместо плоской пружины запаять позистор, который к тому же имеет более стабильные и предсказуемые характеристики. Если сравнивать это решение со схемой на рис. 19б, здесь на один недостаток меньше: после срабатывания позистора ток в проводе линии будет сразу ограничен до уровня в несколько миллиампер.

Вместо этого появляется другая неприятность: после срабатывания разрядника протекающий через позистор импульс тока физически его разрушает. Для этого достаточно относительно небольшой энергии импульса, такие помехи не очень часто, но встречаются. В результате устройство защиты требует замены не только после попадания постороннего напряжения, но, возможно, и после грозы. На эту возможность указывается в работе [57], но авторы справедливо считают ее маловероятной, а применение такой схемы допустимым. Я с этим согласен, но только в одном случае: если устройства защиты с разрядниками 230–250 В уже куплены и их жалко выбросить.

Есть дополнительный аргумент против применения схем с замыканием опасного тока от электроустановок на землю для защиты оборудования проводной связи. Одна из задач при построении системы электропитания по системе

TN-S (с раздельными защитным проводником PE и возвратным проводником N) – обеспечение электромагнитной совместимости. Используя описанные выше схемы, мы подключаем фазный провод удаленной электроустановки к заземляющему устройству объекта связи. Очевидно, что такой подход сулит неприятности, подробнее мы их обсудим в одной из последующих публикаций.

Поэтому приобретение устройств защиты любого из описанных вариантов – это ошибка как для новых объектов, так и для находящихся в эксплуатации. Не обязательно она приведет к аварии, но такая возможность есть. Да и зачем это делать, если уже давно существуют надежные и экономичные схемы защиты, которые за последние пять лет, благодаря совершенствованию элементной базы, стали еще эффективнее?! Так, качественный разрядник с напряжением пробоя 400 В при обычных для телефонной сети помехах обеспечит достаточный уровень защиты для современного коммутационного оборудования. Полимерные позисторы с током срабатывания порядка 100 мА (ток, вызывающий повреждение, обычно выше) и допустимым для применения на цифровых линиях связи затуханием появились на рынке уже несколько лет назад. Это не значит, что производители (в том числе и наша фирма) зря выпускают более сложные и дорогие устройства защиты – их применение вполне оправдано в условиях высокой интенсивности помех, повышенных требований к надежности или при наличии излишков финансирования. Скорее всего, в наиболее массовом секторе устройств защиты оборудования проводной связи в ближайшие годы разрядники будут частично вытеснены полупроводниковыми элементами. Однако это обусловлено чисто экономическими факторами, а вовсе не тем, что разрядники срабатывают медленнее.

***

Закончу эту часть статьи (и начну следующую) постулатом Хорнера: "Опыт растет прямо пропорционально выведенному из строя оборудованию".

ЛИТЕРАТУРА

51. **Семеркин А.** Петля Хеллстрема. – Компания, 2005, № 13 (359) http://ko.ru/articles/11602.
52. **Блох А.** Законы Мерфи. – ЭКО, 1983, №1–3.
53. **Моисеева В.** Применение приборов "Искра" в отделе технического контроля. – Производство электроники, 2006, №4, www.commeng.ru.
54. **Мидлер П.** Плохо сделано в Китае. – СПб.: БХВ-Петербург, 2012.
55. **Пашкевич А.** Уровень опасности высокий – требования ужесточить. – Энергонадзор, 2009, №6(9), www.commeng.ru.
56. **Афанасьев А., Коншин А., Прудинский В.** Применение устройств защиты оборудования и линейных кабелей от перенапряжений и избыточных токов. – Мир связи, 2003, №5.
57. **Афанасьев А., Коншин А., Прудинский В.** Общие рекомендации по выбору устройств защиты оборудования и линейных кабелей от перенапряжений и избыточных токов для различных условий эксплуатации. – Мир связи, 2003, №6.
58. Анализ применения схем защиты с разрядниками и способы регистрации опасных токов в устройствах кроссовой защиты. – www.commeng.ru/files/analiz.pdf

АВАРИИ НА ОБЪЕКТАХ СВЯЗИ

Причина – опасные электромагнитные влияния

Часть 6*

Д.Терентьев
ic@commeng.ru

Конец 1990-х и начало 2000-х годов стали для связистов пиковыми по потерям от воздействия перенапряжений. Вот уже несколько лет не было серьезных аварий, количество повреждений неуклонно снижается. Значит ли это, что можно успокоиться или все-таки следует проанализировать полученный опыт, чтобы быть готовым к новым проблемам? Сравним ситуацию в конце 1990-х – начале 2000-х годов с современной, чтобы понять, что же изменилось и к каким новым проблемам следует быть готовыми.

