

ОСНОВНЫЕ ПРИЧИНЫ ВЫХОДА ИЗ СТРОЯ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

А. Кисельков, Е. Кочетков

Выход из строя оборудования систем охранного телевидения - явление, крайне неприятное для всех, кто использует данные системы для охраны объекта. О том, что является причинами этого и как бороться с подобными проблемами, расскажут специалисты НПО "Защита информации", одного из ведущих российских производителей приборов для передачи видеосигналов на большие расстояния в системах охранного телевидения, Александр Кисельков и Евгений Кочетков.

Выход из строя оборудования систем видеонаблюдения - достаточно распространенное явление, доставляющее "головную боль" как эксплуатационным, так и монтажным организациям. В данной статье мы не будем рассматривать случаи отказов, связанные с проблемами изготовителей видеоборудования (низкие качество и надежность аппаратуры, отсутствие входного контроля элементов, тренинга аппаратуры, прогона и т. д.), а также с неправильной эксплуатацией систем видеонаблюдения (ошибки монтажа, несоблюдение температурных режимов, превышение допустимой влажности воздуха, несоблюдение требований эксплуатационной документации), поскольку такие отказы носят единичный, случайный характер и укладываются в допустимый процент технического отхода. Другое дело, если смонтированное оборудование достаточно долгое время нормально функционировало, условия эксплуатации соблюдались, но в какое-то время неожиданно произошел массовый выход из строя аппаратуры на объекте. В ряде случаев одна и та же аппаратура годами исправно работает при одних условиях эксплуатации (например, в жилых помещениях) и регулярно выходит из строя в других условиях (на промышленных объектах). В данной статье под промышленным объектом следует понимать любой объект кроме жилого дома. Помехи, приводящие к искажению видеозображения - это отдельная тема для разговора. Что явилось причиной массового отказа, почему это произошло и как предотвратить подобные случаи? На эти вопросы мы и попытаемся ответить.

Вначале классифицируем помехи, приводящие к выходу из строя видеоборудование:

- радиопомехи;
- коммутационные импульсные помехи;
- перенапряжения и провалы напряжения в сети питания;
- помехи от разрядов молнии;

- помехи от "блуждающих токов заземления".

Затем отдельно остановимся на каждом типе помех, приводящих к выходу из строя видеоборудования, и определим основные источники помех.

Радиопомехи

Под данным типом будем понимать высокочастотные помехи. ВЧ - помехи представляют собой электромагнитное воздействие на линию связи от мощных близкорасположенных радио- и телепередатчиков, радаров и другого излучающего оборудования. Помехи проявляются в виде частых волн, колебаний, искажающих видеозображение. Выход из строя аппаратуры наблюдается только в случае крайне близкого (десятки метров) расположения линии передачи видеосигнала или телеметрии от передающей антенны. По цепям передачи электропитания ВЧ - помеха какого-либо воздействия приводящего к повреждению аппаратуры не оказывает.

Коммутационные импульсные помехи

Основным источником возникновения коммутационных импульсных помех являются переходные процессы при следующих операциях в электросети:

- включении и отключении потребителей электроэнергии (электродвигатели, лампы накаливания и дневного света, компьютеры и др. аппаратура);
- включении и отключении цепей с большой индуктивностью (трансформаторы, пускатели и т. д.);
- аварийных коротких замыканий в сети низкого напряжения и их последующих отключений защитными устройствами;
- аварийных коротких замыканий в сети высокого напряжения и их последующих отключений защитными устройствами;
- включения и отключения электросварочных установок;

Источником импульсных помех является также городской электрифицированный транспорт, включая метро, а также электрифицированные железные дороги.

