

Защита объектов телекоммуникаций от электромагнитных воздействий



Б.Б. Акбашев, Н.В. Балюк, Л.Н. Кечиев

УДК 621.398.25
ББК 31.27-05
А38

Все права защищены. Воспроизведение всей книги или любой ее части любыми средствами и в какой-либо форме, в том числе в сети Интернет, запрещается без письменного разрешения владельца авторских прав.

Рецензенты:

Э.Н. Фоминич, докт. техн. наук, профессор, лауреат премии Совета министров СССР, действительный член Академии электротехники РФ, почетный энергетик;
В.А. Тухас, докт. техн. наук, профессор

Акбашев Б.Б.

А38 **Защита объектов телекоммуникаций от электромагнитных воздействий / Акбашев Б.Б., Балюк Н.В., Кечиев Л.Н. – М.: Грифон, 2014. – 472 с. – (Библиотека ЭМС)**

ISBN 978-5-98862-164-5

В монографии впервые в отечественной литературе рассматриваются вопросы проектирования, строительства и эксплуатации объектов телекоммуникаций, подверженных воздействию мощных электромагнитных полей. Детально представлены источники подобных полей, их частотные, временные и мощностные параметры, а также механизм воздействия на объекты. Приводятся сведения о путях построения экранирующих систем, реализующих концепцию электромагнитной защиты, и основы теории экранирования, позволяющие оценить эффективность экранирования. Особое внимание уделено инженерным методам и средствам построения электромагнитных экранов в едином цикле строительства объектов.

Авторами представлены соответствующие методы, технические средства и модели для проведения процедуры тестирования как всей системы, так и ее компонентов. Дается описание мониторинга систем, который проводится на протяжении жизненного цикла объекта. Также приводятся практические рекомендации по проектированию объектов телекоммуникаций в виде специальных технических заданий, в том числе с учетом требований информационной безопасности.

Книга будет полезна специалистам, которые занимаются вопросами электромагнитной совместимости и информационной безопасности, а также проектирующим ответственные объекты телекоммуникаций. Издание можно рекомендовать в качестве учебного пособия студентам и аспирантам всех уровней подготовки по соответствующим направлениям.

УДК 621.398.25
ББК 31.27-05

ISBN 978-5-98862-164-5

© Акбашев Б.Б., Балюк Н.В., Кечиев Л.Н., 2014

Содержание

Предисловие.....	9
Список сокращений	16
1. Телекоммуникационные системы СТЗ и обеспечение	18
информационной безопасности	18
1.1. Информационная безопасность	
в телекоммуникационных системах	18
1.2. Учет электромагнитной совместимости	
при проектировании СТЗ	23
1.2.1. Основные понятия ЭМС	23
1.2.2. Виды электромагнитных помех	25
1.2.3. Категории изделий	26
1.2.4. ЭМС и функциональная безопасность.....	27
1.2.5. Электромагнитные эффекты	
и функциональная безопасность	29
1.2.6. Методология учета стандартов	
на жизненном цикле проекта	31
1.3. Специальное техническое здание как объект инсталляции	
телекоммуникационных систем	52
1.3.1. Здание как объект информатизации	52
1.3.2. Структурированные кабельные системы	54
1.3.3. Нарушение целостности информации в ЛВС	57
2. Электромагнитная обстановка	60
2.1. Классификация ЭМО	60
2.2. Электромагнитный импульс ядерного взрыва	61
2.2.1. Общая характеристика электромагнитного импульса	
ядерного взрыва	61
2.2.2. ЭМИ высотного ядерного взрыва	63
2.2.3. Параметры ЭМИ высотного ядерного взрыва.....	64
2.2.4. Действия ЭМИ ВЯВ на СТЗ,	
расположенные на поверхности земли	69
2.2.5. ЭМИ наземного ядерного взрыва	73
2.2.6. ЭМИ воздушного ядерного взрыва	78
2.2.7. Интегральное воздействие ЭМИ	
и проникающих излучений	79
2.2.8. Обобщение параметров ЭМИ различных ядерных взрывов	80
2.3. Источники мощных электромагнитных помех большой энергии	
естественного и техногенного происхождения	82
2.3.1. Молния	82
2.3.2. Геомагнитные бури	91

2.3.3. Высоковольтные линии электропередачи	92
2.3.4. Контактная сеть железных дорог	93
2.3.5. Мощные радиопередающие средства и радиолокационные станции	93
2.4. Преднамеренные мощные электромагнитные воздействия	94
2.4.1. Электромагнитное оружие	94
2.4.2. Преднамеренные электромагнитные воздействия и электромагнитный терроризм	98
2.4.3. Технические средства преднамеренного силового воздействия	103
2.4.4. Рекомендации по защите электронных средств от преднамеренного воздействия	106
2.5. Электромагнитные воздействия на СТЗ	110
2.5.1. Особенности воздействия электромагнитного импульса ядерного взрыва	110
2.5.2. Механизм воздействия ЭМИ на электронные системы СТЗ ..	113
3. Концепция повышения стойкости СТЗ	
к электромагнитным воздействиям	125
3.1. Концептуальные подходы	125
3.1.1. Воздействие полей МЭМИ на электронные системы СТЗ	125
3.1.2. Пути проникновения полей МЭМИ в СТЗ	128
3.2. Концептуальные требования обеспечения стойкости СТЗ.....	131
3.3. Механизм связи внешних полей с элементами электронных систем	135
3.3.1. Взаимодействие через проводники	135
3.3.2. Взаимодействие с экранированными кабелями	138
3.3.3. Взаимодействие с длинными линиями связи	141
3.3.4. Взаимодействие с воздушными линиями	142
3.3.5. Взаимодействие с заглубленными линиями	145
3.3.6. Резонансные явления	146
3.3.7. Проводящие проникновения	146
3.3.8. Внутренние кабели	147
3.4. Восприимчивость оборудования	148
3.4.1. Воздействие ЭМИ на аппаратуру и компоненты	148
3.4.2. Реакция оборудования на электромагнитное возмущение	151
4. Концепция целостности защиты и повышения стойкости СТЗ	161
4.1. Целостность электромагнитной защиты	161
4.2. Предпосылки разработки проекта СТЗ	163
4.3. Верификация проекта.....	164
4.4. Концепция обеспечения стойкости	165
4.4.1. Топология экранирующих систем	165
4.4.2. Реализация экранированных зон.....	170