Переход от аналоговых к цифровым системам передачи

В СССР на местной первичной сети ЕАСС (единая автоматизированная сеть связи) для организации соединительных линий между АТС использовались в основном аналоговые системы передачи (АСП). Первую отечественную 12-канальную систему высокочастотного телефонирования по воздушным медным цепям разработали ЦНИИС и завод "Красная Заря" в 1940 году. Промышленностью СССР выпускалась аппаратура для уплотнения стальных и биметаллических цепей на 3 и 12 каналов, для уплотнения кабельных цепей были разработаны системы емкостью 6, 12, 24 (КНК, К-12, К-24), и 30 каналов ("Кама"). 60-канальная система К-60 использовалась для соединения АТС на ГТС, а также на участке областной центр – районный центр. Поставлялось в СССР и оборудование производства ГДР и Венгрии. Начиная с 1960-х годов, транзисторы начали постепенно заменять лампы, появились стойки и целые системы, целиком выполненные на полупроводниках.

Линейно-технический участок, где я проходил практику в 1983 году, обслуживал несколько систем В-12, а также В-3-3. В августе и сентябре 1983 года грозы случались по несколько раз в неделю, и тогда ламповые разрядники на вводно-коммутационных устройствах ярко светились. Однажды прямой удар молнии повредил биметаллический провод, по которому

* Продолжение. Начало см. Первая миля, 2011, №1, 2, 5, 6; 2012, №1.

работала одна из систем. Приходилось устранять неполадки в стойках (замена предохранителя, лампы), но ни одно повреждение с грозой связано не было.

В середине 1990-х годов, когда я начал заниматься вопросами защиты, аналоговые системы передачи еще находились в эксплуатации. Было несколько обращений по поводу грозозащиты НУП К-60. Основной проблемой, с которой сталкивались связисты, была замена установленных в оборудовании ОУП и НУП разрядников на более современные (это было связано, в частности, с тем, что в ряде старых моделей разрядников использовались радиоактивные вещества). Разработанный в 1981 году стандарт [59] вполне соответствовал требованиям эксплуатации АСП. Можно сделать вывод, что основные проблемы с выходом из строя разрядников были связаны, в первую очередь, с надежностью элементной базы и в значительно меньшей мере – с воздействием перенапряжений.

В 1970-х годах в нашей стране началось внедрение цифровых систем передачи данных (ЦСП). В СССР был принят европейский вариант плезиохронной цифровой иерархии (ПЦИ) цифровых систем передачи. НИИ "Дальняя связь" разработал систему ИКМ-30, производство которой было освоено в Ленинграде и Перми в 1972–1974 годах. В 1977 году для зоновой связи была разработана аппаратура ИКМ-120. Оборудование ИКМ-30 в больших объемах поставлялось на Московскую ГТС в канун Олимпиады-80, после чего началось массовое внедрение ЦСП на местной сети.

По действующим тогда нормам для подключения оконечной АТС емкостью 200 номеров к ГТС требовалось 30 каналов. Так как на сельской сети большинство оконечных станций (СТС – сельские телефонные станции) имело меньшую емкость, то для них были разработаны системы, не входящие в европейскую ПЦИ – ИКМ-12 и ИКМ-15 (начало производства в 1982 году). В конце 1980-х и начале 1990-х годов документация на производство ИКМ 15/30 была по конверсионным программам передана на предприятия России, Украины и Белоруссии. С 1970-х годов и до сих пор оборудование ИКМ называют в честь деревьев: "Ива", "Кедр", "Каштан".

Массовое внедрение ЦСП ИКМ 15/30 и замена АСП на межстанционных линиях СТС наряду с множеством плюсов и возможностей принесло серьезную проблему – число случаев выхода оборудования из строя и нарушений связи из-за воздействия перенапряжений возросло многократно. По всей видимости, это стало неожиданностью для разработчиков и производителей ЦСП и проектных организаций. Операторы связи в районах с высокой грозовой активностью, которые провели цифровизацию межстанционных линий СТС, несли большие потери. Пик неприятностей пришелся на середину 1990-х годов, когда ЦСП были внедрены массово, а опыта по защите их от перенапряжений еще не было.

Когда инженерам компании "Ленсвязь", обслуживающей межстанционные линии Ленинградской области, надоело ремонтировать и заменять регенераторы, один из них обратился в НПО "Инженеры электросвязи" [36]. Это было началом работы, результаты которой позволили обеспечить надежную эксплуатацию систем ИКМ 15/30 в условиях интенсивных электромагнитных помех. "Ленсвязь" была площадкой для отработки технических решений, которые затем применялись другими операторами. Руководство ряда из них, где экономический ущерб был наиболее значительным, назначило ответственных за решение проблемы защиты. Применяя решения и оборудование НПО "Инженеры электросвязи" им удавалось за два-три года снизить число повреждений и нарушений связи в 5–7 раз в масштабах сети. В 1990-х годах такая работа была проведена на предприятиях электросвязи Псковской и Новосибирской областей. Несколько позже аналогичных результатов удалось достигнуть на сети АО "Казахтелеком", где решение вопросов защиты стало на несколько лет одной из основных задач специалистов республиканской производственно-технической лаборатории.