Данный тип помех, как правило, представляет собой одиночные импульсы с амплитудой до нескольких киловольт. В соответствии с [1] считается нормой наличие в сети 220 В импульсов коммутационных помех амплитудой до 4,5 кВ длительностью до 5 мс. Реально частота возникновения одиночных импульсных помех амплитудой до 300 В составляет в среднем для промышленных предприятий 20 помех в час, для жилых домов 0,5 помех в час. Наиболее опасные помехи амплитудой от 1 до 10 кВ составляют до 0,1% от общего числа импульсных помех. Таким образом, в офисе расположенном на территории промышленного предприятия, электронное оборудование подвергается воздействию мощной помехи 3 раза в неделю, а в жилом доме до 4 раз в год.

Кроме одиночных импульсных помех по цепям питания возникают периодические импульсные помехи, связанные с работой люминесцентных ламп, преобразователей блоков питания и т.д. Данный тип помех [2,3] достигает амплитуды до 1 кВ, от-

личается более широким спектром и приводит как к сбоям, так и к повреждению аппаратуры. Коммутационные импульсные помехи различной длительности по цепям питания 220 В видеоборудования при нормальных условиях эксплуатации способны вывести его из строя только в том случае, если амплитуда помех превышает 1 кВ. Вероятность повреждения аппаратуры по цепям питания многократно возрастает в условиях повышенной влажности или в условиях повышенной запыленности, что характерно для промышленных объектов. Повреждения блоков питания видеоборудования являются следствием воздействия импульсных помех по электросети. Причем следует отметить, что значительно чаще повреждаются импульсные блоки питания и реже - линейные.

Перенапряжения и провалы напряжения в сети питания.

Причины возникновения перенапряжения в сетях питания обусловлены, прежде всего, низким качеством электросетей и невысокой культурой энергопотребления. Поэтому подчеркнем лишь наиболее типичные проблемы электроснабжения.

Максимумы напряжения питающей сети, как правило, связаны с минимальной нагрузкой энергосистемы и наблюдаются в ночное время. Наибольшие колебания напряжения в электросети приходятся на начало и конец рабочего дня. Реально на промышленных объектах возможны периодические (день - ночь) колебания электросети 220 В от 160 В до 260 В с кратковременными повышениями до 300 В.

Перенапряжения в электросети выводят из строя стандартные простые схемы защиты от импульсных помех (варисторы и т. д.), импульсные блоки питания. Отдельно можно выделить две распространенные монтажные ошибки, приводящие к перенапряжениям:

- перекос фаз сети электропитания из-за перегрузки одной фазы потребителями электроэнергии;
- перегрузка нейтрали электросети из-за меньшего сечения проводника у нейтрали, чем у фазы.

Помехи от разрядов молнии

Разряды молнии индуцируют на линиях связи и линиях подачи электропитания высоковольтные импульсы напряжения. Разряд молнии характеризуется громадной разницей потенциалов до 10^8 В, токами до 10^6 А, поэтому при прямом или близком (десятки метров) разряде молнии речь может идти только о выходе электронного оборудования из строя, а не о помехах. Системы молниезащиты, включающие в свой состав молниеотводы и заземления, предназначены для защиты зданий и людей от поражения электрическим током, но не для защиты электронного оборудования и линий связи [4, 5]. Типичной ошибкой при монтаже видеоборудования "в полевых условиях" является установка видеокамеры на опоре молниеотвода или рядом с ним. В таком случае при прямом попадании молнии в молниеотвод все видеоборудование и линия связи будут полностью выведены из строя и не ремонтпригодны. О защите

от разряда молнии можно говорить только в том случае, если расстояние от места разряда до линии связи видеоборудования составляет хотя бы сотни метров.

Для центральных регионов России интенсивность воздействия грозы составляет приблизительно 50 часов в год, при этом молния воздействует в среднем 2 раза в год на 1 км^2 местности. Для северных регионов России молния воздействует на 1 км^2 местности 1 раз в год, для южных - до 5 раз в год. Поэтому для средней полосы на линиях связи или линиях электропитания следует ожидать опасные помехи в виде импульсов напряжения 10 кВ один раз в год и до 50 раз в год - импульсы около 1 кВ. Для южных районов с повышенной грозовой активностью частота появления опасных напряжений соответственно увеличивается в 5 раз.