4.4.3. Экранирование кабелей	173
4.4.4. Заземление экранов	173
4.4.5. Концепция выполнения апертур в экранах	175
4.4.6. Реализация концепции экранирования	178
5. Системные инженерные требования	182
5.1. Интеграция электромагнитной защиты	182
5.2. Интеграция защит от МЭМИ и молнии	182
5.3. Интеграция защиты от МЭМИ и обеспечения ЭМС	185
5.4. Учет факторов внешней среды	187
6. Проектирование защищенных СТЗ	189
6.1. Элементы теории экранирования	189
6.1.1. Эффективность электродинамического экранирования	189
6.1.2. Зависимость эффективности экранирования от частоты	197
6.1.3. Влияние апертур на эффективность экранирования	198
6.2. Методология проектирования экранов	201
6.2.1. Требования к показателям экранирования	201
6.2.2. Материал и толщина стенок экрана	203
6.2.3. Однородность экранов	205
6.2.4. Точки входа в экран	206
6.2.5. Последовательность проектирования защиты СТЗ	207
6.3. Экранированные помещения	207
6.3.1. Реализация экранированного помещения	207
6.3.2. Реакция экрана на импульсное воздействие	210
6.4. Сетчатые, перфорированные и сотовые экраны	211
6.4.1. Сетки и перфорированные металлические экраны	211
6.4.2. Использование табличных данных	217
6.4.3. Сотовые панели	218
6.4.4. Слоистые экраны	224
6.5. Стальная арматура железобетонных строений	224
6.5.1. Эффективность экранирования	224
6.5.2. Требования к соединению прутков арматуры	228
6.6. Заглубленные помещения	230
6.7. Соединения и швы в экранах	231
6.7.1. Технологии изготовления экрана	231
6.7.2. Сварные швы	231
6.7.3. Сварные каркасы экранов	233
6.7.4. Паяные швы	239
6.7.5. Механические соединения	240
6.7.6. Экранирование зон доступа	251
6.8. Кабели и соединители	253
6.8.1. Эффективность экранирования	253
6.8.2. Экранированные кабели	254

6.8.3. Витая пара	256
6.8.4. Кабельные соединители и их параметры	259
6.8.5. Материалы соединителя и финишная обработка	261
6.9. Кабелепроводы и их соединения	262
6.9.1. Назначение и требования	262
6.9.2. Жесткий кабелепровод	262
6.9.3. Арматура кабелепроводов и коллекторы	267
6.9.4. Соединение кабелепроводов и экранов	269
6.10. Защита терминалов от перенапряжений	270
6.10.1. Подавители переходных процессов	270
6.10.2. Фильтрация	282
6.10.3. Режекция в режиме общего вида (POB–CMR)	295
6.10.4. Электрическая изоляция	296
6.11. Апертуры	303
6.11.1. Апертуры в экранированном помещении	303
6.11.2. Двери и дверные системы	305
6.11.3. Тамбурные проходы	311
6.11.4. Другие порты доступа персонала	312
6.11.5. Вентиляционные каналы	313
6.11.6. Вводы трубопроводов сервисных служб	314
6.11.7. Структурные проникновения	318
6.12. Соединения элементов экрана	319
6.12.1. Фиксированные соединения элементов экранов	319
6.12.2. Подвижные соединения	323
6.12.3. Защита мест соединений	327
6.13. Заземление экранированных помещений	327
6.13.1. Классификация систем заземления	327
6.13.2. Методы заземления	331
6.13.3. Подсистема электродов заземления	336
6.13.4. Подсистема электробезопасности	340
6.13.5. Системы защиты от молнии	342
6.13.6. Подсистема возвратных токов	347
6.13.7. Конструкция фальшпола	354
6.13.8. Руководящие принципы заземления при модернизации объекта	360
7. Тестирование системы электромагнитной защиты СТЗ	364
7.1. Фазы тестирования	364
7.2. Тестирование восприимчивости	365
7.3. Проверка качества	366
7.4. Приемное тестирование	368
7.5. Оценка стойкости и аттестация	369
7.6. Тестирование на протяжении жизненного цикла	370
7.7. Методология тестирования	371

7.8. Методы тестирования на основе полевых излучателей	372
7.9. Крупные имитаторы ЭМИ	375
7.9.1. Особенности имитаторов	375
7.9.2. Имитаторы электромагнитных полей	375
7.9.3. Имитаторы плоских волн	376
7.9.4. Имитаторы импульсных полей	376
7.9.5. Имитаторы непрерывного излучения гармонических полей	378
7.10. Тестирование масштабной модели	378
7.11. Тестирование инъекцией тока	379
7.11.1. Цель тестирования	379
7.11.2. Прямая инъекция	380
7.11.3. Индуктивная инъекция	381
7.11.4. Методы тестирования инъекцией тока	381
7.12. Методы оценки эффективности экранирования кабельных экранов	385
7.12.1. Оценка эффективности экранирования	385
7.12.2. Триаксиальный метод	387
7.12.3. Метод испытания инжекторным проводом	389
7.12.4. Нормативная база методов экспериментального исследования восприимчивости кабелей	390
7.13. Непроводящие каналы связи	391
7.14. Тестирование помехоподавляющих фильтров	391
7.14.1. Тестирование в частотной области	391
7.14.2. Тест на кондуктивные переходные процессы МЭМИ	393
7.15. Тесты устройств защиты терминалов (УЗТ)	394
7.16. Тестирование эффективности экранирования	396
7.16.1. Типы тестов	396
7.16.2. Эффективность экранирования магнитного поля	397
7.16.3. Эффективность экранирования электрического поля	402
7.16.4. Эффективность экранирования плоской волны	403
7.17. Измерение полного сопротивления электрических соединений	406
8. Мониторинг стойкости СТЗ	409
8.1. Окружающая среда и деградация стойкости	409
8.2. Влияние программы мониторинга на проект объекта	410
8.2.1. Выбор концепции экрана	410
8.2.2. Минимальные требования по поддержанию уровня стойкости	412
8.3. Влияние типа отказа на обслуживание объекта	413
8.4. Структура программы мониторинга	415
8.5. Реализация мониторинга стойкости объекта	418

9. Рекомендации по проектированию СТЗ	420
9.1. Требования к экранам.....	420
9.2. Подход к проектированию.....	421
9.3. Типовой процесс проектирования.....	422
9.3.1. Строительная спецификация	422
9.3.2. Требования к составу и содержанию документации	423
9.3.3. Сборка экрана.....	427
9.3.4. Установка экранированных дверей	428
9.3.5. Проверка качества компонентов	428
9.3.6. Экспертиза проектных решений	431
10. Обеспечение информационной безопасности в СТЗ	434
10.1. Кластеризация оборудования в СТЗ	434
10.1.1. Концепция кластерного разделения оборудования	434
10.1.2. Особенности проекта информационно защищенной системы	436
10.1.3. Кластеры оборудования	438
10.2. Электромагнитная защита кластеров	443
10.2.1. Требования к электромагнитной защите кластеров.....	443
10.2.2. Детальные требования к экранированию кластерных областей	444
10.3. Техника экранирования с учетом информационной безопасности	451
10.3.1. Общие подходы	451
10.3.2. Проект строения при эффективности экранирования 50 дБ	452
10.3.3. Модульные экранированные помещения.....	454
10.3.4. Особенности конструкции экрана	456
10.3.5. Защита проникновений	462
Литература	464

1. Телекоммуникационные системы СТЗ и обеспечение информационной безопасности

1.1. Информационная безопасность в телекоммуникационных системах

Информационная безопасность телекоммуникационных систем непосредственно связана с возможными угрозами, уязвимостью и атаками, которые могут быть в отношении этих систем. Угроза безопасности телекоммуникационной системы – это потенциально возможное происшествие, независимо, преднамеренное оно или нет, которое может оказать нежелательное воздействие на саму систему, а также на информацию, хранящуюся в ней. Уязвимость телекоммуникационной системы – это некая ее характеристика, которая делает возможным возникновение угрозы. Стойкость систем к угрозам электромагнитного характера частично определяется параметрами электромагнитной совместимости (ЭМС) оборудования, систем и установок.