Таким образом, решение проблемы было найдено – разработаны защитные устройства для систем передачи [36, 60] и рекомендации по их применению [61]. Не будем останавливаться на деталях, желающие без труда найдут информацию, да и системы ИКМ 15/30 постепенно уходят в прошлое, уступая место сначала SHDSL, а в последнее время все больше системам, работающим по оптическим кабелям.

Каковы ж причины многократно возросшей в 1990-е годы интенсивности повреждений ЦСП ИКМ 15/30 по сравнению с предшествующим им поколением аналоговых систем передачи?

Изменение элементной базы

Чем меньше физические размеры транзистора, тем меньше энергия помехи, приводящая к его повреждению. Стойки и регенераторы ИКМ-

Таблица 1. Длины усилительных и регенерационных участков при работе систем передачи по одночетверочному кабелю типа КСПП

Оборудование	Число каналов	Расстояние между НУП или НРП, км
АСП КНК-6Т	6	16
АСП КНК-12	12	16
АСП "Кама"	30	13
Неиерархическая ИКМ-12	12	7,5
Субпервичная ИКМ-15	16	7,5
Первичная ИКМ-30	32	3,8

15/30, выпущенные в 1980-е и 1990-е годы, пришли на смену оборудованию на базе дискретных транзисторов и даже электронных ламп и были в значительной степени подвержены влиянию перенапряжений. Однако современная высокоинтегрированная элементная база обладает гораздо большей стойкостью, чем дискретные полупроводниковые приборы и интегральные схемы 30–40-летней давности. Поэтому современное оборудование ИКМ-30 и тем более SHDSL, где одна БИС зачастую заменяет целую плату, выходит из строя значительно реже, чем их предшественники еще 10–15 лет назад на тех же линиях.

Увеличение числа регенераторов

К крупным авариям и катастрофам обычно приводит совпадение ряда факторов. Так и причиной резкого увеличения повреждений ЦСП по сравнению с АСП, которым они пришли на замену, стали не только замена элементной базы и неэффективная схема защиты. Сравним длины усилительных и регенерационных участков при работе систем передачи по одночетверочному кабелю типа КСПП (табл.1).

Представим ситуацию, когда на участке между оконечной (ОС) и узловой (УС) станциями СТС 12-канальная аналоговая система была заменена системой ИКМ-30 (рис.20). Совершенно очевидно, что при прочих равных условиях вероятность выхода из строя хотя бы одного необслуживаемого пункта регенерации (НРП) значительно выше, чем одного необслуживаемого усилительного пункта (НУП). Более того, бросок потенциала на заземляющем устройстве одного регенератора может вывести из строя не только его, но и соседние (этот вопрос мы подробно рассмотрим в одной из следующих публикаций).

Нарушение правил строительства линий связи

Организация молниезащиты подземных кабелей как в соответствии с требованиями Минсвязи СССР, так и с более современными [62, 63] – это мероприятие, затратное для строителей и требующее усилий от проектировщиков. Причем зачастую без знакомства с трассой и без выезда на место технически грамотный проект молниезащиты кабельной линии сделать невозможно. Отсюда происходят две крайности – или на проблему ударов молнии закрывают глаза, или же молниезащита на всей трассе предусматривается, что называется, по полной. В последнем случае требования проекта,

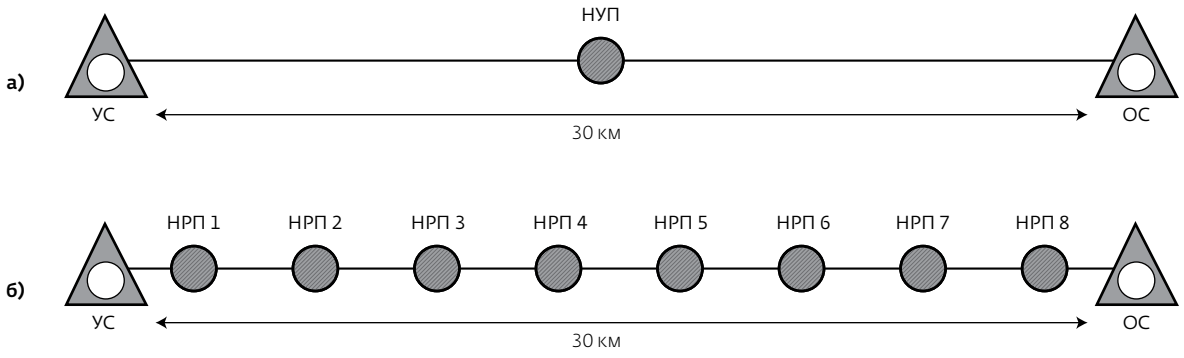


Рис.20. Межстанционная линия между оконечной и узловой станциями СТС, длина 30 км, кабель КСПП 1×4: а) система КНК-12, один НУП; б) система ИКМ-30, 8 НРП

естественно, не выполняются – представьте, сколько нужно усилий, например, чтобы проложить вместе с кабелем два грозозащитных троса, причем соблюсти необходимые расстояния между ними.