Рассмотрим подробнее механизм воздействия высоковольтных импульсных помех на линии связи. Внешние электромагнитные импульсы приводят к образованию на протяженной линии связи разницы потенциалов. Значение разницы потенциалов зависит от напряженности внешнего электромагнитного поля, скорости его изменения, протяженности линии связи и может достигать, при определенных неблагоприятных условиях, десятков киловольт. Помеха на линии связи образуется относительно земли (синфазная помеха). Однако помеха может возникнуть и дифференциально на входах и выходах видеоборудования. Эта ситуация возникает в случае несимметричной линии связи (например: коаксиальный кабель).

На **рис. 1** показаны пути протекания токов помехи при использовании в качестве линии связи неэкранированного кабеля. На **рис. 2** показаны пути протекания токов помехи при использовании в качестве линии связи экранированного кабеля. Из рисунков видно, что в случае неэкранированного кабеля ЭДС помехи образуется на сигнальном проводнике и ток помехи, протекающий по нему, замыкается на землю через приемное видеоборудование, создавая на его входных цепях опасное напряжение. В случае экранированных сигнальных цепей ЭДС помехи образуется на защитном экране, ток помехи протекает по экрану и не создает в сигнальных цепях прибо-

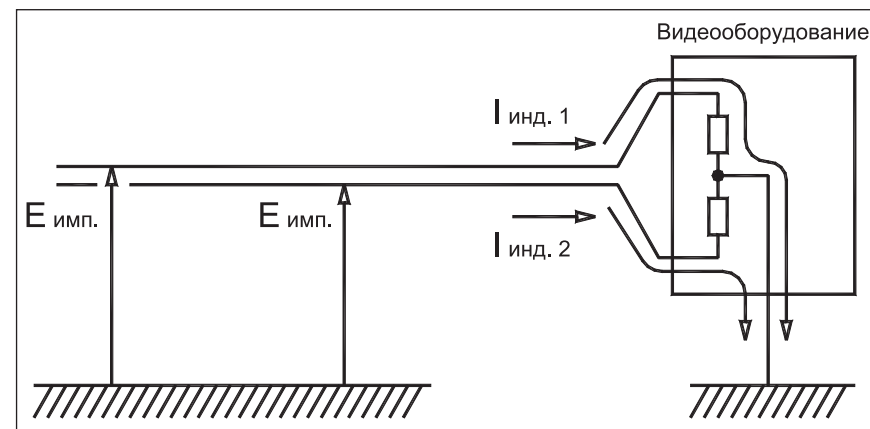


Рис. 1 Пути протекания токов помехи при использовании неэкранированного кабеля

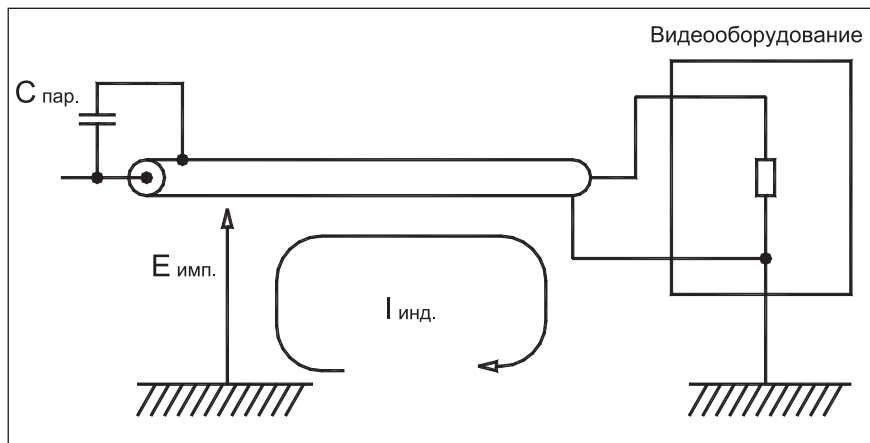


Рис. 2 Пути протекания токов помехи при использовании экранированного кабеля

Ров видеонаблюдения опасных напряжений. В центральном проводе возникает ЭДС помехи за счёт емкостной связи Спар между экраном и проводом. Экранирование с обязательным заземлением ослабляет помеху в среднем в 100 раз. При воздействии атмосферных разрядов (при ударе молнии в землю на расстоянии 1000 м от линии связи) на линию связи может наводиться опасное напряжение амплитудой свыше 10 кВ. В данном случае экранирование ослабит помеху до 100 В, что может привести аппаратуру к выходу из строя.

Помехи от "блуждающих" токов заземления

