**Учреждение образования**
**«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»**
***Отдел студенческой науки и магистратуры***

# 52-я НАУЧНАЯ КОНФЕРЕНЦИЯ АСПИРАНТОВ, МАГИСТРАНТОВ И СТУДЕНТОВ

## ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

***25-30 апреля 2016 года***

Программа и пригласительный билет

**Минск 2016**

Министерство образования Республики Беларусь
учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

# ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

## МАТЕРИАЛЫ 52-Й НАУЧНОЙ КОНФЕРЕНЦИИ АСПИРАНТОВ, МАГИСТРАНТОВ И СТУДЕНТОВ

(Минск, 25–30 апреля 2016 года)

Минск, БГУИР
2016

Телекоммуникационные системы и сети: материалы 52-й научной конференции аспирантов, магистрантов и студентов (Минск, 25–30 апреля 2016 г.). – Минск: БГУИР, 2016. – 27 с.

В сборник включены лучшие доклады, которые были представлены на 52-й научной конференции аспирантов, магистрантов и студентов БГУИР, отобранные по следующим направлениям: метрология и стандартизация; телекоммуникационные системы; сети и устройства телекоммуникаций; защита информации.

Для научных и инженерно-технических работников, преподавателей, аспирантов, магистрантов и студентов вузов.

# СОДЕРЖАНИЕ

# ОСОБЕННОСТИ ПРОСТРАНСТВЕННОГО РАСПРЕДЕЛЕНИЯ СИЛЫ СВЕТА И КОЛОРИМЕТРИЧЕСКИЕ ХАРАКТЕРИСТИКИ СВЕТОДИОДНЫХ ЛАМП РАЗЛИЧНОЙ КОНСТРУКЦИИ

*Машедо Н.В.[1], Крейдич А.В.[2], Никоненко С.В.[2], Гурский А.Л.3*
*[1]Испытания и сертификация бытовой и промышленной продукции «БЕЛЛИС»*
*[2]Институт физики им. Б.И. Степанова НАН Беларуси*
*[3]Белорусский государственный университет информатики и радиоэлектроники*

В последние время светодиоды (СИД) и источники излучения на их основе получили широкое распространение в светотехнике. Одновременно с распространением СИД возникли задачи корректного измерения параметров их излучения и оценки степени его опасности для человека (фотобиологической безопасности).

Особенностью измерения параметров СИД является то, что для измерения оптических характеристик СИД и источников излучения на их основе применяют фотометрические методы, которые разрабатывались и совершенствовались в то время, когда основным видом источника света была лампа накаливания. Как следствие, эти методы не учитывают характерных особенностей излучения светодиодов. Например, пространственное распределение мощности излучения различных СИД могут иметь значимые отличия, что оказывает влияние на оценку фотометрических характеристик их излучения. СИД-лампы конструктивно являются более сложными изделиями, в которых могут использоваться десятки СИД-чипов. Чтобы обеспечить качество и безопасность СИД-ламп, необходимо точно измерять их оптические характеристики, что важно при конструировании, производстве и техническом обслуживании светотехнических изделий на их основе.

В данный момент актуальным также является вопрос о разработке методик ускоренных испытаний для сокращения продолжительности ресурсных испытаний излучателей на основе СИД, которая в настоящее время составляет 6000 часов. Разработка методов ускоренных испытаний позволила бы сократить их продолжительность до экономически и практически целесообразной.

Цель данной работы – сопоставление характеристик различных СИД-ламп (пять различных типоразмеров) в части соответствия ТНПА и исследование влияния их конструкции на пространственное распределение интенсивности излучения.

В результате исследований было установлено, что параметры всех образцов явно не соответствуют требованиям ТНПА, регламентирующих эксплуатационные характеристики излучателей на основе СИД (Регламенты ЕС, стандарты IEC), касательно индекса цветопередачи. Для коррелированной цветовой температуры и координат цветности большинство ламп не соответствуют установленным нормам или изготовителем не указаны номинальные значения данных характеристик. Также изучено влияние конструктивных особенностей СИД-ламп, в том числе расположения СИД-чипов в лампе, на особенности пространственного распределения силы света.

В качестве примера в таблице приведены результаты измерений параметров (координаты цветности x и y, коррелированная цветовая температура CCT, индекс цветопередачи CRI, световой поток TLF, потребляемая мощность) одного из типов ламп.

Таблица

Результаты измерений

| | | x | y | CCT, K | CRI, % | TLF, лм | Мощность, Вт |
|---|---|---|---|---|---|---|---|
| 2W GU5.3 | Ном.[1] | **0,313**[2] | **0,337**[2] | **6500** | **–**[3] | **–**[3] | **2** |
| | №1 | 0,3258 | 0,3416 | 5800 | 71,1 | 94,71 | 1,52 |
| | №2 | 0,3333 | 0,3539 | 5468 | 70,5 | 106,04 | |
| | №3 | 0,3302 | 0,3487 | 5599 | 70,6 | 99,86 | |

[1] – Номинальное значение, декларируемое изготовителем.

[2] – Данные координаты цветности соответствуют CCT = 6500 K в соответствии с Приложением D IEC 60081.

[3] – данные параметры не заявлены изготовителем.

Таким образом при исследовании характеристик излучателей на основе СИД необходимо учитывать влияние особенностей их конструкции на результаты и использовать пригодные методы измерений, основанные на современной практике.

# МЕТОДИКА ВЫПОЛНЕНИЯ ИЗМЕРЕНИЯ КОЭФФИЦИЕНТА ШУМА ПРИЕМНОГО ТРАКТА ППМ АФАР В ПОЛОСЕ ЧАСТОТ 9,5 - 9,8 ГГЦ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Богданов Р. А.*

*Ревин В. Т. – к-т. техн. наук, доцент*

Приемо-передающий модуль (ППМ) является основным функциональным элементом активной фазированной антенной решетки (АФАР), определяющим ее основные характеристики. Основным назначением ППМ АФАР является усиление сигналов передатчика и приемника с регулировкой их по фазе и амплитуде в рабочем диапазоне частот в соответствии с алгоритмом работы системы. ППМ АФАР включает в себя следующие основные функциональные устройства:

- передающий тракт, состоящий из фазовращателя и усилителя мощности излучаемого сигнала;
- приемный тракт в составе малошумящего усилителя принимаемого сигнала, фазовращателя, аттенюатора, а также переключателя, обеспечивающего работу приемного и передающего трактов ППМ на общий элемент антенного системы.

В состав ППМ входят также устройства вторичного электропитания, элементы системы управления, схемы контроля режима работы ППМ и др.

Основным параметром, определяющим качество работы приемо-передающего модуля, является коэффициент шума приемного тракта. Коэффициент шума описывает уменьшение соотношения «сигнал/шум» по мере прохождения сигнала через приемное устройство или его отдельный каскад (усилитель, смеситель). Фундаментальное определение коэффициента шума следующее:

$$F = \frac{(S_{in} / N_{in})}{(S_{out} / N_{out})},$$

где $S_{in} / N_{in}$- соотношение «сигнал/шум» на входе устройства; $S_{out} / N_{out}$- соотношение «сигнал/шум» на выходе устройства.

Для измерения его значений в заданном диапазоне рабочих частот была разработана методика выполнения измерений, основанная на методе $Y$- фактора и используемого при измерении коэффициента шума СВЧ устройств в соответствие с выражением $NF = 10\log_{10}\left[10_{ENR/10}/(10_{Y/10}-1)\right]$. Для проведения измерений используется источник шума с калиброванным значением *ENR* (*Excess Noise Ratio*), который получил название избыточным коэффициентом шума.

Полное измерение коэффициента шума и усиления тестируемого устройства методом $Y$- фактора с коррекцией второго каскада состоит из двух шагов. Следует обратить внимание, что во время измерений и автоматических вычислений специализированные анализаторы коэффициента шума оперируют не коэффициентом шума или фактором шума, а эффективной температурой шума. Перевод результатов в коэффициент шума осуществляется в конце измерения.

Первый шаг называется калибровкой. Он производится без тестируемого устройства. Источник шума с калиброванным значением *ENR* подключают непосредственно к входу прибора (рисунок 1).

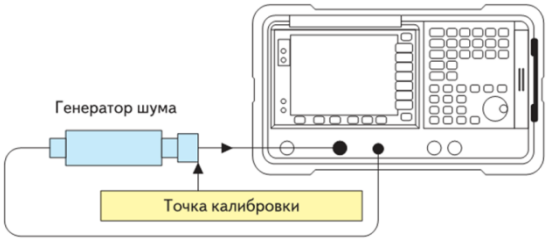



Рис.1 – Калибровка измерителя коэффициента шума

В анализатор спектра вводят таблицу *ENR* в точках частотного диапазона, согласно маркировке источника шума. Некоторые измерители коэффициента шума могут автоматически считывать таблицу *ENR* из источника шума без участия оператора. После того как таблица *ENR* загружена в память анализатора спектра, измеритель коэффициента шума включает и выключает источник шума и измеряет значения мощностей $P_2^{ON}$ и $P_2^{OFF}$. В конце калибровки прибор сохраняет измеренные значения $P_2^{ON}$ и $P_2^{OFF}$, а также вычисляет значения $Y_2$ и $T_2$. Затем прибор приводит кривые коэффициента шума и усиления к номинальному значению 0 дБ. После этого прибор готов к измерению тестируемого устройства (рисунок 2).

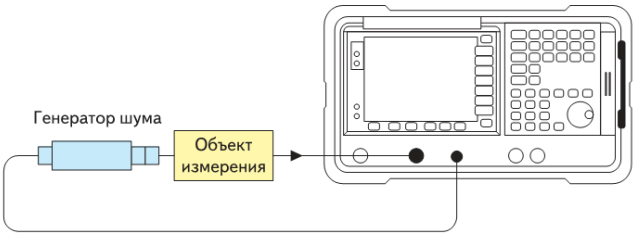



Рис.2 – Схема включения объекта измерения для определения коэффициента шума

Следующим шагом является включение тестируемого устройства в разрыв между источником шума и прибором и повторное измерение методом $Y$ - фактора. Наша система теперь состоит из тестируемого устройства (первый каскад) и прибора (второй каскад), как показано на рисунке 3.

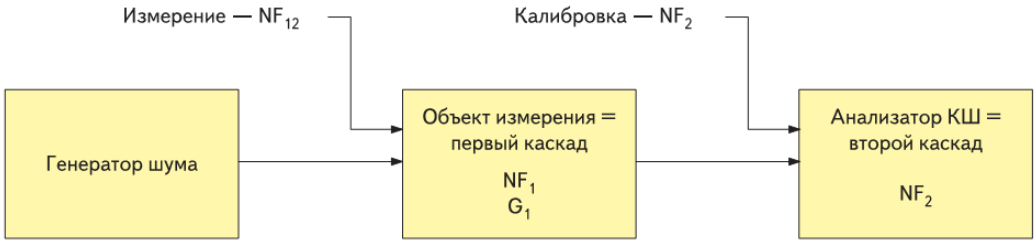



Рис.3 – Структурная схема включения объекта измерения для измерения коэффициента шума

Суммарный $Y$ - фактор системы определяется как:

$$Y_{12} = \frac{P_{12}^{ON}}{P_{12}^{OFF}}.$$

Аналогично уравнению (Y-фактор) общая температура шума системы $T_{12}$ равна:

$$T_{12} = \frac{T_S^{ON} - Y_{12} T_S^{OFF}}{Y_{12} - 1}.$$

Поскольку прибор теперь знает значения $P_{12}^{ON}$ и $P_{12}^{OFF}$, а также прежде сохраненные значения $P_2^{ON}$ и $P_2^{OFF}$, он может высчитать усиление тестируемого устройства:

$$G_1 = \frac{P_{12}^{ON} - P_{12}^{OFF}}{P_2^{ON} - P_2^{OFF}}.$$

Обычно значение $G_1$ отображается прибором в дБ:

$$G_1(\partial Б) = 10 \lg G_1.$$

Таким образом, определяются значения $T_2$, $T_{12}$ и $G_1$. Следовательно, температура шума первого каскада равна:

$$T_1 = \frac{T_{12} - T_2}{G_1}.$$

Теперь у прибора есть вся информация, которая необходима для вычисления температуры шума первого каскада $T_1$, т. е. температуры шума тестируемого устройства с учетом коррекции коэффициента шума самого прибора.