Другая проблема – сближения и пересечения с ЛЭП. Обычная картина – вдоль дороги высоковольтная ЛЭП, буквально в нескольких метрах с ней проложен кабель, установлены регенераторы. Действительно, проложить трассу на уже расчищенном месте гораздо проще и для строительства, и для обслуживания. Более того, в южных регионах Европейской части РФ, где по обе стороны от дорог тянутся бесконечные поля, прокладывать кабель связи подальше от дороги и ЛЭП нет смысла – вероятность того, что его порвут при обработке земли выше, чем вероятность повреждения от ударов молнии.

Конечно, можно (и нужно, наверное) упрекать строителей и проектировщиков – но следует признать, что точное выполнение всех рекомендаций по защите кабельных трасс в новых экономических условиях стало экономически нецелесообразным.

Неэффективная схема защиты регенератора

Если взглянуть на упрощенную схему защиты регенератора (рис.21), то видно, что разрядники подключены к выводам линейного трансформатора и уравнивают потенциалы между проводами пары, по которой ведется прием или передача в одном направлении. Кроме того, два разрядника включены между проводами линии и средней точкой трансформатора, откуда снимается напряжение дистанционного питания (ДП). Защищен также узел, в котором происходит выделение ДП. Обычно для защиты приемника ДП кроме разрядника устанавливались и стабилитроны, необ-

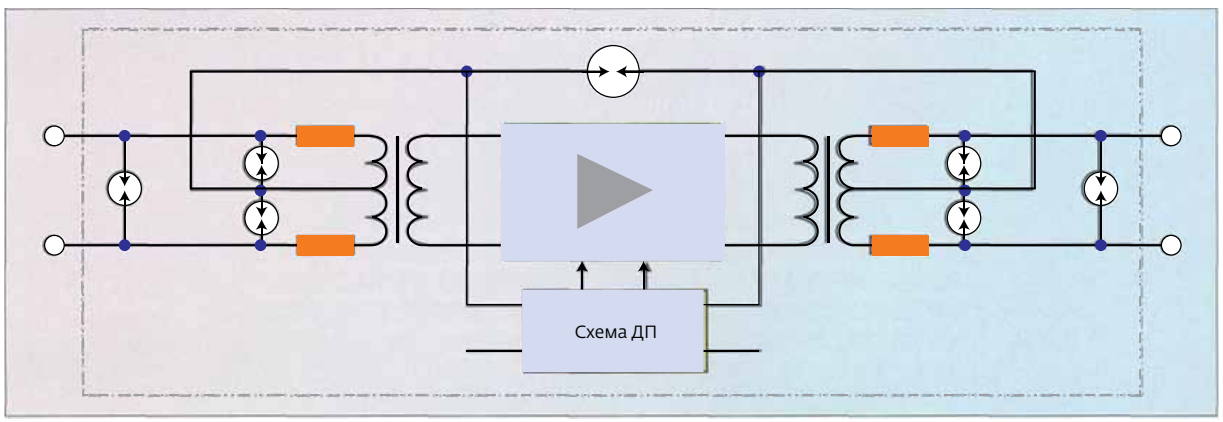


Рис.21. Схема защиты НРП ИКМ 15/30 (производство конца 1980-х и 1990-х годов). Показано только одно направление передачи, схема защиты в другом направлении аналогична

Таблица 2. Максимальная дальность (км) работы современных SHDSL-модемов [67] с вероятностью ошибки не хуже 10^{-7} в кабельных системах с низким уровнем шумов (по одной физической паре)

Скорость, кбит/с	Тип кабеля			
	ТЦП 0,64	КСПП 0,9	КСПП 1,2	ЗКП 1,2
1024	11,5	16	17	25
2048	8,5	11	12	17
4096	5,5	7	8	10
5704	5	6	7	8
8192	3,2	4	5	6

ратимый пробой которых часто становился причиной неисправности. Разработчики аппаратуры не учли, что ЭДС, индуцированная в скрученной паре проводов (да еще и экранированных), в идеальном случае равна нулю. Основная же причина повреждения регенераторов – разность потенциалов между проводом и общей точкой (корпусом регенератора, землей), а вот от этого защита предусмотрена и не была. Констатируем факт: защита от перенапряжений в регенераторах ЦСП ИКМ 15/30 фактически отсутствовала.

Каким образом в 1980-х годах оборудование ИКМ 15/30 прошло испытания, можно только предполагать. Возможно, что уже при серийном производстве были сделаны "рацпредложения" по снижению себестоимости. Но, скорее всего, для ГТС стойкость оборудования была сочтена достаточной, а для использования на СТС предполагалась установка дополнительных разрядников между проводами и защитным заземлением – в узлах связи на вводно-коммутационных устройствах (что было сделано), и в регенераторах (что сделано не было).

