Белорусский государственный университет транспорта
Гомель, Республика Беларусь

ЭЛЕКТРОМАГНИТНЫЙ ТЕРРОРИЗМ КАК НОВЫЙ ВИД УГРОЗ ФУНКЦИОНАЛЬНОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

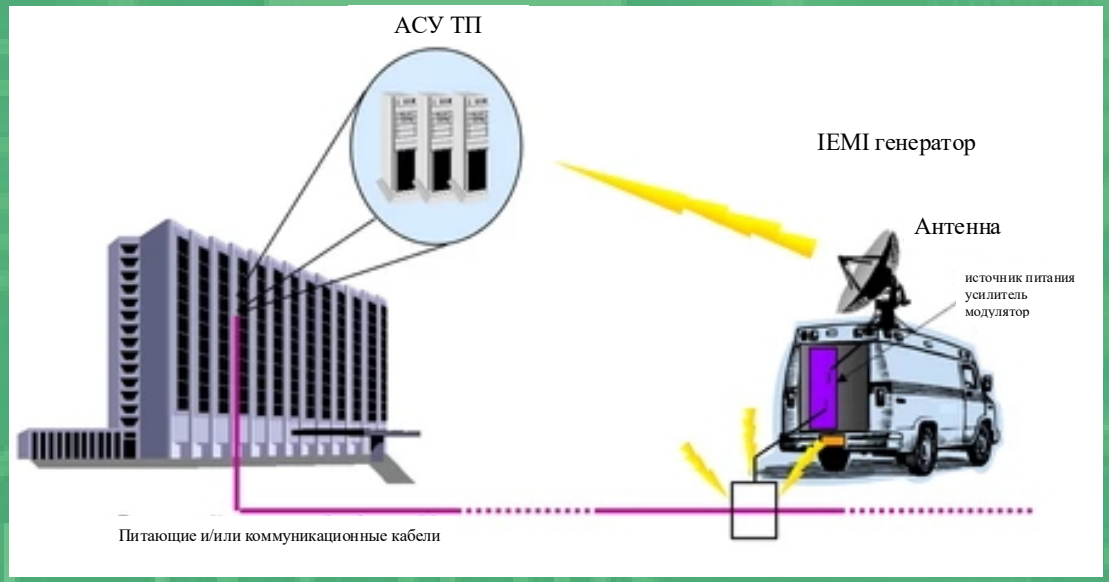
БОЧКОВ К.А. д.т.н., профессор
КОМНАТНЫЙ Д.В. к.т.н., доцент
ЖИГАЛИН И.О. м.т.н.

Научно-исследовательская лаборатория
«БЕЗОПАСНОСТЬ И ЭМС ТЕХНИЧЕСКИХ СРЕДСТВ»

Электромагнитный терроризм (ЭМТ) – воздействие преднамеренной электромагнитной помехой (ПЭМП, IEMI) на микроэлектронную элементную базу.

Под преднамеренной электромагнитной помехой, понимают преднамеренное оказание в преступных или террористических целях мощного электромагнитного воздействия на электронные и электрические системы, нарушающего их функционирование. Этот термин является дословным переводом общепринятого Международной электротехнической комиссией термина Intentional Electromagnetic Interference (IEMI). Воздействие ПЭМП на микроэлектронные системы возможно, как по цепям питания, интерфейсным линиям, так и через свободное пространство.

Воздействие ПЭМП представляет особую опасность для автоматизированных цифровых систем управления ответственными технологическими процессами (АСУ ТП) на транспорте, энергетике, химических производствах.



Генераторы направленного электромагнитного излучения

Техническими средствами создания ПЭМП, как правило, являются специальные генераторы сверхкоротких электромагнитных импульсов, как большие стационарные, так и малогабаритные переносные.