Большинство автоматических анализаторов коэффициента шума отображают результаты измерения либо в виде температуры шума $T(K)$, фактора шума $F$ (отношение, разы) или в виде коэффициента шума $NF$ (дБ). Как правило, автоматические анализаторы коэффициента шума могут выводить на экран не только численные показания коэффициента шума и усиления, но и панорамные графики, обеспечивающие лучшую визуализацию результатов, что существенно упрощает настройку и тестирование приемного устройства в заданной полосе частот.

Список использованных источников:

1. Friis, H. T. Noise Figures of Radio Receivers. Proc. of the IRE, July, 1944.
2. Agilent. Fundamentals of RF and Microwave Noise Figure Measurements. Application note 57-1.
3. Agilent. Noise Figure Measurement Accuracy – The Y-Factor Method. Application note 57-2.
4. Vondran, D. Vector Corrected Noise Figure Measurements // Microwave Journal, March 1999.
5. Anritsu. Noise Figure Accuracy. Application Note No. 11410-00227.

# КОМПЬЮТЕРНАЯ СИСТЕМА ДЛЯ ИССЛЕДОВАНИЯ ХАРАКТЕРИСТИК ТРАНЗИСТОРОВ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Гавриченко А.А.*
*Ревин В.Т. – кандидат техн. наук, доцент*

В данной работе представлено описание компьютерной системы исследования входной и выходной характеристик биполярного транзистора, которое включает краткое описание инструментов и методики измерения.

Разработанная система представляет собой виртуальное средство измерения предназначенное для исследования характеристик транзисторов, представляющее собой персональный компьютер, снабженный дополнительно различными измерительными модулями (например многофункциональной платой ввода-вывода информации) и специальным прикладным программным обеспечением. ВП позволяет автоматизировать операции по сбору, обработке и представлению измерительной информации, имеет удобный пользовательский интерфейс, а его программные и аппаратные средства поддерживают реализацию функций, присущих традиционному средству измерений, и обеспечивают представление результатов на экране монитора в удобной для пользователя форме [1]. PCI, PCI Express, PXI, PXI Express, USB

Для создания компьютерной системы были использованы аппаратные и программные компоненты, разработанные и изготовленные фирмой National Instruments: NI 6251; NI SCB-68 E Series, NI LabVIEW 2015.

NI 6251 - SCB-68 E Series – это экранированный разъемный блок ввода/вывода (далее - коннекторный блок) для устройства сбора данных (DAQ) с 68-ю клеммам. LabVIEW (англ. Laboratory Virtual Instrumentation Engineering Workbench) - среда разработки и платформа для выполнения программ, созданных на графическом языке программирования «G» фирмы National Instruments.

В качестве исследуемого транзистора взят корпусной транзистор типа КТ 306Б, подключенный по схеме с общим эмиттером. Входная вольт-амперная характеристика (далее - ВАХ) выражает связь между током базы $I_б$, являющимся для этой схемы входным, и напряжением между эмиттером и базой $U_{бэ}$ (при постоянном значении напряжения между коллектором и эмиттером). Для измерения входной ВАХ с цифро-аналогового преобразователя (ЦАП) коннекторного блока подается управляющее напряжение на базу транзистора. В свою очередь через аналого-цифровой преобразователь (АЦП) коннекторного блока измеряется ток базы и напряжение между эмиттером и базой. Полученные значения выводятся на график, который представлен на рисунке 1. Выходной вольт-амперная характеристика транзистора называется зависимость коллекторного тока $I_к$ от напряжения между коллектором и эмиттером $U_{кэ}$. снятая при неизменном токе базы. Семейство выходных ВАХ, полученных экспериментальным методом, представлено на рисунке 2.

Экспериментальные результаты измерений хорошо согласуются с теоретической базой.


Рисунок 1 – Входная ВАХ транзистора

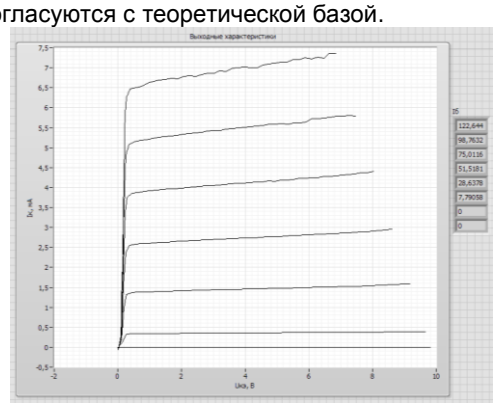



Рисунок 2 – Семейство выходных ВАХ транзистора

Список использованных источников

1. Батоврин В.К., Бессонов А.С., Мошкин В.В LabVIEW - практикум по электронике и микропроцессорной технике, 2005.

# ОСОБЕННОСТИ ИЗМЕРЕНИЯ ПАРАМЕТРОВ СИГНАЛОВ И УСТРОЙСТВ В ДИАПАЗОНЕ ЧАСТОТ 178-220 ГГЦ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Боровская М.А.*

*Гусинский А.В. – к-т. техн. наук, доцент*

Развитие средств точного позиционирования беспилотных автомобилей и летательных аппаратов, обследования и лечение организма человека, улучшение продуктивности сельскохозяйственных культур, повышение точности метеорологических и космических исследований вызвало бурное освоение более высокочастотных диапазонов электромагнитного излучения. Разработка, производство и эксплуатация сложных радиотехнических систем и комплексов, работающих в субмиллиметровом диапазоне длин волн, требуют соответствующего метрологического обеспечения, для осуществления которого требуется вся номенклатура приборов, начиная от генераторов и измерителей мощности и заканчивая скалярными и векторными анализаторами СВЧ-цепей.

К числу наиболее эффективных измерительных средств, предназначенных для инструментального анализа параметров СВЧ-устройств, относятся скалярные и векторные анализаторы СВЧ-цепей, представляющие современные высокопроизводительные информационно-измерительные системы. С их помощью можно провести измерения -параметров, связывающих падающие на $i$-входы СВЧ-устройства волны $a_i$ и отраженные (рассеянные) от них волны $b_i$, где $i = 1,2,\dots, n$ ($n$-число пар полюсов эквивалентного СВЧ-устройству $2n$-полюсника). Связь падающих и отраженных волн в общем случае может быть выражена в виде:

$$b_i(\omega) = \sum_{k=1}^{n} S_{ik}(\omega)\, a_k(\omega)$$

где $k = 1,2,\dots,n$, или в матричном виде

$$[b] = [S][a].$$

В общем случае -параметры являются комплексными величинами, зависящими от частоты. Основными «цепными» параметрами СВЧ-устройства, подлежащими измерению, являются: модули $|S_{ii}|$ и фазы $argS_{ii}$ коэффициентов отражения, модули $|S_{ik}|$ и фазы $argS_{ik}$ коэффициентов передачи. А также производные от них параметры: коэффициент стоячей волны по напряжению -го плеча

$$K_i = \frac{1+|S_{ii}|}{1-|S_{ii}|},$$

вносимое ослабление между плечами $i-k$

$$A_{ik} = 20\lg|S_{ki}|,$$

невзаимный фазовый сдвиг между плечами $i-k$

$$a_{ik} = argS_{ki} - argS_{ik}.$$

Разработка и использование скалярных и векторных анализаторов цепей (ВАЦ) в субмиллиметровом диапазоне волн требуют учета факторов, специфических для этого диапазона волн и оказывающих существенное влияние на технические и метрологические характеристики таких ВАЦ. Во-первых, к таким факторам следует отнести большие потери энергии в линиях передачи. Как показывают результаты расчетов, для субмиллиметрового диапазона длин волн потери мощности в одномодовых металлических волноводах достигают 12 дБ/м при длине волны $\lambda = 1$ мм. Очевидно, что для компенсации этих потерь необходим источник испытательных сигналов с большим уровнем выходной мощности. Выпускаемые промышленностью ГКЧ обычно имеют средний уровень выходной мощности в пределах 5-10 мВт. При среднем значении ослабления в СВЧ-тракте (15-25 дБ) и необходимом пределе измерения ослабления 60-80 дБ этого уровня выходной мощности ГКЧ явно недостаточно. Для обеспечения требуемого предела измерения необходимо уменьшить ослабление, вносимое СВЧ-трактом анализатора цепей, что может быть осуществлено путем лучшего согласования составляющих элементов тракта и/или его существенного конструктивного упрощения.

Во-вторых, с уменьшением длины волны значительно возрастают фазовые погрешности измерений, обусловленные неповторяемостью устанавливаемого значения частоты при измерении и калибровке, а также от измерения к измерению и из-за нестабильности частоты. В общем случае удобнее назвать их «погрешностью из-за неопределенности значения частоты». Эта погрешность может иметь две составляющие: первую, связанную с неопределенностью электрической длины объекта измерения, и вторую, зависящую от частотной характеристики измеряемого параметра. Количественная оценка абсолютной погрешности измерения фазового сдвига показывает, что при относительной погрешности установки частот $\delta \mathrm{f} = \pm 0{,}002$, характерной для большинства ГКЧ, при длине отрезков волновода 10 мм, значение этой погрешности на частоте 100 ГГц достигает $\Delta \mathrm{up} = \pm 3{,}0$ град. С увеличением длины отрезка волновода погрешность линейно возрастает.

Третья проблема связана с точностью изготовления каналов волноводных элементов измерительного тракта и калибровочных мер в процессе их производства. Проводимые исследования показывают, что фактические размеры каналов волноводов, как правило, превышают номинальные значения и такая «сверхразмерность» имеет тенденцию к увеличению с ростом частоты, особенно заметную на частотах выше 90 ГГц. Это может привести к значительным фазовым и амплитудным погрешностям в результатах измерений, если в память анализатора цепей вводится в качестве постоянной величины номинальная расчётная частота среза волновода, а не фактически измеренная, которая может на несколько гигагерц

отличаться от номинальной. Говоря о точности изготовления каналов волноводов в коротковолновой части миллиметрового диапазона ($\lambda \leq 2$ мм), необходимо отметить и важность соблюдения формы апертуры волновода, в частности, во фланцах, так как наличие деформаций, скруглений углов, других искажений контура и т.п. отрицательно сказывается на результатах измерений.

В-четвёртых, очень серьёзной проблемой, от решения которой во многом зависит достоверность результатов измерений на миллиметровых волнах, является проблема волноводных фланцевых соединений, проблема допусков на основные присоединительные размеры фланцев. Исследования влияния на качество согласования смещения и перекосов волноводов из-за допусков на присоединительные размеры фланцев показали, что допуски на размеры штифтов и штифтовых отверстий фланцев в диапазонах частот выше 100 ГГц должны быть обратны частоте:

(допуск на частоте f ГГц)=(допуск для волновода WR-10)×(100/f)

В соответствии с данным соотношением на частоте 200 ГГЦ максимально допустимое смещение (перекос) фланца может быть 0,08 мм, что на практике трудновыполнимо при использовании традиционной технологии механической обработки фланцев.

Все это накладывает определенные условия и ограничения на выбор соответствующего метода измерения и конструкции ВАЦ, обеспечивающих высокие метрологические характеристики. Вследствие чего возникают трудности в практической реализации и разработке анализаторов цепей в диапазоне частот 178-220 ГГц. Проведенный патентный поиск, показал, что на данный момент в мире не существует ни скалярного ни векторного анализатора цепей, охватывающих диапазон частот 178-220 ГГц. Данную измерительную задачу можно решить с помощью частотных расширителей различных зарубежных фирм (Oleson Microwave Labs, Virginia Diodes Inc., Farran Microwave), перекрывающих диапазон частот до 1000 ГГц и совместимых с любым из продаваемых в настоящее время микроволновых ВАЦ.

