

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 654.1:621.391.8

Цецерская
Наталья Сергеевна

Аппаратно-программный комплекс для исследования устойчивости
телекоммуникационных систем в условиях мощных импульсных помех

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-98 80 01 Методы и системы защиты информации,
информационная безопасность

Научный руководитель
Мельничук Виталий Витальевич
кандидат технических наук, доцент

Минск 2016

ВВЕДЕНИЕ

В настоящее время электромагнитные помехи являются серьезной угрозой для электронных систем. Проблема намеренных силовых воздействий на радиоэлектронные средства в последние годы приобрела большое значение в связи с развитием техники генерации, усиления и излучения мощных ЭМИ.

В связи с этим, важным этапом при решении задач, направленных на обеспечение наибольшей устойчивости ТКС к действию электромагнитных факторов, является проведение исследований с использованием экспериментальных методов.

Проблема защиты технических систем и объектов от действия мощных электромагнитных помех фундаментальна, актуальна, сложна и многогранна. Базируется с одной стороны на фундаментальных исследованиях физики явления, механизмов взаимодействия полей с объектами, а с другой стороны на возможностях методов воспроизведения, испытаний и существующих средств защиты.

Проблема не решена. Исследования проводятся, физика уточняется, испытания объектов на имитаторах продолжаются. Ведется работа по следующим направлениям:

- задание требований по параметрам помех;
- создание и модернизация имитаторов, генераторов помех и средств измерения; проведение испытаний;
- разработка методов и средств защиты;
- обеспечение электромагнитной совместимости технических систем.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Разработка и развитие методов обеспечения надежной передачи, обработки и защиты информации в телекоммуникационных сетях и системах, эффективная защита самих систем имеют огромную значимость в быстроразвивающемся информационном мире.

Связь работы с крупными научными программами и темами. Исследование выполнялось в рамках постановления Совета Министров РБ от 12 августа 2010 г. №1196 «Перечень приоритетных направлений научных исследований РБ на 2011-2015 годы», в частности по направлениям «Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы» и «Средства контроля параметров систем и средств связи и телекоммуникации».

Цели и задачи исследования. Цель магистерской работы – исследование телекоммуникационных систем для улучшения их технических характеристик, повышения устойчивости и эффективности функционирования в условиях мощных импульсных помех.

Для реализации цели необходимо решить следующие поставленные задачи:

- произвести анализ значимых технических характеристик ТКС;
- произвести анализ существующих методов и способов защиты ТКС;
- исследовать предложенные аспекты по проблематике в данном направлении;
- исследовать способы воздействия и создания помех на оборудование ТКС;
- разработать методику проведения испытаний;
- скомпоновать аппаратную часть для обеспечения проведения испытаний на реальных объектах ТКС;
- вывести параметры поддержания эффективного функционирования систем;
- представить анализ тестируемых макетов и наработки по улучшению характеристик систем.

Объект и предмет исследования. Объектом исследования являются составляющие телекоммуникационных систем, и в целом ТКС, структуры передачи данных. Предметом исследования – способы обеспечения защиты компонентов системы на этапах проектирования, повышение их устойчивости и защита информации при обмене данными.

Основные положения исследования, выносимые на защиту.

1. Анализ методов и способов защиты ТКС, проникновение помех, угрозы целостности данным.
2. Средства вывода оборудования из строя, параметры эффективного функционирования.
3. Методика экспериментальных исследований ПЭМВ на устройства, входящие в состав телекоммуникационных систем, анализ сконструированных моделей.

Опубликованность результатов. По результатам выполненных исследований опубликована 1 научная работа в материалах научных конференций.

Структура и объем диссертации. Структурными частями диссертации являются: общая характеристика работы, введение, 5 глав, заключение, библиографический список, состоящий из 32 наименований, приложения. Работа изложена на 93 страницах и включает в себя 39 рисунков, 17 таблиц.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В главе 1 приведен анализ методов и средств решения проблемы защищенности телекоммуникационных систем (ТКС). Выявлены наиболее подверженные электромагнитным воздействиям элементы ТКС, к которым относятся цифровые электронные средства (ЭС), функциональные узлы цифровых электронных средств на основе печатных плат, структурированная кабельная система, металлоконструкции, система электропитания. Определены семь основных задач в проблеме физической защиты информации в цифровых ЭС. Описана методика оценки устойчивости объектов ТКС к воздействию ЭМИ. Проанализированы экспериментальные аспекты авторов в сфере защиты и испытаний ТКС.