Любая система видеонаблюдения, даже простейшая, содержит передающее видеоборудование (видеокамеру), линию связи (коаксиальный кабель, витую пару), приемное видеоборудование (в простейшем случае монитор), а также источники питания передающего и приемного видеоборудования. Рассмотрим простейший случай системы видеонаблюдения, содержащей видеокамеру, линию связи (коаксиальный кабель) и монитор. Структурная схема системы приведена на рис. 3.

В соответствии с требованиями безопасности, предъявляемыми к электромонтажу оборудования, аппаратура должна быть заземлена, причем разводка сигнальных цепей всей системы (в том числе передающей и приемной аппаратуры) должна иметь только одну точку заземления. Реально, особенно в многоканальных системах, установщики видеоборудования по тем или иным причинам не выполняют или просто игнорируют правило заземления аппаратуры в одной точке. Часто это требование нельзя выполнить по очень простой причине: в недорогой зарубежной и отечественной аппаратуре входные и выходные разъемы BNC не изолированы от корпуса, корпус выведен на заземляющий контакт питающей вилки, который в свою очередь соединен с клеммой зануления сети 220 В, т. е. в качестве земляной шины используется ноль электрической сети. В системе образуются несколько точек зануления и, соответственно, присутствие блуждающих токов заземления, что приводит к разли-

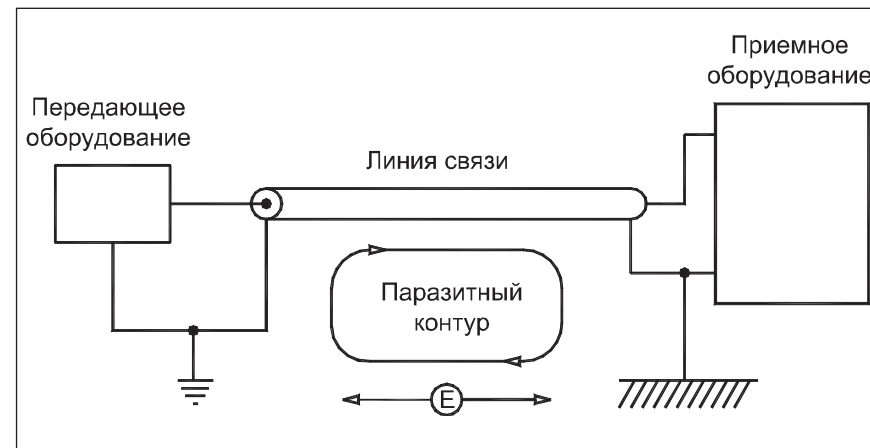


Рис. 3 Структурная схема системы видеонаблюдения

це потенциалов между двумя любыми точками зануления. Для удаленных объектов и, соответственно, для протяженных линий связи разница потенциалов может достигать сотни вольт за счет протекания через образованные паразитные контуры заземления токов от промышленного оборудования, либо от неравенства потенциалов нулевых шин питающего напряжения 220 В/50 Гц приемного и передающего оборудования. Можно перечислить значительное количество объектов, в которых паразитные контуры заземления будут присутствовать в обязательном порядке. В первую очередь это объекты с длиной кабельных линий более 300 м. Далее - это объекты с многоканальными системами видеонаблюдения. И, наконец, - это все производственные объекты и прилегающие к ним территории. Источниками тока промышленной частоты в цепях заземления служат генераторы, станки, электропечи, электросварка, холодильное оборудование, компьютерные сети, системы вентиляции и кондиционирования, электроподстанции, медицинское оборудование, наземный электрифицированный транспорт, метрополитен и т.д.