Технические средства систем телекоммуникаций в обязательном порядке должны отвечать требованиям ЭМС. Электромагнитная совместимость – это свойство технического средства не создавать помех другим техническим средствам, штатно функционируя в заданной электромагнитной обстановке. Если электромагнитная обстановка отличается от стандартной, например, из-за преднамеренного воздействия мощного электромагнитного импульса, то оборудование телекоммуникационной системы функционирует со сбоями, а при значительной интенсивности импульса может выйти из строя. Практически все характеристики ЭМС определяют степень уязвимости систем и установок.

Атака на телекоммуникационную систему, в том числе и за счет электромагнитного воздействия, – это действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости. Таким образом, атака – это реализация угрозы. Часто бывает невозможно различить преднамеренные и случайные действия, и хорошая система защиты должна адекватно реагировать на любое из них [3–5]. Это говорит о том, что методы и средства обеспечения ЭМС могут быть с успехом применены для обеспечения информационной безопасности при атаках электромагнитного характера.

Обычно выделяют три основных вида угроз безопасности: угрозы раскрытия, целостности и отказа в обслуживании.

Угроза раскрытия заключается в том, что информация становится известной тому, кому не следовало бы ее знать. В терминах компьютерной безопасности угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в вычислительной системе или передаваемой от одной системы к другой. Иногда вместо термина «раскрытие» используются термины «кража» или «утечка» и, соответственно, «каналы утечки информации». Например, перехват электромагнитного поля от кабелей или оборудования систем телекоммуникаций в ряде случаев позволяет восстановить информацию по параметрам перехваченного поля.

Угроза целостности включает в себя любое умышленное изменение (искажение или уничтожение) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую. Обычно считается, что угрозе раскрытия подвержены в большей степени государственные структуры, а угрозе целостности – деловые или коммерческие. Здесь можно говорить о нарушении целостности информации за счет электромагнитных воздействий на систему. Современные достижения в генерировании и излучении сверхширокополосных электромагнитных импульсов большой энергии выводят проблему обеспечения целостности информации на ведущие позиции.

Угроза отказа в обслуживании возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным, так чтобы запрашиваемый ресурс никогда не был получен, или оно может вызвать только задержку запрашиваемого ресурса, достаточно длительную для того, чтобы он стал бесполезным. В таких случаях говорят, что ресурс исчерпан.

Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений, реализованных в виде структурированных кабельных систем (СКС) (коаксиальный кабель, витая пара, оптоволокно и т.п.) и программно – при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной телекоммуникационной системы (ТС), передаются по сетевым соединениям в виде пакетов обмена.

Оборудование в пределах СТЗ может быть источником электромагнитных полей, связанных с информационным содержанием, которые могут быть перехвачены вне объекта. Если эта информация расшифрована, то злоумышленник получит доступ к конфиденциальной информации. В этом случае требуется электромагнитный барьер, препятствующий эмиссии полей от объекта в окружающую среду.

Результаты проведенного анализа позволяют представить методы и средства обеспечения безопасности в каналах телекоммуникаций в виде схемы, показанной на рис. 1.1.

Технические средства защиты реализуются в СТЗ в виде электрических, электромеханических и электронных устройств, совокупность которых можно разделить на:

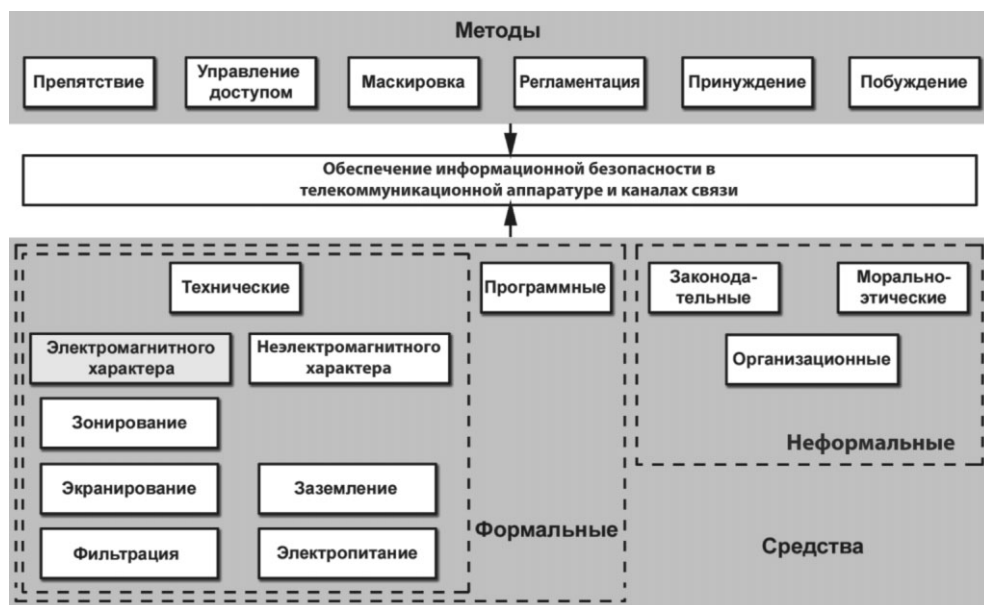


Рис. 1.1. Блок-схема основных методов и средств обеспечения безопасности телекоммуникационной сети

- аппаратные – устройства, встраиваемые непосредственно в телекоммуникационную аппаратуру, или устройства, которые сопрягаются с подобной аппаратурой по стандартному интерфейсу. Из наиболее известных аппаратных средств можно отметить схемы контроля информации по четности, схемы защиты полей памяти по ключу и т.д.;
- физические – реализуются в виде автономных устройств и систем. Например, системы ограничения доступа, электронно-механическое оборудование охранной сигнализации; системы видеонаблюдения и т.п.;
- технические – создание препятствий для электромагнитных полей или кондуктивной эмиссии; ограничение перенапряжений на терминалах оборудования, минимизация помех по цепям питания и заземления, гальваническая развязка разнесенных устройств;
- программные средства, специально предназначенные для выполнения функций защиты информации.