На рисунках 1 и 2 приведены упрощенные блок-схемы частотных расширительных модулей V05VNA2-T/R и V05VNA2-T фирмы Oleson Microwave Labs:

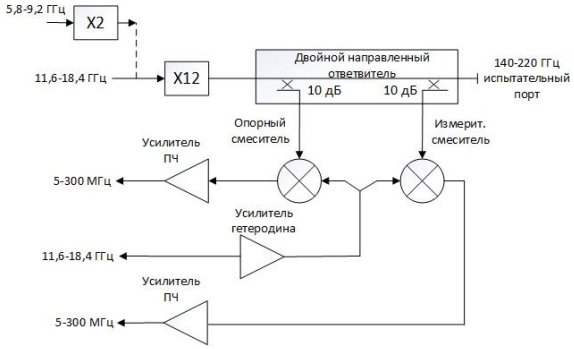



Рис. 1 – Упрощенная блок-схема V05VNA2-T/R

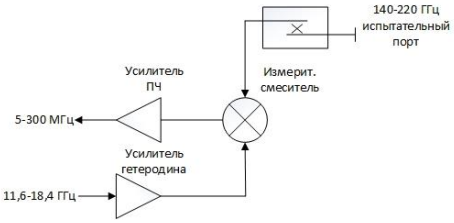



Рис. 2 – Упрощенная блок-схема V05VNA2-T

Модуль V05VNA2-T/R включает в себя умножитель на двенадцатой гармонике, который действует как системный источник РЧ-сигнала. Входная частота меняется от 11,6 до 18,4 ГГц. При использовании синтезаторов диапазона до 10 ГГц возможно применение недорогого добавочного удвоителя (x2) к умножительной цепочке. Измерительная секция V05VNA2-T/R содержит двойной направленный ответвитель, который обеспечивает получение прямого связанного сигнала (-10 дБ) для опорного понижающего преобразователя и обратного связанного сигнала (-10 дБ), поступающего к измерительному понижающему преобразователю. Ответвитель имеет направленность 35 дБ. Используемые смесители накачиваются субгармонически сигналом гетеродина частотой от 11,6 до 18,4 ГГц. Уровень этого сигнала поддерживается постоянным для каждого смесителя усилителем гетеродина с ограничением для обеспечения хороших характеристик в полной частотной полосе. Смесители представляют собой два диода в единой балансной конструкции с ПЧ в пределах между 5 и 300 МГц в зависимости от того, какая измерительная система ВАЦ используется. Коэффициент шума ПЧ составляет менее 1,7 дБ, а усиление ПЧ устанавливается в зависимости от используемой системы ВАЦ.

Модуль V05VNA2-T использует единственный понижающий преобразователь, идентичный с используемым в T/R-модуле. Дополнительно для уменьшения входных потерь на отражение Т-модуля (для улучшения согласования нагрузки измерительной системы) применяется ответвитель типа аттенюатора с максимально плоской (равномерной) характеристикой переходного ослабления.

Таким образом, в связи с перечисленными особенностями проведения измерений в субмиллиметровом диапазоне волн разработка и изготовление скалярного и векторного анализатора цепей в диапазоне 178-220 ГГц является трудноосуществимой задачей, которая на данный момент не реализована. Для инструментального анализа параметров СВЧ-устройств предлагается использовать частотные расширители, перекрывающие рассматриваемый диапазон частот и имеющие высокие метрологические характеристики.

Список использованных источников:

1. Гусинский,А.В. Векторные анализаторы цепей миллиметровых волн:монография. В 3 ч. Ч.3 (кн.2). Принципы построения и анализ схем векторных анализаторов цепей / А.В.Гусинский, Г.А. Шаров, А.М. Кострикин. – Минск: БГУИР, 2008. – с.241-507.
2. ГОСТ 13317-89. Элементы соединения СВЧ трактов радиоизмерительных приборов. Присоединительные размеры.

# ТНПА В ОБЛАСТИ НОРМИРОВАНИЯ ПОКАЗАТЕЛЕЙ КАЧЕСТВА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ. ОСНОВНЫЕ ПОКАЗАТЕЛИ КАЧЕСТВА ЭЛЕКТРОЭНЕРГИИ И ИЗМЕРИТЕЛЬНОЕ ОБОРУДОВАНИЕ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Янченко В.С.*

*Гурский А.Л. – д-р физ.-мат. наук, профессор*

Одним из универсальных видов продукции является электрическая энергия. Параметры качества электроэнергии непосредственно или косвенно влияют на качество продукции и услуг, на надежность, безопасность и сроки службы производственного и бытового оборудования, на условия окружающей среды. Таким образом, отклонения параметров качества электрической энергии от нормируемых значений приводят к значительным убыткам, как в промышленности, так и в бытовом секторе. Поэтому в настоящее время актуальной стала проблема оценки качества электроэнергии.

Для поддержания системы электроснабжения на необходимом уровне, система должна быть метрологически обеспечена. Метрологическое обеспечение включает такое основы как: научную, организационную, правовую, техническую. Научная основа подразумевает развитие метрологии как науки об измерениях, методах и средствах обеспечения их единства, способах достижения требуемой точности. Организационную основу представляет метрологическая служба. Правовая основа включает в себя комплексы общих правил, требований и норм, а также другие вопросы (нуждающиеся в регламентации со стороны государства), направленные на обеспечение единства измерений и единообразия средств измерений в республике. В тоже время техническая основа – это система эталонов, система передачи размеров единиц, система разработки и выпуска, система обязательного метрологического контроля, стандартных образцов, а также система стандартных справочных данных.

В Республике Беларусь вопросы в области нормирования показателей качества электрической энергии регламентированы: ТКП 183.1-2009 и ТКП 183.2-2009 Содержащие методические указания по контролю и анализу качества электрической энергии в системах электроснабжения общего назначения, а также ГОСТ 32144-2013 Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения, в которых устанавливаются требования к качеству электроэнергии, погрешностям измерений и интервалам усреднения, которые должны реализовываться в приборах контроля при измерениях показателей и их обработке. Данный ГОСТ включает как показатели КЭ установившегося режима работы электрооборудования, так и показатели КЭ, характеризующие кратковременные помехи.

На сегодняшний день в Государственный реестр Республики Беларуси внесен широкий спектр приборов различных производителей, позволяющих проводить измерения ПКЭЭ. В РБ наиболее популярны следующие: устройство контроля параметров качества электрической энергии УК-1 и УК-2, «Энергомонитор 3.3», «Энергомонитор 3.3Т», анализаторы «Elspec» серии G4500, G4400, а также анализаторы качества сети серии 43B (однофазные), 434, 435 (трехфазные), производимые фирмой «Fluke Corporation».

Для метрологического контроля приборов контроля ПКЭЭ наиболее часто используются следующие эталонные средства измерений: калибратор переменного тока «Ресурс-К2», производства ООО НПП «Энерготехника» (Россия), калибратор многофункциональный Fluke 5520A с модулем PQ (производства фирмы «Fluke Corporation», США) и калибратор многофункциональный Fluke 6130A (производства фирмы «Fluke Corporation», США). Данные средства контроля метрологически обеспечены на территории Республики Беларусь и прослеживаются до национальных эталонов:

Национальный эталон единиц: времени - секунды, частоты - герца и шкалы времени № НЭ РБ 1-95;

Национальный эталон единицы напряжения переменного тока в диапазоне частот 10 Гц – 2 ГГц № НЭ РБ 5-01;

Национальный эталон единицы напряжения – вольта
№ НЭ РБ 10-02;

Национальный эталон единицы электрической мощности
№ НЭ РБ 14-04;

Национальный эталон единицы электрической ёмкости
№ НЭ РБ 19-10.

Тема контроля показателей качества электрической энергии становиться все более востребованной в связи с мировым ростом количества электропроизводящих субъектов, использующих солнечные панели, ветряки и другие мобильные станции. Данные субъекты широко распределены географически и являются как потребителями электроэнергии так и производителями. Таким образом возникает спрос на автоматизированные системы оценки качества электрической энергии как отданной в сеть, так и потребленной, также появляется спрос на системы логистики, оптимизации внутрисуточного потребления, экономической оптимизации энергетического снабжения предприятий и организаций.

# СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА: УПРАВЛЕНИЕ ОБОРУДОВАНИЕМ ДЛЯ МОНИТОРИНГА И ИЗМЕРЕНИЙ

*Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь*

*Кунцевич В.В. гр. 5М0911*

*Ляльков С.В. – к.т.н., доцент*

Активное внедрение радиоэлектроники во все сферы человеческой деятельности неизбежно сопровождается расширением потребности в электрорадиотехнических измерениях. Трудно представить современные сложные радиоэлектронные изделия, которые можно разрабатывать и эксплуатировать без проведения измерений, необходимых для оценивания их качества и технического состояния. [1]

Сегодня предприятия, желающие выпускать качественную продукцию для внешнего и внутреннего рынка, а также устанавливать долгосрочные и взаимовыгодные отношения со своими потребителями, считают своим долгом иметь на своем предприятии систему менеджмента качества (СМК).

СМК – это составная часть общей системы управления предприятием, которая призвана обеспечить стабильность качества продукции или услуг. Она разрабатывается с учетом конкретной деятельности предприятия и должна охватывать все стадии жизненного цикла продукции или предоставления услуги, а также обеспечивать участие в управлении качеством всех работников предприятия.

Мониторинг означает слежение, надзор, держание под наблюдением с использованием оборудования для наблюдения; он может включать в себя проводимые через определенные интервалы времени измерения или испытания, особенно с целью регулирования или управления.

Измерение - совокупность операций, выполняемых для определения количественного значения величины. [2]

Процесс управление оборудованием является одним из основных элементов системы управления качеством. Правильное управление оборудованием необходимо для обеспечения точных, надежных и своевременных результатов.

Цель процесса: обеспечение управления оборудованием для подтверждения соответствия процессов и их результатов установленным требованиям.

Для управления процессом необходимо установить требования:

- к учету измерительного, испытательного и контрольного оборудования и документации на них;
- вводу в эксплуатацию, маркировке приобретенного измерительного, контрольного и испытательного оборудования;
- подтверждению пригодности измерительного оборудования
- эксплуатации, хранению, консервации измерительного и испытательного оборудования;
- техническому обслуживанию и ремонту измерительного и испытательного оборудования;
- порядку списания средств измерений;
- отчетным документам
- управлению компьютерными программными средствами
- анализ результативности СИ.

Требования к процессу управления оборудованием для мониторинга и измерений применяют наряду с метрологическими правилами и нормами, имеющими обязательную силу на территории Республики Беларусь, которые содержатся в нормативных документах по обеспечению единства измерений, утверждаемых Госстандартом Республики Беларусь в соответствии с Законом Республики Беларусь «Об обеспечении единства измерений».

Для осуществления данного процесса и управления им, необходима разработка Инструкции по управлению оборудованием для мониторинга и измерений, задача которой обеспечение единства измерений при разработке, изготовлении, испытаниях, обслуживании и установление единого порядка выбора, эксплуатации и хранении, а так же поверки, калибровки и аттестации оборудования.

Список использованных источников

1. Метрология и электрорадиоизмерения в телекоммуникационных системах. Учебное пособие / под общ. Ред. Б.Н. Тихонова. – М. : Горячая линия – Телеком, 2007. – 374 с.
2. [Электронный ресурс] – Режим доступа : http://metrologu.ru/info/metrologia/teoria/terminologia.html.

# ИСХОДНЫЙ ЭТАЛОН ЕДИНИЦ КОЭФФИЦИЕНТА И УГЛА МАСШТАБНОГО ПРЕОБРАЗОВАНИЯ СИНУСОИДАЛЬНОГО НАПРЯЖЕНИЯ И ТОКА

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

Магистрант гр. 5М0911 Валенда А. Г.

Белошицкий А. П. - канд. техн. наук, доцент

Повышение точности измерений качественных и количественных показателей электроэнергии всегда являлось приоритетной задачей метрологии и измерительной техники, поскольку результаты этих измерений служат основанием для финансовых расчетов между производителем и потребителем энергии, а также позволяют оценить экономическую эффективность технологических процессов и оборудования, управлять ими или создавать новые энергосберегающие технологии.

Решение этой задачи обеспечивается с помощью исходного эталона единиц коэффициента и угла масштабного преобразования синусоидального напряжения и тока на частоте 50 Гц, который создан и эксплуатируется в Белорусском государственном институте метрологии (БелГИМ). Исходный эталон применяется при метрологическом контроле измерительных трансформаторов тока и напряжения на месте их эксплуатации и позволяет проводить работы по созданию более современной нормативной и методической базы, а также существенно повысить достоверность измерений при поверке и калибровке трансформаторов.

В состав эталона входят: компаратор СА507, прибор сравнения КНТ-05А, магазин нагрузок СА5055, магазин нагрузок МН1200/100, эталон коэффициента масштабного преобразования электрического напряжения КТГ-110-I, эталон коэффициента масштабного преобразования электрического напряжения НОМО-15-I, магазин нагрузок СА5018/5, магазин нагрузок СА5018/1, трансформатор тока ТС(п)-08, трансформатор тока ТС(п)-010, трансформатор тока ИТТ-3000.5, вольтметр универсальный В7-54/3.

Эталон имеет следующие метрологические характеристики: в режиме измерения напряжения переменного тока частотой 50 Гц от 3/√3 до 110/√3 кВ, класс точности 0,1; в режиме измерения силы переменного тока от 0,5 до 5000 А при cos φ = 0,8÷1, класс точности 0,01.

В докладе приводятся результаты экспериментальных исследований метрологических характеристик эталона при различных номинальных значениях силы тока, напряжения и нагрузки.

При проведении исследований метрологических характеристик эталонных масштабных преобразователей использовались: прибор сравнения КНТ-05А, магазин нагрузок СА5055, магазин нагрузок МН1200/100, магазин нагрузок СА5018/5, трансформатор тока ИТТ-3000.5, ТС(п)-08 и трансформаторы напряжения эталонные ТН(п) – 10, НОМО-15-I.

Результаты исследований при номинальном токе 1000//5 А и значениях нагрузки (Sном), равных 100 и 25 % от номинальной приведены на рисунках 1 и 2.

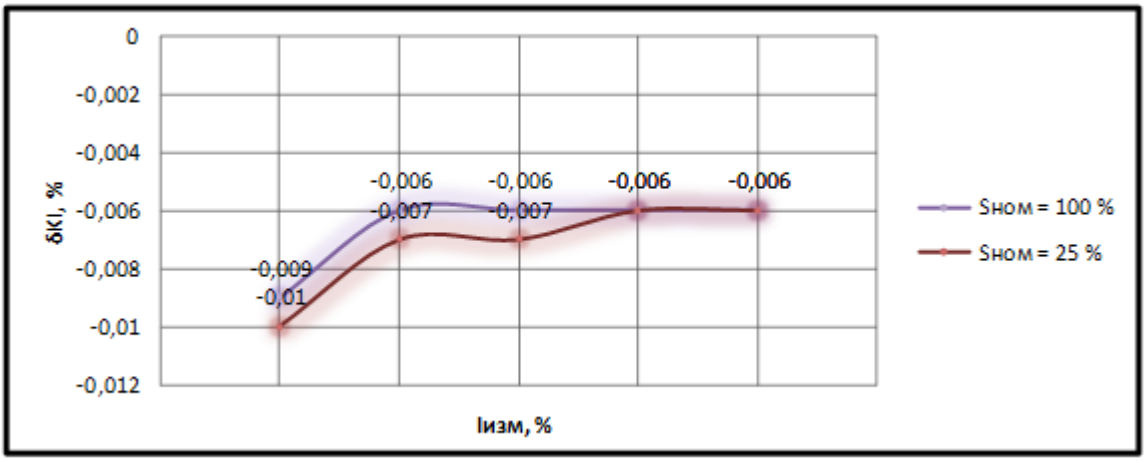



Рисунок 1 - Относительная токовая погрешность

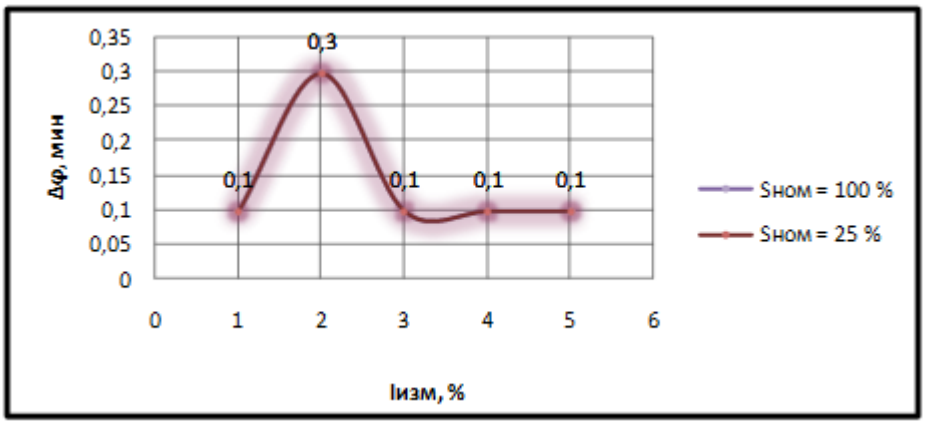



Рисунок 2 - Абсолютная угловая погрешность

Результаты исследований при номинальном напряжении 10000//100 В и значениях нагрузки (Sном), равных 100 и 25 % от номинальной приведены на рисунках 3 и 4.

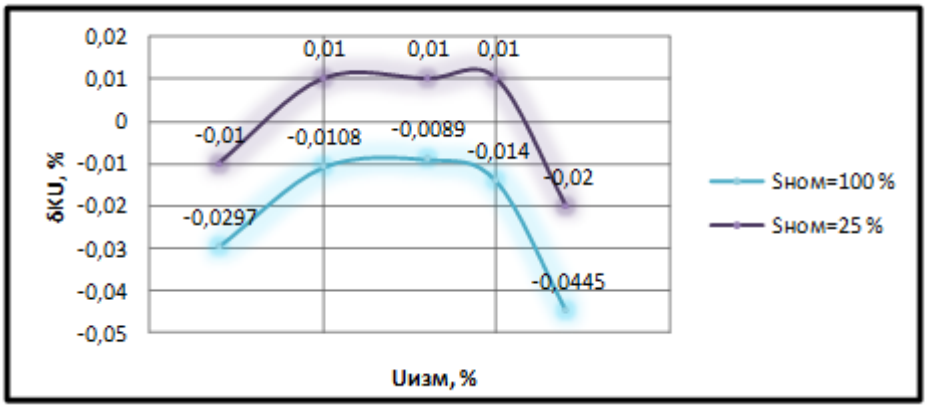



Рисунок 3 - Относительная погрешность трансформации напряжения

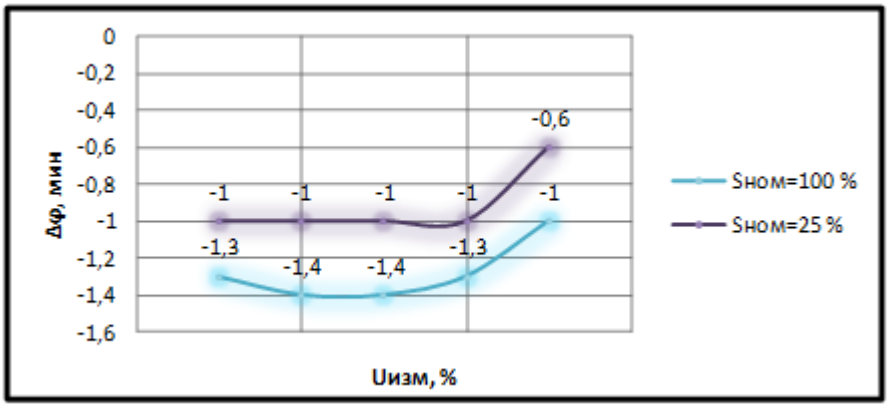



Рисунок 4 - Абсолютная угловая погрешность

Проведенные исследования показывают необходимость дальнейших усовершенствований эталона: повышения точностных характеристик, расширения диапазона измерений и более глубокой автоматизации. Это становится особо актуальным в связи с резким многократным ростом потребления электроэнергии, что приводит к необходимости значительного повышения точностных параметров приборов учета и непосредственно связанных с ними трансформаторов тока и напряжения.

# НАЦИОНАЛЬНЫЙ ЭТАЛОН ЕДИНИЦЫ ЭЛЕКТРИЧЕСКОЙ МОЩНОСТИ И ОСНОВНЫЕ НАПРАВЛЕНИЯ ЕГО МОДЕРНИЗАЦИИ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Арловская Л. С..*

*Белошицкий А. П. – к-т. техн. наук, доцент*

В последнее время предъявляются более жесткие требования к точности измерения электрических величин, а также обеспечения международного признания размеров величин электрической мощности и энергии. В связи с этим актуальными являются задачи разработки эталонных средств измерения и исследования их метрологических характеристик.

В Белорусском государственном институте метрологии (БелГИМ) создан и используется Национальный эталон единицы электрической мощности, в состав которого входят: источник токов и напряжений Calsource 200; калибратор Fluke 5520A-PQ; калибратор Fluke 6100A; компаратор электрической мощности однофазный К2005; компаратор электрической мощности трехфазный К2006; измеритель Calport 300; измеритель токов и напряжений PWS 3.3; мера электрической мощности RD 33-211.

Национальный эталон единицы электрической мощности – это комплекс средств измерений, обеспечивающий воспроизведение и хранение единицы электрической мощности с целью передачи ее размера нижестоящим по поверочной схеме эталонным средствам измерений.

На рисунке представлена структурная схема Национального эталона единицы электрической мощности.

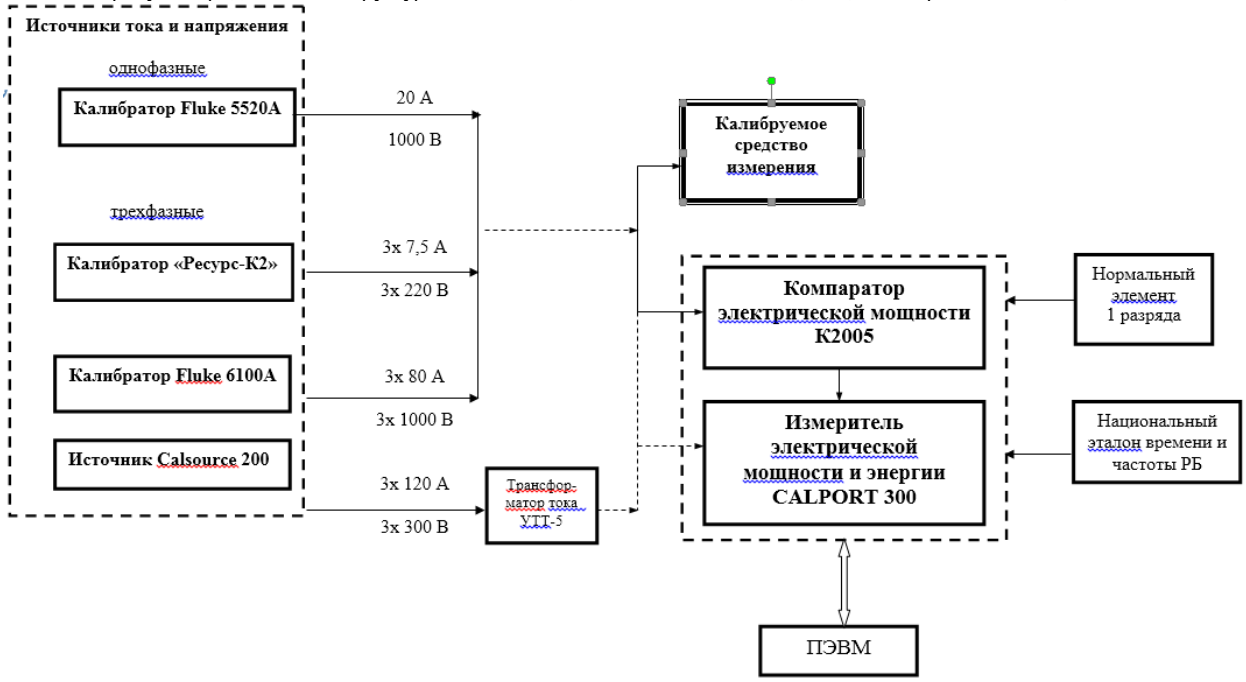



Рисунок – Структурная схема Национального эталона единицы электрической мощности

В состав эталона входят однофазные и трехфазные источники токов и напряжений, представленные в основном калибраторами, компаратор и измеритель мощности, персональный компьютер. калибруемое средство измерения.

МЕТРОЛОГИЧЕСКИЕ ХАРАКТЕРИСТИКИ ЭТАЛОНА

Диапазон воспроизведения активной, реактивной и полной мощности, составляет от $29 \cdot 10^{-9}$ до 1000000 Вт в диапазоне частот от 10 Гц до 500 кГц.

Диапазон воспроизведения напряжения составляет от 0,001 до 1000 В в диапазоне частот от 10 Гц до 500 кГц.

Диапазон воспроизведения силы тока составляет от 29 мкА до 1000 А в диапазоне частот от 10 Гц до 30 кГц.

Диапазон измерения активной, реактивной и полной мощности составляет от 0,03 до 76800 Вт в диапазоне частот от 15 до 70 Гц.

Диапазон измерения напряжения составляет от 5 до 600 В в диапазоне частот от 15 до 70 Гц.

Диапазон измерения силы тока составляет от 1 мА до 200 А в диапазоне частот от 15 до 70 Гц.

Эталон обеспечивает воспроизведение и измерение единицы величины со следующими характеристиками точности:

неисключенная систематическая погрешность не более $1 \cdot 10^{-4}$,

случайная погрешность от $1 \cdot 10^{-4}$ до $1 \cdot 10^{-3}$,

В докладе приводятся результаты исследования точностных характеристик Национального эталона единицы электрической мощности. В результате этих исследований установлено, что:

среднеквадратическое отклонение результата измерения напряжения не превышает 0,0003 %.

среднеквадратическое отклонение результата измерения силы тока не превышает 0,0004 %.

среднеквадратическое отклонение результата измерения активной мощности не превышает 0,0008 %.

стабильность трехфазного источника Calsource 200 №30079 не превышает значений:

0,0003 % при воспроизведении напряжения;

0,0010 % при воспроизведении силы тока;

0,0011 % при воспроизведении активной мощности.

Полученные результаты исследования Национального эталона единицы электрической мощности позволяют использовать эталон обеспечения:

- повышения точности измерения и повышения качества метрологического обслуживания;
- единства измерений, улучшение и совершенствование точностных характеристик вновь разрабатываемых СИ электрической мощности и подтверждение метрологических характеристик СИ электрической мощности, поступающих в Республику Беларусь;
- развитие приборостроения, проведение научно-исследовательских работ, направленных на повышение эффективного использования энергетических ресурсов;
- возможность калибровки и поверки эталонных СИ электрической мощности и энергии класса точности 0,05 на территории Республики Беларусь;
- подтверждение наилучших возможностей при калибровке, возможность участия в дополнительных сличениях и признания результатов калибровки на мировом уровне.

С целью улучшения характеристик эталона и автоматизации поверочных и калибровочных работ проводится его модернизация. В докладе представлены возможные способы ее реализации.

# КАЛИБРОВКА ИСПЫТАТЕЛЬНОЙ КАМЕРЫ GTEM ТИПА И ОСНОВНЫЕ НАПРАЛЕНИЯ ЕЕ АВТОМАТИЗАЦИИ

*Белорусский государственный университет информатики и радиоэлектроники*
*Г. Минск, Республика Беларусь*

*Герасимова А. А.*

*Белошицкий А. П. – канд. тех. наук, доцент*

Учитывая развитие технологий в сфере создания радиоэлектронных средств с значительным увеличением количества выпуска и использования радиооборудования проблема электромагнитной совместимости (ЭМС) становится все более острой и актуальной. Для обеспечения ЭМС необходимо определять уровни электромагнитного излучения испытываемого оборудования и таким образом оценивать влияние этого оборудования на работоспособность окружающей аппаратуры.

При измерениях и испытаниях радиотехнического оборудования, излучающего радиоволны в свободное пространство, широко применяются безэховые камеры (БЭК). Во многих случаях испытания радиоэлектронных средств в таких камерах позволяет резко сократить и полностью исключить натурные испытания, что приводит к значительной экономии средств, а главное – времени разработки сложной радиотехнической аппаратуры. Для практического использования БЭК в метрологической практике необходимо определить их метрологические и электромагнитные характеристики, что возможно при калибровке БЭК.

Одной из разновидностей таких камер является *GTEM*-камера, которая представляет собой ТЕМ-волновод с верхней границей частоты, захватывающей гигагерцовый диапазон. Это недорогое альтернативное устройство для измерений, как параметров излучения, так и устойчивости к излучению.

В докладе рассматривается методика калибровки *GTEM*-камеры и способ ее автоматизации.

Методика калибровки (МК) распространяется на *GTEM*-камеру, предназначенную для испытаний на ЭМС и измерений излучаемого уровня мощности электромагнитного поля и напряженность электрического поля в полосе частот от 30 МГц до 1 ГГц от малогабаритного радиоэлектронного оборудования. Под ним понимается оборудование, размеры которого не превышают объем рабочий области камеры. Важнейшими параметрами *GTEM*-камеры являются: коэффициент затухания ($K_{kp}$), который определяет величину характеризующую степень ослабления сигнала, излучаемого объектом испытаний, в рабочей области *GTEM*-камеры на определенной частоте и напряженность электрического поля ($E$) в данной точке рабочей области камеры. При калибровке камеры определяются действительные значения указанных параметров и сопровождающие их неопределенности измерений с использованием метода косвенных.

Математическая модель измерения коэффициента затухания имеет следующий вид:

$$K_{kp} = (\alpha_f + \lambda_{\alpha f}) - (\alpha_{pf} + \lambda_{\alpha pf}) + \Delta_{поз}, \quad (1)$$

где $K_{kp}$ – коэффициент затухания, дБ;

$\alpha_f$ – уровень мощности, излучаемый эталонным генератором тестового сигнала при вертикальной поляризации на частоте f, определяемый на расстоянии трех метров от измерительной антенны по результатам калибровки генератора, дБм;

$\alpha_{pf}$ – измеренное значение уровня мощности на частоте $f$ на выходе камеры, дБм;

$\lambda_{\alpha f}$ – поправка обусловленная неопределенностью калибровочных характеристик генератора тестового сигнала, дБ;

$\lambda_{\alpha pf}$ – поправка, обусловленная неточностью измерения уровней мощности анализатором спектра, дБ;

$\Delta_{поз}$ – поправка на неточность установки генератора тестового сигнала в одну и ту же точку рабочей области, дБ.

Математическая модель измерения напряженности поля имеет следующий вид:

$$E = E_{CNE} + [(\beta(f_i) + \gamma_{\beta(f_i)}) - (\beta_{c(f_i)} + \gamma_{\beta_{c(f_i)}})] + \Delta_{поз}, \quad (2)$$

где $E$ – измеряемая напряженность поля, дБмкВ/м;

$E_{CNE}$ – напряженность поля, определяемая из калибровочных характеристик эталонного генератора тестового сигнала, дБмкВ/м;

$\beta(f_i)$ – измеренная амплитуда сигнала от испытуемого устройства на частоте $f_i$, дБмкВ;

$\beta_c(f_i)$ – измеренная амплитуда сигнала от генератора тестового сигнала на частоте $f_i$, дБмкВ;

$\gamma_{\beta f}$ – поправка обусловленная неточностью анализатора спектра при измерениях напряжения, дБ;

$\gamma_{\beta pf}$ – поправка обусловленная неопределенностью калибровочных характеристик генератора тестового сигнала при измерениях напряжения от испытуемого оборудования, дБ;

$\Delta_{поз}$ – поправка на неточность установки генератора тестового сигнала в одну и ту же точку рабочей области, дБ.

Для автоматизации процедуры калибровки был разработан алгоритм работы программы и ее скрипт. Интерфейс пользователя программного обеспечения *UniTesS* представляет собой совокупность базы данных, автоматизированного рабочего места, а также скриптового языка программирования *UniTesS Script Language*. Преимущество данного языка программирования заключается в его пошаговом выполнении команд без предварительной обработки программы, с помощью которых производится управление, используемыми в процессе калибровки генератором тестового сигнала, анализатором спектра, а также снимаются результаты измерений. Управление приборами и измерение контролируемых параметров производится автоматически под управлением персонального компьютера, с помощью которого также производится обработка результатов измерений с определением указанных метрологических характеристик и неопределенности их измерения. Процедура оформления протокола калибровки также автоматизирована.

Автоматизация калибровки позволяет значительно сократить время, затраченное на калибровку, ускорить вычисления и максимально возможно исключить человеческий фактор.

Список использованных источников:

1. Мицмахер, М. Ю., Торгованов В. А. Безэховые камеры СВЧ. – Москва : Радио и связь, 1982. – 128 с.

2. *IEC* 61000-4-20:2010 *Electromagnetic Compatibility* (*EMC*) – *Part* 4-20: *Testing and Measurement Techniques – Emission and Immunity Testing in Transverse Electromagnetic* (*TEM*) *Waveguides*.

*3. IEC* 61000-4-3:2006 *Radiated, Radio-frequency, Electromagnetic Field Immunity Test.*

# СИСТЕМА КВАНТОВОЙ КРИПТОГРАФИИ С ПОЛЯРИЗАЦИОННЫМ КОДИРОВАНИЕМ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Зеленин А.С.*

*Урядов В.Н. – к-т. техн. наук, доцент*

В волоконно-оптических системах передачи под поляризацией понимают ориентацию световой волны, которая сразу же нарушается, как только свет входит в оптоволокно. В настоящее время применение новых типов оптоволокна, сохраняющего состояние поляризации, определяет перспективы дальнейшего развития ВОСП.

В существующих системах квантовой криптографии дисперсия поляризационных мод деполяризует фотоны. По этой причине практическая реализация подобных систем затруднялась, а поляризационное кодирование не представлялось лучшим выбором при построении волоконно-оптических систем квантовой криптографии.

Таким образом, нестабильные во времени изменения поляризации требуют создания механизма активной компенсации поляризационных изменений, что уже накладывает на систему криптографии серьёзные ограничения (рисунок 1).

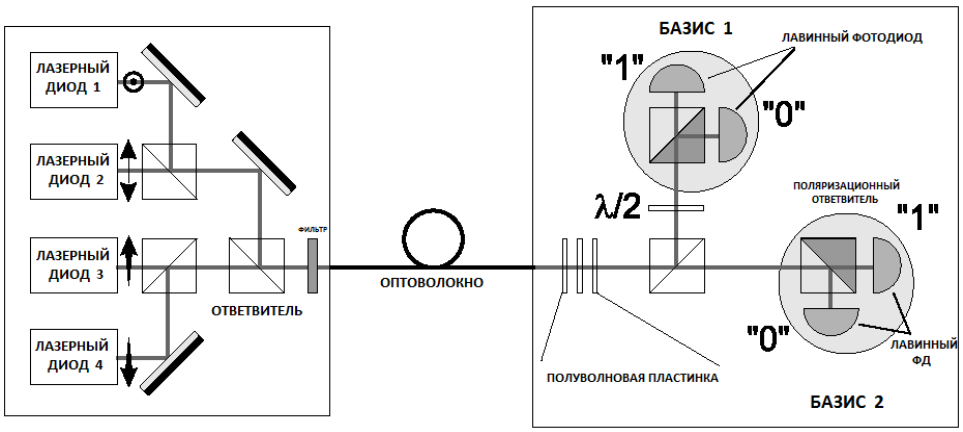



Рис. 1 – Структурная схема системы квантовой криптографии с механизмом компенсации поляризационных изменений

Импульсы при извлечении из волокна проходят через набор волновых пластинок, используемых для восстановления исходных поляризационных состояний путём компенсации трансформаций, внесённых волокном. Затем импульсы достигают ответвителя, осуществляющего выбор базиса. Переданные фотоны анализируются в базисе вертикальной/горизонтальной поляризации при помощи поляризационного ответвителя и двух счётчиков фотонов, далее фотоны анализируются вторым набором из поляризационного ответвителя и счётчиков фотонов.

Новое решение задачи о поляризационной балансировке лежит в области применения новых типов волокон с сохранением состояния поляризации и внедрения нового механизма компенсации (рисунок 2).

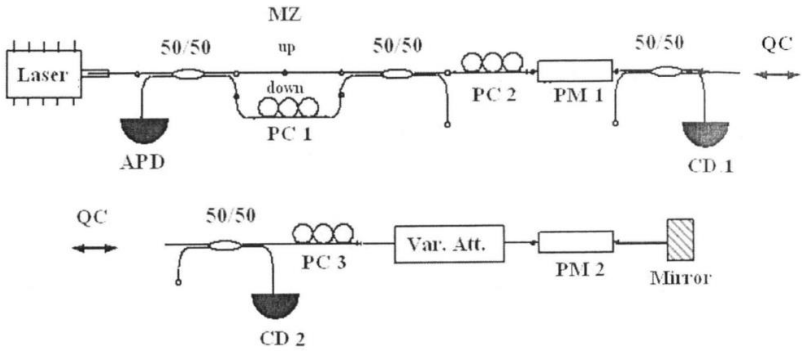



Рис. 2 – Структурная схема технического решения задачи о поляризационной балансировке

Сущность способа состоит в том, что для серии классических синхронизирующих лазерных импульсов на передающей-принимающей станции создают поляризационные состояния при помощи поляризационного контроллера в одном из плеч интерферометра и поляризационного контроллера на выходе интерферометра.

Они обеспечивают интерференционную балансировку интерферометра, серию однофотонных состояний после отражения от зеркала в преобразующей станции детектируют на передающей-принимающей станции и по полученной статистике фотоотсчетов вычисляют допустимую ошибку, которую затем сравнивают с определенным пороговым значением ошибки для получения известного только на передающей-принимающей и преобразующей станциях криптографического ключа.

В результате применения новых типов волокон с сохранением состояния поляризации, а также представленного механизма поляризационной балансировки расширяется диапазон возможных искажений поляризации лазерных и однофотонных импульсов при передаче ключей между передающей-принимающей и преобразующими станциями. Данное техническое решение, в свою очередь, даёт импульс к появлению нового поколения криптографических систем, призванного обеспечить конфиденциальность передаваемой информации, недостижимую для классических криптосистем.

Список использованных источников:

1. Martinelli M., A universal compensator for polarization changes induced by birefringence on a retracting beam. Opt. Commun., 1989, vol. 72, pp. 341-344.

2. Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, Hugo Zbinden. Quantum Cryptography, submitted to Reviews of Modern Physics, January 19, 2001.

3. Федеральный институт промышленной собственности: способ квантового кодирования и передачи криптографических ключей. [Электронный ресурс]. – Режим доступа: http://www1.fips.ru. – Дата доступа: 11.02.2016.

# МАТЕМАТИЧЕСКОЕ И ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Герострёнок Ю. А.*

*Тарченко Н.В. – к-т. техн. наук, доцент*

В настоящее время при проектировании, вводе в эксплуатацию и непосредственной эксплуатации сетей, предназначенных для передачи разнородного трафика, основной проблемой является обеспечение качества обслуживания, что обуславливает необходимость анализа моделей и методов исследования процессов функционирования сетей передачи данных (СПД).

Для оценки параметров качества необходимо выявить зависимость показателей качества от характеристик функционирования сети. Для этого рассматриваются две математические модели узла коммутации (УК) типа $M_r/M/V/K$ и $M_r/D/V/K$ с ограниченным буфером и конечными значениями производительности УК, на вход которого поступают простейшие Пуассоновские потоки, описываемые вероятностью поступления $P_i(t)$:

$$P_i(t)=\frac{(\lambda t)^i}{i!}e^{-\lambda t}.$$

Для модели УК типа $M_r/M/V/K$ определено стационарное распределение вероятностей состояний УК:

$$P_i(r,V)=\begin{cases}\frac{\rho'_R}{i!}P_0(R,V), 0\le i<V;\\ Q\left(\frac{\rho_r}{V}\right)^{i-V}\left(1-\frac{\rho_r}{V}\right)\left[1-\left(\frac{\rho_r}{V}\right)^{k+1}\right]^{-1}, \rho_r\ne V, V\le i\le(V+K).\\ \frac{Q}{K+1}, \rho_r=V, V\le i\le(V+K)\end{cases}$$

где $P_0(R,V)$ – вероятность того, что в УК на обслуживании нет пакетов приоритетов $\overline{1,R}$;

$Q$ – вероятность того, что все каналы УК заняты обслуживанием суммарного потока пакетов приоритетов $\overline{1,R}$;

$\rho_r$ – суммарная входящая нагрузка пакетов с приоритетами $\overline{1,r}$

На основе стационарного распределения производится расчет основных показателей функционирования сетей передачи данных для бесприоритетных систем и систем с приоритетами: вероятность потери пакетов, средняя длина очереди УК и задержка доставки пакетов в зависимости от объема буфера, производительности УК, входящей нагрузки и количества обслуживающих приборов на сети.

Также проведен анализ модели УК типа $M_r/D/V/K$ с простейшими входящими потоками, коммутацией пакетов фиксированной длины, ограниченным буфером и управлением качеством обслуживания разнородного трафика на основе относительных приоритетов.

Вероятность потери пакетов различных приоритетов для $M_r/D/V/K$ определяется выражением:

$$P_{V+K}(r)=P_{i>V-1}(R,V)\cdot\frac{1-\frac{\rho_r}{V}}{1-\left(\frac{\rho_r}{V}\right)^{2K+1}}\cdot\left(\frac{\rho_r}{V}\right)^{2K},$$

где $P_{i>V}(R,V)$ характеризует вероятность того, что обслуживающий прибор занят обслуживанием пакетов суммарного потока всех приоритетов $\rho_R$.

Модель УК типа $M_r/D/V/K$ применима для реальной системы, и может использоваться для исследования функционирования УК при времени поступления заявок, описываемых экспоненциальными функциями, детерминированном времени их обслуживания и при ограниченности сетевых ресурсов.

Расчеты показывают, что:

– вероятность потери пакетов увеличивается с ростом нагрузки в системе;

– увеличение объема буфера приводит к увеличению задержки передачи пакетов и уменьшению вероятности потери пакетов для модели $M_r/M/V/K$. Для модели $M_r/D/V/K$ увеличение размера буфера эффективно для нормального режима работы и не эффективно при режиме перегрузки.

– вероятность потери пакетов для модели $M_r/M/V/K$ значительно больше чем для $M_r/D/V/K$. Однако в режиме перегрузки, эта разница становится минимальной

– при увеличении интенсивности обслуживания среднее время пребывания пакетов в УК уменьшается, за счет уменьшения среднего времени обслуживания.

Для отражения поведения работы УК, т.е. отражения изменения состояния УК во времени при заданных потоках заявок, поступающих на его входы, проведено имитационное моделирование (ИМ), которое в общем случае является действенным средством проверки результатов аналитического моделирования.

Для реализации имитационного моделирования был проведен анализ программных средств, имеющих широкое практическое применение: Arena, AnyLogic, GPSS World. Также был проведен анализ программных систем ориентированных на моделирование сетей: Modeler OPNET, NetMaker XA, BONES. Выявлено, что максимально полно для проведения ИМ подходит система GPSS World, которая ориентирована на описание широкого класса систем массового обслуживания в различных предметных областях. GPSS World обладает удобным пользовательским интерфейсом, встроенными средствами визуализации и интерактивного управления процессом моделирования, обширной библиотекой встроенных процедур, включающей, в том числе, генераторы случайных величин для множества вероятностных распределений. Все это делает процесс ИМ эффективным и наглядным.

Имитационное моделирование в среде GPSS World позволяет исследовать модели при различных типах входных потоков и интенсивностях поступления заявок на входы, при вариациях параметров УК, при различных дисциплинах обслуживания заявок.

Результаты диссертационной работы, полученные в ходе математического и имитационного моделирования, позволяют:

- сделать вывод, что модели УК типа $M_r / M / V / K$ и $M_r / D / V / K$ позволяют оценить соответственно пессимистичные и оптимистичные значения показателей функционирования СПД;

- определить предельные нагрузки, при которых обеспечиваются установленные нормы, а также, зная предполагаемую нагрузку на УК выбрать, какое коммутационное оборудование необходимо будет использовать.

Выявленные зависимости параметров качества функционирования сети от характеристик сети и коммутационного оборудования позволят принимать обоснованные решения на этапе проектирования и повысить эффективность функционирования узлов коммутации сетей связи при передаче разнородного трафика с различными требованиями к качеству обслуживания.

Список использованных источников:

6. Алиев, Т. И. Основы моделирования дискретных систем / Т. И. Алиев. – СПб.: СПбГУ ИТМО, 2009. – 363 с.

7. Назаров, А.Н. Модели и методы исследования процессов функционирования и оптимизации построения сетей связи следующего поколения / А.Н. Назаров, К.И. Сычев // Электросвязь. – 2011. – №3. – С. 43–49.

8. Назаров, А.Н. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения / А.Н. Назаров, К.И. Сычев. – Красноярск: Поликом, 2010. – 389 с.

# МЕТОДЫ ФОРМИРОВАНИЯ РАДИОСИГНАЛОВ С МНОГОПОЗИЦИОННОЙ МОДУЛЯЦИЕЙ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Лапицкий П. А.*

*Капуро П.А. – старший преподаватель*

Цифровые методы модуляции используются для передачи кодированных сообщений дискретными методами. Сущность цифровой модуляции заключается в том, что передаваемый непрерывный сигнал дискретизируется во времени, преобразуется в кодовые комбинации. Большим недостатком систем с цифровым сигналом является расширение занимаемой полосы сигналов.

Для устранения данного недостатка используются методы многопозиционной модуляции. Рассматриваются способы преобразования сигнала и анализ спектра. Большей спектральной экономией обладают амплитудная и фазовая манипуляция.

Основная экономия спектра осуществляется за счет увеличения длительности бита эквивалентной кодовой последовательности.

Для построения такой последовательности используются карты созвездий. В зависимости от кода первичной кодовой последовательности осуществляется переход к альтернативному сигналу с некоторой амплитудой и фазой. В картах созвездий в качестве шкалы используются относительные единицы. Этот подход определяет максимальную абсолютную амплитуду. Поэтому при увеличении длительности бита эквивалентной последовательности ухудшается помехозащищенность выходного сигнала.

Рассматриваются два способа математического представления сигнала:

-полярное $s(t) = A(t) \cdot \cos\left(2\pi ft + \theta(t)\right)$

-квадратурное $s(t) = x(t) \cdot \cos(2\pi ft) - y(t) \cdot \sin(2\pi f)$

Вышеуказанные способы определяют структуру будущего модулятора.

Большей популярностью при построении модуляторов пользуется квадратурное построение. По следующим причинам:

1) Генерация гармонического сигнала осуществляется в ограниченные промежутки времени
2) При формировании сигнала происходят многократные операции умножения и деления сигнала

Следующим недостатком цифрового представления сигнала является наличие скачка фазы на $180^0$ при переходе между битами «0» и «1».

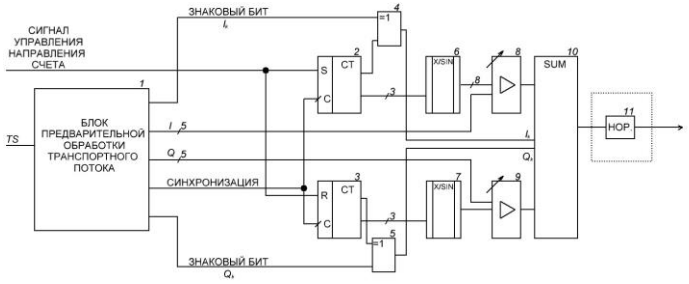
Для устранения скачков фазы в многопозиционных модуляторах могут использоваться линии задержки в канале (OQPSK), переход между двумя созвездиями (pi/4-QPSK), использование формирующих импульсов.

Для создания формирующих импульсов используются следующие функции:

•Корень из приподнятого косинуса (QPSK)
• Половина синуса(MSK )
• Функция Гаусса (GMSK)
• Парциальная квадратурная характеристика (QPR)

QAM совмещает свойства амплитудной и фазовой модуляций. Рассматривается помехоустойчивость QAM, искажения созвездий при воздействии различного рода искажений: плохое ОСШ, «шумы ингрессии», нелинейность AX, IQ нестабильность, уход несущей.

Для демонстрации подхода применяемого при построении многопозиционных модуляторов в качестве примера был выбран QAM модулятор системы DVB-C. QAM созвездия данного стандарта является довольно специфическим. Для реализации модулятора проведен анализ созвездия и определены правила его формирования. Проведено построение отдельных блоков и их синтез в конечное устройство. Принятая при реализации структура основана на анализе современных вариантов построения QAM модуляторов на основании патентного поиска для классических и неклассических вариантов построения QAM.




Большинство предлагаемых модуляторов осуществляют обработку в цифровом виде, с задействованием ПЗУ. Для увеличения быстродействия системы и исключения ПЗУ разработка функциональной схемы устройства произведена на уровне логических элементов «И», «ИЛИ», «НЕ», с использованием языка параллельной обработки процессов VHDL.

Список использованных источников:

9. L.Hanzo “Single- and Multi-carrier QAM”. Manchester, 1999.
10. S.Chua “Variable-rate variable-power mQAM for fading channels” Atlanta, 1996.

# ФОРМИРОВАНИЕ КОМПОЗИЦИОННЫХ СИГНАЛОВ НА ОСНОВЕ ПРЯМЫХ МЕТОДОВ ДИСКРЕТНОЙ СВЕРТКИ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Леонович А. В.*

*Печень Т. М. – ассистент каф. СТК*

Существуют многочисленные алгоритмы цифровой обработки сигналов (ЦОС) как общего типа для сигналов в их классической временной форме (телекоммуникации, связь, телевидение и пр.), так и специализированные в самых различных отраслях науки и техники (геоинформатике, геологии и геофизике, медицине, биологии, военном деле, и пр.). Все эти алгоритмы, как правило – блочного типа, построенные на сколь угодно сложных комбинациях достаточно небольшого набора типовых цифровых операций, к основным из которых относятся свертка (конволюция), корреляция, фильтрация, функциональные преобразования, модуляция.

В дискретном случае различают два вида сверток: линейную (или апериодическую) и циклическую.

Ниже рассмотрим понятие линейная свертка.

***Линейная свертка*** – основная операция цифровой обработки сигналов (ЦОС), особенно в режиме реального времени. Для двух последовательностей h(n) и y(k) длиной соответственно N и K свертка определяется выражением [1]:

$$s(k) = h(n) \otimes y(k) \quad h(n) * y(k) = h(n)\ y(k - n),$$

где: $\otimes$ или $\times$ - символьные обозначения операции свертки. Как правило, в системах обработки одна из последовательностей y(k) представляет собой обрабатываемые данные (сигнал на входе системы), вторая h(n) – оператор (импульсный отклик) системы, а функция s(k) – выходной сигнал системы.

Свойства свертки:

1. Закон коммутативности

$$x1(t) \otimes x2(t) = x2(t) \otimes x1(t).$$

2. Закон дистрибутивности

$$x1(t) \otimes [x2(t) + x3(t)] = x1(t) \otimes x2(t) + x1(t) \otimes x3(t).$$

3.Закон ассоциативности

$$x1(t) \otimes [x2(t) \otimes x3(t)] = [x1(t) \otimes x2(t)] \otimes x3(t).$$

Мною же были рассмотрены примеры, как свойства автосвертки проявятся при замене:

1. $S(k)$ на $-S(k)$;

Пусть первый вектор равен $\{1;1;1;1\}$, а второй $\{1;1;1;1\}$. Тогда свертка будет равна $\{1;2;3;4;3;2;1\}$.

2. $S(k)$ на $S(k - k_0), k_0 > 0$;

Пусть первый вектор равен $\{0;0;1;1;1;1\}$, а второй $\{0;0;1;1;1;1\}$. Тогда свертка будет равна $\{0;0;0;0;1;2;3;4;3;2;1\}$.

3. $S(k)$ на $A \cdot S(k)$.

Пусть первый вектор равен $\{2;2;2;2\}$ а второй $\{2;2;2;2\}$. Тогда свертка будет равна $\{4;8;12;16;12;8;4\}$.

Композиционные сигналы – это сложные сигналы, формирование которых производится по определенному алгоритму. Актуальность применения данного класса сигналов обусловлена требованием повышения помехоустойчивости системы связи. В большинстве случаев расширение спектров сигналов органичено. Одним их эффективных способов решения данной проблемы является использование сложных сигналов [2]. Методы цифровой обработки таких сигналов разнообразны и в большинстве случаев основываются на процедурах быстрого преобразования Фурье (БПФ). Следует отметить, что широко известны методы додетекторной свертки сигналов, которые позволяют устранять негативную фазовую манипуляцию сигналов [3]. Важное преимущество этих методов – это высокая помехоустойчивость при отношении сигнал/шум от 2 дБ.

Список использованных источников:

11. Оппенгейм, А. Цифровая обработка сигналов / А. Оппенгейм, Р. Шафер. – М.: Техносфера, 2006. – 856 с.

12. Быстров, Н. Е. Квазиоптимальная обработка когерентных квазинепрерывных сигналов с большой базой в заданном дальностно-доплеровском диапазоне / Н. Е. Быстров, И. Н. Жукова, Д. В. Чеботарев // Радиотехника. - 2011. - № 3. - С. 39-45.

13. Щербина, Р. Г. Метод распознавания вида модуляции цифровых сигналов, инвариантный к оценкам несущей / Р. Г. Щербина, О. В. Яковлев // Телекоммуникации. - 2004. - №11.-С.28-31.

# КОЛОРИМЕТРИЧЕСКИЕ ПРОСТРАНСТВА И СИСТЕМЫ ИЗМЕРЕНИЯ ЦВЕТА

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Ремизова Д.Н., Ткаченко А.П.*

*Ткаченко А.П. – к-т. техн. наук, доцент*

Качество цветного изображения в аналоговой и цифровой телевизионной (ТВ) системе (ТВС) зависит от многих факторов как и в любой системе телекоммуникаций. Но в ТВС необходимо дополнительно произвести анализ цветного изображения на передающей стороне и синтез на приемной.

Для этого в ТВ передающей камере построение оптического изображения (ОИ) на светочувствительной поверхности трех передающих трубок (ПТ) осуществляют вариообъектив, свето- и цветоделительное устройство – оптические фильтры. Последние расщепляют поток ОИ на три цветоделительных, образующих на выходе ПТ сигналы основных цветов $U_R^*$, $U_G^*$ и $U_B^*$ («*» означает, что сигналы не точно отображают содержание цвета в объекте). Цвет же представляет собой результат воздействия светового излучения $p(\lambda)$, Вт/нм на зрительную систему (ЗС). Поэтому его можно оценить субъективно.

В докладе рассматриваются основы колориметрии – науки об измерении и количественном выражении цвета. Известно, что всякое измерение состоит в определении числа эталонных единиц, содержащихся в измеряемой величине. Измерение цвета стало возможным, когда путем изучения свойств ЗС и экспериментальных исследований, были найдены способы выражать цвет через эталонные единицы. Их роль выполняют единичные количества заранее выбранных линейно независимых первичных или основных цветов.

Анализируются различные формы представления цвета в пространстве (рисунки 1, 2, 3), а также способы измерения цвета, позволяющие рассчитывать необходимые для передачи ТВ сигналы, оптимизировать их обработку в цветокорректирующей матрице, определять величины цветовых искажений и т.п.

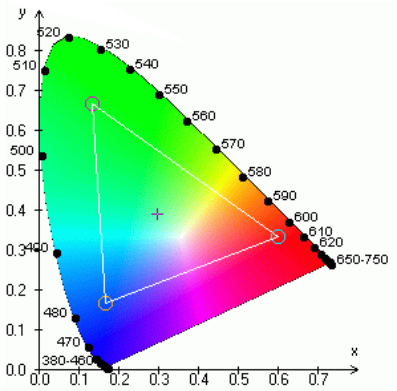



Рис.1 − Диаграмма цветности МКО 1931г.

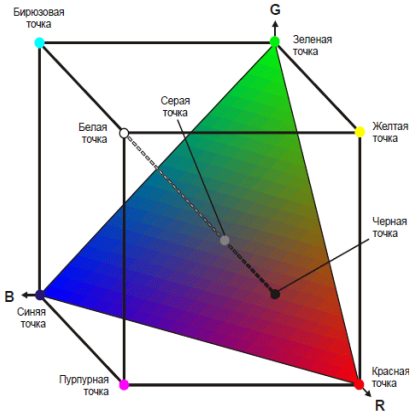



Рис. 2 – Цветовая модель RGB

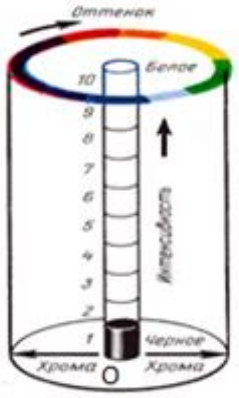
Экспериментально установлено, что любой цвет Ц может быть выражен не отличимой на глаз смесью основных цветов (R), (G), (B): m(Ц) = r'(R)+g'(G)+b'(B), где r', g', b' - количества основных цветов, т.е. абсолютные трехцветные коэффициенты или координаты цвета, m – модуль цвета Ц. Отсюда следует, что любой цвет может быть представлен вектором в трехмерном пространстве, например, RGB [1, 2].

При одновременном наблюдении изображения и оригинала в одинаковых условиях следует стремиться к получению высокой колориметрической точности. Благодаря изучению свойств ЗС было выяснено, что для хорошего цветовоспроизведения колориметрически правильная цветопередача не обязательна, если можно создать более благоприятное восприятие цветов относительно опорного белого цвета. В колориметрии все вычисления основываются на законах Грассмана (ранее в виде гипотезы были высказаны М.В. Ломоносовым).

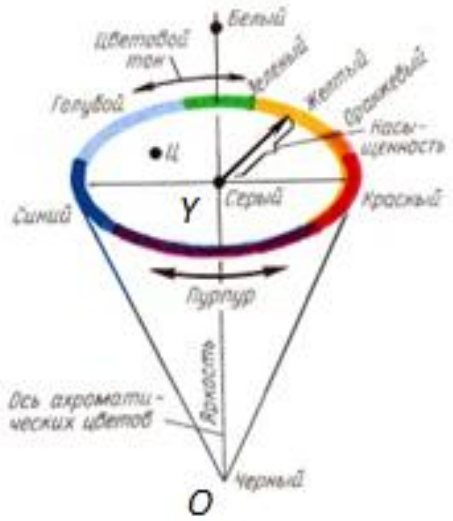
Обсуждаются критерии точности цветовоспроизведения – колориметрическая и психовизуальная. На основании колориметрических расчетов обосновывается вид трех компонентных сигналов: сигнала яркости $U_Y$ и двух цветоразностных (ЦРС) $U_{R-Y}$ и $U_{B-Y}$, (которые должны передавать информацию о цветности), необходимых для и цифрового представления [3].