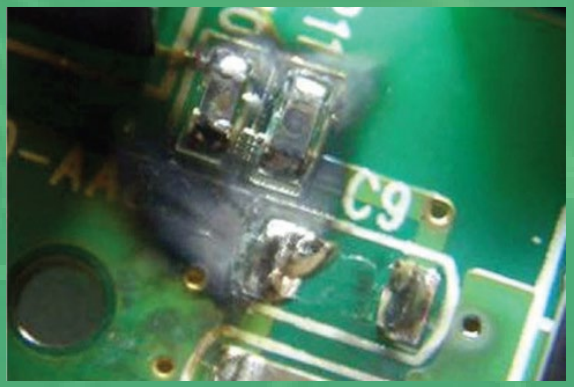
Сверхмощные ультраширокополосные импульсные генераторы

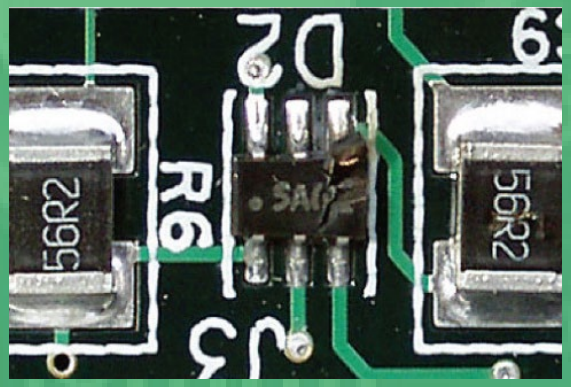
Носимые генераторы

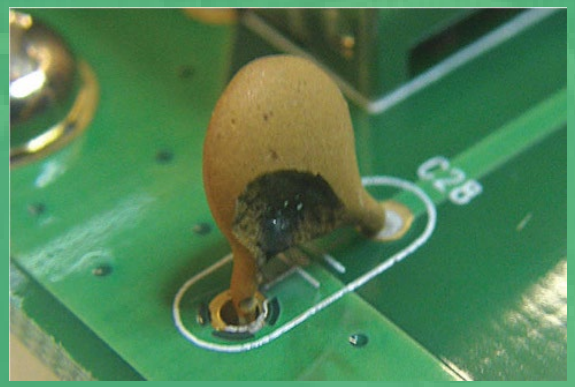
Повреждения от преднамеренного электромагнитного воздействия

Наибольшую опасность для цифровых ИТ систем и АСУ ТП представляют малогабаритные переносные наносекундные импульсные генераторы, излучающие энергию в диапазоне до 10 ГГц. Воздействие таким генератором с близкого расстояния может вывести из строя до 20 компьютеров.

Это связано как с высоким быстродействием современных микроэлектронных компонентов, так и с низким значением напряжения пробоя переходов. Так, например, у запоминающих устройств пороговое напряжение составляет порядка 7 В, а логических интегральных микросхем на МОП-структурах от 7 до 15 В.







Воздействие ПЭМП

Воздействие ПЭМП на цифровые информационные системы и АСУ ТП как правило приводят к нарушению требований по обеспечению как информационной, так и функциональной безопасности.

Свойство информационной безопасности должно обеспечить доступность, целостность и конфиденциальность данных системы управления. Свойство функциональной безопасности должно обеспечить корректное выполнение функций системы управления, а при возникновении отказов перевести объект управления в так называемое защитное состояние.

Анализ отказов и повреждений в оборудовании цифровых систем не позволяет порой однозначно идентифицировать причину возникновения повреждений, так как причиной может быть как ПЭМП, так и непреднамеренные помехи, вызванные индуктированными перенапряжениями в цепях питания и другими природными и паразитными техногенными процессами.

Последствия нарушения работы средств информатизации и АСУ ТП в различных отраслях

Сферы применения	Возможные последствия
Управление технологическими процессами	Инициирование запроектных аварий для вывода из строя технологического оборудования, остановка/замедление технологических процессов.
Мониторинг и кризисное управление	Выход кризисной ситуации из-под контроля, неадекватное управление ситуацией с непредсказуемыми последствиями.
Банковская инфраструктура	Парализация банковской деятельности, создание условий для несанкционированного снятия денежных средств с банковских счетов.
Энергетика	Нарушение электроснабжения предприятий, инициирование аварий систем электроснабжения.
Транспорт	Нарушение работы систем обеспечения безопасности движения поездов; нарушение управления транспортными перевозками и контроля над ними; нарушение работы средств управления и навигации воздушных судов.

Особенности микроэлектронных СЖАТ

Особое место среди автоматизированных систем управления технологическими процессами занимают современные микроэлектронные системы железнодорожной автоматики и телемеханики (СЖАТ) призванные обеспечивать в первую очередь безопасность движения поездов.

Это обусловлено предъявляемым к ним техническими нормативно-правовыми актами (ТНПА) самыми высокими требованиями уровня полноты безопасности SIL4 по основополагающему международному и гармонизированному с ним межгосударственному стандарту ГОСТ МЭК 61508 «Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью.