ПРИМЕР 14

В конце 1990-х годов, перед грозовым сезоном, в одном из узлов связи на нескольких линиях в регенераторы ИКМ-15 "Ива" были установлены модули защиты систем передачи типа МЗСП-Е1. Регенераторы горели каждый год, а так как установлены они были на небольших островах, чтобы добраться до них, нужна была не только машина, но и лодка. Не прошло и месяца, как позвонил главный инженер районного узла связи и попросил срочно приехать – после сильной грозы две линии, на которые были установлены устройства защиты, перестали работать, причем до этого такого количества поврежденных регенераторов никогда не было.

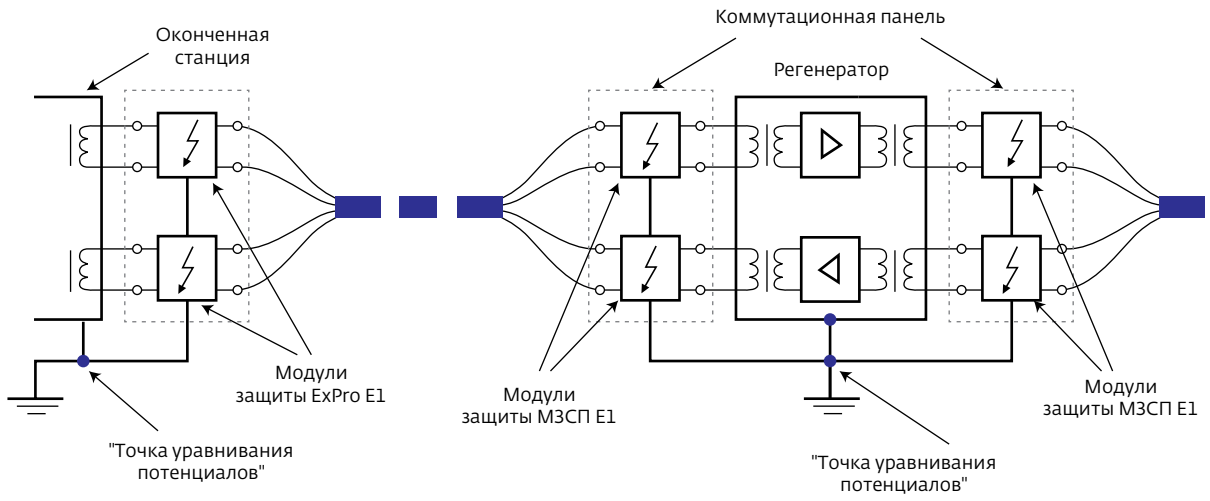


Рис.22. Схема установки устройств защиты оборудования ЦСП ИКМ 15/30

Модули защиты были выполнены в виде коммутационных дужек, с маркировкой линия/оборудование, неправильно установить их в гнезда было практически невозможно. На месте выяснилось, что монтеры подключили контакты защитного заземления модулей МЗСП-Е1 следующим образом: многожильные провода (всего четыре, по числу МЗСП) длиной около 1,5 м каждый зачистили и привязали узлами к трубе, через которую в ящик регенератора заводился кабель. Надо добавить, что труба была покрашена кузбасслаком, хотя в принципе это ничего не меняет, так как при таком подключении при самых лучших параметрах модулей защиты уравнивания потенциалов при импульсной помехе не происходит (см. часть 4).

Подняв крышку ящика, я увидел четыре трехэлектродных разрядника Р-27. Подключены они были правильно, как того требует инструкция [61] (см. рис.22). Жгутовой монтаж был явно сделан на заводе. Хотя с точки зрения специалиста монтаж был сделан с ошибками, защита должна была быть вполне работоспособной. Монтеры же, установив, но фактически не подключив МЗСП-Е1, обрезали провода, которыми были подключены установленные на заводе Р-27, и таким образом существующую защиту отключили.

Больше я регенераторов с дополнительными внешними разрядниками не видел, из чего делаю вывод, что изначально для применения на СТС их установка предполагалась, но затем это правильное решение утонуло в волнах перестройки и конверсии. Вернуться к нему, уже на более современном уровне, заставила жизненная необходимость.

SHDSL-модемы для транспортных сетей

С середины 2000-х годов в России началось массовое внедрение цифровой телекоммуникационной аппаратуры нового поколения. Это, в частности, и переход к оптическим технологиям, и к системам xDSL на различных участках медных линий связи. Для оборудования цифровых абонентских линий (мультиплексоров DSLAM) вопросы защиты рассматриваются аналогично и совместно с защитой цифровых АТС. Более сложна и интересна проблема защиты малоканальных систем уплотнения абонентских линий, работающих в сельской местности по подземным и подвесным кабельным линиям [64, 65].