Рассмотрим механизм образования опасных напряжения для видеоборудования при наличии паразитных контуров заземления. Эквивалентная схема системы приведена на рис.4.

- R_{вых} = 75 Ом** - выходное сопротивление передающего оборудования;
- R_{вх} = 75 Ом** - входное сопротивление приемного оборудования;
- R₂** - сопротивление оплетки кабеля;
- R₁ > 10 x R₂** - сопротивление центральной жилы кабеля;
- E** - паразитный источник ЭДС.
- E_{вх.пр.} = (E / (150 + R₁)) x 75 (В)**

Пример: Реальная линия 300 м кабеля RG 59 имеет сопротивление центральной жилы R₁ > 100 Ом. При E = 100 В значение E_{вх.пр.} составит 30 В, а это уже напряжение которое выведет из строя входные цепи приемного видеоборудования, если они не защищены специальными средствами. Аналогичное напряжение будет воздей-

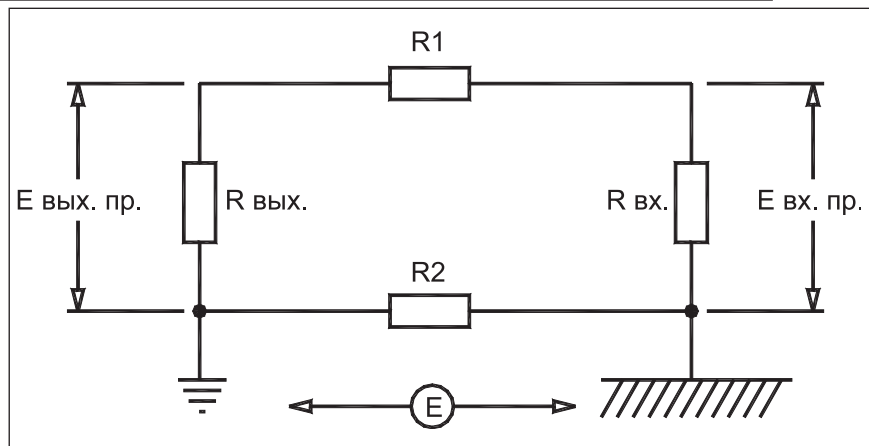


Рис. 4 Эквивалентная схема при наличии паразитных контуров заземления

вать на выходные цепи передающей аппаратуры. Таким образом, рассмотренный случай показывает следующее:

- на реальных объектах при наличии протяженных линий связи и в многоканальных системах видеонаблюдения образуется несколько точек заземления аппаратуры и соответственно, несколько паразитных контуров заземления;
- разница потенциалов между двумя точками заземления может привести к неисправности монтируемого оборудования;
- использование вместо специальной земляной шины нулевого провода электросети приводит к увеличению опасного напряжения между приемной и передающей аппаратурой;
- видеокамеры и другое передающее оборудование с неизолированными от корпуса разъемами BNC должны быть надежно изолированы от шин заземления и нулевого провода электросети.

