УДК 621.37/.39

Б.Б. Акбашев, Н.В. Балюк, Л.Н. Кечиев

Обеспечение информационной и функциональной безопасности в специальных технических зданиях при электромагнитных воздействиях

Рассматривается содержание проблемы обеспечения функциональной и информационной безопасности при проектировании специальных технических зданий (СТЗ). Дается характеристика узловых моментов функциональной и информационной безопасности, архитектурного экранирования, формулируются требования к объектам, определяются актуальные направления дальнейшего развития теории и практики обеспечения функциональной и информационной безопасности СТЗ.

специальные технические здания, информационная безопасность, функциональная безопасность, электромагнитные воздействия

Специальные технические здания

Специальные технические здания (СТЗ) выполняют в настоящее время разнообразные функции, являясь объектами инсталляции значительного числа электронных систем. Эти системы с одной стороны выполняют функции жизнеобеспечения СТЗ, а с другой – выполняют функции по обработке информации, которые соответствуют назначению здания.

По мере развития микроэлектроники электронные устройства стали выполнять все более сложные функции при одновременном увеличении скорости обработки информации. На них построены системы обработки информации, которая может представлять государственную, военную или коммерческую тайну. Эти функции не должны подвергаться воздействиям, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней. В этом случае речь идет об информационной безопасности. Но если следствием изменений информации будет ущерб здоровью человека, окружающей среде, собственности, то речь идет о функциональной безопасности [1]. Таким образом, функциональную безопасность можно рассматривать как особый случай нарушения информационной безопасности, в результате чего обществу, людям и/или окружающей среде нанесен значительный ущерб.

Особый класс таких внешних воздействий, приводящих к нарушению функциональной и информационной безопасности (ФИБ), представляют естественные и техногенные электромагнитные воздействия. Внешний источник электромагнитного излучения охватывает своим влиянием конструкции зданий и сооружений. Не исключены варианты локального воздействия на объект т.н. «электромагнитного оружия». Современные технические средства деструктивного электромагнитного воздействия способны дистанционно, скрытно и внезапно поразить практически любую электронную систему [2, 3].

Перспективная технология создания электронной аппаратуры, которая обеспечивает высокие скорости обработки информации, обладает повышенной чувствительностью к наведенным напряжениям и токам, вызванных электромагнитными полями от различных источников гармонических сигналов или переходных процессов. Совокупность электромагнитных полей определяют конкретную электромагнитную обстановку (ЭМО), в которой находится СТЗ и его электронные системы. Для устранения возможности нарушения ФИБ электронное оборудование должно быть электромагнитно изолировано от среды, в которой оно находится.

Особое значение имеют вопросы информационной безопасности. Оборонные сведения и дипломатическая информация имеют высокую классификацию секретности и должны быть защищены от несанкционированного перехвата или преднамеренных деструктивных электромагнитных воздействий. Связь и центры обработки секретных данных должны отвечать требованиям соответствующих стандартов в области информационной безопасности.

В России действует ряд стандартов [4, 5] по защите информации, в которых рассматриваются электромагнитные воздействующие факторы. Эти факторы делятся на объективные и субъективные подклассы, каждый из которых разделяется на внутренние и внешние факторы. Внутренние факторы, такие как побочные электромагнитные излучения и наводки, предотвращаются на этапе разработке аппаратуры и ее монтажа. В этом случае ответственность в большей мере лежит на разработчиках аппаратуры. Внешние факторы предусматривают воздействие непреднамеренных электромагнитных излучений, а также электромагнитных факторов естественного происхождения, например, молний. Преднамеренные силовые воздействия рассматриваются применительно к автоматизированным системам в защищенном исполнении.

В США документом по обеспечению информационной безопасности на объектах информатизации является руководство TEMPEST [6]. Основными элементами защиты оборудования в этом случае являются зонирование, экранирование зданий и помещений, заземление, фильтрация. При создании СТЗ выполнение экранов в цикле строительства является дополнительной, а в ряде случаев и основной, защитой оборудования в целях обеспечения ФИБ.

Элементами подсистем СТЗ, на которые осуществляется электромагнитное воздействие или от которых необходимо анализировать электромагнитное излучение, являются [7, 8]:

- ЭС различного назначения и аппаратура в их составе,
- структурированная кабельная система локальных вычислительных сетей СТЗ,
- металлоконструкции СТЗ,
- система электропитания СТЗ.