SECRET – SECurity of the Railways against Electromagnetic aTtacks (Защита железнодорожных систем от воздействия электромагнитных атак)

SECRET PROJECT
SECURITY OF RAILWAYS AGAINST ELECTROMAGNETIC ATTACKS

Цель проекта: анализ влияния ЭМ атак на европейскую железнодорожную сеть.
Задачи:

1. Оценка угроз и анализ рисков ЭМ атак
2. Техническая защита АПК СЖАТ и беспроводной связи (функциональная и информационная безопасность)
3. Разработка рекомендаций по повышению устойчивости ж.д. инфраструктуры от ЭМ атак (включая организационные и технические мероприятия)

SECRET – SECurity of the Railways against Electromagnetic aTtacks (Защита железнодорожных систем от воздействия электромагнитных атак)

SECRET PROJECT
SECURITY OF RAILWAYS AGAINST ELECTROMAGNETIC ATTACKS

Оценка рисков и последствий электромагнитных атак на микроэлектронные СЖАТ.
Виды ЭМ атак:

1. ЕМ-атаки, целью которых является разрушение электронного оборудования (ФБ)

2. ЕМ-атаки, целью которых является изменение передаваемой информации компонентам железнодорожных систем (ИБ)

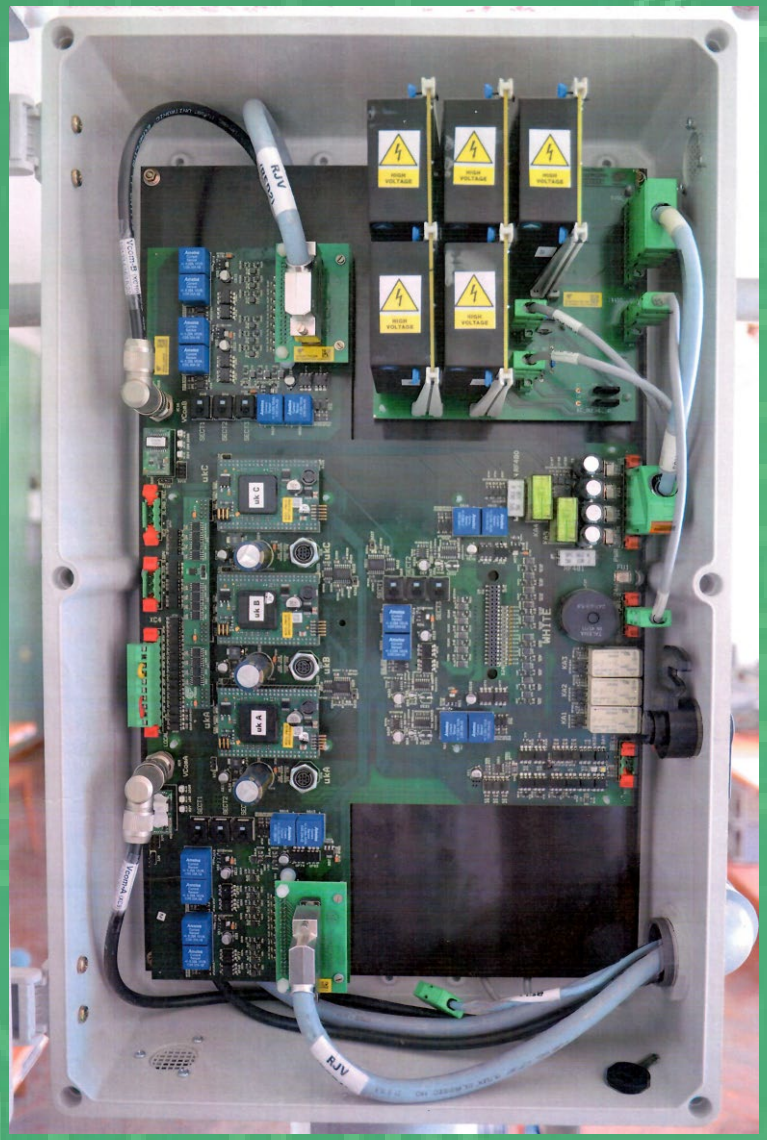
Микропроцессорная сигнализация переездной сигнализации.