Сопоставление существующих методов и средств защиты и эволюции технологии обеспечения безопасности связи в каналах телекоммуникаций показывает, что на первой фазе развития этой технологии преимущественное развитие имели программные средства, вторая фаза характеризовалась интенсивным развитием всех основных методов и средств защиты, на третьей

фазе развития, которая характерна для перспективных СТЗ, все определеннее вырисовываются следующие тенденции:

- аппаратная реализация основных функций защиты;
- создание комплексных средств защиты, выполняющих несколько защитных функций;
- унификация и стандартизация алгоритмов и технических средств;
- расширение сферы применимости отработанных методов и средств обеспечения ЭМС и повышения стойкости аппаратуры к деструктивным электромагнитным воздействиям для обеспечения информационной безопасности.

На целостность информации влияют электродинамические процессы и ограничения, связанные с возможностью распространения электромагнитных волн (ЭМВ) в определенной среде в заданной электромагнитной обстановке. Для управления средой распространения ЭМВ и локализации электромагнитного поля должно применяться эффективное экранирование, причем не только технических компонентов телекоммуникационных систем, но и помещений, в которых устанавливается ТС. Это говорит о комплексности проблемы обеспечения информационной безопасности, которая решается на всех этапах жизненного цикла телекоммуникационной системы: от проработки ее концепции до инсталляции и вывода из процесса эксплуатации. Учет всех факторов реализации технических методов и средств обеспечения информационной безопасности на возможно ранней стадии проектирования СТЗ поможет избежать дорогостоящих переделок на этапах строительства и эксплуатации здания.

Расширенное понимание вопросов информационной безопасности требует, кроме рассмотрения побочных электромагнитных излучений и наводок (ПЭМИН) от аппаратуры, говорить еще о целостности сигнала в межсоединениях. Злонамеренное искажение информационного сигнала в телекоммуникационной системе может привести к потере информации или ее искажению. Эти искажения, в свою очередь, относительно просто вызвать инъекцией помех в сеть питания телекоммуникационной системы [6], мощным электростатическим разрядом, нарушением заземления системы, мощным электромагнитным импульсом. Подобные приемы и соответствующие технические средства, попадая в руки злоумышленников, могут привести к существенному ущербу и уже получили, как отмечалось выше, название «электромагнитный терроризм» [7].

Для оценки возможности утечки информации необходимо провести инженерно-технические исследования (ИТИ), которым подвергается каждое конструктивно обособленное устройство телекоммуникационной сети (компьютер, принтер, модем и т.п.), а также экранированное помещение или здание в целом. По результатам исследований оценивается защищенность объекта. Можно считать, что устройство считается защищенным, если вероятность правильного определения единицы информации (буквы, цифры, знака, фрагмента изображения) по результатам приема сигналов в каналах

возможной утечки на границе контролируемой (охраняемой) зоны не превышает определенного значения, называемого нормой верхнего уровня, или величина отношения «информативный сигнал / нормированная помеха» не превышает определенного значения, называемого нормой нижнего уровня или просто нормой.

Здесь уместно подчеркнуть различие между подходами в области информационной безопасности и электромагнитной совместимости, хотя природа и физика явлений одинакова. В проблеме ЭМС испытания и измерения устойчивости и помехоэмиссии устройств ведутся при строго нормированных условиях, оговоренных в соответствующих стандартах. При анализе эффективности защиты информации технический потенциал злоумышленника известен только предположительно, согласно принятой модели и априорной оценке. Кроме этого, дистанция расположения приемника информации также известна только предположительно, исходя из конкретной ситуации. Это привносит вероятностный характер оценок технических решений, в отличие от задач ЭМС, где результаты трактуются как «не более», «не менее» относительно заданных норм на помехоэмиссию и устойчивость. При разработке средств электромагнитной защиты следует использовать данные нормативно-технической документации и стандартов, которые получены в результате глубоких исследований и отражают современный уровень науки и техники. Например, стандарты США в области информационной безопасности оговаривают требуемую эффективность экранирования в 50 и 100 дБ для экранированных зданий и выделенных помещений.

Возвращаясь к проблеме информационной безопасности, можно принять, что

- объект считается защищенным, если защищены все компоненты телекоммуникационной системы, включая структурированную кабельную систему объекта;
- выбор требований проводится в соответствии с видом обрабатываемой в системе информации: текстовой, формализованной или графической.

Возможные каналы утечки информации возникают за счет:

- побочных электромагнитных излучений от электронных и кабельных компонентов телекоммуникационной системы внутри объекта;
- ПЭМИН на провода и кабели (цепи электропитания, заземления, структурированные кабельные системы) и т.п., несущих сигналы, содержащих скрываемую информацию, за пределы контролируемой (или проверяемой) зоны объекта;
- ПЭМИН от сигналов, несущих скрываемую информацию, на стороне провода и иные токопроводящие конструкции, гальванически не связанные с компонентами системы, но расположенные вблизи нее и имеющие выход (по проводам или по полю) за пределы контролируемой территории объекта (переизлучение информационного сигнала).

1.2. Учет электромагнитной совместимости при проектировании СТЗ

1.2.1. Основные понятия ЭМС

Проблема электромагнитной совместимости тесно связана с тем, что составляет обширную область радиотехники, электроники и электротехники [8–10]. Миниатюризация оборудования, а также его возрастающая сложность, интеграция и взаимодействие делают электронные системы и компоненты более уязвимыми при электромагнитных воздействиях от источников искусственного и техногенного происхождения.

Функционирование многочисленных промышленных предприятий, интеллектуальных зданий и офисных помещений, сетей электроснабжения целых областей (регионов) зависит от информационно-управляющих систем. Известны многочисленные случаи выхода из строя банковских информационных систем из-за мощных грозových разрядов, нарушения электропитания. Можно привести примеры из других областей, когда помехи в информационных системах приводили к серьезным, а порой и к катастрофическим последствиям. Поэтому функциональная надежность электронных систем является также экономическим фактором первостепенной важности. Перечислим наиболее существенные причины, вызывающие обострение проблемы ЭМС, которые должны быть учтены при проектировании СТЗ:

- возрастает общее число одновременно действующих радиотехнических устройств, в особенности устанавливаемых на подвижных объектах;
- повышается мощность радиопередатчиков, достигая для некоторых типов радиосредств десятков мегаватт;
- расширяются полосы частот, используемые многими современными радиосредствами;
- увеличивается загрузка диапазона радиочастот, несмотря на то что многие участки его уже в настоящее время сильно загружены;
- непрерывно повышается быстродействие электронных средств автоматического управления, контроля, диагностики и т.д. на основе аналоговой и особенно цифровой техники, в частности микро-ЭВМ и микропроцессоров. Такие средства становятся источниками непреднамеренных помех и одновременно более чувствительны к их воздействию;
- возрастает вероятность применения преднамеренных электромагнитных воздействий с террористическими целями;
- бурно развивается электромагнитное оружие, основным воздействием которого является мощный электромагнитный импульс или микроволновое излучение.