Определить наличие паразитных контуров заземления можно, измерив вольтметром напряжение между корпусом приемного оборудования и не подсоединенным кабельным разъемом линии связи. Наличие напряжения переменного тока говорит о том, что при подсоединении кабеля к приемной аппаратуре возникнет паразитный контур заземления, который, скорее всего, приведет к неисправностям системы видеонаблюдения. Устранение данной ситуации возможно при грамотном монтаже системы видеонаблюдения, а именно обязательном заземлении всей системы в одной точке, лучше на приемной стороне системы. Если по каким-либо причинам это невозможно, то необходимо принимать специальные меры для защиты видеоборудования. Самым эффективным решением в данном случае является гальваническая развязка передающего и приемного видеоборудования (изолирующие трансформаторы, оптоэлектронные приборы развязки и т. п.). Приборы гальванической развязки включаются в разрыв кабельной линии связи и тем самым разрывают паразитный контур заземления (рис.5).

Механизм образования опасных напряжений при передаче сигнала по витой па-

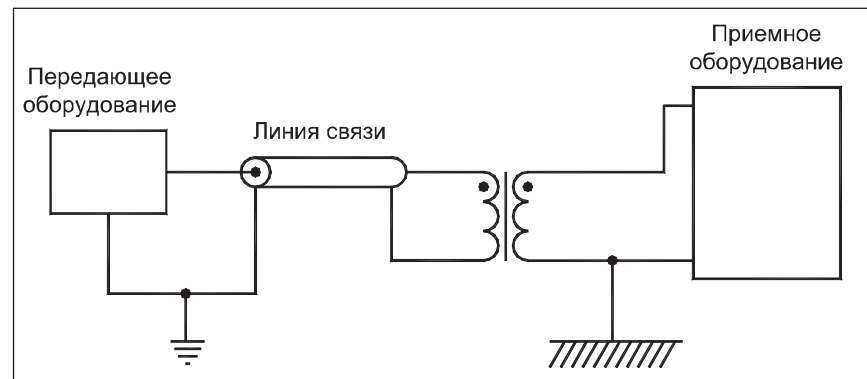


Рис. 5 Гальваническая развязка передатчика и приемника видеонаблюдения

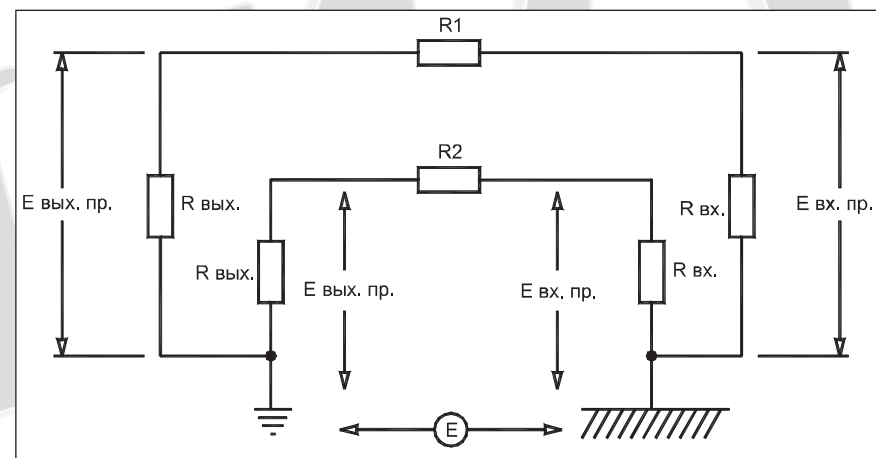


Рис. 6 Эквивалентная схема передачи сигнала по витой паре

ре при наличии паразитных контуров заземления точно такой же, что и при передаче сигнала по коаксиальному кабелю, с той лишь разницей, что в случае с коаксиальной передачей опасное напряжение формируется дифференциально, а в случае с витой парой - синфазно (синхронно) по входным цепям. Эквивалентная схема для случая с витой парой приведена на рис. 6.

Пример: Реальная линия 1000 м витой пары ТПП N x2x0,5 имеет электрическое сопротивление центральной жилы $R1 = R2 = 100 \text{ Ом}$. Значение $E \text{ вх. пр.}$ составит 27 В при напряжении помехи $E=100\text{В}$. Таким образом порядок опасного напряжения точно такой же, а воздействие синфазно для входных цепей оборудования передачи изображения по витой паре. Использование изолирующих трансформаторов так же решает в этом случае проблему паразитных контуров заземления.