Архитектурное экранирование

В последнее десятилетие требования по обеспечению соответственной электромагнитной изоляции объектов с целью обеспечения информационной и функциональной безопасности стало неотъемлемой частью проектов и конструкций СТЗ [9, 10]. Это объясняется появлением новых угроз электромагнитного терроризма, повышением требований к защищенности ответственной информации, расширением перечня опасностей при нарушении функциональной безопасности, снижением чувствительности быстродействующих систем, наличием значительных по протяженности распределенных локальных сетей. Потребности в интегрированных экранирующих средствах и необходимость комплексного решения означает, что не только специалисты в области электроники, но и архитекторы и строители должны быть знакомы с проектом, спецификацией, конструкцией и методами тестирования экранирующих строительных конструкций.

Участие различных специалистов в создании СТЗ требует их четкой координации, расширения области знаний и системного подхода к решению поставленных задач. Уместно разработку проекта, конструкций экранов и процедур тестирования экранированных участков помещений традиционно оставлять специалистам по электромагнитной совместимости (ЭМС) и ФИБ. Специфические задачи архитектурного проектирования и строительства должны оставаться за соответствующими специалистами, которые должны достаточно глубоко разбираться в смежных вопросах.

Необходимость в электромагнитной защите расширилась как в части широты охвата электромагнитных проблем, так и в части защиты технических средств, которые стали намного более разнообразны. Из-за отсутствия развитой теории электромагнитного экранирования применительно к строительным конструкциям технические решения зачастую либо излишне дорогие из-за избыточности конструкции, либо имеют существенные изъяны, которые нару-

шают фундаментальные принципы экранирования. Кроме них к специфическим вопросам создания экранированных строений и помещений СТЗ можно отнести [9]:

- выбор материалов, которые одновременно отвечают требованиям эффективного экранирования для электрических, магнитных или электромагнитных полей и строительства в зависимости от поставленной задачи;
- выбор методов и способов соединений элементов конструкций экранов, обеспечивающих минимальные неоднородности в экране;
- проектирование электромагнитной защиты вводов питания, связи, вентиляции, кондиционирования, отопления (HVAC);
- разработка защищенных систем доступа персонала и перемещения оборудования;
- выбор и реализация процедур тестирования, гарантирующих получение необходимых данных для проверки выполнения требований технического задания.

Теория и практика создания экранированных помещений и СТЗ рассматривается как новое направление – архитектурное экранирование [9, 10]. Систематизацию основных задач архитектурного экранирования дает топологическое представление [11–16], которое помогает комплексно и наглядного представить перечисленные выше компоненты системы экранирования и найти наиболее рациональные пути контроля над электромагнитными помехами.

На рис. 1 приведено обобщенное топологическое представление экранирующей системы, заключенной в объеме, окруженном внешней экранирующей поверхностью. Экранирующие поверхности могут быть пронизаны точками проникновения электромагнитной энергии такими, как швы, зазоры в обшивке и в корпусах, вводы кабельных линий электропитания, данных, управления, системы доступа персонала и т.д.

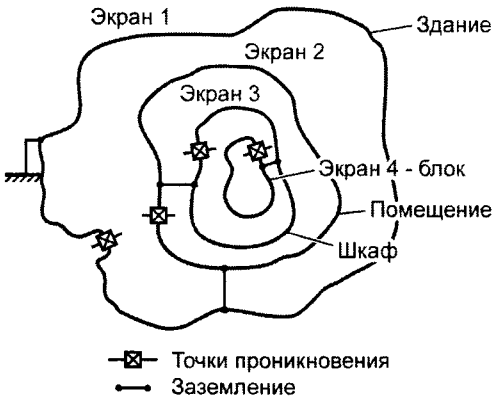

Рис. 1. Топологическая модель системы экранирования

Формальный топологический подход описания системы экранирования может быть применен: для описания системы, для разработки требований к средствам защиты оборудования, для рационального распределения степеней защиты между отдельными барьерами, для минимизации точек проникновения и формализации требований к ним. На основе топологического подхода возможна декомпозиция системы на более мелкие и более простые части.

Факторами, которые нужно рассмотреть при выборе концепции экранирования СТЗ, являются: сложность требуемых взаимодействий с техническими средствами, затраты на проектирование и создание, технологичность, затраты на обслуживание, требования надежности, гибкость для модернизации системы, поддержка в процессе эксплуатации.