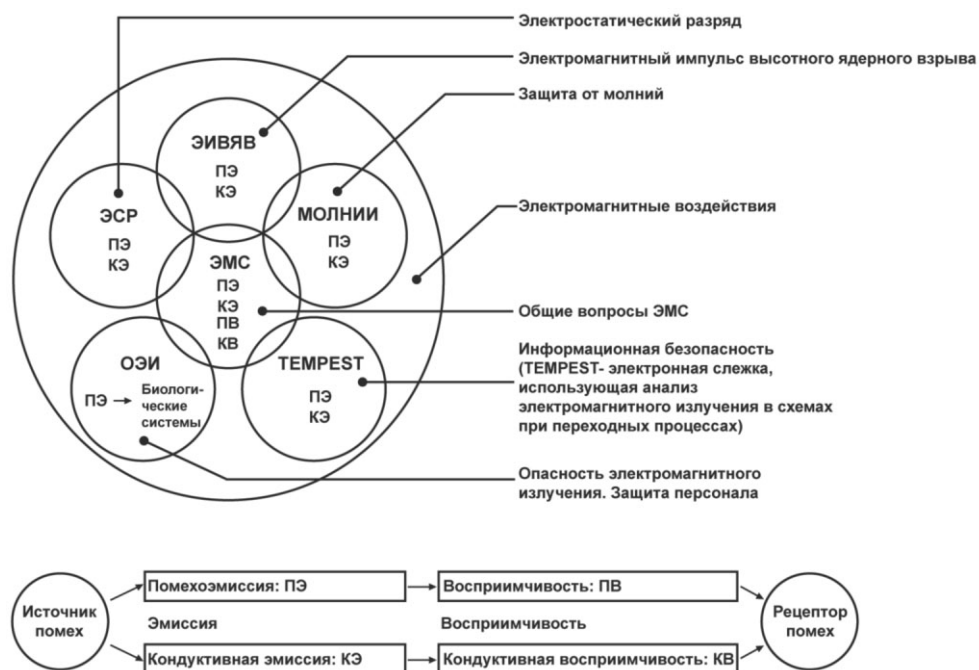


Рис. 1.2. Взаимовязанные области стандартов по ЭМС

Это объясняет, почему стандарты и требования, касающиеся ЭМС, признаны во всем мире или согласованы на региональном уровне, приветствуются изготовителями и пользователями электрического и электронного оборудования, в то время как другие стандарты иногда рассматриваются как мешающие изготовителям продукции. В Технических регламентах РФ на соответствующие виды продукции оговорены требования к ЭМС. 9 декабря 2011 г. утвержден Технический регламент Таможенного союза «Электромагнитная совместимость технических средств» (ТР ТС 020/2011), который вступил в силу с 15 февраля 2013 г.

Стандарты ЭМС являются предпосылкой к обеспечению того, чтобы многочисленные виды электронного оборудования при их одновременной работе не оказали влияния друг на друга или, еще хуже, не вызвали нарушения функционирования оборудования. Они устанавливают требования для оборудования как в отношении максимально допустимой эмиссии излучаемых и кондуктивных электромагнитных помех, так и работоспособности оборудования в условиях влияния этих помех.

Стандартизация – только один аспект проблем, связанных с ЭМС. Стандарты устанавливают общие требования к качеству функционирования в условиях внешних помех, которому должно соответствовать изделие, но его

обеспечение оставляют за изготовителями. Однако требования стандартов могут выполняться только в том случае, если существуют необходимые технические знания, умения и решения, касающиеся проблемы ЭМС.

Решением проблемы ЭМС на глобальном уровне занимаются многочисленные международные организации под эгидой ООН. Наиболее широко ведет работу Международная электротехническая комиссия (МЭК) и ее Специальный комитет по радиопомехам (СИСР), а также Европейский комитет по стандартизации в области электротехники (СЕНЕЛЕК).

На рис. 1.2 показаны взаимоувязанные направления стандартизации в области ЭМС [11]. Эти направления включают общие стандарты по ЭМС, стандарты по высотному ядерному взрыву, молнии, электростатическому разряду, информационной безопасности и охраны здоровья. Они рассматривают параметры помехоэмиссии и устойчивости оборудования, параметры воздействующих факторов, методы и средства испытаний, описание электромагнитной обстановки.

1.2.2. Виды электромагнитных помех

Технический комитет (ТК) 77 МЭК установил классификацию электромагнитных явлений, представленную в таблице 1.1.

Таблица 1.1

Классификация электромагнитных явлений, вызывающих помехи

Явления	Проявление
Кондуктивные низкочастотные	• гармоника, интергармоника • системы передачи сигналов по сетям электроснабжения • колебания напряжения • провалы и прерывания напряжения • разбаланс напряжений (в многофазных цепях) • изменение частоты электропитания • наведенные низкочастотные напряжения • постоянный ток в сетях переменного тока
Низкочастотные, в виде поля излучения	• магнитные поля: – непрерывные – переходные • электрические поля
Кондуктивные высокочастотные	• непосредственно введенные или наведенные напряжения или токи: – незатухающие колебания – модулируемые волны • однонаправленные переходные процессы* • колебательные переходные процессы*

Явления	Проявление
Высокочастотные, в виде поля излучения	• магнитные поля • электрические поля • электромагнитные поля: – незатухающие колебания – модулируемые волны – переходные процессы
Разряд электростатического электричества (ЭСР)	• кратковременный переходной процесс • магнитные поля • электрические поля
Электромагнитный импульс высотного ядерного взрыва (ЭМИ ВЯВ)	• мощные магнитные поля • мощные электрические поля • мощные электромагнитные поля
<i>Примечание.</i> * – отдельные или повторяющиеся (пачки).	

Как видно, электромагнитные явления в виде электромагнитных воздействий различного проявления могут являться существенными источниками угроз безопасности. Здесь необходимо сделать следующие замечания:

- термин ЭМС больше не ограничен областью высоких частот и применяется к целому спектру явлений в полосе частот от 0 Гц до нескольких десятков гигагерц;
- по практическим соображениям (различные характеристики явлений, опыт соответствующих экспертов) было принято целесообразным разделить явления по составу спектра на низкочастотные и высокочастотные. Граница была установлена на уровне 9 кГц (согласно области СИСПР);
- помехи, с которыми имеет дело СИСПР, включаются в кондуктивные или излучаемые высокочастотные явления;
- программа работы ТК 77 также включает электромагнитные эффекты высотных ядерных взрывов (ЯЭМИ), но эта тема не входит в программу работы других организаций, например ТК 210 СЕНЕЛЕК.