Мы рассмотрели случаи паразитного гальванического соединения приемного и передающего видеоборудования и способы устранения возможности возникнове-

ния опасных напряжений для устройств видеонаблюдения.

Анализ отказов видеооборудования показывает, что основными "поражающими факторами" для аппаратуры являются разряды молнии, коммутационные импульсы помех и перенапряжения в сети питания. Например, для уличных видеокамер статистика отказов из-за помех следующая:

- до 50 % отказов: повреждение или полное разрушение блоков питания видеокамер и цепей, связанных с линиями передачи видеосигнала или телеметрии в результате воздействия разрядов молнии и коммутационных импульсных помех. Типичными последствиями являются повреждение изоляции, выгорание проводников печатных плат, разрушение электрорадиоэлементов;
- до 45% отказов: повреждение блоков питания видеокамер в результате перенапряжений в сети питания. Как правило, чаще выходят из строя импульсные блоки питания. Реже - линейные. Типичные неисправности - разрушение элементов из-за теплового пробоя;
- остальные отказы являются следствием других причин, чаще всего связанных с недостаточной герметизацией кожуха видеокамер.

Для приемного видеооборудования, находящегося в помещении и непосредственно соединенного с линиями передачи видеосигнала и телеметрии картина отказов несколько иная:

- до 90 % отказов: повреждение или полное разрушение цепей связанных с линиями передачи видеосигнала или телеметрии в результате воздействия разрядов молнии и импульсных помех;
- остальные отказы являются следствиями других причин, в том числе перенапряжений в электросети.

При анализе отказов уличных видеокамер, как правило, выявляются:

- отсутствие каких-либо специальных средств защиты от импульсных помех, грозовых разрядов и перенапряжений по цепям питания;
- недостаточное экранирование линий передачи видеосигнала, телеметрии и питания (экран коаксиального кабеля не является серьезным препятствием для повреждения аппаратуры грозowymi разрядами);
- отсутствие специальной аппаратуры защиты от грозовых разрядов по цепям передачи видеосигнала и телеметрии;
- конструктивные недостатки видеооборудования приводящие к возникновению "блуждающих" токов заземления;
- некачественный монтаж видеооборудования (отсутствие или недостаточная изоляция и герметизация, монтаж рядом с молниеотводами и т. д.);
- некачественное проектирование систем видеонаблюдения в целом (прокладка длинных сигнальных цепей параллельно высоковольтным линиям, отсутствие защитных средств, и т. д.).

При анализе отказов приемного видеооборудования основной причиной является отсутствие каких-либо средств защиты от импульсных помех и грозовых разрядов на вводе в здание по цепям передачи видеосигнала и телеметрии. Типичной ошибкой является копирование функциональной схемы системы видеонаблюдения,

приведенной в рекламном проспекте зарубежной фирмы. Например, уличные видеокамеры через длинные линии связи подключаются к мультиплексору без аппаратуры защиты от опасных напряжений. При первой же грозе на расстоянии несколько километров от смонтированной "видеосистемы" все компоненты ее безвозвратно выйдут из строя. При проектировании систем видеонаблюдения необходимо учитывать следующее:

- практически в любых импортных и отечественных видеоприборах отсутствуют элементы способные поглотить энергию мощных импульсных помех 10 кВ, индуцированных разрядами молнии по цепям сигнала и сети. Это делается с целью уменьшения габаритов и стоимости видеооборудования;
- элементы защиты, поглощающие энергию грозовых разрядов, выпускаются отдельно и устанавливаются на вводе линий связи и электросети в здания, а для уличных устройств - на вводе в термокожух.

