Белорусский государственный университет транспорта
Гомель, Республика Беларусь

АНАЛИЗ И ПРОГНОЗИРОВАНИЕ УСТОЙЧИВОСТИ КРИТИЧЕСКИХ СИСТЕМ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ К ЭЛЕКТРОМАГНИТНЫМ ИМПУЛЬСАМ ПРЕДНАМЕРЕПННОГО ВОЗДЕЙСТВИЯ

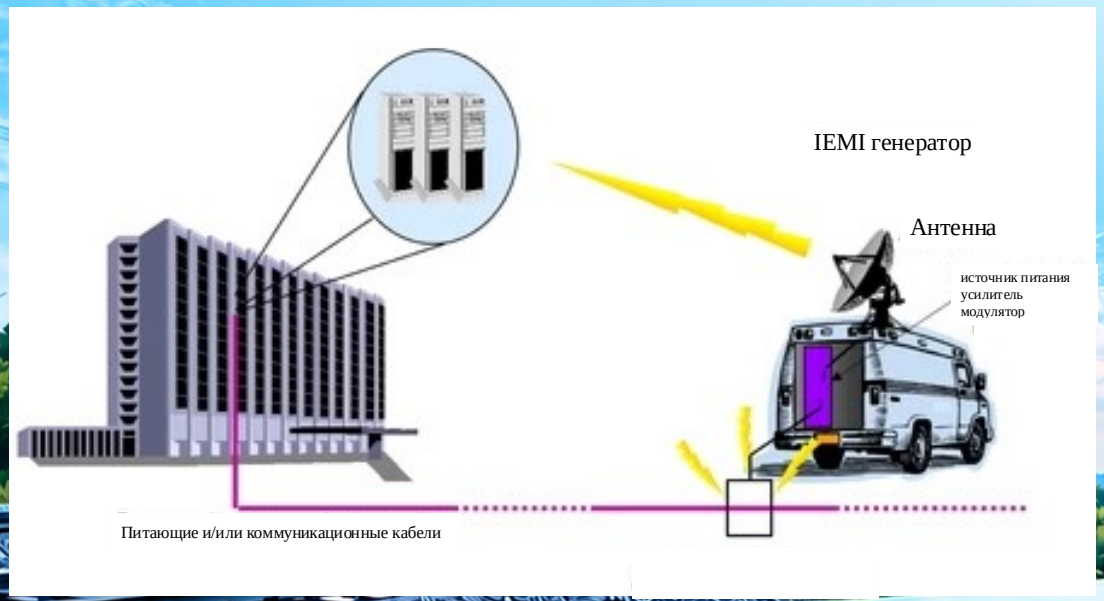
БОЧКОВ К.А. д.т.н., профессор
КОМНАТНЫЙ Д.В. к.т.н., доцент
ЖИГАЛИН И.О. м.т.н.

Научно-исследовательская лаборатория
«БЕЗОПАСНОСТЬ И ЭМС ТЕХНИЧЕСКИХ СРЕДСТВ»

IEC 61000-4-36:2020 Электромагнитная совместимость (ЭМС). Часть 4-36. Методы испытаний и измерений. Методы определения невосприимчивости к преднамеренным электромагнитным помехам (IEMI, ЭИПВ) оборудования и систем.

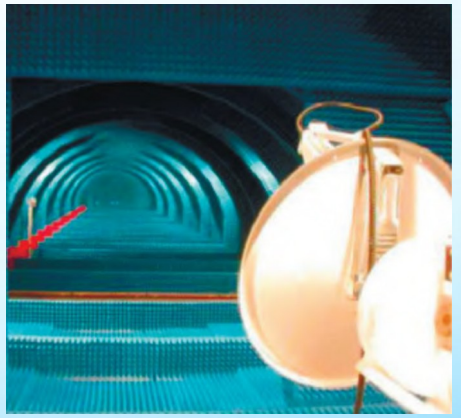
IEC определяет IEMI (Intentional Electromagnetic Interference) как преднамеренное создание электромагнитной помехи, приводящей к сбоям, отказам или необратимым повреждениям элементов в электрических и электронных системах в террористических или преступных целях.