1.2.3. Категории изделий

Из практических соображений при анализе ЭМС было установлено, что удобно различать четыре категории изделий согласно их области применения и условиям сертификации на рынке: компоненты, аппараты, системы, установки. Они также соответствуют общему духу применения Европейской директивы по ЭМС. Компонент – электрический или электронный модуль, который сам по себе не имеет конечной функции, но который предназначен для встраивания в аппарат. Аппарат – отдельное готовое изделие с прямой

функцией (функциями), предназначенное для конечного использования. Система – в контексте ЭМС, комбинация аппаратов и/или (активных) компонентов, составляющих отдельный функциональный блок и предназначенных для установки и использования при выполнении определенной задачи (вычислительная система, состоящая из центрального процессора, клавиатуры, принтера, монитора и т.д.).

С целью стандартизации ЭМС имеются две опции:

- либо стандарт по ЭМС может разрабатываться, как упомянуто выше, для каждого компонента или аппарата, особенно в отношении «внутрисистемной» совместимости;
- либо общий стандарт по ЭМС может рассматриваться для всей системы в целом, особенно в отношении «внешней» совместимости. Этот второй стандарт может служить для целей сертификации.

Что касается установки в контексте ЭМС, комбинации аппаратов, компонентов и систем, объединенных вместе и/или смонтированных (индивидуально) в заданном пространстве, то по физическим причинам (например, большие расстояния между индивидуальными элементами) во многих случаях невозможно испытывать установку или набор ее модулей (промышленные предприятия, электрические подстанции, системы телеуправления для больших территорий, телекоммуникационное оборудование СТЗ и т.п.).

Для целей стандартизации ЭМС требования могут в некоторых случаях определяться для всей установки. В особенности это может относиться для ограничений помехоэмиссии (например, в отношении гармоник, радиопомех), но это требует измерений на месте.

В других случаях требования ЭМС должны определяться для каждого элемента, в особенности для помехоустойчивости. Поставщик каждого модуля должен тогда указать условия установки для своих изделий (линии связи, заземление), которые гарантируют правильное функционирование всей установки.

Очевидно, что трудно, а иногда даже невозможно выполнить испытания на помехоэмиссию или помехоустойчивость на наборе модулей системы, сосредоточенных на большом пространстве СТЗ. Также необходимо принимать во внимание тот факт, что испытания могут подвергаться влиянию условий окружающей среды и не соответствовать целям сертификации.

1.2.4. ЭМС и функциональная безопасность

Термин «безопасная система» обычно используется для описания таких систем, которые требуют специфических функций, чтобы уменьшить риски до допустимого уровня. Система, требующая решения вопросов безопасности, может быть реализована в любой технологии, но в контексте ЭМС интерес представляют электротехнические и электронные системы (включая системы телекоммуникаций) [12]. Ошибки в работе и сбои электронного оборудования

в результате нарушений требований ЭМС или преднамеренных ЭМВ могут вести к опасным ситуациям и риску нанесения вреда здоровью людей, оборудованию и окружающей среде.

Исторически складывалось так, что подразделения, которые занимались ЭМС и безопасностью, в пределах одной организации работали в значительной степени независимо друг от друга. В этом случае безопасность, определяемая ЭМС (ЭМС-безопасность), оказалась вне поля зрения специалистов по обеспечению безопасности. Для гражданских приложений, которые опираются, например, на Директиву ЕС по ЭМС [9], требования по функциональной безопасности могут быть почерпнуты, например, в стандарте ГОСТ Р 51317.1.2-2007 (МЭК 61000-1-2:2001) «Совместимость технических средств электромагнитная. Методология обеспечения функциональной безопасности технических средств в отношении электромагнитных помех». Наличие знака соответствия «СЕ», отмечающего соответствие требованиям Директивы ЭМС (или ее гармонизированным стандартам), не может гарантировать, что вопросы ЭМС-безопасности правильно идентифицированы и законодательно решены.

Различные электронные технологии имеют отличающийся потенциал сохранения качественных показателей при воздействии ЭМВ. Многие традиционные информационные технологии, которые на определенном этапе своего развития были не восприимчивы к ЭМВ, при усложнении электромагнитной обстановки и увеличении уровня возмущений стали чувствительны к ним. Кроме этого, современная элементная база имеет тенденцию к увеличению восприимчивости ЭМВ.

Для того чтобы корректно управлять ЭМС-безопасностью, необходима оценка последствий опасности и риска. При этом следует принимать во внимание следующее:

- электромагнитные возмущения, которым может быть подвергнута аппаратура;
- разумно обозримые результаты воздействия таких возмущений;
- эффект воздействия ЭМВ от одного аппарата на другой;
- разумно обозримые параметры безопасности (серьезность, масштаб риска, уровень целостности безопасности), которые могут быть нарушены ЭМВ;
- уровень требований, которые необходимо выполнить, чтобы обеспечить желаемый уровень ЭМС-безопасности.

Такие опасности и оценки рисков вместе с законченными решениями, техническими требованиями, проектными решениями и тестами должны формировать часть из требований обеспечения функциональной безопасности и должны быть документированы. Проектные решения и связанная с ними документация существенно отличаются между организациями и между проектами, но там, где опасности и риски выше (т.е. применяются более высокие уровни целостности безопасности), требуются более высокие уровни деятельности и документации.

Безопасность – термин, используемый, чтобы обозначить понятие согласованного понимания опасностей и их рисков, которые являются приемлемыми для данного общества в конкретной ситуации. Законы о безопасности требуют, чтобы продукты были разработаны и произведены настолько безопасными, насколько ожидает общество.

Функциональная безопасность – термин, использованный, чтобы охватить опасности и риски, связанные с ошибками или сбоями при функционировании систем, устройств или аппаратов. Это отлично от безопасности, которая определяет потенциал устройства противостоять таким опасностям, как возгорание, удар током и образование ядовитых паров. Базовыми документами в области функциональной безопасности следует считать стандарты [13–19], которые гармонизированы с международным стандартом МЭК 61508. Он соотносится с гражданскими системами и в явном виде не затрагивает взаимосвязанные вопросы ЭМС и функциональной безопасности.

При проектировании связанных с безопасностью систем, в частности инсталлированных в СТЗ, необходимо включать анализ опасностей и исследования рисков, которые принимают во внимание по крайней мере в следующих направлениях:

- ошибки применения – или случайные (такие, как ошибки при инсталляции оборудования или ошибки оператора), или преднамеренные (перегрузка или использование для непредусмотренных целей);
- обозримые ошибки проекта СТЗ или в выборе, установке или эксплуатации оборудования;
- применение в экстремальной среде, включая, среди других, интенсивные электромагнитные эффекты, высокие температуры, вибрации и т.п.;
- последствия (опасности) с их вероятностями (рисками), которые вызваны отмеченными выше факторами.