В главе 2 вводится разработка методик испытаний ТКС на устойчивость к мощным импульсным помехам, приводятся требования к испытательному оборудованию, дается последовательность проведения испытаний на устойчивость к электромагнитному полю, кондуктивным помехам. Приведены основные виды испытательных воздействий, регламентируемых базовыми стандартами, и простейшие схемные реализации испытательных генераторов для каждого вида имитируемых помех.

В главе 3 проводится анализ средств тестирования и измерений для обеспечения испытаний телекоммуникационных систем, так как для проведения испытаний необходимо определить оборудование, подходящее по параметрам, чтобы обеспечить достоверность тестирования ТКС. Описываются основные характеристики сигнала, по которым можно будет судить о степени влияния помех на функционирование оборудования. Приводится алгоритм выбора генераторов помех, их структурные схемы и характеристики. В частности, представлены описания по: прибору Teseq NSG 3040, испытательному генератору микросекундных импульсных помех, испытательному генератору VCS 500M10. Даются рекомендации по осциллографическим измерениям и выбору измерительного оборудования. Приведены описания осциллографов серии HAMEG, RTE и TDS2000B.

В главе 4 описаны непосредственно испытания на реальных объектах телекоммуникационных систем и их макетах. Испытания на ТКС проводились методом сравнения. Результаты испытаний классифицировались на основе приведенных критериев качества функционирования, либо иными требованиями, установленными в стандартах на технические средства конкретного вида или технической документации на них. Приведены схемы собранных макетов, которые являются аналогами полноценного источника вторичного электропитания (ИВЭ) персонального компьютера (ПК),

системного блока ПК. Протестирована система событийного видеоконтроля в составе ПК, видеокамера, блок питания, кабель RG-59, блок обработки видеосигнала. Приводятся результаты испытаний и даются рекомендации по повышению устойчивости системы событийного видеоконтроля к воздействию ЭМИ.

В главе 5 проводится разработка организационно-технических мероприятий по защите от силового деструктивного воздействия (СДВ). Приведены основные каналы деструктивного воздействия на интегрированную систему безопасности и рубежи защиты. Дается классификация технических средств СДВ по данным каналам. Устойчивость и надежность систем определяется мощностью воздействия, выбранными средствами защиты, имеющимися финансовыми возможностями. Эти обстоятельства определяют выбор стратегии защиты. Разработаны меры и способы усовершенствования защиты систем безопасности от СДВ.

ЗАКЛЮЧЕНИЕ

Было произведено исследование телекоммуникационных систем, а также способов повышения устойчивости и эффективности функционирования объектов ТКС в условиях мощных импульсных помех.

Проведен аналитический обзор, который показывает:

- наиболее характерным является экспериментальный подход для решения задачи ПЭМВ;
- подача ЭМИ в кабели здания представляет серьезную угрозу цифровым ЭС, которая в свою очередь может стать причиной искажения, уничтожения или блокирования важной информации;
- изучение ПЭМВ на цифровые ЭС ЭМИ миллисекундного диапазона является перспективным направлением;
- необходима и важна работа в сфере обнаружения средств ПЭМВ, подключенных в сеть здания.

Все вышесказанное подчеркивает большую актуальность данной научной задачи.

По результатам анализа существующих методов и способов испытаний разработана методика испытаний устройств ТКС на устойчивость к мощным импульсным помехам. Определены требования к испытательному оборудованию и условиям проведения испытаний. Выбраны виды испытательных воздействий, конкретные параметры которых скорректированы в зависимости от тестируемого оборудования.

Проанализировав устройства, необходимые для обеспечения проведения испытаний, определили наиболее подходящие по требованиям для осуществления исследования. Среди представленных генераторов выбрали доступный и подходящий по параметрам испытательный генератор микросекундных импульсных помех. Из приведенного перечня осциллографов отдали предпочтение осциллографу Tektronix TDS2022B.

Проведены испытания на устройствах, входящих в состав ТКС. Созданы макеты, аналоги ИВЭ персонального компьютера и системного блока ПК. Макеты протестированы на воздействие микросекундных ЭМИ. Была проанализирована и протестирована система видеоконтроля.

Приведен состав уязвимых частей интегрированных систем безопасности. Выработаны способы защиты от силового деструктивного воздействия по различным каналам распространения, созданы конструкции технических средств, способных осуществить данное воздействие.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. Цецерская, Н.С Устройство контроля полимерных материалов, используемых в экранах электромагнитного излучения, на трекинговость / Н.С. Цецерская // Тез. докладов 51 научно-технической конференции аспирантов, магистрантов и студентов БГУИР «Телекоммуникационные системы и сети» – Минск, БГУИР, 2015 – С.24.

Библиотека БГУИР