Из всего спектра xDSL-оборудования остановимся на модемах SHDSL, работающих в условиях, аналогичных рассмотренным выше ЦСП. Применение современных методов обработки сигналов и многоуровневых кодов позволили значительно увеличить скорость и качество передачи информации по сравнению с предшествующими стандартами HDSL и HDSL2 и уж тем более – с системами ИКМ 15/30, в которых используется трехуровневый линейный код (табл.2). Сравнив с данными табл.1, видим, что регенерационный участок для модема SHDSL-bis, работающего по одной паре со скоростью 2048 кбит/с, в три раза больше, чем для ИКМ-30, работа-

ющей по двум парам. Если же задействовать две пары, то регенераторов SHDSL нужно будет еще меньше.

Повреждения из-за опасных электромагнитных влияний оборудования SHDSL на межстанционных соединительных линиях и на транспортной сети происходили и будут происходить всегда. Тем не менее, эта проблема никогда не достигала таких масштабов, как с ИКМ 15/30, и уже сведена большинством операторов к минимальным масштабам. В чем причина столь кардинального снижения уровня аварийности? Сравним потенциальные причины возможных повреждений оборудования SHDSL и ИКМ 15/30 из-за перенапряжения по аналогии сравнения ЦСП ИКМ 15/30 с АСП.

Применяемые в современном оборудовании СБИС более стойки к перенапряжениям, чем элементная база оборудования ИКМ-30/4 (четвертого поколения). За счет высокой степени интеграции в SHDSL-модемах значительно меньше компонентов, что положительно влияет на его надежность. Однако этот фактор едва ли можно считать существенным.

Что касается регенераторов, то при сохранении скорости передачи в линии при замене ЦСП ИКМ 15/30 на SHDSL можно значительно сократить число регенераторов или вовсе обойтись без них. Однако скорость передачи данных постоянно растет, для чего требуется установка регенераторов, причем зачастую в тех же местах, что и раньше. Так что и этот аспект не внес принципиального отличия.

Если говорить о линиях связи в целом, то пять лет назад, во время тотальной "интернетизации" страны, чуть больше чем за год в авральном порядке были установлены десятки тысяч единиц оборудования. При этом новое оборудование во многих случаях устанавливалось на старые линии, из-за спешки о подверженности вновь прокладываемых линий электромагнитным влияниям зачастую даже не задумывались. Поэтому к 2007 году принципиальных отличий в состоянии линий связи по сравнению с 1997 годом не было.

Так что же повлияло на то, что множество установленных модемов и регенераторов SHDSL не начали вылетать десятками за одну грозу, как это происходило 10–15 годами раньше с оборудованием ИКМ 15/30? Дело в том, что и операторы, и производители, и поставщики оборудования были к этому готовы, пусть и в разной степени. Инженеры знали, что установка устройств защиты многократно снижает риск повреждения аппаратуры, знали, где и как их устанавливать. Производители устройств защиты имели готовые решения и могли произвести их в необходимом объеме и ассортименте. Большинство производителей оборудования уплотнения уже к середине 2000-х годов применяли более или менее эффективные встроенные схемы защиты. Оптимальным как для производителя, так и для потребителей вариантом является выпуск согласованных по техническим параметрам оборудования связи и устройств защиты для него.

ПРИМЕР 15

Весной 2008 года регенераторы и модемы на 10 линий SHDSL одного из региональных филиалов "Ростелекома" были защищены с помощью устройств ExPro SDL и МЗСП-СДЛ. По результатам испытаний предполагалось принять решение о целесообразности их применения на всей сети регионального филиала. В середине июля в службе электросвязи было собрано совещание по этому вопросу. Результаты испытаний оказались противоречивыми – на четырех линиях

все хорошо, на шести остальных возникли проблемы. На подобных совещаниях, в случае неудовлетворительного результата применения устройств защиты, обычно высказываются следующие мнения:

- устройства защиты плохие, толку от них нет никакого (см. пример 7 в части 3);
- ничего поделать нельзя, остается только надеяться, что в следующий раз пронесет и дожидаться замены медного кабеля на оптический;
- нужно попытаться разобраться, найти и устранить причину.

Сторонником последнего мнения в этот раз был только я, пока один из инженеров службы не обратил внимание на то, что оборудование на двух линиях, которыми занимался лично он, повреждено не было. А вот на остальных восьми линиях монтаж защитных устройств выполнялся с ошибками, возможно, где-то они не устанавливались вовсе. Осознав ситуацию, руководству для принятия решения о защите регенераторов SHDSL потребовалось всего несколько месяцев. Десятью же годами раньше (см. часть 4) только через три года безаварийной работы нескольких десятков систем ИКМ 15/30 оператор принял решение о необходимости распространения опыта на всю сеть.

Примеры различного подхода к обеспечению защиты оборудования (середина 1990-х – начало 2000-х)

"Ростелеком", филиал ТЦМС-3

В середине 1990-х годов на обслуживании у ТЦМС-3 находилось более 7 тыс. км кабельных линий, 2,5 тыс. км радиорелейных линий, почти 900 объектов связи. Филиал обеспечивал магистральную связь на территории Санкт-Петербурга, Ленинградской, Новгородской, Псковской, Тверской областей, а также выход на международные сети связи.