При проектировании СТЗ следует понимать значения этих факторов и необходимо предпринять меры для сведения риска в части функциональной безопасности к минимуму.

1.2.5. Электромагнитные эффекты и функциональная безопасность

В зависимости от показателей помехозащищенности и функциональной безопасности объектов электромагнитные эффекты могут проявляться в виде опасностей для персонала, оборудования, вооружения и летучих материалов (топлива). Рассмотрим основные электромагнитные эффекты более детально.

Электромагнитные шумы – любое ЭМВ, которое прерывает, затрудняет или, иначе, ухудшает или ограничивает эффективность функционирования электроники и электрического оборудования. Эти ЭМВ могут быть вызваны преднамеренно, как в некоторых формах радиоэлектронной войны или при использовании оружия направленной энергии, или непреднамеренно, в резуль-

тате паразитной эмиссии или продуктов взаимной модуляции и т.п. Связанная с электромагнитными шумами «восприимчивость» является мерой неспособности объекта выполнять свою функцию без деградации при наличии ЭМВ.

Электромагнитные возмущения могут быть в форме излученной или кондуктивной эмиссии (помехи электромагнитной энергии). Особенности электромагнитных шумов объектов нужно управлять, чтобы получить высокую степень гарантии, что эти элементы будут функционировать в намеченных инсталляциях без взаимодействий с другим оборудованием, подсистемами или внешней электромагнитной обстановкой, которая в пределах системы является сложной и переменной в зависимости от режимов работы и частот встроенного в СТЗ оборудования. Кроме того, конфигурации электронных систем СТЗ непрерывно изменяются, поскольку устанавливается новое или модернизированное оборудование, а элементы, разработанные для одной платформы, могут использоваться для других платформ.

Электромагнитный импульс (ЭМИ) [20] является неионизированным электромагнитным излучением от ядерного взрыва (ЯВ). Электрические и магнитные поля ЯВ могут взаимодействовать с электрическими или электронными системами и связанными с ними интерфейсами, генерируя разрушительные для работы многих электрических и электронных систем токи и выбросы напряжения [21, 22].

Выделяют следующие основные эффекты и вызванные ими опасности влияния электромагнитных возмущений. Они должны быть приняты во внимание при проектировании СТЗ. Возможные последствия включают опасности: деградацию свойств и безопасность.

Потенциальная опасность для персонала, который подвергнут влиянию электромагнитного поля достаточной интенсивности (HERP), заключается в нагреве человеческого тела. Персонал, занимающийся ремонтом и обслуживанием, с большой вероятностью может попасть под излучение высокой интенсивности из-за его нахождения вблизи излучающих элементов и необходимости ускоренного проведения работ.

Потенциальная опасность возникает, когда летучее горючее, такое как топливо, подвергается воздействию электромагнитных полей, энергии которых достаточно для того, чтобы вызвать воспламенение (HERF). Для того чтобы топливные пары воспламенились, должна присутствовать огнеопасная смесь паров топлива и воздуха в дополнение к интенсивному ЭМ-полю. Излучение может вызвать токи в любом металлическом объекте. Интенсивность тока и, таким образом, сила искры через промежуток между двумя проводниками зависит от интенсивности энергии поля и от того, насколько эффективны проводники в качестве приемной антенны.

Потенциальная опасность существует, когда на вооружение, которое содержит электрически инициализируемые взрывные устройства, неблагоприятно воздействует электромагнитная среда (HERO). Радиочастотная энергия достаточной интенсивности для стрельбы или приведения в действие электрически иницируемых взрывных устройств может быть получена от внеш-

него ЭМВ или по проводам взрывных подсистем, или посредством индуктивно-емкостной связи от соседних источников излучения.

Электромагнитная уязвимость (EMV) – особенность объекта, которая вызывает ухудшение его качества функционирования или соотносится с неспособностью выполнить требуемую задачу в рабочей электромагнитной обстановке. Элемент уязвим, если его параметры стали хуже допустимого уровня из-за незащищенности по отношению к рабочей электромагнитной обстановке или индуцированному переходному процессу.

Проект СТЗ должен учитывать вероятные риски нарушения функциональной безопасности телекоммуникационного оборудования из-за непреднамеренных или преднамеренных электромагнитных воздействий. Степень защиты должна с определенной вероятностью минимизировать риски нарушения функциональной безопасности.

1.2.6. Методология учета стандартов на жизненном цикле проекта

Учет требований стандартов ЭМС является неотъемлемой частью проекта телекоммуникационной системы СТЗ и обеспечения информационной и функциональной безопасности. В определенной мере СТЗ должно быть спроектировано таким образом, чтобы создать условия для работы телекоммуникационного оборудования, отвечающие требованиям стандартов по ЭМС, даже в том случае, если внешняя электромагнитная обстановка по интенсивности превышает требования стандартов.

Общие (универсальные) стандарты ЭМС – это общие и несколько упрощенные стандарты ЭМС на группы продукции, применимые к изделиям, для которых еще не существует конкретных стандартов ЭМС. Они служат как общая ссылка для стандартов для группы продукции. Здесь рассмотрим самые общие вопросы концепции, типизации, содержания и применения общих (универсальных) стандартов ЭМС.

Помехоустойчивость оборудования характеризует его способность противостоять внешним электромагнитным возмущениям. Помехоэмиссия – способность генерировать непредусмотренное электромагнитное возмущение, которое может быть перехвачено и представляет угрозу для качественного функционирования какого-либо другого устройства или системы. Таким образом, видно, что нормы и требования ЭМС непосредственно определяют потенциальную способность электронного оборудования и технических средств (ТС) обеспечивать информационную безопасность.

Концепция и определение общих (универсальных) стандартов ЭМС. Основная цель заключается в том, чтобы для каждой группы изделий или каждого конкретного продукта имелся специализированный стандарт ЭМС (или пункты, касающиеся ЭМС в общем стандарте на продукцию). Ясно, что это длительная и трудная задача, когда оптимальные технические и экономические требования могут находиться в противоречии.

Идея использования общих (универсальных) стандартов по ЭМС как общих стандартов по ЭМС на изделия вначале возникла из-за желания избежать необходимости ожидания продуктовых стандартов, которые будут разрабатываться для каждого конкретного случая. В будущем общие (универсальные) стандарты по ЭМС могут даже иметь постоянный статус.

В соответствии с определением, приведенным в Руководстве 107 МЭК «Руководство по составлению Публикаций ЭМС», «...общие (универсальные) стандарты по ЭМС применяются к изделиям, работающим в определенной среде и для которых не существуют специализированные стандарты на группу продукции. Они определяют наборы существенных требований, процедуры испытаний и обобщенные критерии качества функционирования, применимые к таким изделиям или системам, работающим в этой среде».