Угроза IEMI (ПЭМП) атаки

Микропроцессорная сигнализация переездной сигнализации (состояние при испытании на ЭМС)

Микропроцессорная сигнализация переездной сигнализации (модуль управления)

Микропроцессорная сигнализация переездной сигнализации (плата модуля управления)



Подходы к решению проблемы защиты от ПЭМП

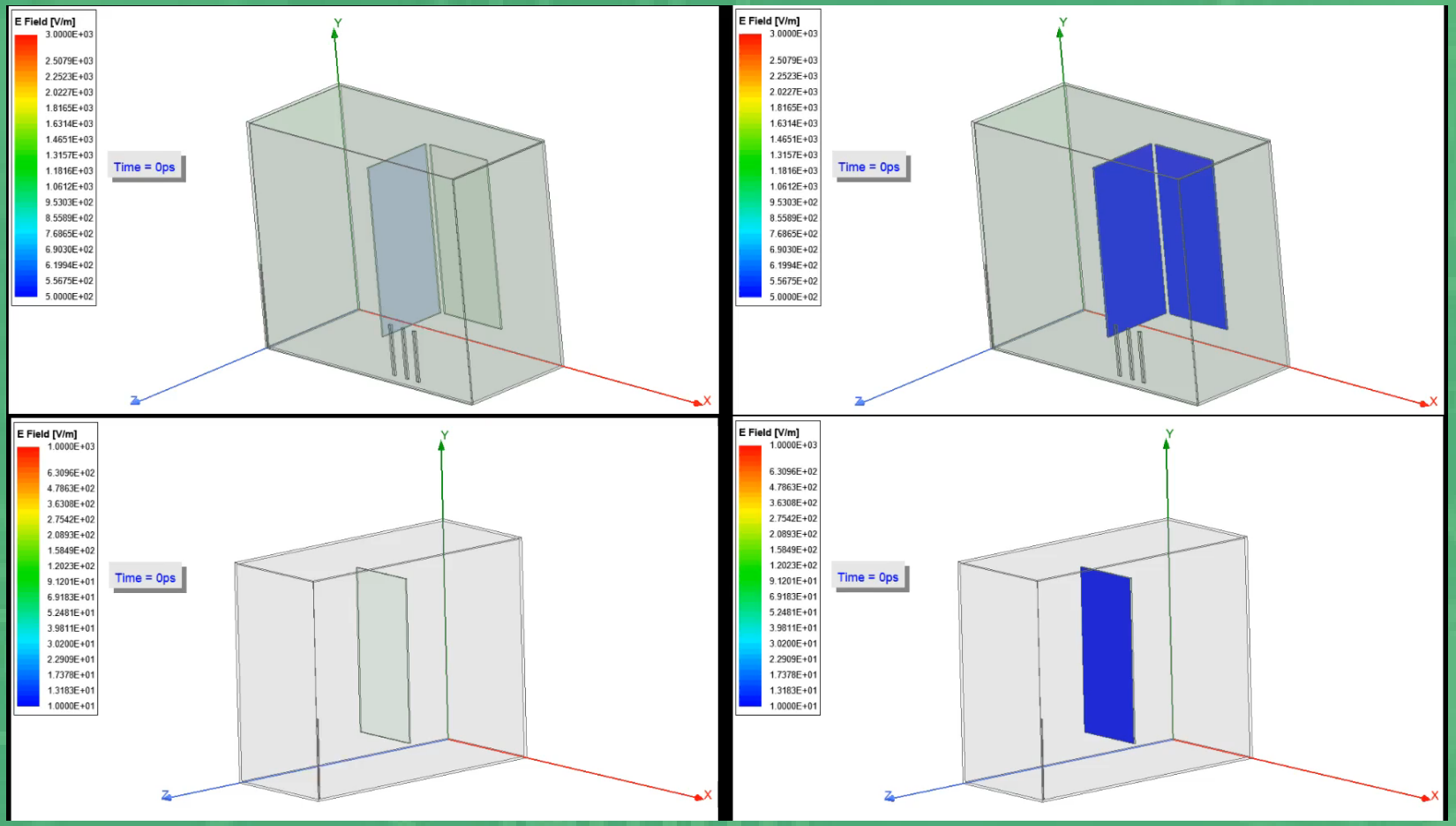
- Физическое моделирование воздействия ПЭМП на аппаратуру при помощи генератора тестовых воздействий