Инженеры ТЦМС-3, одними из первых начав массово внедрять на сети современное цифровое оборудование, обнаружили, что при ударах молнии в антенно-мачтовые сооружения, наводках на магистральные кабели стойки систем передачи, цифровые РРС, мультиплексоры, импульсные выпрямители выходят из строя или работают со сбоями. Ситуация осложнялась тем, что подобного опыта ни у кого не было, нормативная база устарела, необходимая информация была труднодоступна. Неудивительно, что именно здесь была проведена работа, которую скорее можно назвать исследованием. Многие решения были найдены самостоятельно, и лишь потом оказалось, что они уже применятся за рубежом [68].

К концу 1990-х годов удалось значительно снизить повреждаемость оборудования и количество нарушений связи из-за ударов молнии и низкого качества электропитания. Следует отметить, что система защиты от помех, разработанная специалистами "Ростелекома" для узла связи в Кингисеппе, была повторена практически без изменений на другом конце подводной магистрали – в Дании.

Ведомственные операторы (трубопроводный транспорт)

В середине и конце 1990-х и начале 2000-х годов ведомственные операторы, обеспечивающие связь и передачу сигналов телемеханики для добычи и транспортировки нефти и газа, стали массово получать современное телекоммуникационное оборудование. На смену малоканальным аналоговым РРС стали приходить цифровые, электромеханические АТС, и ручные коммутаторы заменялись коммутационными системами с функциями ISDN, выпрямители с диодными и тиристорными схемами – на импульсные. Внедрялись системы, обеспечивающие радиосвязь вдоль трасс трубопроводов. Ежегодно вводились новые объекты связи, обеспечивающие связью не только предприятия, но и население.

Такие изменения не могли не вызвать резкого увеличения случаев выхода нового оборудования из строя. Руководители нескольких предприятий обратились в НПО "Инженеры электросвязи", где для них был отработан алгоритм работы, включающий анализ электромагнитной обстановки и причин выхода из строя оборудования; обследование объектов связи; повышение квалификации персонала (семинар на месте или курсы повышения квалификации в Санкт-Петербурге); подготовку отчетов и разработку рекомендаций. Как правило, для обследования выбиралось несколько типовых объектов. Получив от нас начальную помощь, связисты в течение двух-трех лет приводили свои объекты в порядок, при необходимости обращаясь за консультациями и закупкой оборудования. Объектов таких могло быть 70–80, причем раскиданных по тайге и тундре на тысячи километров.

"Казахтелеком"

Огромная территория и низкая плотность населения Казахстана во многом определили

особенности построения местной телефонной сети: большая средняя длина абонентских линий и межстанционных линий, широкое применение беспроводных терминалов (радиоудлинителей) и спутниковых терминалов, которые устанавливались в отдаленных местах в рамках национального проекта. Как и в России, массовое внедрение современного оборудования сопровождалось значительными потерями от перенапряжений. В чем-то казахстанским связистам приходилось даже тяжелее – дефицит квалифицированных кадров в отдаленных местностях был больше, в республике не было ни специализирующихся в области ЭМС фирм, ни производителей защиты. Удаленность от производителей оборудования и центров техподдержки усугубляла сложности с ремонтом.

В этих условиях в центральном аппарате "Казахтелекома" были выделены специалисты, ответственные за защиту от перенапряжений систем связи и электроустановок, заземляющих устройств. На повышение квалификации в Санкт-Петербург несколько лет подряд приезжали специалисты из Казахстана. Сотни инженеров и техников из всех областных дирекций телекоммуникаций были обучены на курсах в Алматы. Разработан технический регламент предприятия по грозозащите электроустановок. Это единственный известный мне случай, когда работа в подобных масштабах проводилась централизованно.

Особенности современной ситуации

Так что же кардинально изменилось за последние 10 лет, что столь коренным образом повлияло на аварийность объектов связи в целом и на отношение к системам защиты оборудования от перенапряжений – в частности?

Замена медных кабелей на оптические на магистральной сети и межстанционных линиях (а в последние годы – и на сети доступа), сокращение длины абонентских линий при переходе на сети FTTB (FTTC) многократно сократили опасные воздействия на линейные сооружения на новых и реконструируемых сетях. В то же время, в связи с децентрализацией сети, возникла серьезная потребность в обеспечении качества электропитания для выносов, шкафов с активным оборудованием. Массовое внедрение на сетях проводного и беспроводного доступа стандарта Ethernet 100/1000 BASE-TX, изначально разработанных для ЛВС, потребовало разработки методики и устройств для защиты оборудования Ethernet. Одни проблемы решаются и тут же возникают другие. Впрочем, масштаб значительно меньше, а средства для их решения становятся все доступнее.