Применяются следующие правила:

- общие (универсальные) стандарты по ЭМС не включают детальное описание методов измерения и испытаний и т.д., а для этой цели обращаются к Основным стандартам по ЭМС;
- они рассматривают требования и испытания, относящиеся к помехоэмиссии и устойчивости, возможно в отдельных документах;
- они определяют ограниченное число необходимых испытаний на помехоэмиссию и устойчивость, а также как минимум испытательных уровней с тем, чтобы обеспечить достаточную совместимость при достижении технико-экономического оптимума;
- они должны быть идентифицированы на титульном листе надписью «Общий (универсальный) стандарт ЭМС».

Типы общих (универсальных) стандартов ЭМС. Было признано целесообразным разработать только два набора Общих (универсальных) стандартов по ЭМС, каждый набор для двух типов сред:

- среда жилых и коммерческих зон, а также среда на предприятиях легкой промышленности;
- среда промышленных предприятий.

Каждый набор включает стандарт на помехоэмиссию и стандарт на помехоустойчивость. Также считается целесообразным иметь те же самые общие (универсальные) стандарты по ЭМС на базе всемирного признания в случае необходимости с некоторыми общими изменениями в данном регионе (например, Европа).

В будущем только МЭК будет иметь дело с общими (универсальными) стандартами по ЭМС, и любые изменения должны быть темой параллельного утверждения.

Требования Общих стандартов соотносятся с представлением технического средства в виде черного ящика с соответствующими портами (рис. 1.3).

Для каждого вида порта стандарты представляют таблицу с:

- электромагнитными возмущениями, подлежащими рассмотрению;
- соответствующие Основные стандарты;

- предписанные нормы помехоэмиссии или уровни испытаний на помехоустойчивость;
- критерии качества функционирования;
- примечания по применению, в случае необходимости.

В соответствии с целью общих (универсальных) стандартов по ЭМС из подлежащих рассмотрению возмущений ограничиваются (нормируются) наиболее существенные. Они включают (или могут включать):

- в отношении норм помехоэмиссии:
 - гармоники напряжения электропитания;
 - колебания напряжения электропитания;
 - кондуктивные радиочастотные напряжения от 0,15 до 30 МГц;
 - излучаемые радиочастотные поля от 30 до 1000 МГц;
- в отношении испытаний на помехоустойчивость:
 - гармоники напряжения электропитания;
 - колебания напряжения, провалы, прерывания;
 - магнитные поля на промышленной частоте;
 - кондуктивные радиочастотные напряжения от 0,15 до 80 МГц;
 - излучаемые радиочастотные поля от 26 до 1000 МГц (в СЕНЕ-ЛЕК только свыше 80 МГц);
 - радиополя от мобильных телефонов с частотой около 900 МГц;
 - импульсы перенапряжения;
 - быстрые переходные напряжения;
 - разряды электростатического электричества.

Что касается помехоустойчивости, существенными являются критерии качества функционирования. В соответствии с важностью явления и характером порта (рис. 1.3) сформулированы три критерия:

А: аппарат должен функционировать в соответствии с назначением в течение и после испытания.

В: аппарат должен функционировать в соответствии с назначением после испытания. В течение испытания допускается некоторое ухудшение качества функционирования, как определяется изготовителем.

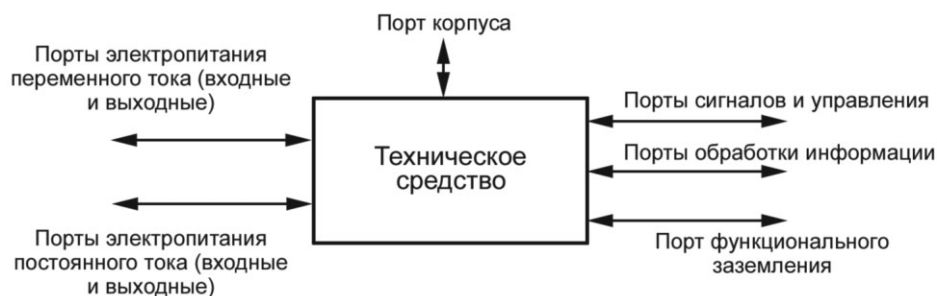


Рис. 1.3. Примеры портов технического средства

С: допускается временное отсутствие функционирования в течение и после испытания, если функция самовосстанавливаемая или может быть восстановлена с использованием средств управления оборудованием.

Определения среды. Определения сред «жилая, коммерческая, легкая промышленность» и «промышленная» не очень ясны и объясняются примерами местоположений. Интеллектуальные здания и вычислительные центры попадают в разряд жилых, коммерческих и легкоиндустриальных сред (деловые помещения, например офисы и банки). Специальные технические здания могут не вписываться в стандартные понятия. Изготовитель оборудования должен объявить, для какой среды его изделие предназначено.

1.2.6.1. Жизненный цикл изделия и решение проблемы ЭМС

Относительная стоимость проекта СТЗ устанавливается в процессе развития проекта. Каждый рубль, потраченный на решение проектных задач на этапе концептуальной проработки, может сохранить десятки тысяч на стадии строительства и эксплуатации. Следует учитывать, что при строительстве зданий и сооружений нет возможности создания «опытных образцов» для проведения всесторонних испытаний. Ошибка в проекте СТЗ приведет к дорогостоящим переделкам и реконструкциям, которые во много раз могут увеличить стоимость объекта. Поэтому все технические решения, принятые на концептуальном уровне, должны быть тщательно выверены.

Практически любой проект должен определяться сферой применения СТЗ и кругом пользователей. Это позволит выявить технические требования и стандарты, которым должен соответствовать объект. При этом должны быть учтены стадии инсталляции оборудования, включая охранные системы, и техобслуживания, так чтобы объект был защищен регулирующими документами на всех этапах его жизненного цикла.

Качество принятых решений будет определяться квалификацией специалистов, участвующих в разработке проекта. Чем раньше в жизненном цикле объекта эти навыки и знания будут проявлены, тем более рентабельными они станут. Деньги, потраченные на решение вопросов согласования с регулирующими требованиями на этапе разработки концепции, транслируются в более низкие затраты в конце жизненного цикла проекта. В процессе развития цикла создания объекта степень свободы в принятии решений снижается.

Стадия концептуальной проработки. На начальных стадиях создания нового объекта на основе подготовленных маркетинговых исследований и технического задания формулируются технические требования – определенный перечень необходимых функций и требований к объекту. Технические требования к проекту охватывают требования к уровню электромагнитной защиты, размещению технических средств на объекте, устанавливают связи с помощью монтажных схем, оговаривают ряд других требований, включая информационную безопасность.