Весьма важной и ответственной стадией создания СТЗ является разработка и реализация системы заземления оборудования, которая отличается от требований СНиП.

Практическая реализация системы экранирования зависит от сложности и назначения системы, которая должна быть защищена. Если определено, что для наиболее чувствительных компонентов требуется эффективность экранирования 80 дБ, а для остальных компонентов требуется эффективность только 60 дБ, то тогда могут быть установлены зоны с различным эффективностями экранирования. На сегодня актуальной остается задача оптимального

распределения общей эффективности экранирования на значения эффективности для каждого уровня экранирования по критерию минимизации стоимости проекта на всем жизненном цикле СТЗ. Ее решение требует знания комплекса как технических, так и экономических аспектов создания СТЗ.

Особое внимание должно быть уделено тестированию готового объекта на эффективность экранирования.

Создание экранированных помещений требует развитой спецификации (паспорта) объекта, в которой будут детально отражены не только их архитектурные, строительные и инженерные особенности, но и требования к свойствам экранов, технологии их монтажа, выбору материалов и т.п. В ней должна быть отражена природа строительного объекта, специфика защищаемого оборудования, возможные условия электромагнитного воздействия. Широкое применение САПР при проектировании СТЗ требует развития электронного документооборота, в проектной документации которого должны быть учтены мероприятия по электромагнитной защите объекта с целью обеспечения ФИБ.

Функциональная безопасность и СТЗ

Функциональная безопасность при учете электромагнитных факторов охватывает опасности и риски, связанные с ошибками или сбоями при функционировании систем, устройств или аппаратов. При разработке СТЗ необходимо для критических электронных систем обеспечить достижение приемлемого риска сбоев систем в пределах ограничений функциональной эффективности и пригодности, времени и стоимости по всем фазам жизненного цикла. Это отлично от безопасности, которая определяет потенциал устройства противостоять таким опасностям как, например, возгорание, удар током и образование ядовитых паров. Базовыми документами в области функциональной безопасности следует считать стандарты [17–23], которые гармонизированы с международным стандартом МЭК 61508. Он соотносится с гражданскими системами и, к сожалению, в явном виде не затрагивает взаимоувязанные вопросы ЭМС и функциональной безопасности.

Ошибки в работе и сбои электронного оборудования в результате нарушений требований ЭМС могут вести к опасным ситуациям и риску нанесения вреда здоровью людей, оборудованию и окружающей среде. Для гражданских приложений, которые опираются, например, на Директиву ЕС по ЭМС [24], требования по функциональной безопасности не определены. Соответствие требованиям Директивы ЭМС (или ее гармонизированным стандартам), не может гарантировать, что вопросы функциональной безопасности правильно идентифицированы и законодательно решены.

При решении вопросов функциональной безопасности следует принимать во внимание следующее [25]:

- электромагнитные возмущения (ЭМВ), которыми могут быть подвергнуты системы СТЗ,
- разумно обозримые результаты воздействия таких возмущений,
- результаты воздействия ЭМВ от одного аппарата на другой,
- параметры безопасности (серьезность, масштаб риска, уровень целостности безопасности), которые могут быть нарушены ЭМВ,
- уровень требований, которые необходимо выполнить, чтобы обеспечить желаемый уровень функциональной безопасности.

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. Под опасностью понимают любое реальное или потенциальное условие, которое может вызвать ранение, болезнь или смерть персонала; повреждение или потерю оборудования или ухудшение окружающей среды. Например, электромагнитное воздействие на автоматизированную систему пожаротушения может привести к распылению воды и пены в помещениях, что может вызвать нанесение вреда здоровью человека, и выведет находящееся в них оборудование из строя.

При проектировании СТЗ необходимо включать анализ опасностей и исследование рисков в следующих направлениях:

- ошибки применения – или случайные (такие, как ошибки при монтаже оборудования) или преднамеренные (токовые перегрузки или использование для непредусмотренных целей),
- ошибки проекта в части обеспечения электромагнитной защиты здания и помещений,
- размещение СТЗ в экстремальной среде, включая, среди других, электромагнитные эффекты, высокие температуры, сейсмическую активность и т.п.,
- последствия (опасности) с их вероятностями (рисками), вызванные отмеченными выше факторами.