- Математическое моделирование процесса проникновения ПЭМП в корпуса аппаратуры микроэлектронных СЖАТ численными методами либо по аналитическим выражениям для электромагнитного излучения паразитных антенн-неоднородностей (апертур) корпусов технических средств СЖАТ

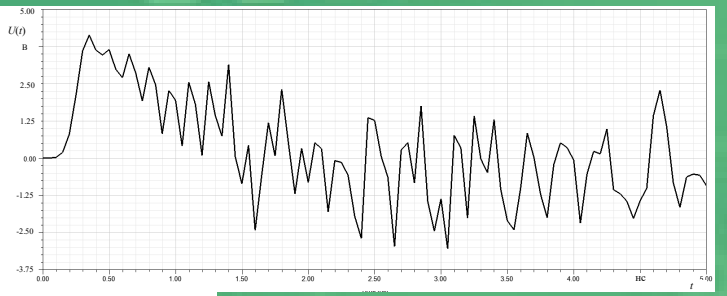
Методы защиты от ЭМ-помех:

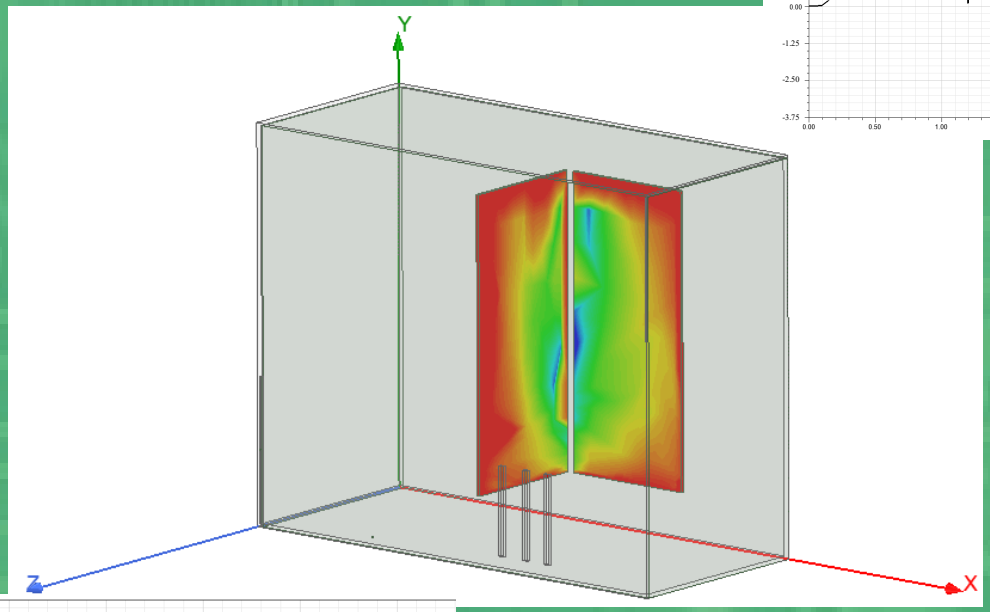
- Периметр охраны
- Гальваническое разделение по питанию
- Фильтрация
- Защита от перенапряжений
- Экранирование

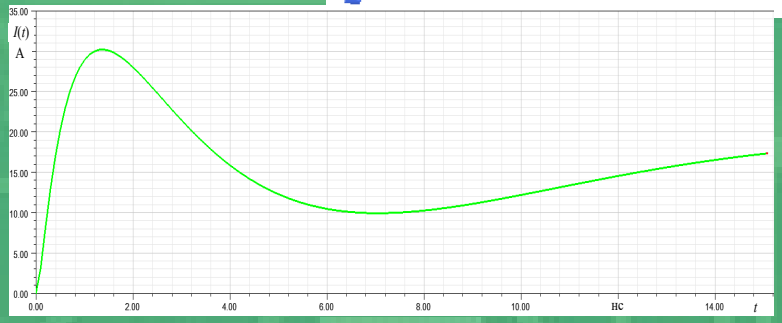
Математическое моделирование процесса проникновения ПЭМП через неоднородности корпусов испытуемой аппаратуры численными методами при облучении узконаправленной антенной (в программном комплексе Ansys HFSS)



Представление результатов моделирования
ГОСТ 30804.4.2
IEC 61000-4-2







Спасибо за внимание!