Типовые решения пришли на место "зоопарку" и самодеятельности. В конце 1990-х – начале 2000-х годов один оператор порой имел на сети пять-шесть систем коммутации, разнообразные системы передачи, выпрямители и т.п. – действительно, "зоопарк" оборудования. Проблема была крайне острой и отрицательно влияла на все параметры сети, прежде всего на надежность, качество связи и затраты на эксплуатацию. Еще хуже было то, что новое оборудование монтировалось на объектах, введенных в эксплуатацию десятки лет назад: взаимные помехи, съеденные коррозией заземляющие устройства, отсутствие исполнительной документации, плохое состояние электроустановок и ужасное – линий связи. Но уже тогда появились примеры того, каким должен быть современный объект связи – смонтированные за рубежом "газпромовские" контейнеры, базовые станции мобильных операторов, автозалы АТС, смонтированные об-

ученными специалистами в соответствии с требованиями поставщиков.

Сегодня ситуация по сравнению с 1990-ми – началом 2000-х годов изменилась кардинально. Уже совсем не обязательно разбираться в технике защиты от перенапряжений и ЭМС, чтобы обеспечить надежную работу систем связи в условиях электромагнитных помех. Достаточно смонтировать оборудование и сооружения в соответствии с предлагаемыми проектировщиком, системным интегратором или поставщиком оборудования решениями и, с большой долей вероятности, все будет хорошо. Зачастую поставляется уже не отдельное оборудование, а готовые решения в виде собранного контейнера: остается его только подключить – правильно, по прилагаемой инструкции.

Не менее важно, что изменилась скорость принятия решений по вопросам защиты от опасных электромагнитных влияний, от нескольких лет 10–15 лет назад до нескольких месяцев сегодня.

Принципиально более доступной стала информация. В 1997 году дефицит информации был таким, что в 1997 году на семинар компании "Инженеры электросвязи" по проблемам защиты собралось почти 50 человек не только из Москвы, Петербурга и Центрального и Северо-Западного регионов, но и из Сибири и Дальнего Востока. Сегодня никуда ехать не надо – час в Интернете, несколько звонков по телефону обычно достаточно, чтобы узнать все, что нужно. Раньше на курсах повышения квалификации (проводились Государственным университетом телекоммуникаций им. М.А.Бонч-Бруевича и Военной академией связи им. С.М.Буденного) по теме "Защита объектов связи от опасных электромагнитных влияний" обучалось по 40–50 человек ежегодно. Сейчас вряд ли найдется предприятие, готовое на несколько дней отвлечь квалифицированных инженеров на такое мероприятие. Это – лучший индикатор того, что защита от перенапряжений превратилась в абсолютно рутинную задачу: технические решения изначально заложены в проекты и программы поставок, информация и необходимое оборудование доступны, специализированные предприятия готовы предложить любые услуги.

На этой оптимистической ноте можно было бы и закончить. Однако тот уровень повреждений и нарушений качества связи, который операторы сочли для себя нормальным (и прекратили дальнейшие усилия по его снижению) может быть сокращен в еще большей степени, причем без всяких материальных затрат. Более того, после того, как устройства и мероприятия по защите стали привычной строкой в сметах и перечнях закупаемого оборудования, значительная часть выделенных на них средств стала тратиться бессмысленно (по правде сказать, и раньше это было).

А самое главное, есть еще множество серьезных проблем, о которых многие не знают (до поры до времени) или если знают, то не очень хорошо понимают, как их решать.

Продолжение следует

ЛИТЕРАТУРА

59. ГОСТ 5238-81. Установки проводной связи. Схемы защиты от опасных напряжений и токов, возникающих на линиях.
60. Как защитить оборудование линейного тракта малоканальных цифровых систем передач. / В сб. "Защита оборудования и объектов связи от опасных токов и напряжений. Подготовка к грозовому сезону". – СПб., 1999. www.commeng.ru/публикации.
61. Инструкция по применению устройств ExPro и МЗСП для защиты оборудования цифровых систем передачи. – НПО "Инженеры электросвязи", 2003, www.commeng.ru/техническая документация/архив технической документации.
62. ВСН 116-93 Инструкция по проектированию линейно-кабельных сооружений связи. – Минсвязи России, 1993.
63. Руководство по защите металлических кабелей от ударов молнии.– М.: Госкомсвязи России, 1997.
64. **Терентьев Д.Е.** Защита оборудования последней мили от импульсных помех. – "Телекоммуникационное поле регионов", 2006, №4, www.commeng.ru/публикации.
65. **Терентьев Д.Е.** Устройства защиты от перенапряжений оборудования последней мили, работающего по медным кабелям. – Первая миля, 2007, №2, www.commeng.ru/убликации.
66. www.shdsl.org
67. www.nateks.ru
68. Молниезащита объектов связи. Рекомендации. – СПб.: ТЦМС-3 ОАО "Ростелеком", 1997.
69. Материалы семинара "Защита оборудования связи от опасных токов и напряжений". – СПб, 1997, www.commeng.ru/публикации.