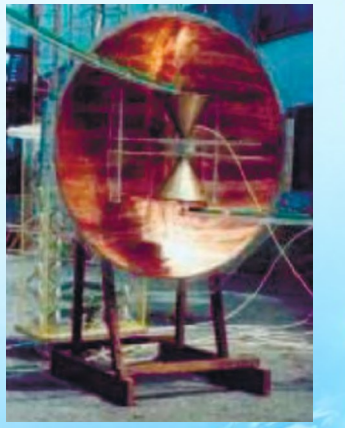
Воздействие ЭИПВ на микроэлектронные системы возможно, как по цепям питания, интерфейсным линиям, так и через свободное пространство.



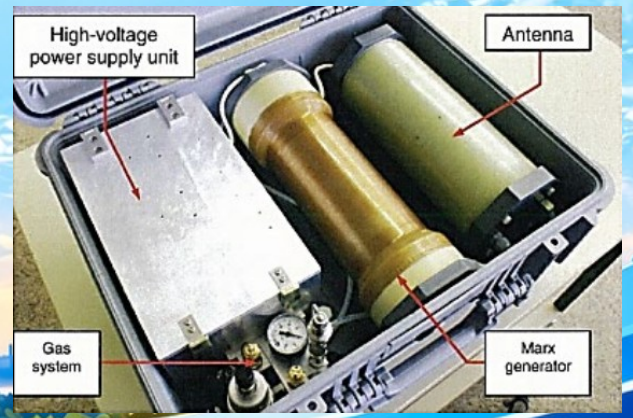
Генераторы направленного электромагнитного излучения

Техническими средствами создания ЭИПВ, как правило, являются специальные генераторы с узконаправленными антеннами сверхкоротких электромагнитных импульсов, как возимые, так и малогабаритные переносные.





Сверхмощные ультраширокополосные импульсные генераторы



Возимые и носимые импульсные генераторы

Особенности электромагнитного терроризма

Для понимания механизмов проникновения ЭИПВ и принятия необходимых организационных и технических решений, предотвращения или уменьшения рисков деструктивного воздействия на КССИ (КВОИ) необходимо учитывать следующее:

Угроза электромагнитного терроризма возрастает при применении малогабаритных генераторов ЭИПВ в связи с развитием мощной твердотельной электроники (сверхбыстродействующих полупроводниковых коммутаторов) с одной стороны и использование накопителей (современных) энергии с другой стороны

Электромагнитный терроризм с использованием ЭИПВ может осуществляться тайно и анонимно без особого ослабления через стены, стеклянные ограждения и т.д.

Направлен на нарушение требований по ФБ и ИБ КСИИ (КВОИ)

Необходимы дополнительные исследования механизмов проникновения ЭИПВ и методов защиты.

SECRET – **SEC**urity of the **R**ailways against **E**lectromagnetic a**T**tacks
(Защита железнодорожных систем от воздействия электромагнитных атак),
Франция, Германия, Испания, Италия и Бельгия,
(бюджет 4,2 млн. евро)

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)

Современные компьютеры и аппаратура МСЖАТ в небезопасном исполнении по отношению к ЭИПВ

Использование современных компьютеров (модных у молодежи) в критической инфраструктуре ИТ опасно из-за высокой проницаемости энергии ЭИПВ через неоднородности экранов, наличия радиопрозрачных стенок и вентиляционных отверстий.

Методы анализа воздействия ЭИПВ на КСИИ (КВОИ)

Методы анализа	Недостатки
Физическое моделирование	1. Дорогое, малодоступное, зачастую уникальное оборудование генераторов ЭИПВ 2. Разрушающий характер испытаний 3. Для выявления механизма проникновения и повреждения аппаратуры требуется программа длительных экспериментов
Математическое моделирование численными методами конечных элементов	1. Присущие численным методам внутренние ограничения сходимости и устойчивости 2. Методы реализованы в программах третьих производителей, которые не декларируют ограничения заложенных ими методов 3. Существенные затраты времени на разработку адекватной модели внутреннего расположения микроэлектронных блоков и связей между ними

Методы анализа и прогнозирования устойчивости КСИИ (КВОИ) к ЭИПВ

Суть предлагаемого нами метода анализа и прогнозирования устойчивости критической инфраструктуры к воздействию ЭИПВ заключается в следующем:

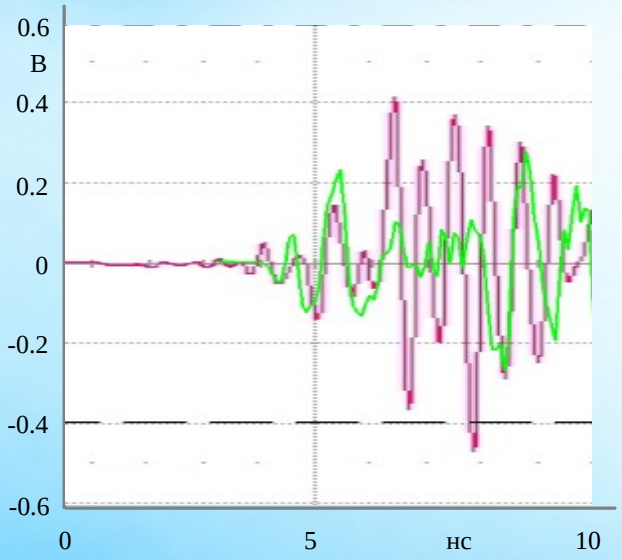
1) Стандартными генераторами ЭСР по ГОСТ 30804.4.2-2013 и ГОСТ Р 56115-2014 проводятся испытательные воздействия на неоднородности корпусов аппаратных средств критической инфраструктуры контактным ЭСР с возрастающей амплитудой испытательных импульсов до появления устойчивых сбоев (или отказов).

2) По условиям эквивалентности импульсов помех различной формы определяем характеристики импульса ЭИПВ эквивалентного импульсу ЭСР из п.1. Полученные характеристики импульса ЭИПВ являются основой для решения двух взаимосвязанных задач:

- **Определение размеров периметров охраны** объектов КСИИ (КВОИ) на основе разработанных в НИЛ «БЭМС ТС» аналитических моделей проникновения ЭИПВ через неоднородности экранов и процессов затухания энергии от генераторов ЭИПВ

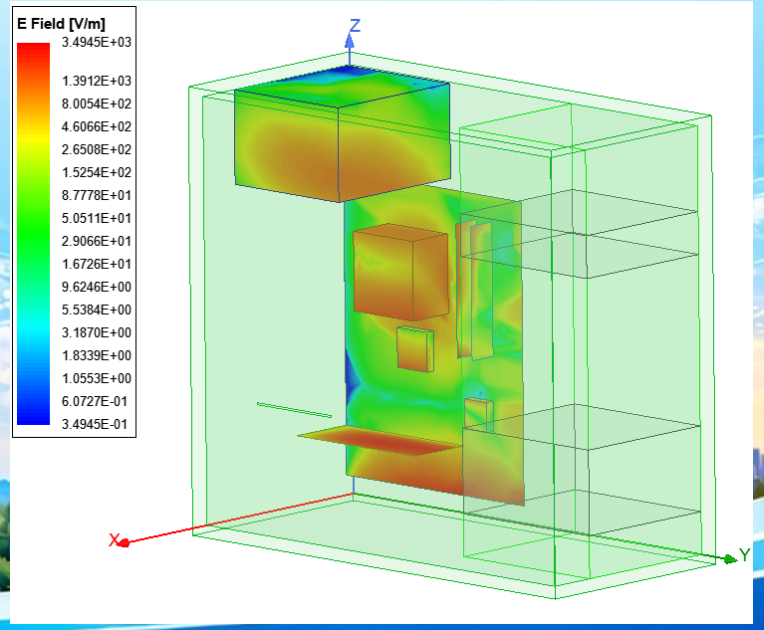
- **Определяется мощность генератора ЭИПВ**, воздействие которого с определенного расстояния способно вызвать сбой или отказ объектов КСИИ (КВОИ).

Сравнение результатов испытаний и моделирования

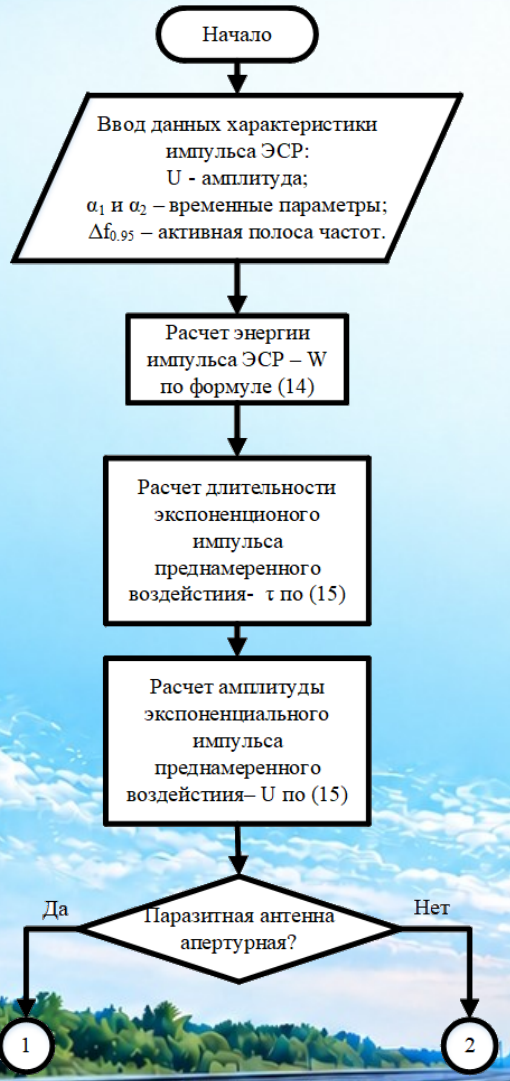


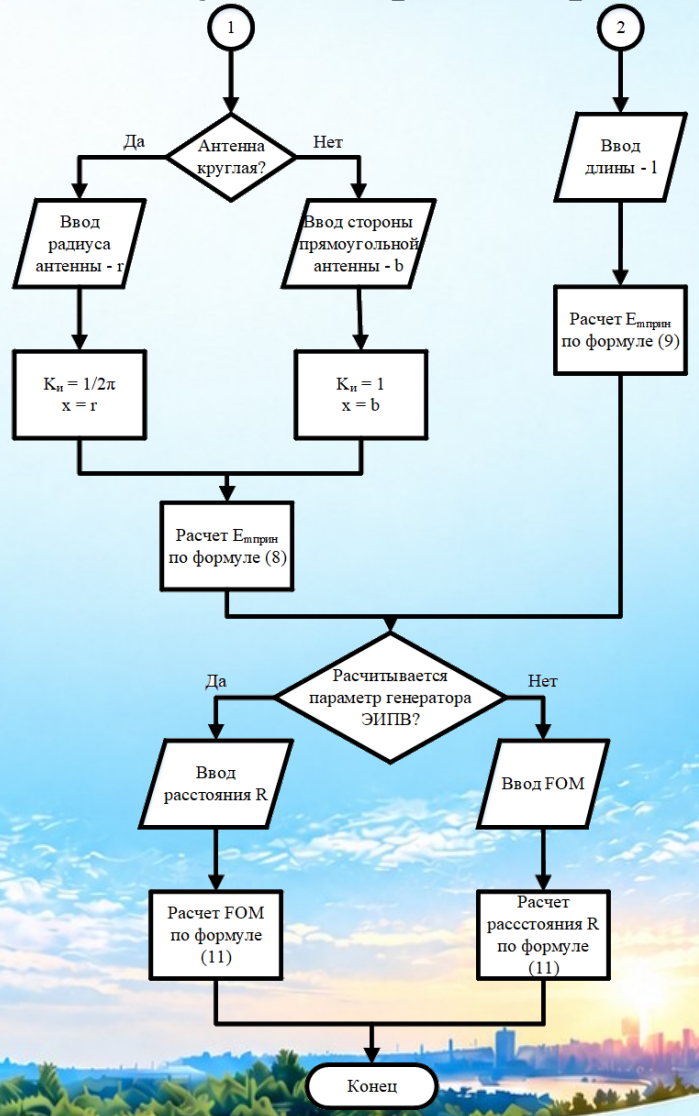
Результат моделирования

Результат измерения

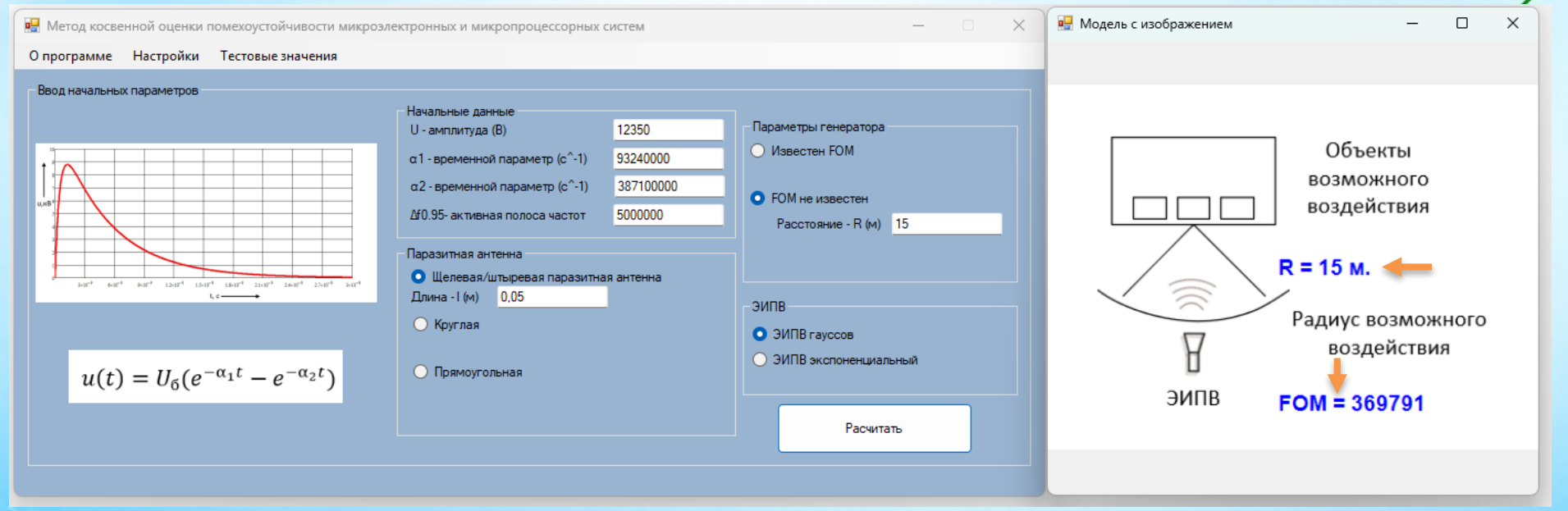


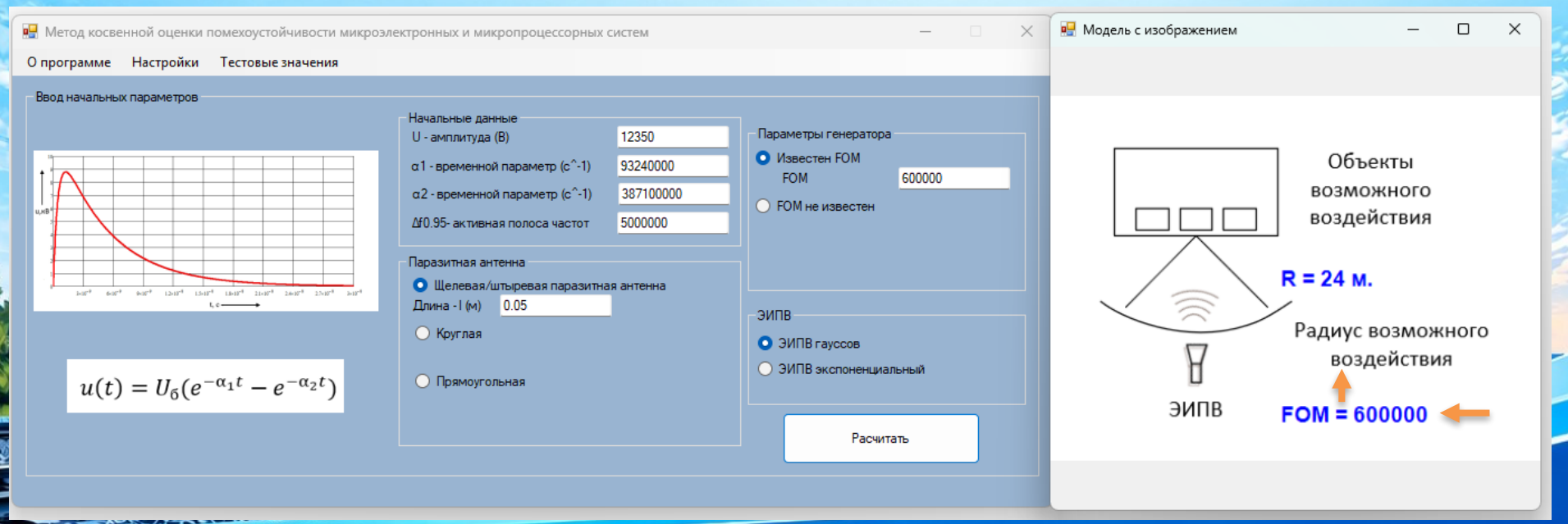
Алгоритм реализации метода косвенной оценки помехоустойчивости микроэлектронных и микропроцессорных систем к электромагнитным импульсам преднамеренного воздействия



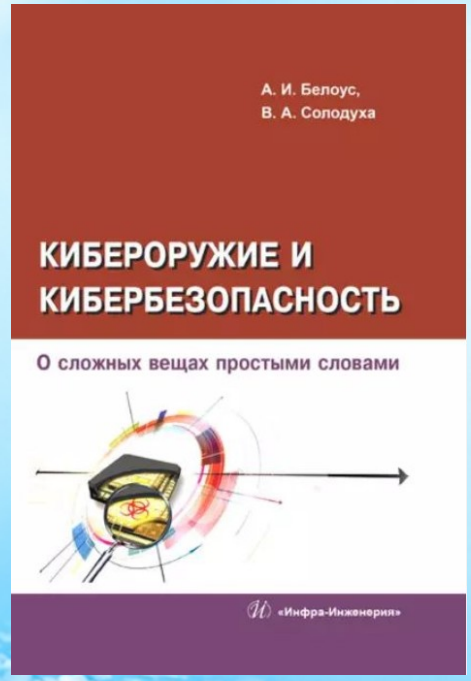


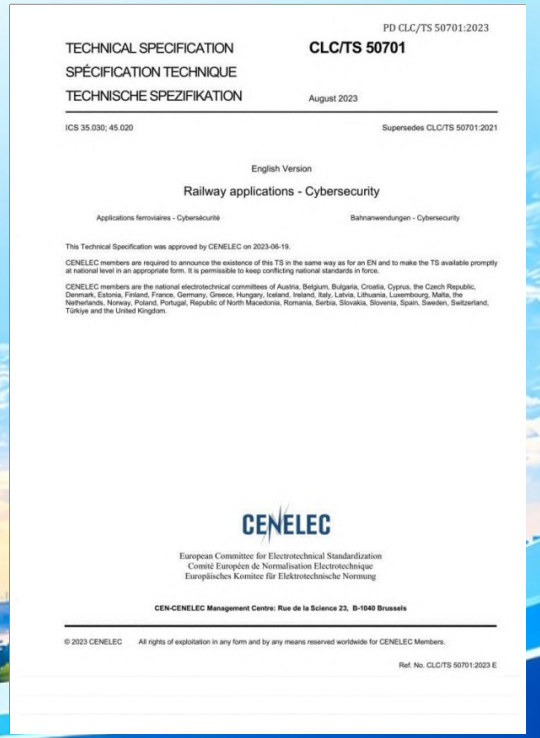
Определение размеров периметра охраны и мощности генератора ЭИПВ





Актуальные издания





Заключение

Для повышения устойчивости КСИИ (КВОИ) к ЭИПВ исходя из предлагаемого нами метода необходимо выполнять следующие мероприятия:

1.На этапе разработки объектов критической инфраструктуры необходимо провести испытания стандартными генераторами ЭСР с целью выявления неоднородностей корпусов и выполнить мероприятия по дополнительному экранированию или изменения конструкции корпусов.

2.Для существующих объектов КСИИ (КВОИ) провести обследование неоднородностей экранов и их геометрическое расположение исходя из возможных зон использования злоумышленником генераторов ЭИПВ. После этого либо изменить геометрию расположения оборудования КСИИ (КВОИ), либо принять меры по экранированию радиопрозрачных стен, окон со стороны зон возможного применения злоумышленником генераторов ЭИПВ.

Спасибо за внимание!