Технические требования для целостности безопасности могут быть получены, анализируя опасности и риски и определяя степень снижения риска, которую вызывает специфическая функция безопасности. Общий принцип, – чем выше уровень требуемой целостности безопасности, тем более жесткие требования предъявляются к разработке СТЗ, чтобы достичь более низких интенсивностей сбоев и отказов установленного в нем оборудования, которые требуются для достижения допустимого риска.

Требования безопасности для электрического или электронного оборудования, используемого в безопасных системах, должны быть специфицированы и определены в контексте опасности системы и оценки риска на возможно более ранней стадии ее жизненного цикла. Аспект безопасности должен быть учтен на стадии обслуживания и эксплуатационных процедур, поэтому и на этих этапах следует рассматривать доминирующие электромагнитные эффекты. Программные изменения и обновления электронных систем могут также негативно затрагивать ЭМС систем и оборудования и, следовательно, функциональную безопасность.

Когда планируется применить в СТЗ новое оборудование, должны быть предприняты шаги, гарантирующие одновременную совместную работу этого оборудования и ранее установленного таким образом, чтобы имеющие место электромагнитные возмущения не вызывали уход функциональных параметров оборудования за пределы установленных границ.

Стандартные испытания на соответствие требованиям ЭМС не всегда дают полное представление о функциональной безопасности оборудования, работающего в реальной электромагнитной обстановке. Поэтому обеспечение ЭМС в контексте функциональной безопасности требует специальных программ испытаний. Особенно важно, чтобы вопросы обеспечения ЭМС рассматривались на возможно ранних стадиях проектирования оборудования и его инсталляции в СТЗ, поскольку именно тогда могут быть приняты наиболее эффективные меры (это вероятно будут и наиболее рентабельные способы гарантировать ЭМС).

Когда система спроектирована с некоторой избыточностью для обеспечения резервирования и повышения надежности работы, меры, принятые для повышения надежности системы, могут оказаться бесполезными в условиях ЭМВ.

Там, где используются защитные устройства (например, устройства амплитудного ограничения) для достижения требуемого уровня помехоустойчивости, отказ такого устройства может вызвать снижение этого уровня и привести к нарушению функциональной безопасности. В этом случае отказ защитного устройства должен обнаруживаться автоматически (например, действием диагностических подсистем) или путем регулярных проверок с целью выявления любых отказов. Периодичность таких испытаний должна быть определена на основе приемлемой вероятности отказа защитного элемента в конкретном специфическом приложении.

Необходимо, чтобы информация о методах и способах обеспечения ЭМС была доступной для проектировщиков СТЗ и применяемого оборудования, операторов и инсталляторов, чтобы гарантировать осуществление и поддержку предпринятых в проекте мер. Это необходимо для сохранения уровней эмиссии и восприимчивости оборудования в предусмотренных проектом пределах.

Важно отметить следующие особенности построения безопасных систем, инсталлированных в СТЗ:

- не всегда признается, что система управления связана с безопасностью,

- блокирующая функция для обеспечения безопасности должна быть выполнена схемами гарантированной работоспособности;
- устойчивость электронных систем СТЗ к электромагнитным воздействиям (ЭМВ) может быть достигнута и аппаратными и программными средствами.

При модернизации оборудования необходимо провести анализ рисков и опасностей, и разработать технические задания по обеспечению целостности безопасности после внесенных изменений.

Защита информации в электронных средствах СТЗ при ЭМВ

В задачах физической защиты информации в электронных системах СТЗ при электромагнитных воздействиях можно выделить следующие направления, связанные с возможным искажением, уничтожением или блокированием информации при обработке, хранении или ее передаче [26, 27] при непреднамеренных и преднамеренных ЭМВ:

- по полю от мощных источников излучения природного (молнии) и техногенного происхождения, в том числе от высотного ядерного взрыва, электромагнитного оружия, средств радиоэлектронной борьбы и электромагнитного терроризма,
- по сети питания,
- по металлоконструкциям,
- по проводным линиям связи,
- по системе заземления.

Кроме этого при инсталляции оборудования и его эксплуатации следует учитывать факторы защиты информации, связанные с побочным электромагнитным излучением (ПЭМИ) при обработке, хранении или передаче информации, с побочной кондуктивной передачей информации через проводные линии связи, а также возможность нарушения целостности информации электростатическими разрядами (ЭСР). Эти вопросы, скорее, в компетенции поставщиков оборудования, но проект СТЗ должен предусматривать условия для такой инсталляции оборудования, при которой не будут нарушены условия обеспечения ЭМС и технических условий.

Учет электромагнитной обстановки

Важнейшим этапом создания «безопасного» СТЗ является идентификация электромагнитной обстановки, в которой находится объект во время всех фаз жизненного цикла. Воздействие на аппаратуру в определенной электромагнитной среде зависит от особенностей ее восприимчивости, амплитуды и частоты ЭМВ, особенностей строения и окружающей среды и т.д. Чтобы предотвратить проблемы нарушения информационной и функциональной безопасности, при разработке СТЗ должны быть учтены возможные электромагнитные эффекты среды. Требования к среде должны быть включено в спецификацию строения или помещения, чтобы гарантировать удовлетворительную работу электронных систем в определенной ЭМО.

В разработке требований работоспособности и безопасности технических средств, которые предъявляются к электромагнитной среде, рассматриваются следующие основные аспекты [28–30]:

- конфигурация среды, в которой расположено СТЗ,
- конфигурация систем СТЗ и особенности строения,
- требования к информационной и функциональной безопасности,
- восприимчивость систем и оборудования СТЗ,
- перспективы модернизации, развития и обновления систем в СТЗ на протяжении жизненного цикла.

Электромагнитная обстановка – результирующий продукт мощностного и временного распределения в различных частотных диапазонах излученных или кондуктивных электромагнитных полей, токов и напряжений, который определяет условия, в которых находится

СТЗ при выполнении предусмотренной функции. ЭМО влияет на функциональные возможности систем, и требуют специфических методов защиты от их отрицательного воздействия, которые включают:

- электромагнитные излучения и кондуктивные помехи от источников естественного и техногенного происхождения, что требует выполнения требований ЭМС для технических средств,
- электромагнитные помехи и шумы различной природы в широком диапазоне частот,
- электромагнитные воздействия, определяющие электромагнитную уязвимость технических средств,
- электромагнитный импульс от источников техногенного происхождения, как правило, высокой интенсивности и сверхширокополосный,
- электростатический разряд,
- молнии.

Результаты электромагнитных воздействий могут привести к опасностям для персонала, вооружения, летучих материалов типа топлива.

Электромагнитная обстановка соответствует специфическому времени и местоположению СТЗ, которое не будет изменяться, но среда может претерпевать изменения за время эксплуатации СТЗ.

Идентификация опасностей

В настоящее время разработаны и используются многочисленные подходы, чтобы идентифицировать системные опасности. Ключевой аспект многих из этих подходов заключается в идентификации опасностей для последующего управления разработкой и сопровождением программ обеспечения безопасности, связанных с проектом [31].

Оценка риска. Следует оценить серьезность и вероятность риска причинения ущерба, связанного с каждой идентифицированной опасностью, то есть, определить потенциальное воздействие опасности на персонал, технические средства, оборудование, топливо, выполняемые операции или окружающую среду. Чтобы оценить риск могут также использоваться другие факторы, например, число людей, которым может быть нанесен ущерб здоровью.

Категории последствий. Категории последствий нанесения ущерба определяются для обеспечения качественной меры самого разумного вероятного ущерба, следующего из ошибки персонала, влияния условий окружающей среды, погрешностей проекта, процедурных неточностей, ошибок в работе системы и подсистем. Принятые следующие категории последствий: катастрофические, критические, граничные, незначительные. Стоимость ущерба должна быть установлена в зависимости от размера системы.

Вероятность опасного события. Вероятность опасного события – вероятность, что событие произойдет в течение запланированного срока службы системы. Определение количественной вероятности события для проекта невозможно на ранних стадиях проекта. Здесь качественная вероятность опасного события может быть получена из результатов исследований, анализа и оценки исторических данных безопасности подобных систем. Различают следующие качественные уровни вероятности опасного события: частые, вероятные, случайные, редкие, невероятные.

Оценка риска опасного события. Классификация риска опасного события, последствий события и вероятность опасного события может быть выполнена с помощью матрицы оценки риска. Эта оценка позволяет назначать значение оценки риска в зависимости от опасности, основанной на последствиях опасного события и вероятности события. Это значение часто используется, чтобы ранжировать различные опасности относительно связанных с ними рисков.

Значения оценки риска часто используются в группировании индивидуальных опасностей в категории риска, которые используются для генерирования определенных действий, такое как мер по предотвращению опасностей или формального принятия риска.

Оценка риска может быть выполнена по мере необходимости, используя другие коэффициенты, чтобы различить опасности, имеющие одинаковую оценку риска. Можно было бы различить опасности с тем же самым значением оценки риска в терминах возможностей систем или коэффициентами, учитывающими социальные, экономические и политические последствия. При разработке и сопровождении программ обеспечения безопасности в этом случае необходимо консультироваться со специалистами относительно приоритетов решений.

Опасности должны быть расположены по приоритетам так, чтобы корректирующие усилия могли быть сосредоточены сначала на самых серьезных опасностях. Классификация опасностей может быть проведена согласно потенциалу риска, который они представляют.

Окончательная цель программы безопасности состоит в том, чтобы проектировать системы, которые не содержат опасностей. Однако природа большинства сложных систем не позволяет или делает экономически неприемлемым их проектирование полностью без опасностей. Однако успешная программа обеспечения безопасности позволяет проектировать системы, в которых не существуют опасности, приводящие к недопустимому уровню риска.

Соответствие Директиве ЭМС не гарантирует ЭМС оборудования в реальной жизни и отсутствия рисков безопасности из-за нарушения ЭМС.

Концепция защиты СТЗ от электромагнитных воздействий

Основные положения концепции включают:

- разработку математической модели внешней электромагнитной обстановки, в которой сооружение обеспечивает выполнение своих функций,
- разработку моделей, обеспечивающих определение возможных путей распространения (проникновение) электромагнитных помех во внутренние объемы сооружения,
- разработку конструкционных мер защиты от электромагнитных воздействий для сооружения в целом и системных мер защиты на уровне отдельно взятой системы или устройства (например, электромагнитное экранирование, создание отдельных экранированных помещений, раздельная прокладка и ввод в сооружение информационных и силовых кабелей, защита входов, вводов коммуникаций, вентиляционных и газовоздушных трактов, устройство системы заземления, использование сетевых фильтров и оптоэлектронных пар, оптимизация геометрии тоководов и т.п.),
- оценку уровней стойкости и помехоустойчивости всех технических средств инфраструктуры и локальных сетей здания.

Собственно процесс проектирования электромагнитной защиты сооружения производится с помощью математических и физических моделей для численного решения задачи, и лабораторных испытаний отдельных систем.

При разработке проекта электромагнитной защиты в качестве базового критерия должна быть положена концепция «разумной достаточности», смысл которой заключается в том, чтобы при минимальном использовании дополнительных (специальных) средств и мер защиты обеспечить функциональную и информационную безопасность сооружения в условиях предполагаемого электромагнитного воздействия.

На этапе проектирования допускается использование моделей, разработанных применительно к упрощенным идеализированным (т.е. «каноническим») геометрическим формам объектов (сооружений). Такие модели дают возможность качественно оценить влияние системы на электромагнитную обстановку во внутренних объемах сооружений, но не позволяют дать точные количественные оценки. Правильность предварительной оценки результатов проектирования может быть проверена экспериментально, путем лабораторных (стендовых) испытаний. Сопоставление результатов, полученных с помощью аналитических методов с результатами экспериментальных исследований (тестов) позволяет уточнить параметры моделей, используемых при проектировании защиты объектов от электромагнитных излучений.

Список литературы

1. Смит Д.Д. Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов/ Дэвид Дж. Смит, Кеннет Дж. Л. Симпсон – М. Издательский Дом «Технологии», 2004. – 208 с.
2. Газизов Т.Р. Преднамеренные электромагнитные помехи и авионика. – Успехи современной радиоэлектроники. – 2004. – № 2. – С. 37–51
3. Балюк Н.В., Кечиев Л.Н., Степанов П.В. Мощный электромагнитный импульс: воздействие на электронные средства и методы защиты. – М.: ООО «Группа ИДТ», 2008. – 478 с.
4. ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие положения. – М.: Стандартинформ, 2008. –34 с.
5. ГОСТ Р 51275-2007 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. – М.: Стандартинформ, 2007. – 10 с
6. Electromagnetic Pulse and TEMPEST for Facilities / EP-1110-3-2. – 1990. – 630 p.
7. Агапов С.В., Гизатуллин З.М., Чермошенцев С.Ф. Защита информации в цифровых электронных средствах интеллектуальных зданий при электромагнитных воздействиях. – Технологии ЭМС. – 2010. № 3. – С. 3–21.
8. Кечиев Л.Н., Степанов П.В., Арчаков О.Н. Предотвращение катастроф электромагнитного характера в информационных системах. – Технологии ЭМС. – 2005. – № 4 (15). – С. 7–19.
9. Акбашев Б.Б. Архитектурное экранирование: состояние проблемы и перспективы. – Технологии ЭМС. – 2009. – № 1(28). – С. 3–14.
10. Hemming L.H. Architectural Electromagnetic Shielding Handbook. A Design and Specification Guide. – IEEE Press, 1992. – 222 p.
11. Акбашев А.А., Кечиев Л.Н., Соколов А.Б. Топологический подход к экранированию электронных средств летательных аппаратов. – Технологии ЭМС. – 2008. – № 2(25). – С. 63–71.
12. Teshe F. Topological Concepts for Internal EMP Interaction. – IEEE Trans. on A&P. – 1978. – V. AP-26. – № 1. – P. 60–64.
13. Messeir M. EMP Hardening Topology Expert System. – Electromagnetics. – 1986. – № 6. – P. 79–93.
14. Vetri J. L., Costache G.I. An Electromagnetic Interaction Modeling Advisor. – IEEE Trans. on EMC. – 1991. – V. 33 – № 3. – P. 241–251.
15. Baker G., Castillo J.P. Potential for a Unified Topological Approach to Electromagnetic Effects Protection. – IEEE Trans. on EMC. – 1992. – V. 34. – № 3. – P. 267–274.
16. Baum C.E., Degauque P., Ianoz M. Electromagnetic Topology and Soil Effects applied to EMC Problems // Symp. on EMC, Zurich. – 1993. – P. 87–91.
17. ГОСТ Р МЭК 61508-1–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования. – М.: Стандартинформ, 2008. – 50 с.
18. ГОСТ Р МЭК 61508-2–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам. – М.: Стандартинформ, 2008. – 22 с.
19. ГОСТ Р МЭК 61508-3–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению. – М.: Стандартинформ, 2008. – 42 с.
20. ГОСТ Р МЭК 61508-4–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения. – М.: Стандартинформ, 2008. – 22 с.

21. ГОСТ Р МЭК 61508-5–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности. – М.: Стандартинформ, 2008. – 27 с.
22. ГОСТ Р МЭК 61508-6–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Рекомендации по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3. – М.: Стандартинформ, 2008. – 22 с.
23. ГОСТ Р МЭК 61508-7–2007. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства. – М.: Стандартинформ, 2008. – 73 с.
24. Directive 2004/108/EC of the European Parliament and of the Council. – 2004. – 14 p.
25. Armstrong Keith. EMC-Related Functional Safety of Electronically Controlled Equipment. Compliance Engineering, 2001. [Электронный ресурс]. www.ce-mag.com.
26. Агапов С.В., Гизатуллин З.М., Чермошенцев С.Ф. Защита информации в цифровых электронных средствах интеллектуальных зданий при электромагнитных воздействиях. – Технологии ЭМС. – 2010. № 3. – С. 3–21.
27. Кечиев Л.Н., Степанов П.В. ЭМС и информационная безопасность в системах телекоммуникаций. – М.: Издательский Дом «Технологии», 2005. – 320 с.
28. MIL-HDBK-764(MI), Military Handbook. System Safety Engineering Design Guide for Army Material. – 1990. – 346 p
29. MIL-HDBK-237D. DoD Handbook. Electromagnetic Environmental Effects and Spectrum Supportability Guidance for Acquisition Process. – 2005. –172 p.
30. Electromagnetic Compatibility & Functional Safety. A Factfile provided by The Institution of Engineering and Technology, 2006, 69 p.
31. MIL-STD-882D, DoD. Standard Practice for System Safety. – 2000. – 31 p.

Организация: Московский государственный институт электроники и математики, ФГУП «Проектный институт» ФСБ России.
Статья поступила 20.11.2010.

Akbashev B.B., Baljuk N.V., Kechiev L.N.

Maintenance of information and functional safety in special technical buildings At electromagnetic influences

The maintenance of a problem of maintenance of functional and information safety is considered at designing of special technical buildings (STB). The characteristic is given to the central moments of functional and information safety, architectural shielding, requirements to objects are formulated, actual directions of the further development of the theory and practice of maintenance of functional and information safety STB are defined.

special technical buildings, information safety, functional safety, electromagnetic influences

The Moscow state institute of electronics and mathematics, FGUP «Project institute» of FSB of Russia