Зачастую, по причине отсутствия финансовых средств, проектировщики систем видеонаблюдения вынуждены экономить на оборудовании защиты от помех. Поэтому в заключение **попробуем определить основные действия**, которые при минимальных затратах на оборудование и монтаж уменьшат риск массового выхода видеооборудования из строя.

При выборе и монтаже оборудования передающего видеосигнал на длинные линии связи необходимо придерживаться следующих элементарных правил (пример - видеокамера): Металлический корпус видеокамеры не должен иметь электрический контакт с ее схемой (общим проводом) и выходным разъемом. Если такой контакт присутствует (а он, как правило, есть), то при установке камеры в кожух корпус камеры (и выходной разъем, и линия связи) должны быть надежно изолированы от элементов конструкции кожуха. При питании видеокамеры от электросети 220 В (через встроенный блок питания камеры) может возникнуть паразитная гальваническая цепь между корпусом камеры, ее схемой и нулевым проводом электросети, что недопустимо. В свою очередь, кожух и его кронштейн крепления должны быть надежно заземлены. Т.е. для удаленных постов видеонаблюдения подходят далеко не все типы видеокамер, а только те, у которых электрическая схема изолирована от корпуса и нулевого провода электросети. В противном случае необходимо дополнительно устанавливать электрическую изоляцию между корпусом камеры и кожухом, ставить гальваническую развязку по сигнальной цепи, телеметрии и цепи питания. В качестве уличных камер с питанием от сети 220 В настоятельно рекомендуем использовать только камеры с линейным внутренним или внешним, а не с импульсным блоком питания (конечно, лучше устанавливать суперфильтры или трансфильтры по электросети). В качестве защиты от атмосферных разрядов рекомендуем устанавливать внешние (вне кожуха) устройства грозозащиты по всем цепям, включая телеметрию и электросеть, или хотя бы искроразрядники.

Необходимо определить на этапе проектирования системы возможно ли ее создание с заземлением в одной точке на приемной стороне аппаратуры видеонаблюдения, т.е. предусмотреть прокладку шин заземления. Если по каким-либо причинам

этого сделать нельзя, то необходимо предусмотреть дополнительное оборудование, позволяющее гальванически развязать передающую и приемную части аппаратуры. Причем развязка должна быть по всем цепям, соединяющим аппаратуру: видео, телеметрии, питание и т. д. Цепи стекания заряда должны быть обязательно заземлены (а не занулены), иначе эффективной грозозащиты не будет. Следует также учитывать, что аппаратура повреждается не только по цепям прохождения видеосигнала, пробой может произойти по цепям питания, телеметрии и т.д. Самым тщательным образом необходимо подходить к прокладке сигнальных линий связи между передающим и приемным видеооборудованием. Наличие общего экрана, заземленного с приемной стороны, резко снижает риск выхода аппаратуры из строя при воздействии на нее наводок различного физического происхождения. Особенно это важно при протяженности линии связи более 300 м, поскольку уровень возникающей помехи тем больше, чем длиннее линия связи. При построении системы приемного видеооборудования рекомендуем руководствоваться следующим принципом: дешевле заменить входной усилитель стоимостью 30 у.е., чем отремонтировать мультимплексор стоимостью 1000 у.е.

Мы надеемся, что правильно спроектированная Вами система видеонаблюдения с учетом тех рекомендаций, которые изложены в настоящей статье, будет достаточно защищена от внешних факторов, а не построена по принципу: "Пока гром не грянул ...".

Нормативные ссылки

В статье использовались ссылки на следующие стандарты:

1. ГОСТ 13109-97

Нормы качества электрической энергии в системах электроснабжения общего назначения.

2. ГОСТ Р МЭК 60065-2002

Аудио-, видео- и аналоговая электронная аппаратура. Требования безопасности.

3. ГОСТ Р 50009-2000

Технические средства охранной сигнализации. Требования и методы испытаний.

4. РД 34.21.122-87

Инструкция по устройству молниезащиты зданий и сооружений.

5. ГОСТ 12.1.019-79

Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты.