

На правах рукописи

Акбашев Беслан Борисович

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СПЕЦИАЛЬНЫХ
ТЕХНИЧЕСКИХ ЗДАНИЙ ПРИ ЭЛЕКТРОМАГНИТНЫХ
ВОЗДЕЙСТВИЯХ

Специальность – 05.13.19 Методы и системы защиты информации,
информационная безопасность

Автореферат диссертации
на соискание ученой степени
доктора технических наук

Москва
2009

Работа выполнена в Московском государственном институте электроники и математики (техническом университете).

Научный консультант:

Доктор технических наук, профессор Кечиев Леонид Николаевич

Официальные оппоненты:

доктор технических наук, профессор Саксонов Евгений Александрович

доктор технических наук, профессор Балюк Николай Васильевич

доктор технических наук, профессор Царегородцев Анатолий Валерьевич

Ведущая организация:

ФГУП «Московский научно-исследовательский радиотехнический институт»

Защита состоится «15» декабря 2009 г. в 16.00 часов на заседании диссертационного совета Д212.133.03 Московского государственного института электроники и математики (технического университета) по адресу:

109028, Москва, Б. Трехсвятительский пер., д. 3.

С диссертацией можно ознакомиться в библиотеке МИЭМ.

Автореферат разослан "___" _____ 2009 г.

Ученый секретарь
диссертационного совета, к.т.н., доцент

Ю.Л. Леохин

Общая характеристика работы

Актуальность проблемы. Телекоммуникационные системы (ТКС) являются основой современного информационного общества. Локальные вычислительные сети, Интернет – основа динамичного роста страны. Информационно-телекоммуникационные технологии являются одним из наиболее важных факторов в формировании общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, возникающих при этом общественных отношений, а также взаимодействия правительства и гражданского общества.

По мере развития микроэлектроники электронные устройства и ТКС стали выполнять все более сложные функции при одновременном увеличении скорости обработки информации. Электронные системы, построенные на их основе, находят применение во всех сферах деятельности человека, играя жизненно важные роли в медицине, финансах, производстве и национальной безопасности. Эти роли не могут быть подвергнуты опасности, нарушению или повреждению от естественных и искусственных электромагнитных воздействий. К сожалению, та же технология, которая обеспечивает высокие скорости обработки информации, обладает повышенной чувствительностью к наведенным напряжениям и токам, вызванным электромагнитными полями от различных источников: молний, переключающих устройств и других переходных процессов. Следовательно, есть много ситуаций, в которых электронное оборудование должно быть электромагнитно изолировано от среды, в которой оно находится.

Особое значение имеют вопросы информационной безопасности. Оборонные сведения, сведения по линии ФСБ 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 США таким документом является TEMPEST. Основными элементами защиты оборудования в этом случае являются зонирование и экранирование, которое выполняется в специальных технических зданиях (СТЗ) и выделенных помещениях. При их создании выполнение экранов в цикле строительства является одной из основных мер по защите оборудования в целях информационной безопасности.

Принципы создания электромагнитных экранов применительно к зданиям и помещениям известны больше 50 лет. Модульные помещения, основанные на этих принципах, были коммерчески доступны уже в течение приблизительно 40 лет. Однако за последние 20 лет возникли многочисленные приложения, где традиционные решения в

виде прямоугольного объема с двойными стенками не будут достаточными. В последнее десятилетие требования по обеспечению соответственной электромагнитной изоляции становятся неотъемлемой частью проектов и конструкций СТЗ. Это объясняется новейшими достижениями в области генерации и изучения сверх мощных широкополосных электромагнитных полей, появлением угроз электромагнитного терроризма, повышением требований к защищенности ответственной информации, снижением чувствительности быстродействующих систем, наличием значительных по протяженности распределенных локальных сетей.

Преднамеренные электромагнитные воздействия являются новым фактором криминальных и террористических угроз безопасности критически важных объектов государства. Результаты исследований в ведущих странах мира показывают, что эту угрозу следует оценивать как долговременную, требующую принятия адекватных защитных мер со стороны государства.

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 проектными и конструкторскими решениями, спецификацией и методами тестирования экранирующих строительных конструкций.

Одновременно претерпевают изменения и информационные технологии. В последние десятилетия происходит непрерывная конвергенция компонентов телекоммуникационной инфраструктуры: информационный терминал абонента, сеть доступа и транспортная сеть связи и превращение их в единую инфокоммуникационную технологию на основе базовых технологий (объединении математических, физических и технических методов). Под влиянием развития базовых технологий развиваются внутренние телекоммуникационные процессы и системы в сторону увеличения быстродействия. Это накладывает отпечаток на оборудование СТЗ, информационную инфраструктуру которого следует рассматривать как единое целое. Нарушение информационной безопасности в одном ее звене может оказаться катастрофическим.

9 сентября 2000 года Президентом РФ была утверждена Доктрина информационной безопасности Российской Федерации, которая вызвала широкий резонанс в обществе. Об этом свидетельствует и практика работы Межведомственной комиссии Совета безопасности РФ по информационной безопасности. Сегодня Доктрина является официальной основой для формирования национальной политики в области обеспечения информационной безопасности Российской Федерации в информационных и

телекоммуникационных системах, имеющих как общегосударственное значение, так и в интересах общества и корпоративных групп, защиты интересов личности.

Одним из основных направлений обеспечения информационной безопасности РФ в общегосударственных информационных и телекоммуникационных системах указывается предотвращение специальных технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбой в работе средств информатизации.

В целях выявления, противодействия и минимизации последствий электромагнитных атак в России создается Система национальных стандартов по защите информации от преднамеренного электромагнитного воздействия. В 2007 году в основополагающих стандартах (ГОСТ Р 50922 и ГОСТ Р 51275) введены понятия и определения «защиты информации от преднамеренного силового электромагнитного воздействия». С июля 2008 г. введен «ГОСТ Р 52863-2007. Защита информации. Автоматизированные системы в защищённом исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования».

Повышение быстродействия телекоммуникационных систем выражается в динамике развития элементной базы с временами переключения единицы и доли наносекунд, повышении тактовых частот и, в целом, определяется увеличением объема информации, обрабатываемой в единицу времени. Особенно высокие требования по быстродействию предъявляются к системам, работающим в реальном масштабе времени, при оценке степени совершенства систем отношение стоимость/быстродействие с повышением быстродействия при неизменной стоимости значение оценки снижается, что характеризует более совершенную систему.

Одновременно с увеличением быстродействия возрастает интенсивность электродинамических процессов, происходящих в ТКС. Системы становятся более чувствительными к помехам, которые генерируются в самой системе или привносятся извне. Кроме этого, повышенное быстродействие расширяет спектр излучаемых аппаратурой и кабельными соединениями сигналов, что способствует утечке информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Если рассматривать технические аспекты обеспечения информационной безопасности, базирующиеся на электродинамических подходах, то практически все характеристики электромагнитной совместимости (ЭМС) технических средств (ТС) определяют уязвимость системы.

Обычно выделяют три основных вида угроз безопасности – это угрозы раскрытия, целостности и отказа в обслуживании. Угроза раскрытия имеет место всякий раз, когда получен доступ к некоторой конфиденциальной информации, хранящейся в информационной системе или передаваемой от одной системы к другой. Уязвимость

системы может быть снижена, например, установкой электромагнитных экранов, локализирующих электромагнитное поле. Угроза целостности включает в себя любое умышленное изменение (модификацию или даже удаление) данных, хранящихся в системе или передаваемых из одной системы в другую. Уязвимость по этому показателю может быть снижена разработкой мероприятий по защите системы от внешних помех, электростатических и молниевых разрядов, повышением качества электропитания. Угроза отказа в обслуживании возникает всякий раз, когда в результате некоторых действий блокируется доступ к некоторому ресурсу информационной системы. Блокирование может происходить при воздействии мощных электромагнитных помех, непредсказуемых задержек распространения сигналов в кабельных соединениях. Таким образом, видно, что характеристики ЭМС необходимо принимать во внимание при разработке мероприятий по снижению уязвимости ТС.

Основной особенностью любой сети 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.).

Промежуточную позицию между информационной безопасностью и удовлетворением требований ЭМС занимает функциональная безопасность. Уязвимость системы в этой сфере может повлечь нарушение качества функционирования аппаратуры, вплоть до катастрофических последствий.

Электромагнитная обстановка, при которой функционирует ТКС, наиболее вероятные каналы утечки информации и воздействия на нее определяются объектом, где инсталлирована система. В наиболее ответственных случаях таким объектом выступают «специальные технические здания». Они насыщены системами охраны, автоматики, связи, телекоммуникаций, системами гарантированного электропитания и являются основной территорией для нанесения атаки на ТС. Для оборудования СТЗ в настоящее время наибольшее развитие получили СКС, проектирование которых охвачено действующими стандартами. Однако, потребности в повышении быстродействия заставляют периодически пересматривать стандарты и нормативную документацию на проектирование СТЗ, что требует научного обоснования новых норм и правил проектирования. Предусматривая только формальные нормы размещения оборудования, кабельных соединений, технологии монтажа, эти стандарты не затрагивают области информационной и функциональной безопасности.

Проектные решения в области информационной и функциональной безопасности должны приниматься с учетом действующей нормативно-технической документации, а в

области ЭМС – с учетом стандартов по ЭМИ. Глобализация мирового сообщества, объединение рынков, в преддверии вступления России в ВТО, особую роль начинают играть стандарты, на соответствие которым проводится обязательная сертификация технических средств. Обязательное соответствие их требованиям является неотъемлемым фактором создания конкурентоспособной продукции, качественной и надежной работы телекоммуникационных систем. К этой группе стандартов относятся, в частности, стандарты по информационной безопасности и ЭМС. В настоящий момент Россия вступила на путь гармонизации стандартов в рамках глобализации мирового сообщества. Поэтому методология проектирования, инсталляции, эксплуатации электронного оборудования должна претерпеть изменения, ориентируясь на безусловное выполнение требований стандартов при минимальных временных и материальных затратах.

Для предупреждение угроз информационной безопасности техническими средствами в СТЗ следует:

- провести анализ глобальных направлений в области развития телекоммуникационных технологий, как объектов электромагнитных атак;
- проанализировать особенности обеспечения информационной безопасности в объектах градостроительной деятельности и сформулировать требования к эффективности защиты;
- разработать требования к СТЗ как составной части иерархической структуры электромагнитной защиты объектов при мощных электромагнитных воздействиях;
- разработать методы оценки воздействия мощных электромагнитных импульсов на технические средства СТЗ;
- разработать методы оценки экранирующих свойств строительных конструкций с учетом неоднородностей, типичных для них;
- провести экспериментальные исследования по оценке защитных свойств экранов и стойкости систем СТЗ к сверхширокополосным импульсным воздействиям;
- разработать методологию комплексного решения задач информационной безопасности в структуре СТЗ и реализовать ее в виде нормативного документа – электронного паспорта объекта.

Анализ литературных источников показывает, что вопросам информационной безопасности для компьютерных систем уделялось и уделяется значительное внимание. Широко известны работы российских специалистов Барсукова В.С., Петрова В. А., Петракова А. В., Ярочкина В. И., Батурина Ю. М., Жодзинского А. М., Герасименко В. А., Мироничева С. Ю., Сюнтюренько О. В., Степанова П.В., Царегородцева А.В. и др. Практические рекомендации по защите от несанкционированного доступа и смежным

вопросам для средств вычислительной техники даны в материалах Гостехкомиссии, а организационно-технические вопросы компьютерной безопасности в США изложены в «Оранжевой книге» и в стандарте TEMPEST. В этих работах охвачены все аспекты обеспечения информационной безопасности: от работы с персоналом до технических аспектов, включая описания соответствующей аппаратуры. Но, как правило, приведенные материалы носят характер законченных решений и затрагивают электромагнитную обстановку СТЗ при мощных электромагнитных воздействиях на объект. Это не позволяет разрабатывать опережающие технические решения на серьезном теоретическом фундаменте.

Значительный опыт теоретического решения вопросов взаимодействия электромагнитных полей с конструкциями электронных средств накоплен в области ЭМС. Методы и технические решения, эффективно применяемые для обеспечения ЭМС, могут быть успешно использованы для снижения уязвимости телекоммуникационных систем.

По мере роста быстродействия ТС, требования к электрическим параметрам систем и помехозащищенности устройств ужесточались, что заставляло проводить более детальный анализ, основанный на более совершенных математических моделях. В решение задач проектирования линий связи для ТКС, конструирования электронной аппаратуры и оценке стойкости систем к мощным электромагнитным воздействиям внесли большой вклад советские и российские ученые Балюк Н.В., Вуль В. А., Воршевский А.А., Воскобович В.В., Гизаттулин З.М., Кечиев Л.Н., Комягин С.И., Костроминов А.М., Михеев О.В., Мырова Л.О., Ольшевский А.Н., Петров Б.В., Пожидаев Е.Д., Сахаров К.Ю., Соколов А.А., Сухоруков С.А., Туркин В.А., Тухас В.А., Файзулаев Б.Н, Фоминич Э.Н., Чермошенцев С.Ф. и др.

Наличие математических моделей является неременным условием научно-обоснованной оценки уязвимости при электромагнитном характере атаки. При проектировании ТКС повышенного быстродействия существенно возрастает значимость вопросов обеспечения помехозащищенности и внутрисистемной электромагнитной совместимости. Комплексное решение этих вопросов предусматривает разработку соответствующих мероприятий на всех этапах проектирования ТКС. Важность и необходимость обеспечения требований ЭМС отмечали Князев А. Д., Князь А. И., Гурвич И. С., Петров Б.В., Кечиев Л.Н., Уильямс Т., Отт Г. и др. Однако, комплексные требования снижения уязвимости ТКС, обуславливают необходимость разработки единого цикла проектирования, включающего электрофизический анализ конструкции и оценку на его основе помехозащищенности и внутрисистемной ЭМС ТС и сопоставления с требованиями стандартов и норм в области строительства, создания электронных средств

и электромагнитной совместимости. В этом случае удается при помощи вычислительного эксперимента проанализировать функционирование ТС с учетом влияния электрофизических параметров конструкции кабельной системы на показатели системы и устранить дорогостоящий этап физического моделирования изделия. Результаты в области разработки методов алгоритмов и программ, обеспечивающих выполнение требований внутрисистемной ЭМС при проектировании ТКС представлены в работах Князева А. Д., Кечиева Л. Н., Петрова Б. В., Отта Г., Уайта Дж., Пауля К., Барнса Дж.

Автор в течение длительного времени непосредственно принимал участие в работах по обеспечению информационной безопасности и в проектировании СТЗ. Развивая представления о целостности информации, автор в своих работах показал, что методология обеспечения ЭМС электронных средств может быть успешно применена для обеспечения качественного функционирования оборудования СТЗ, для защиты устройств телекоммуникаций от ПЭМИН, для решения задач проектирования СКС. Комплексное решение проблемы ЭМС, ЭМИ и снижения уязвимости телекоммуникационных систем реализуется на всех этапах. Комплекс работ автора посвящен повышению защищенности СТЗ, что адекватно снижению уязвимости систем. Ряд вопросов теоретических и экспериментальных исследований в области воздействия СШП ЭМИ на объекты СТЗ отражены в работах автора. Комплексное представление об информационной безопасности, взаимосвязанных задачах ЭМС и учета глобальных тенденций стандартизации получило обобщение в публикациях автора. Обобщенное представление об обеспечении информационной безопасности и ее реализации в комплексе архитектурно-строительных работ позволили предложить новую идеологию сопровождения проекта на всем жизненном цикле СТЗ в виде электронного паспорта объекта, на который получен патент.

Обобщая выводы опубликованных работ, можно заключить, что *разработка методологии предупреждения угроз информационной безопасности техническими средствами в структуре СТЗ при мощных электромагнитных воздействиях является весьма актуальной проблемой*, решение которой естественным образом вписывается в современные тенденции развития науки и техники и позволит повысить качество функционирования СТЗ, повысить эффективность соотношения цена/качество при проектировании, строительстве и эксплуатации СТЗ.

Цель и задачи работы. Для обеспечения качественного и в короткие сроки ввода в эксплуатацию СТЗ, которые отличаются минимальной уязвимостью к мощным электромагнитным воздействиям, и оптимизации затрат на их проектирование, строительство и функционирование в течение всего срока эксплуатации необходимы

научно обоснованные методы разработки физической защиты, что позволит формирование внутренней электромагнитной обстановки, обеспечивающей выполнение требований по информационной безопасности и обязательных стандартов в области ЭМС и защиты информации.

Можно отметить в настоящее время отсутствие комплексных технических решений по повышению информационной безопасности при атаках электромагнитного характера в СТЗ. Данная работа призвана восполнить отмеченный пробел. Целью работы является теоретическое обоснование новых научно-технических положений, направленных на решение проблемы предупреждения угроз и обеспечение информационной безопасности СТЗ при атаках электромагнитного характера в виде мощных сверхширокополосных электромагнитных импульсов.

Для достижения поставленной цели необходимо решить следующие задачи:

- провести анализ глобальных направлений в области развития телекоммуникационных технологий, как объектов электромагнитных атак;
- проанализировать особенности обеспечения информационной безопасности в объектах градостроительной деятельности и сформулировать требования к эффективности защиты;
- разработать требования к защите СТЗ как составной части иерархической структуры электромагнитной защиты объектов при мощных электромагнитных воздействиях;
- разработать методы оценки воздействия мощных электромагнитных импульсов на технические средства СТЗ;
- разработать методы оценки экранирующих свойств строительных конструкций с учетом неоднородностей, типичных для них;
- провести экспериментальные исследования по оценке защитных свойств экранов и стойкости систем СТЗ к сверхширокополосным импульсным воздействиям;
- разработать методологию комплексного решения задач информационной безопасности в структуре СТЗ и реализовать ее в виде нормативного документа – электронного паспорта объекта.

Таким образом, можно следующим образом определить направление диссертационной работы.

Сформулировать и теоретически обосновать новые научно-технические положения, направленные на решение проблемы снижения уязвимости к атакам электромагнитного характера и обеспечение функциональной безопасности телекоммуникационной инфраструктуры СТЗ, функционирующей в сложной

электромагнитной обстановке, путем рационального экранирования и формирования внутриобъектовой электромагнитной обстановки.

Научные результаты. К основным научным результатам, которые получены лично автором, включенным в диссертацию и представляемых к защите, относятся:

- обоснование требований к системам СТЗ, как составной части иерархической структуры электромагнитной защиты объектов информатизации;
- новые математические модели расчета взаимодействия мощных импульсных электромагнитных полей с экранами и системой проводников;
- результаты экспериментальных исследований воздействия мощных электромагнитных полей на телекоммуникационные и охранные системы СТЗ.
- разработку рекомендаций и предложений по развитию нормативной базы по обеспечению информационной безопасности в инфраструктуре СТЗ при воздействии преднамеренных мощных импульсных электромагнитных полей.
- создание электронного паспорта СТЗ, отвечающего требованиям информационной безопасности.

Материалы, представленные в диссертации, характеризуются общей направленностью разработок. Они содержат совокупность новых научных обобщений и отвечают задачам современного развития теории и практики в области обеспечения информационной безопасности техническими средствами.

Практическая значимость. Практическими результатами диссертационной работы являются:

- разработанные и находящиеся в эксплуатации методики оценки наведенных токов и напряжений на протяженные проводящие объекты;
- разработанная и находящаяся в эксплуатации методика расчета неоднородных экранов;
- научно обоснованные рекомендации по проектированию экранированных помещений и строений;
- предложения по созданию ведомственных норм и правил по защите информации от деструктивных электромагнитных воздействий;
- методика экспериментальных исследований технических средств на стойкость к мощным электромагнитным импульсам;
- результаты экспериментальных исследований систем контроля доступа и видеонаблюдения, выводы и рекомендации по их совершенствованию в части повышения стойкости к мощным электромагнитным воздействиям;

- комплект документации «Электронный паспорт объекта», внедренный в проектную деятельность ряда организаций;
- методические разработки на базе основных результатов диссертационной работы, предназначенных для инженерной деятельности и совершенствования учебного процесса в вузах.

Реализация результатов. Результаты диссертационной работы внедрены и нашли практическое использование на ряде предприятий и организаций: Московский государственный институт электроники и математики (МИЭМ), Московском государственном институте радиотехники, электроники и автоматики (МИРЭА); ЗАО «АСТ», ФГУП «Проектный институт» ФСБ России, ФГУП «ЦентрИнформ», ЗАО «РНТ», ЗАО «Орбита», ОАО «ИркутскГипродорНИИ», Концерн «ИНТЕГРА-С».

Результаты диссертационной работы находят широкое применение в учебном процессе в МИЭМ и МИРЭА. На их основе для подготовки студентов и магистров на кафедре РТУиС доработаны курсы «Основы проектирования РЭА», «Радиотехнические средства защиты информации», «Электромагнитная совместимость», «Инженерно-технические методы обеспечения информационной безопасности» (кафедра МОСОиУ), дисциплины по кафедре «Информационная безопасность». Научные результаты работы использованы для написания учебных пособий, методических указаний для конструкторского практикума, курсового и дипломного проектирования для студентов направления 210200, а также при написании целого ряда наименований методической литературы.

Соответствующие методические материалы неоднократно докладывались на различных конференциях.

Исследования и практическая реализация результатов диссертационной работы проводилась в Московском Государственном институте электроники и математики на кафедре «Радиоэлектронные и телекоммуникационные устройства и системы» и использовались при выполнении НИР по тематическому плану:

- «Исследование мощных электромагнитных колебаний СВЧ диапазона и сверхширокополосных импульсных полей большой энергии при взаимодействии с техническими средствами»;
- «Создание научных основ обеспечения стойкости радиоэлектронных средств наземного и бортового базирования к деструктивным ионизирующим и электромагнитным воздействиям»;
- «Теория и практика обеспечения стойкости технических средств бортового базирования к деструктивным электромагнитным воздействиям».

Апробация работы. Основные положения диссертационной работы докладывались и обсуждались на конференциях и симпозиумах, в том числе: Всесоюзная школа семинар молодых ученых и специалистов по вопросам проектирования и внедрения в народное хозяйство автоматизированных систем управления и обработки информации, «Электромагнитная совместимость и интеллектуальные здания», Москва, 2000 г., IV Международный симпозиум по ЭМС и электромагнитной экологии ЭМС-2004, Санкт-Петербург, 2004; научно-практическая конференция «Проблемы качества, безопасности и диагностики в условиях информационного общества» 2004 г., X Российская НТК «ЭМС и электромагнитная безопасность», С.-Петербург, 2008 г.; VIII Международный симпозиум по электромагнитной совместимости и электромагнитной экологии, С.-Петербург, 2009 г., научно-практические конференции МИЭМ 2003–2008 г., закрытые научно-технические советы ряда федеральных служб и ведомств, 2004–2009 гг., а также на научных семинарах кафедры РТУиС МИЭМ.

Публикации. Научные и практические результаты диссертационной работы отражены в 39 опубликованных работах, в т.ч. в журналах из перечня ВАК – 16 и одной монографии. На электронный паспорт объекта получен патент.

Таким образом, в диссертационной работе, на основе проведенных исследований в области проектирования телекоммуникационных систем осуществлено теоретическое обобщение и решение крупной научно-технической проблемы, имеющей важное народнохозяйственное значение, позволившее повысить информационную надежность и функциональную безопасность ТКС в пределах СТЗ.

Структура диссертации. Диссертация изложена на 400 страницах текста, содержит 143 рисунков, 47 таблиц и приложения с документами, подтверждающими внедрение основных результатов работы. Диссертация состоит из введения, шести глав, общих выводов по диссертации, списка литературы (244 наименования).

Основное содержание работы

Во введении обоснована актуальность проблемы. Выделены вопросы, составляющие основу научных исследований по обеспечению требований информационной безопасности и ЭМС для СТЗ в условиях возникновения новых угроз электромагнитных атак в виде мощных сверх коротких электромагнитных импульсов. Очерчиваются границы исследований и применимости их результатов. Оценивается вклад отечественных и зарубежных ученых и специалистов в решение проблемы. Приведены сведения об апробации и внедрении достигнутых результатов. Сформулированы цели и

задачи работы. Дается структура и объем работы, а также ее краткое содержание по главам.

В первой главе рассматривается современное состояние проблемы обеспечения информационной безопасности в инфраструктуре СТЗ. Оно рассматривается как объект градостроительной деятельности, в котором наиболее уязвимыми для атак электромагнитного характера являются телекоммуникационные системы и электронные системы обеспечения жизнедеятельности и охраны объекта. Дается общая характеристика методам и средствам физической защиты объектов информатизации. Рассматриваются возможные электромагнитные воздействия на СТЗ, требования стандартов и методология их учета на всем жизненном цикле объекта. Подчеркивается особенность настоящего момента развития электронных средств, при котором возникли новые угрозы нападения на информационные ресурсы в виде мощных электромагнитных воздействий.

Безопасность в градостроительной деятельности опирается на ряд технических регламентов, законов, нормативных актов и стандартов. Новые угрозы, связанные с возможностью генерирования и излучения сверхширокополосных электромагнитных импульсов (СШП ЭМИ), определяют возможность возникновения новой угрозы – «электромагнитного терроризма». Основные понятия противодействия террористическим актам установлены в законе РФ «О противодействии терроризму». Применительно к собственно строительной деятельности, можно говорить об инженерно-технической задаче профилактики терроризма, т.е. задаче выявления и устранения технических причин и условий, способствующих совершению умышленных вредных несанкционированных воздействий, включая преднамеренные мощные электромагнитные воздействия на градостроительный объект, а также о задаче разработки мер по предотвращению или хотя бы минимизации и ликвидации последствий от таких воздействий. Эти задачи решаются при проектировании объекта путем обеспечения его комплексной безопасности на основе анализа аварийных режимов функционирования объекта с учетом определенных факторов техногенного и природного характера. Показано, что решение этих задач должно опираться на научно-обоснованные рекомендации, что особенно актуально для новых видов деструктивных воздействий, которые до последнего времени не могли быть среди перечня угроз безопасности. Это, прежде всего, электромагнитное взаимодействие электронных и электротехнических устройств и систем в составе зданий, приводящее к нарушению их совместной работы, а также преднамеренные мощные электромагнитные воздействия. В техническом плане целесообразнее использовать понятия угроз и защиты объекта от преднамеренных (умышленных) силовых воздействий (ПСВ), что позволяет

устанавливать в проектной и технической документации технические требования к стойкости и устойчивости объекта к этим воздействиям.

Предложено концептуальное представление задач обеспечения информационной безопасности и противодействия терроризму при осуществлении градостроительной деятельности. Среди всего разнообразия факторов, определяющих информационную безопасность объекта, в рамках диссертационной работы разрабатываются вопросы, связанные с непреднамеренными и ПСВ электромагнитного характера, которые до настоящего времени не нашли должного отражения применительно к строительным объектам. В этом случае основными задачами по обеспечению информационной безопасности при проектировании объектов капитального строительства являются:

- синтез моделей угроз электромагнитных воздействий непреднамеренного и преднамеренного характера и анализ аварийных режимов функционирования проектируемого объекта;
- развитие теории обеспечения электромагнитной совместимости и электромагнитной защиты применительно к задачам информационной безопасности объектов;
- разработка теоретически обоснованных проектных решений электромагнитной защиты объекта при угрозе несанкционированного воздействия на объект источников электромагнитных воздействий;
- совершенствование технических методов контроля и обнаружения источников угроз ПСВ;
- создание комплексных технологий противодействия (предупреждения) угроз ПСВ;
- разработка мероприятий (специальных технических условий) по учету в проектной документации новых угроз информационной безопасности, носящих электромагнитный характер.

В главе приведен анализ телекоммуникационных систем СТЗ как объектов электромагнитных атак. Рассмотрены возможные средства защиты и потенциальные нарушения функционирования технических средств при воздействии ЭМИ.

Приведены базовые сведения о эффективности защиты и формировании норм защищенности.

Учитывая физическую общность процессов и явлений электромагнитной совместимости (ЭМС) технических средств и технических методов обеспечения информационной безопасности, проанализированы базовые понятия ЭМС, свойства помехозащищенности аппаратуры, действующие стандарты и нормы, а также взаимосвязь вопросов информационной безопасности, ЭМС и функциональной безопасности. Важным выводом является необходимость обеспечения внутренней электромагнитной обстановки

(ЭМО) внутри СТЗ и в его отдельных зонах, которая не нарушает требования ЭМС и гарантирует работоспособность технических средств согласно их сертификатам соответствия.

В главе проведен анализ возможных механизмов деструктивных воздействий на технические средства с целью нарушения целостности информации: по полю, по сети питания, по кабельным каналам.

В результате приводятся базовые рекомендации по защите информационных систем от преднамеренных деструктивных воздействий, а также сформулирована методология учета стандартов в жизненном цикле проекта.

В заключение формулируется цель и задачи работы.

Во второй главе разрабатываются требования к защите СТЗ как к составной части иерархической структуры электромагнитной защиты объектов информатизации. Структурированные кабельные системы, которые являются основной средой передачи информационных сигналов, рассматриваются как случайные антенны. Показано, что в локальных кабельных сетях важно с позиций анализа целостности сигнала различать режимы работы – дифференциальный и режим общего вида. Они определяются качеством монтажа и заземления кабельной системы в составе СТЗ. Многофункциональное хозяйство СТЗ требует серьезного внимания к технике прокладки кабельных соединений и компоновки кабельных каналов. В работе приведены рекомендации по группировке кабелей в них, приводящие к уменьшению перекрестных помех.

В главе проведен анализ угроз нарушения информационной безопасности в СТЗ. Показано, что основные виды угроз при этом: несанкционированный доступ (НСД) к информации, проявление недеklarированных возможностей (ПНВ), средства специального программно-технического воздействия (СПТВ), компьютерные вирусные воздействия (КВВ), сбои и отказы технических средств.

В целом система обеспечения информационной безопасности СТЗ представляет собой распределенную структуру, включающую в свой состав:

1. Средства администрирования безопасности информационной инфраструктуры.
2. Специализированные средства защиты информации: средства защиты информации от НСД (СЗИ НСД) к серверам и автоматизированным рабочим местам; средства защиты удаленного доступа на основе использования межсетевых экранов (МЭ); антивирусные средства; сетевые сканеры и средства защищенности ОС, СУБД и протоколов обмена информацией в сети.
3. Встроенные средства защиты ОС и СУБД, а также средства контроля качества функционирования программного обеспечения.

4. Технические средства защиты от перехвата ПЭМИН и предотвращения деструктивных электромагнитных воздействий.
5. Технические средства обеспечения целостности сигнала и качества функционирования систем по цепям питания и заземления.
6. Средства обеспечения отказоустойчивости и живучести отдельных технических средств и сетей здания в целом.

Проведенный анализ показал, что СТЗ функционируют в критических условиях и ЭМО. Поэтому их создание требует специальных норм, правил и стандартов. До настоящего времени в отечественной практике этот вопрос не нашел должного решения.

В работе предлагается концепция стандарта, основанная на действующих законодательных актах, проектах технических регламентов, действующих строительных нормах и правилах, федеральных нормах и правилах в области использования атомной энергии (ПНАЭ) и соответствующая рекомендациям межгосударственного стандарта ГОСТ 2.114-95 по содержанию технических условий.

С целью проведения экспериментальных исследований в главе сформулированы требования к методам и средствами испытаний и измерений, их составу, метрологическим характеристикам, конструктивным и эксплуатационным параметрам. Учитывая поставленные задачи, экспериментальная база является уникальной и исследования проводились на базе ВНИИОФИ.

По материалам главы сделаны выводы.

В третьей главе приводятся результаты теоретических исследований воздействия мощных электромагнитных импульсов на протяженные объекты. Эти объекты, к которым относятся СКС, моделируются в виде тонкопроволочных структур, для которых развиваются расчетные методики и оцениваются наведенные токи для модельной геометрии и оценивается эффективность поражающего действия электромагнитных импульсов.

Для определения ЭМО проанализированы пути проникновения электромагнитных полей в СТЗ (рис. 1).

Теоретические исследования были сгруппированы на совершенствование расчетных методик оценки устойчивости технических средств СТЗ к воздействию мощных ЭМИ. На основе проведенного анализа возможных методов расчета наведенных токов и напряжений в случайных антеннах предложена тонкопроволочная аппроксимация кабельных соединений, как наиболее эффективных антенн.

Расчет токов и напряжений, наведенных на проводящий объект, осуществляется с использованием интегрального уравнения электрического поля (ИУЭП) в частотном

представлении. При этом сначала вычисляются токи на частотах, а временная форма импульсов тока находится обратным преобразованием Фурье для свертки частотного представления токов со спектром воздействующего импульса поля.

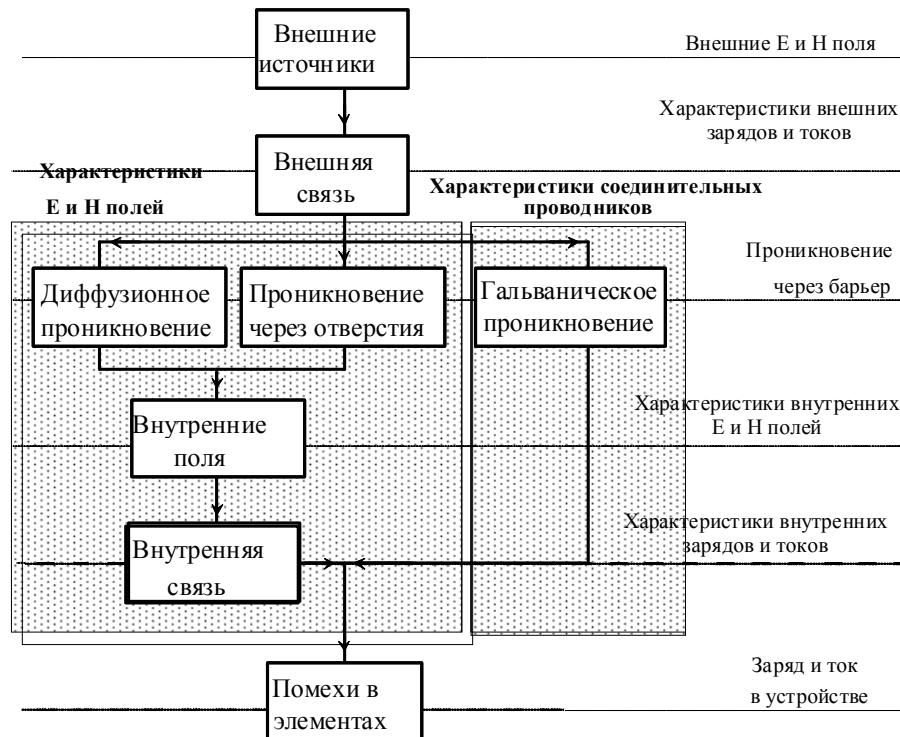


Рис. 1. Диаграмма последовательности взаимодействия сооружения с внешним электромагнитным полем

При выводе ИУЭП полное электрическое поле представляется в виде суммы падающего \vec{E}^i (поля без объекта) и рассеянного \vec{E}^s (обусловленного токами и зарядами, наведенными падающим полем на поверхности объекта) полей:

$$\vec{E}(\vec{r}, t) = \vec{E}(\vec{r}) \cdot \exp(j\omega t) = \vec{E}^i + \vec{E}^s,$$

где \vec{r} – радиус-вектор точки пространства; ω – частота падающего поля.

Рассеянное поле выражается через токи $\vec{J}(\vec{r})$ и заряды $\sigma(\vec{r})$ на поверхности проводника S через векторный магнитный потенциал $\vec{A}(\vec{r})$ и скалярный электрический потенциал $\Phi(\vec{r})$ следующим образом (опуская зависимость от времени):

$$\vec{E}^s(\vec{r}) = -j\omega\vec{A}(\vec{r}) - \nabla\Phi(\vec{r}),$$

где

$$\vec{A}(\vec{r}) = \frac{\mu}{4\pi} \int_S \vec{J}(\vec{r}') \frac{\exp(-jkR)}{R} dS';$$

$$\Phi(\vec{r}) = \frac{1}{4\pi\epsilon_s} \int_S \sigma(\vec{r}') \frac{\exp(-jkR)}{R} dS' = -\frac{1}{4\pi j\omega\epsilon_s} \int_S \nabla_s \cdot \vec{J}(\vec{r}') \frac{\exp(-jkR)}{R} dS';$$

$k=2\pi/\lambda$ – волновое число; $R = |\vec{r} - \vec{r}'|$ – расстояние между произвольно расположенной точкой наблюдения \vec{r} и точкой источника \vec{r}' на поверхности проводника S ; μ, ϵ – параметры окружающей среды; $\nabla_s \cdot \vec{J}$ – поверхностная дивергенция вектора \vec{J} .

После преобразований получаем интегральное уравнение электрического поля:

$$\left(j\omega\vec{A}(\vec{r}) + \nabla\Phi(\vec{r}) \right)_{\text{tan}} = \vec{E}_{\text{tan}}^i - Z_S \vec{J}(\vec{r}),$$

где $\vec{E}_{\text{tan}}^i(\vec{r})$ – касательная к S составляющая падающего электрического поля.

Для идеально проводящих объектов ИУЭП имеет несколько более простой вид:

$$\left(j\omega\vec{A}(\vec{r}) + \nabla\Phi(\vec{r}) \right)_{\text{tan}} = \vec{E}_{\text{tan}}^i.$$

Введение поверхностного полного сопротивления позволяет при решении задач рассеяния или излучения моделировать элементы активного и реактивного сопротивления.

Для тонких протяженных проводников ИУЭП решается методом моментов с использованием тонкопроволочного формализма. При этом исследуемая линия моделируется участками проволоки круглого сечения, и делаются следующие приближения:

- ток течет только в направлении оси проволоки;
- плотности тока и заряда аппроксимируются нитями тока \vec{I} и заряда σ на оси проволоки;
- граничное условие Леонтовича применяется только к аксиальной компоненте поля на поверхности проволоки.

С целью численного решения уравнения геометрия объекта аппроксимируется прямолинейными проволочными отрезками. Каждому месту соединения двух проволочных отрезков (неграничному узлу) поставлена в соответствие базисная функция, отличную от нуля лишь на соответствующей паре отрезков, где она имеет вид:

$$\vec{f}_n^\pm(\vec{r}) = \frac{\pm(\vec{r}_n^\pm - \vec{r})}{l_n^\pm},$$

где n – номер узла; знаки «-» и «+» в качестве индексов приписаны первому (W_n^-) и второму (W_n^+) отрезку в паре, соответственно; l_n^\pm – длина проволочного отрезка W_n^\pm ; \vec{r}_n^\pm – радиус-вектор второго (отличного от n -го узла) конца проволочного отрезка W_n^\pm .

Расчет велся по следующему алгоритму (рис. 2).

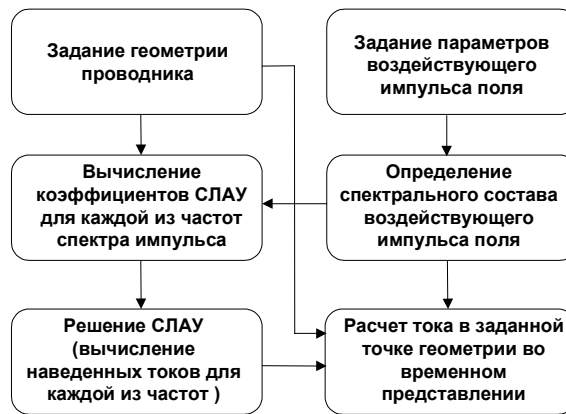


Рис. 2. Алгоритм расчета тока, наведенного на проводящий объект импульсным электромагнитным полем

Полученные расчетные данные сравнивались с результатами измерения импульсов тока в несимметричной штыревой антенне длины L , расположенной над проводящей поверхностью (сигнал снимался с шунта с сопротивлением $R = 1$ Ом). Геометрия тестовой задачи представлена на рис. 3.

Приведенные примеры тестовых расчетов доказывают корректность расчетных формул для тонкопроволочных структур и правильность работы программы. Один из графиков, иллюстрирующих расчетные и экспериментальные данные, приведен на рис. 4.

Таким образом, результаты тестовых расчетов свидетельствуют о правильности математической модели для проводящих поверхностей и соответствующей расчетной программы.

В работе выполнены расчеты при импульсном воздействующем поле и оценена эффективность поражающего действия сверхширокополосных ЭМИ.

Эффективность воздействия СШП импульсов в значительной степени определяется их широкополосностью, которая обеспечивает воздействие электромагнитного излучения на различные элементы электронной аппаратуры с включением различных механизмов взаимодействия.

Воздействие СШП ЭМИ на объект может быть описано с помощью передаточной функции:

$$G = \frac{F_{\text{out}}(j\omega)}{F_{\text{in}}(j\omega)},$$

где $F_{\text{out}}(j\omega)$ – спектр выходной функции; $F_{\text{in}}(j\omega)$ – спектр воздействия.

Эффективность воздействия может быть определена как отношение энергий:

$$\eta_E = \frac{\int_0^{\infty} |F_{\text{out}}(j\omega)|^2 d\omega}{\int_0^{\infty} |F_{\text{in}}(j\omega)|^2 d\omega}.$$

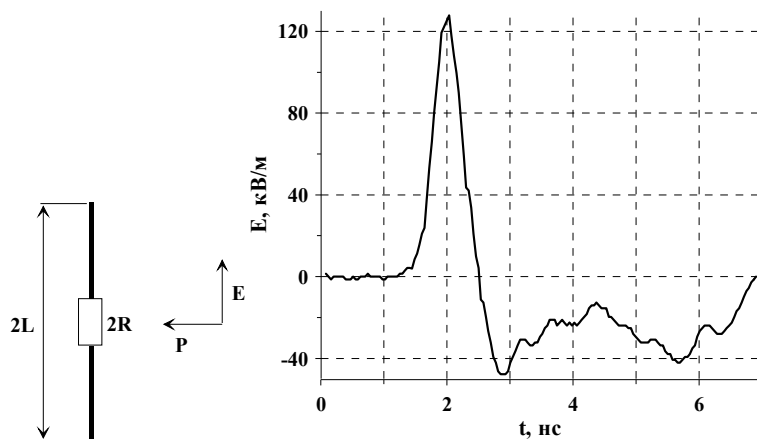


Рис. 3. Геометрия тестовой задачи (слева) и осциллограмма воздействующего импульса поля

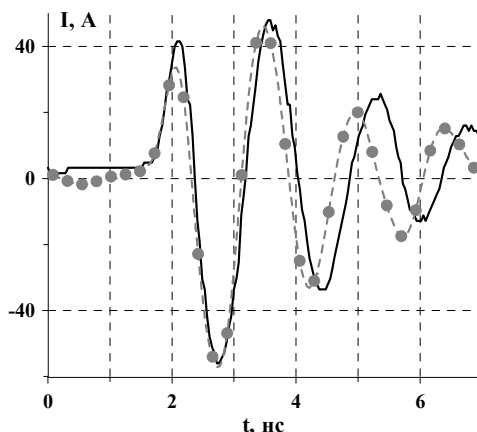


Рис. 4. Импульсы тока в нагрузке проволочной антенны с диаметром 5 мм при длине антенны 10 см (пунктир – расчет, сплошная линия – эксперимент)

Результаты оценки эффективности воздействия для проволочных проводников различной длины L приведены в табл. 1, 2. Верхняя и нижняя частоты диапазона были определены на половине высоты амплитудно-частотной характеристики проводников, нагруженных в средней точке на $R = 50$ Ом, при воздействии ЭМП с электрической составляющей E , направленной параллельно проводнику.

Анализ приведенных данных показывает, что СШП импульсы обладают высокой эффективностью воздействия на линии длиной до нескольких метров. При $L < 1$ м они могут оказать большее влияние на технические средства, чем другие типы импульсов, даже, несмотря на их сравнительно малую энергетику.

Типы исследуемых импульсов и их параметры

| № п/п | Тип импульса | Длительность фронта импульса | Постоянная спада импульса | $W_{вх}$, Дж/м ² |
|-------|-----------------|------------------------------|---------------------------|------------------------------|
| 1 | СШП ЭМИ | 0,1 нс | 2,5 нс | $7,05 \cdot 10^{-2}$ |
| 2 | «Быстрый» ЭМИ | 1,5 нс | 80 нс | 2,19 |
| 3 | «Средний» ЭМИ | 5 нс | 300 нс | 8,19 |
| 4 | «Медленный» ЭМИ | 10 нс | 500 нс | 13,72 |

Таблица 2

Эффективность воздействия импульсного ЭМП на проводники различной длины

| L , м | Полоса частот, МГц | Эффективность воздействия импульса η_E (номера импульсов соответствуют табл. 1) | | | |
|---------|--------------------|---|---------------------|---------------------|---------------------|
| | | 1 | 2 | 3 | 4 |
| 0,1 | 840-2040 | $2 \cdot 10^{-2}$ | $3,3 \cdot 10^{-6}$ | $7 \cdot 10^{-8}$ | $1,5 \cdot 10^{-9}$ |
| 1 | 84-204 | $2,7 \cdot 10^{-2}$ | $4 \cdot 10^{-6}$ | $9,2 \cdot 10^{-8}$ | $2 \cdot 10^{-9}$ |
| 10 | 8,4-20,4 | $1,3 \cdot 10^{-2}$ | $8,5 \cdot 10^{-2}$ | $4,5 \cdot 10^{-3}$ | $2,4 \cdot 10^{-7}$ |
| 100 | 0,8-2 | $2,8 \cdot 10^{-4}$ | $1,2 \cdot 10^{-2}$ | $5,9 \cdot 10^{-2}$ | $6,2 \cdot 10^{-3}$ |

Можно сделать вывод, что ЛВС и узлы технических средств с резонансными частотами между 100 МГц и 1 ГГц СШП ЭМИ оказывает наибольшее влияние по энергии (напряжению) несмотря на то, что его общая энергия значительно меньше, чем энергия других импульсов с $E = 100$ кВ/м.

Таким образом, опасность воздействия конкретного СШП ЭМИ определяется не только амплитудой, фронтом импульса и энергией, но и эффективностью его воздействия по энергии и напряжению.

По материалам главы сделаны выводы.

В четвертой главе на основе топологического подхода (рис. 5) развивается теория экранирования применительно к неоднородным экранам, которые моделируют экранирующие строительные конструкции. Экранирование является основным методом защиты объектов от деструктивных внешних преднамеренных электромагнитных воздействий.

В работе приведены расчетные данные по эффективности экранирования различных материалов, применяемых при строительстве СТЗ, а также в зависимости от конфигурации металлической арматуры железобетонных зданий.

Особое внимание уделено аперттурам в строении неоднородностям в экранах, которые вызваны необходимостью обеспечения жизнедеятельности объекта (окна, различные трубопроводы, вентиляция и т.п.).

Для экранирующих окон получены зависимости экранирования от поверхностного сопротивления наносимых на стекло проводящих пленок (рис. 6).

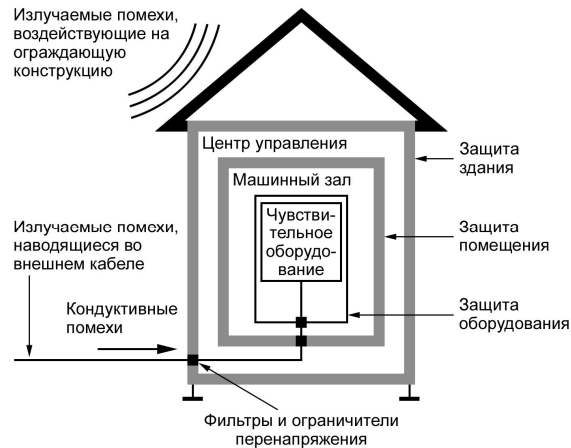


Рис. 5. Топологическое представление экранов СТЗ с фильтрами в точках проникновения

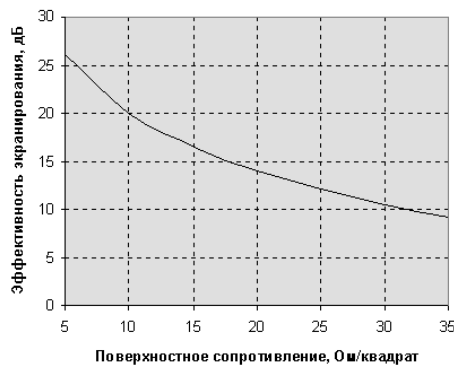


Рис. 6. Зависимость эффективности экранирования от поверхностного сопротивления пленки

Проведенный анализ позволил выработать научно-обоснованные рекомендации по минимизации утечек через разнообразные аперттуры.

На основе анализа действующих стандартов даны рекомендации по проведению измерений эффективности экранирования неоднородных экранов.

Для получения численных оценок развивается коэффициентный метод расчета эффективности экранирования неоднородных экранов. Это обусловлено сложностью для реальной ситуации получения значений эффективности экранирования для отдельных апертур и неоднородностей в экране. В данном методе влияние апертур и неоднородностей учитывается с помощью некоторых поправочных коэффициентов. Для металлического листа с аперттурами можно записать эффективность экранирования в следующем виде

$$S_{ap} = A_{ap} + R_{ap} + B_{ap} + K_{ap1} + K_{ap2} + K_{ap3}, \text{ дБ},$$

где: A_{ap} – потери на поглощение, R_{ap} – потери на отражение, B_{ap} – поправочный коэффициент отражения, K_{ap1} – поправочный коэффициент числа отверстий, K_{ap2} – поправочный коэффициент проникновения поля на низких частотах, K_{ap3} – поправочный коэффициент объединения близко расположенных отверстий.

Зная эффективности экранирования металлической стенки экрана и отдельных зон расположения апертур, определяется суммарная эффективность экранирования. В диссертационной работе приводятся необходимые соотношения для апертур круглого и прямоугольного сечения, а также классические выражения для сплошного однородного экрана. Для вычисления суммарной S_{Σ} эффективности экранирования неоднородного экрана соответствующие эффективности экранирования переводятся в коэффициенты экранирования по формуле

$$K = \frac{1}{10^{S/20}},$$

а затем проводится расчет по формуле

$$S_{\Sigma} = -20 \lg \left[K + \sum_{i=1}^n K_{apn} \right], \text{ дБ},$$

где K – коэффициент экранирования сплошного экрана, K_{apn} – коэффициент экранирования в зоне n утечки, n – число зон апертур, вызывающих утечки.

Приведенные расчеты и анализ их результатов показывают, что предложенная методика дает более адекватный результат, чем известные подходы.

Для уточнения механизма экранирования новых строительных материалов был выполнен анализ экранирования электрического поля в квазистатическом приближении при помощи программы ELCUT на основе метода конечных элементов (рис. 7)

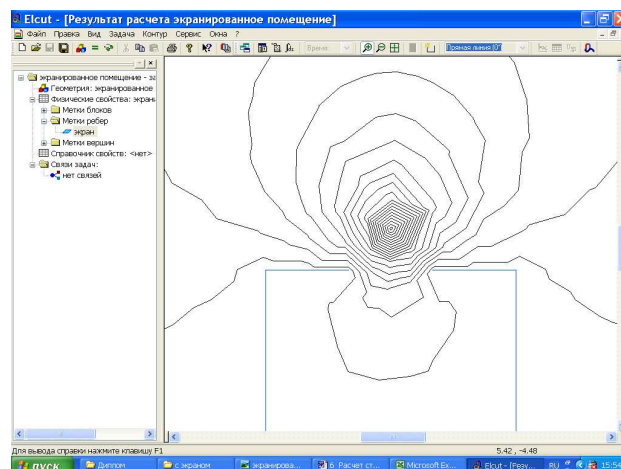


Рис. 7. Картина поля: проникновение поля через проем (отверстие): (эквипотенциали)

По главе сделаны выводы.

В пятой главе представлены результаты экспериментальных исследований.

Экспериментальные исследования проведены для оценки стойкости некоторых важных систем обеспечения информационной безопасности и отработки мероприятий по экранированию и защите этих средств от наиболее опасных преднамеренных электромагнитных воздействий. Уникальность подобных экспериментальных исследований заключается в применяемом оборудовании и приборном парке. Все исследования проводились на базе ВНИИОФИ, где сосредоточены ведущие в России кадры и исследования в области СШП ЭМИ. Осциллограмма типичного СШП ЭМИ, полученного на одном из излучателей, показана рис. 8. Фронт импульса по уровню 0,1–0,9 составляет около 250 пс, а длительность импульса по уровню 0,5 составляет около 400 пс.

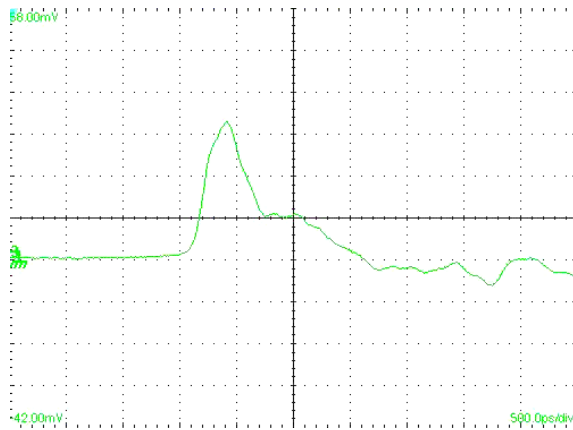


Рис. 8. Осциллограмма сигнала СШП ЭМИ (по оси времени – 500 пс/дел.)

При проведении экспериментальных исследований решены следующие задачи:

- обоснована и выбрана система генерации, усиления, излучения и регистрации СШП ЭМИ;
- разработаны программы-методики проведения экспериментальных исследований в безэховых камерах;
- проведены экспериментальные исследования на примере систем контроля доступа (СКД), которыми оснащаются СТЗ, и системы видеонаблюдения (СВ).

Генераторы СШП ЭМИ можно разделить по принципу действия на следующие группы: искровые генераторы с маслонаполненными разрядниками, искровые с газовыми разрядниками и полупроводниковые генераторы (рис. 9).

Был выполнен анализ этих типов генераторов, в результате чего были выбраны излучатели ВНИИОФИ на основе полупроводниковых генераторов производства ЗАО «НПАО ФИД-Технология» с выходным напряжением (на нагрузке 50 Ом) на 1, 10, 20, 30 и 90 кВ. При использовании специальных обостряющих головок на выходе

перечисленных генераторов, получены следующие значения времени нарастания импульсов напряжения – для 1 кВ – 60 пс, для 10, 20 и 30 кВ не более 150 пс и для 90 кВ – 200 пс. Предполагается довести амплитуду выходного сигнала этого генератора до 100 кВ при частоте следования импульсов 1 кГц. Габариты генератора 480×480×180 мм, вес не более 25 кг.



Рис. 9. Классификация принципов построения генераторов СШП ЭМИ

Характерной особенностью генераторов «НПАО ФИД-Технология» является эффективная работа на низкоомную нагрузку. По данным разработчиков при работе генератора на 2, 3 и 4 кабеля с волновым сопротивлением по 50 Ом каждый, отдаваемая генератором мощность увеличивается в полтора-два раза.

Анализ антенно-фидерных систем позволил выбрать решетку из ТЕМ-рупоров, которая в сочетании с волновым трансформатором позволяет передать энергию генератора практически полностью к раскрыву антенны. Рабочее напряжение на каждом рупоре снижается в несколько раз, поле практически равномерное в раскрыве, решетка вписывается в любой прямоугольный габарит, имеет малую толщину, а наличие гибких кабелей позволяет осуществлять ее поворот.

Система регистрации построена на разработанном во ВНИИОФИ полосковом датчике. Их преимущества следующие:

- ступенчатая переходная характеристика в течение времени двойного пробега сигнала по датчику;
- время нарастания переходной характеристики при поперечных размерах датчика порядка 1 мм может составлять порядка 10 пс;
- потери в кабеле компенсируются изменением поперечных размеров датчика.

Экранированная камера предназначена для размещения средств регистрации СШП ЭМИ (стробоскопического осциллографа). Поэтому главной целью камеры является защита электронных средств, размещённых внутри, от воздействия СШП ЭМИ. В ходе работы определялось расчётным и экспериментальным путём эффективность этой

защиты. Расчет эффективности экранированной камеры с учетом апертур по предложенной методика дал значение 36,7 дБ.

Для устранения помех по цепи питания были установлены и исследований помехоподавляющие фильтры. Коэффициент ослабления фильтром СШП ЭМИ длительностью импульса порядка 0,19 нс составляет 33,2 дБ.

Проводились экспериментальные исследования воздействия СШП ЭМИ на системы контроля доступа (СКД) (рис. 10) и системы видеонаблюдения (рис.11).

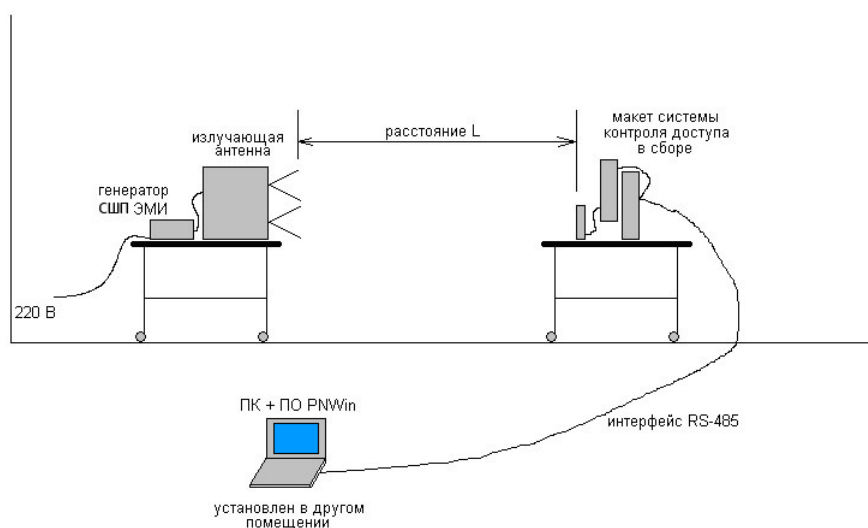


Рис. 10. Схема проведения эксперимента по исследованию воздействия СШП ЭМИ на СКД

Был установлен факт сбоев систем при различных интенсивностях воздействия. В диссертации приведены сводные данные по результатам экспериментов.



Рис. 11. Исследование СВ

Были проведены исследования распространения ЭМИ в помещениях. Результаты исследований показали, что при распространении СШП ЭМИ на большие расстояния по неоднородной трассе (распространение через несколько помещений с расположенными в них металлическими конструкциями и оборудованием) в структуре принимаемого

сверхкороткого сигнала происходит неконтролируемое изменение поляризации и амплитуды переотраженных импульсных сигналов. При этом из-за случайного наложения их друг на друга возможна ситуация, при которой амплитуда отдельного суммарного принимаемого импульса превосходит по амплитуде прямой сигнал. Длительность суммарного сигнала возрастает до 160–180 нс. При этом должно возрасти и число отдельных импульсных воздействий на облучаемую аппаратуру, а также и энергия этого воздействующего сложного суммарного сигнала. Зафиксированное явление концентрации излученного электромагнитного поля СШП ЭМИ при их распространении в объеме рабочего помещения объясняет увеличение восприимчивости ТС к воздействию СШП ЭМИ при размещении их в помещении.

По главе сделаны выводы.

В **шестой главе** обобщаются базовые подходы по обеспечению информационной безопасности как комплексной задачи для СТЗ. Рассматриваются технология проектирования платформ безопасности, фреймовая модель технологии и математическая модель построения политики безопасности.

Итоговым результатом стал документ «электронный паспорт объекта» (приоритет защищен патентом), который позволяет учесть все требования к СТЗ на этапах проектирования, строительства, эксплуатации и модернизации. Электронный паспорт объекта это электронная информационная система, выполняющая следующие задачи:

- ввод, хранение, модификацию и представление в едином электронном формате полного комплекта проектной и исполнительной документации на объект, выпущенной в процессе проектных и строительных работ, с учетом изменений, внесенных в ходе эксплуатации объекта;
- создание электронной трехмерной модели объекта;
- обеспечение программными средствами постоянной логической взаимосвязи между элементами электронной трехмерной модели и ИРД, ПСД, исполнительной документацией.
- мониторинг состояния объекта в процессе эксплуатации;
- анализ вероятных угроз (моделей угроз) и обработка событийных сценариев в критических и чрезвычайных ситуациях.

Подобный электронный паспорт (ЭПО) объекта разработан автором и внедряется в ФГУП «Проектный институт» ФСБ России (евразийский патент № 009827).

Структура ЭПО приведена на рис. 12, и он характеризуется следующим:

- вся информация об объекте представлена в электронном виде;

- ЭПО разрабатывается только на основе стандартов (международных, государственных, отраслевых, информационных);
- ЭПО разворачивается на программно-аппаратных средствах участников.

При автоматизации отдельных процессов используются существующие прикладные программные средства, однако к ним предъявляется требование – наличие стандартного интерфейса к предоставленным данным.

По главе сделаны выводы.

Характеризуя работу и полученные результаты следует заключить, что на основе созданных моделей, методов, программных средств и методик разработана методология предупреждения угроз информационной безопасности техническими средствами в структуре СТЗ, составляющих научную основу защиты перспективных объектов информатизации.

В **Заключении** обобщены основные результаты работы.

Диссертация подготовлена на основании работ, выполненных автором с 2003 г. по настоящее время, и завершена при обучении в докторантуре на кафедре «Радиоэлектронные и телекоммуникационные устройства и системы» Московского государственного института электроники и математики.

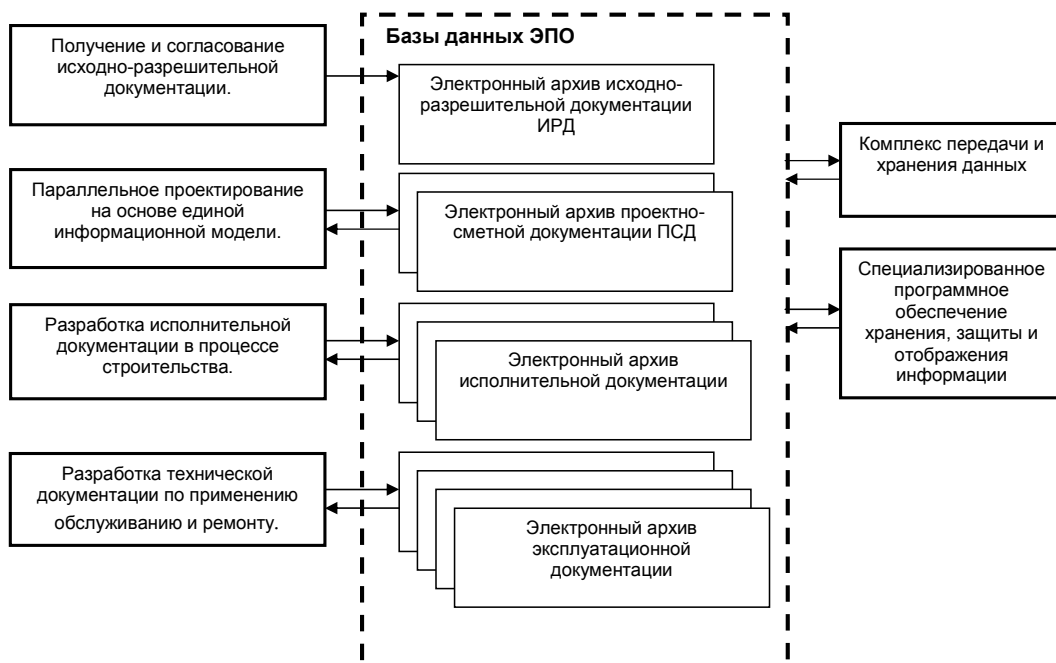


Рис. 12. Структура электронного паспорта объекта

Основные результаты работы

Научная и практическая значимость выполненных в работе исследований

Основным результатом, определяющим научную и практическую значимость, выполненных в работе исследований, является решение проблемы формирования комплекса средств противодействия нарушениям информационной безопасности в структуре СТЗ в условиях воздействия преднамеренных мощных ЭМИ, позволяющих повысить обоснованность и эффективность процессов выработки целей и генерации рациональных проектных решений, а также сократить сроки проектирования и снизить затраты на создание СТЗ, отвечающих требованиям информационной безопасности.

Результаты включают в себя:

- обоснование требований к системам СТЗ, как составной части иерархической структуры электромагнитной защиты объектов информатизации;
- разработку математических моделей расчета взаимодействия мощных импульсных электромагнитных полей с экранами и системой проводников;
- проведение комплекса экспериментальных исследований воздействия мощных электромагнитных полей на телекоммуникационные и охранные системы СТЗ;
- разработку рекомендаций и предложений по развитию нормативной базы по обеспечению информационной безопасности в инфраструктуре СТЗ при воздействии преднамеренных мощных импульсных электромагнитных полей;
- создание электронного паспорта СТЗ, отвечающего требованиям информационной безопасности;
- разработку методологии предупреждения угроз информационной безопасности в структуре СТЗ при электромагнитных воздействиях.

Наиболее важные конкретные научные результаты, полученные в ходе исследований, состоят в следующем:

1. Потребность в защите электронного оборудования от внешних электромагнитных воздействий с одной стороны и обеспечение скрытости обработки информации электронными средствами с другой стороны непрерывно возрастает, охватывая все новые приложения – от объектов государственного и военного подчинения до госпиталей и коммерческих банков. Появление новых угроз в виде электромагнитного терроризма и электромагнитного оружия увеличивает риски нарушения информационной безопасности.

2. Сформировано новое научно-техническое направление – архитектурное экранирование, базирующееся на фундаментальных основах теории электромагнитного экранирования электронных средств, но отличающееся применяемыми материалами, техническими решениями, особенностями экранируемых объектов.
3. Развита теория экранирования в части построения иерархических экранирующих структур с целью снижения затрат на строительство при выполнении заданных технических требований по эффективности экранирования. Для этих целей предложено использовать топологические подходы описания многорубежной системы экранирования СТЗ, что позволяет дать интегрированную информацию о зонах экранирования, наличии апертур и точек проникновения коммуникаций в защищаемые пространства.
4. Разработан метод учета неоднородностей экрана, которые в экранировании зданий и помещений играют решающую роль. Метод расчета основан на коэффициентом учета влияния типовых апертур и интегральном учете всех зон неоднородного экрана. Показана возможность применения численных методов и программных средств на их основе для анализа эффективности экранирования строительных конструкций. По разработанной методике проведён анализ эффективности экранирования камеры для испытаний СШП ЭМИ: стенок камеры, сетки для наблюдения, рукава из проводящей ткани. Общая эффективность защиты размещаемой в экранированной камере аппаратуры от СШП ЭМИ составляет 33, 2 дБ, что хорошо совпадает с экспериментальными данными.
5. Проведена оценка эффективности поражающего действия ЭМИ различных источников. Анализ приведенных данных показывает, что СШП импульсы обладают высокой эффективностью воздействия на линии длиной до нескольких метров. При $L < 1$ м они могут оказать большее влияние на технические средства, чем другие типы импульсов, даже, несмотря на их сравнительно малую энергетику. Эти обстоятельства имеют принципиальное значение при оценке наведенных токов и напряжений в элементах телекоммуникационных и охранных систем СТЗ, так как приводят к необходимости уточнения расчетных моделей и требований к средствам защиты.
6. На основе интегрального уравнения электрического поля и метода моментов разработана математическая модель проволочного объекта и программа для расчета токов и напряжений, наводимых в проводниках при воздействии импульсного электромагнитного поля. Правильность расчетных соотношений и программы проверялась путем сравнения результатов тестовых расчетов с данными из других

источников. С использованием программы решена модельная задача о наводке на прямой провод, приведены результаты расчетов и оценок максимальных значений наводимых токов. Максимальная амплитуда тока для проводников длиной до 20 м при амплитуде воздействующего импульса 1 В/м составила 5,5 мА. Соответствующее этому току напряжение на нагрузке 50 Ом (при условии, что сопротивление нагрузки расположено в точке, где достигается максимальная амплитуда тока) составит около 0,25 В. Разработанные и усовершенствованные математические модели применительно к воздействию сверхширокополосных электромагнитных импульсов реализованы на современных ПЭВМ и позволяют оперативно рассчитать амплитудно-временные параметры токов и напряжений, наводимых во внешних кабельных линиях систем контроля доступа.

7. Обоснованы требования к экспериментальной базе для проведения исследований. Проведен анализ параметров существующих генераторов СШП ЭМИ и перспективных разработок. Анализ характеристик излучателей показывает, что методы оценки устойчивости СКД и требования к средствам защиты их от СШП ЭМИ должны разрабатываться, исходя из следующих параметров ЭМП:
 - напряженность электрического поля в диапазоне от 1 до 200 кВ/м;
 - длительность фронта импульса – от 100 до 500 пс;
 - длительность импульса – от сотен пикосекунд до единиц наносекунд;
 - частота повторения импульсов – от 1 до 1000 Гц.
8. Рассмотрены особенности построения элементов систем охраны и обеспечения информационной безопасности (СКД и видеонаблюдения) СТЗ с точки зрения поражающего действия СШП ЭМИ различных видов. Анализ устойчивости элементов показал, что для обеспечения надежного функционирования этих систем в условиях воздействия СШП ЭМИ необходимо проведение комплекса исследований по оценке этого воздействия и разработке методов и средств их защиты.
9. Проведен анализ механизмов воздействия СШП ЭМИ на технические средства СТЗ. Установлено, что оценку влияния СШП ЭМИ на СКД необходимо осуществлять комплексным методом, включая такие направления, как проникновение ЭМИ через антенны, воздействие на кабельные соединения, проникновение ЭМИ в экраны, воздействие наведенных в соединительных линиях перенапряжений на входы-выходы аппаратуры.
10. Разработана система тестирования завершенных объектов занимает значительную долю времени в общем цикле его создания. При проведении тестов в реальной обстановке требуется значительно больше времени, чем при тестировании модульных

помещений в лабораторных условиях. Это следует учитывать при определении сроков строительства. Показания тестов на объекте имеют большую погрешность из-за влияния реальной электромагнитной обстановки.

11. Разработан математический аппарат формирования структурно-функциональной целостности объектов защиты информации и определены конструктивные (аналитические) объекты проектирования, реализующие функцию «носителей» свойства структурно-функциональной целостности на всех этапах синтеза технических средств СТЗ. Для формализации разносторонних требований к СТЗ и экранированным помещениям для различных приложений предложены развернутые спецификации (паспорта) объектов, в которых отражаются не только требования к строительным конструкциям и инженерным сооружениям, но и к его экранирующим свойствам.
12. Проведен анализ состояния работ по разработке национальных и международных стандартов в части задания требований к техническим средствам по параметрам мощных импульсных электромагнитных полей, методам и средствам испытаний. Даны предложения по развития нормативной базы и разработки новых стандартов. Реализация проектов СТЗ требует совместных усилий специалистов различных отраслевых направлений – строителей и специалистов в области ЭМС. Это определяет необходимость создания междисциплинарных курсов повышения квалификации, разработку рекомендаций по строительству и монтажу экранирующих помещений.

Основное содержание диссертации опубликовано в следующих работах

1. Акбашев Б.Б., Алешко А.И., Михеев О.В., Сахаров К.Ю., Семин В.В., Соколов А.А., Туркин В.А. Экспериментальные исследования воздействия сверхкоротких электромагнитных импульсов на систему контроля доступа в помещения. // Технологии ЭМС. – 2006. – № 1(16). – С. 3–7.
2. Сахаров К.Ю., Михеев О.В., Туркин В.А., Корев А.Н., Долбня С.Н., Певнев А. В., Акбашев Б.Б. Исследование функционирования персональных компьютеров в условиях воздействия сверхкоротких электромагнитных импульсов. // Технологии ЭМС. – 2006. – № 2(17). – С. 44–50.
3. Акбашев Б.Б., Кечиев Л.Н., Соколов А.Б. Эффективность экранирования перфорированных экранов. // Технологии ЭМС. – 2008. – № 2(25). – С. 19–26.
4. Акбашев Б.Б., Алешко А.И., Галич Ю.В., Здоренко О.В., Михеев О.В., Ольшевский А. Н., Сахаров К.Ю., Семин В.В., Туркин В.А. Результаты экспериментальных исследований систем видеонаблюдения в условиях мощных электромагнитных полей. // Технологии ЭМС. – 2008. – № 1(24). – С. 22–27.

5. Акбашев Б.Б., Кечиев Л.Н., Соколов А.Б. Топологический подход к экранированию электронных средств летательных аппаратов. // Технологии ЭМС. – 2008. – № 2(25) – С. 16–19.
6. Акбашев Б.Б., Соколов А.Б. Композиционные материалы для электромагнитного экранирования. // Технологии ЭМС. – 2008. – № 3(26). – С. 42–53.
7. Акбашев Б.Б., Соколов А.Б. Электропроводящие покрытия для повышения эффективности экранирования. // Технологии ЭМС. – 2008. – № 3(26). – С. 54–61.
8. Акбашев Б.Б. Архитектурное экранирование: состояние проблемы и перспективы. // Технологии ЭМС. – 2009. – № 1(28). – С. 3–8.
9. Акбашев Б.Б., Мартынюк Д.В. Электронный паспорт объекта. // Технологии ЭМС. – 2009. – № 1(28) – С. 9–14.
10. Акбашев Б.Б. Программно-техническая платформа создания электронного паспорта объекта. // Технологии ЭМС. – 2009. – № 1(28) – С. 15–22.
11. Акбашев Б.Б., Никифоров Н.В., Сафронов Н.Б. О специальных технических условиях обеспечения безопасности объектов градостроительной деятельности. // Технологии ЭМС. – 2009. – № 1(16) – С. 29–34.
12. Акбашев Б.Б., Жуковский М.И., Мартынюк Д.В., Сафронов Н.Б., Чванов В.П. Направление создания ведомственных норм и правил по защите от электромагнитных воздействий. // Технологии ЭМС. – 2009. – № 1(16). – С. 35–40.
13. Акбашев Б.Б., Сахаров К.Ю., Михеев О.В., Туркин В.А., Алешко Б.Г., Катков Б.Г., Бердышев А.В. Исследование распространения сверхкоротких электромагнитных импульсов в помещениях. // Технологии ЭМС. – 2009. – № 1(16). – С. 41–47.
14. Акбашев Б.Б., Куприенко В.М. Концепция проектирования защиты объектов от внешних электромагнитных воздействий. // Технологии ЭМС. – 2009. – № 1(28). – С. 58–63.
15. Акбашев Б.Б., Колбанев М.О., Ларионов С.М. Методы и средства радиочастотной идентификации на основе ПАВ-технологий. // Технологии ЭМС. – 2009. – № 1(28). – С. 64–69.
16. Акбашев Б.Б., Володин А.В. Методы пассивной защиты от электромагнитных излучений радиоэлектронных средств. // Технологии ЭМС. – 2009. – № 1(28). – С. 77–81.
17. Акбашев Б.Б. Экранирующие системы зданий и помещений // Монография. – М.: Изд-во МИЭМ, 2007. – 110 с.

18. Акбашев Б.Б. Степанов П.В. ЭМС и обеспечение информационной безопасности в системах телекоммуникаций. // Сборник докладов VIII НТК по ЭМС и электромагнитной безопасности. ЭМС-2004. – С.-Пб, ВИТУ, 2004. – с. 382 – 386.
19. Акбашев Б.Б. Степанов П.В. Эффективность экранирования терминалов при наличии щелей в их корпусе. // Электромагнитная совместимость, проектирование и технология электронных средств. – М.: Изд. МИЭМ, 2004. – С. 9–12.
20. Акбашев Б.Б., Автоматизация идентификация личности на основе идентификационных документов нового поколения. // Проблемы качества, безопасности и диагностики в условиях информационного общества. Материалы научно-практической конференции/ Под ред. В.Г. Домрачева, С.У. Увайсова. – М.: Изд-во МИЭМ, 2004. – 247 с.
21. Акбашев Б.Б. Методы и средства оценки воздействия сверхширокополосных импульсных полей на системы контроля доступа. // Электромагнитная совместимость, проектирование и технология электронных средств. – М.: Изд-во МИЭМ, 2004. – С. 9–12.
22. Акбашев Б.Б. Базовые требования к построению системы идентификации личности на основе интеллектуальных документов. // Электромагнитная совместимость, проектирование и технология электронных средств. – М.: Изд-во МИЭМ, 2004. – С. 7–8.
23. Акбашев Б.Б. Базовые принципы организации и состав автоматизированной системы идентификации личности на основе внедрения электронного удостоверения личности. // Проблемы качества, безопасности и диагностики в условиях информационного общества: Материалы научно-практической конференции/ Под ред. В.Г. Домрачева, С.У. Увайсова. – М.: Изд-во МИЭМ, 2004. – 247 с.
24. Акбашев Б.Б., Туркин В.А., Семин В.В., Ольшевский А.Н. Экспериментальные исследования воздействия СШП ЭМИ на СКД. // Сборник научных трудов МИЭМ/ Под ред. Кечиева Л.Н. – М.: Изд-во МИЭМ, 2006. – С. 21–22.
25. Акбашев Б.Б., Михеев О.В., Ольшевский А.Н., Степанов П.В. Основные направления исследований по проблеме ЭМС устройств телекоммуникаций. // Сборник научных трудов МИЭМ / Под ред. Кечиева Л.Н. – М.: Изд-во МИЭМ, 2006. – С. 18–20.
26. Акбашев Б.Б., Ольшевский А.Н. СШП ЭМИ и системы контроля доступа. Сборник научных трудов МИЭМ под ред. Кечиева Л.Н., 2006, с. 62–64.
27. Акбашев Б.Б., Степанов П.В., Ольшевский А.Н. Современное состояние телекоммуникационных технологий. // Сборник научных трудов МИЭМ / Под ред. Кечиева Л.Н. – М.: Изд-во МИЭМ, 2007. – С. 7–15.

28. Акбашев Б.Б., Комягин С.И., Михайлов В.А. Определение состава и видов электромагнитных воздействий на технические средства. // Сборник научных трудов МИЭМ / Под ред. Кечиева Л.Н. – М.: Изд-во МИЭМ, 2008. – С. 26–28.
29. Акбашев Б.Б. Состояние проблемы исследований устойчивости систем телекоммуникаций специальных технических зданий (СТЗ) при внешних электромагнитных воздействиях. // Сборник научных трудов МИЭМ / Под ред. Кечиева Л.Н. – М.: Изд-во МИЭМ, 2008. – С. 97–99.
30. Акбашев Б.Б., Кечиев Л.Н., Соколов А.Б. Эффективность экранирования неоднородных экранов. // Сборник докладов 10 Российской НТК по ЭМС и электромагнитной безопасности. ЭМС-2008. – СПб.: Изд-во ВИТУ, 2008. – С. 360–363.
31. Акбашев Б.Б., Кечиев Л.Н., Соколов А.Б., Степанов П.В. Расчет многослойных магнитных экранов. // Сборник научных трудов МИЭМ / Под ред. Кечиева Л.Н. – М.: Изд-во МИЭМ, 2008. – С. 111–115.
32. Акбашев Б.Б. Методы и средства испытаний телекоммуникаций специальных технических зданий (СТЗ). // Сборник научных трудов МИЭМ / Под ред. Кечиева Л.Н. – М.: Изд-во МИЭМ, 2008. – С. 99–100.
33. Акбашев Б.Б. Расчетно-экспериментальные методы оценки стойкости телекоммуникационных систем СТЗ к электромагнитным воздействиям. // Сборник докладов 10 Российской НТК по ЭМС и электромагнитной безопасности. ЭМС-2008. – СПб.: Изд-во ВИТУ, 2008. – С. 363–366.
34. Акбашев Б.Б. Расчетные методы оценки стойкости телекоммуникационных систем к электромагнитным воздействиям. // Сборник научных трудов МИЭМ / Под ред. Кечиева Л.Н. – М.: Изд-во МИЭМ, 2008. – С. 25–26.
35. Акбашев Б.Б. Требования стандартов по параметрам мощных импульсных электромагнитных полей (МИЭМП). // Сборник научных трудов МИЭМ / Под ред. Кечиева Л.Н. – М.: Изд-во МИЭМ, 2008. – С. 7–12.
36. Акбашев Б.Б., Кечиев Л.Н., Эффективность экранирования экранов при наличии апертур. //Труды VIII Международного симпозиума по ЭМС и электромагнитной экологии/ 16-19 июня 2009 г., С.-Петербург. – СПб.: Изд-во ЛЭТИ, 2009. – С. 95 – 98.
37. Акбашев Б.Б. Способ создания электронного паспорта объекта недвижимости и система для его осуществления.//Евразийский патент № 009827. – 2008.
38. Акбашев Б.Б., Захарьина О.С., Кечиев Л.Н. Экранирование оптически прозрачных апертур. – М.: Изд-во МИЭМ, 2005. – 54 с.

39. Акбашев Б.Б., Кечиев Л.Н., Мазуренко М.Н. Экранирование шкафов и стоек электронной аппаратуры. – М.: Изд-во МИЭМ, 2005. – 46 с.