Анализ последних показывает, что из ЦРС не полностью исключена информация о яркости: значения ЦРС зависят от $U'_Y$ так, что при неизменной цветности эта зависимость линейна. Так, например, при изменении в k раз сигналов $U_R$, $U_G$ и $U_B$ ( в результате увеличения яркости источника освещения объекта), то во столько же раз изменятся как $U'_Y$, так и $U'_{R-Y}$ и $U'_{B-Y}$. Поэтому ЦРС фактически передают информацию не о

цветности, а о хроматичности (окраске) [2]. Полное исключение информации из ЦРС о яркости было бы при формировании и передаче сигналов $U'_{R-Y}$/ $U'_{Y}$ и $U'_{B-Y}$/ $U'_{Y}$, которые остаются неизменными при пропорциональных изменениях сигналов основных цветов $U_R$, $U_G$ и $U_B$. Различия между понятиями "цветность" и "окраска" поясняются рисунком 3, на котором показаны диаграммы построения цвета, основанные на этих понятиях: черный цвет лежит в точке О, белый − в точке Y, длина вертикального вектора выражает яркость. В плоскостях постоянной яркости образуются полярные системы координат, которые определяют цветность (рисунок 3(а)) и окраску (рисунок 3(б)). При этом длина вектора передает насыщенность, угловое положение – цветовой тон; окраска на рисунке 3(б) равна произведению насыщенности на яркость.




а) по Маселлу;




б) при синтезе изображения передаваемого сигналами яркости и ЦРС

Рис. 3 – Геометрические модели зрительного восприятия.

Детальный анализ колориметрических пространств и систем измерения цвета будет представлен непосредственно в докладе на конференции.

Список использованных источников:

1. Ткаченко, А.П. Цветное телевидение / А.П. Ткаченко. – Минск : Беларусь, 1981. – 254 с.
2. Певзнер, Б.М. Качество цветных телевизионных изображений / Б.М. Певзнер. – 2-е изд., доп. и перераб. – М.: Радио и связь, 1988. – 224 с.
3. Ткаченко, А.П. Цифровое телевидение. В 2 ч. Ч.1. Кодирование источника сообщений в системах цифрового телевизионного вещания: учеб.- метод. пособие / А.П. Ткаченко, А.Л. Хоминич. – Минск: БГУИР, 2015. – 162 с.

# МЕТОДЫ И СРЕДСТВА БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ПОПУЛЯРНЫХ СИСТЕМ УПРАВЛЕНИЯ СОДЕРЖИМЫМ ВЕБ-САЙТОВ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Цалко А. С.*

*Кучинский П. В. – д-р. техн. наук, профессор*

С каждым годом растет доля сайтов, использующих широко распространенные системы управления содержимым (CMS). В 2016 году из 10 миллионов крупнейших веб-сайтов 26.2% работают на CMS WordPress. Суммарно же доля данной системы составляет 59.3% среди всех используемых CMS [1]. Широкое распространение как данной, так и других популярных систем делает их мишенью для злоумышленников.

Как правило, использование самих CMS не несет угрозы. Однако в декабре 2015 года была найдена критическая уязвимость в системе «Joomla», затрагивающая все использующие данную CMS сайты (около 3 миллионов веб-сайтов) [2]. Основная же опасность использования популярных систем заключается в расширении функционала веб-сайтов с помощью дополнительных модулей (плагинов) от сторонних разработчиков, не уделяющих проблеме безопасности должного внимания.

Исследована безопасность веб-сайтов, написанных на скриптовом языке PHP и обслуживаемых ЦИИР БГУИР. Был проведен поиск вредоносного ПО методами сигнатурного сканирования и эвристического анализа исходных файлов веб-сайтов. В результате на небольшом количестве сайтов (менее 50) было найдено более 200 образцов вредоносного программного обеспечения.

В абсолютном большинстве доступ был получен злоумышленниками через популярные системы управления содержимым веб-сайтов и их модули. Веб-сайты и системы, разработанные ЦИИР БГУИР не были скомпрометированы. При анализе исходных кодов были обнаружены образцы вредоносного ПО различного характера действия и разной степени шифрования.

С каждым днем вредоносный код (веб-шеллы, скрипты для рассылки спама и т.п.) становится более изощренным и сложным в обнаружении. Кроме обфускации идентификаторов и шифрования кода злоумышленники повсеместно начали использовать неявные вызовы функций посредством методов с callable аргументами, handler'ы и косвенные вызовы функций.

Вредоносных скриптов с линейной структурой и статическими переменными и функциями среди найденных образцов практически не было обнаружено. Исходный код стараются замаскировать и сделать как можно более изменчивым, «полиморфным» или наоборот, сделать максимально простым и похожим на обычный скрипт.

Вредоносное ПО размещается не только в новых файлах, а также и в системных файлах CMS, на которой функционирует сайт. В большинстве случаев это не влияет на работу сайтов, либо влияет незначительно, тем самым усложняя обнаружение атаки администраторами.

Зачастую, анализируя вредоносный скрипт, невозможно выделить фиксированный фрагмент, по которому однозначно можно было бы идентифицировать «вредонос». Очевидно, что подобный вредоносный код невозможно найти по простой базе сигнатур (антивирусной базе), которая используется в подавляющем большинстве веб-антивирусов и сканеров исходных кодов. Для эффективного поиска современных «вредоносов» необходимо использовать более сложные методики определения вирусных паттернов, а в некоторых случаях - эвристику.

В качестве минимизации риска сетевых атак на веб-сайты, использующие популярные системы управления содержимым (CMS) предлагается использовать следующие методы и средства:

- Использование сложных паролей к администраторским панелям любых сайтов и систем
- Ограничение доступа к панелям администрирования, ограничение попыток неудачного входа
- Запрещение регистрации пользователей при возможности
- Запрещение прав редактирования системных файлов CMS
- Запрещение возможности выполнения скриптов в тех папках, права на запись в которых невозможно выставить без сохранения функционирования CMS
- Регулярное создание резервных копий файлов и БД, на разных серверах и хранилищах
- Минимизация использования дополнительных модулей от сторонних разработчиков
- Регулярное обновление самих CMS и модулей к ним
- Осуществлять проверку файлов сканерами вредоносного кода (AI-Bolit, maldet, clamav и др.)

Все вышеописанные методы позволяют снизить риск сетевой атаки, но не гарантируют полную безопасность веб-сайтов. Максимально эффективным средством является использование систем обнаружения вторжений (IDS).

Для серверов ЦИИР БГУИР, на которых размещаются сайты, работающие на скриптовом языке PHP была выбрана система OSSEC - хостовая система обнаружения вторжений (Open Source Host-based Intrusion Detection System). Данная система обладает открытым исходным кодом, а значит ее использование безопасно. С ее помощью были решены задачи проверки контроля целостности файлов, логирования

различных действий на серверах, получения событий безопасности (анализ системных журналов) и оповещений об этих событиях.

В результате всех описанных методов и средств удалось существенно повысить безопасность сайтов, использующих популярные системы управления содержимым. Количество успешных сетевых атак злоумышленников значительно снизилось: на том же количестве сайтов за месяц наблюдения не было выявлено успешных атак. Проведенная работа подтверждает актуальность выбранного направления исследования информационной безопасности веб-узлов.

Список использованных источников:

14. W3Techs, Software Quality Management Consulting: [Электронный ресурс]. Режим доступа: http://w3techs.com/technologies/overview/content_management/all (Дата обращения: 11.03.2016).

15. Sucuri Security, Critical 0-day Remote Command Execution Vulnerability in Joomla [Электронный ресурс]. Режим доступа: https://blog.sucuri.net/2015/12/remote-command-execution-vulnerability-in-joomla.html (Дата обращения: 10.03.2016).

16. Wikipedia, OSSEC [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/OSSEC (Дата обращения: 10.03.2016).

# ТЕОРЕТИЧЕСКИЙ АНАЛИЗ МЕТОДОВ ПАРАМЕТРИЗАЦИИ ЛИНИЙ НА ИЗОБРАЖЕНИЯХ

*Кирилюк Д.И., Костусев А.В.*
*Белорусский государственный университет информатики и радиоэлектроники*

В представляемой работе исследуются методы параметризации линий на основе геометрических признаков.

В настоящее время в связи с развитием робототехники специального назначения стоит актуальная задача – обработка изображений в реальном масштабе времени. Для ее решения широко используются методы, которые учитывают распределение градиента яркости в окрестностях реперных точек. Однако, в условиях проекционных искажений эффективность градиентного подхода снижается. Устранение данного недостатка возможно за счет геометрического подхода. Геометрические методы применялись в задачах для обработки изображений, имеющих искусственную природу (например, печатные платы, САПР). Поэтому актуальной задачей в настоящее время является модернизация существующих геометрических методов и создание новых методов для обработки изображений, имеющих естественный характер (например, спутниковые, ландшафтные). Целью настоящей работы является теоретический анализ методов геометрической параметризации линий на изображениях.

Основными требованиями к дескрипторам линий являются: устойчивость к проективным преобразованиям; устойчивость к шуму; высокая скорость формирования; произвольность формы кривой. Теоретический анализ показал, что для решения поставленной задачи, с учетом вышеуказанных требований, наиболее эффективны методы на основе Фурье-дескрипторов, сигнатур или цепных кодов.

Методы на основе Фурье-дескрипторов используют дискретное преобразование Фурье конечной последовательности комплексных чисел (координаты точек рассматриваются как комплексные числа), позволяют по коэффициентам преобразований восстановить линию.

Сигнатуры – одномерные функции, взаимно-однозначно определяющие кривую линию, строятся относительно некоторой фиксированной точки (центра). Особенностью цепных кодов является кодирование направлений и длин прямых отрезков линии.

Вычислительная сложность вышеназванных методов примерно одинаковая. Методы на основе Фурье-дескрипторов устойчивы к повороту, параллельному переносу. Устойчивость методов на основе сигнатур и цепных кодов зависит от выбора начальной точки.

# DLP – СИСТЕМЫ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Бородюк О.В., Михальков Н.В.*

*Бойправ О.В. – м.т.н.*

В последнее время упоминания об утечках информации из самых разных организаций (коммерческих, некоммерческих, государственных и прочих) в новостных лентах информационных агентств и Интернет становятся фактически ежедневными. В связи с ростом таких инцидентов растет и интерес к системам, которые могли бы противостоять подобного рода угрозам.

Идеального решения по защите от внутренних угроз не существует — все зависит от требований, заложенных в политиках ИБ. Для реализации этих политик могут использоваться продукты пяти различных классов: системы блокировки портов, системы контроля доступа, криптосистемы, DLP-системы и IrM-системы. В мировой практике информационной безопасности считается, что наиболее действенными системами являются DLP-системы (Data Loss/Leak Prevention), так как они позволяют обеспечить не только защиту конфиденциальной информации в местах ее хранения, но и дают возможность контролировать данные в процессе их обработки и передачи.

DLP-системы направлены на минимизацию рисков внутренних угроз информационной безопасности, или, иными словами, на защиту корпоративной информации от инсайдеров. Инсайдерами являются абсолютно все сотрудники компании, ведь утечки могут происходить не только по злому умыслу, но и по невнимательности сотрудников или незнанию правил информационной безопасности. Согласно статистике, свыше 80 % зарегистрированных инцидентов приходится именно на случайные утечки.

Основной признак любой современной DLP-системы — способность анализировать информацию, передаваемую по различным коммуникационным каналам, на предмет ее конфиденциальности. Фактически DLP-система — своеобразный черный ящик, на вход которого поступает информация, а в результате выдается вердикт — является ли она конфиденциальной. В дальнейшем на основе такого анализа система принимает решение: разрешить ли эту передачу данных или заблокировать ее.

Существует два основных подхода к анализу информации в DLP-системах. Первый – контентный подход предполагает, что из каждого передающегося файла извлекается текстовая составляющая, которая в дальнейшем каким-то образом исследуется. Второй — контейнерный метод, в его рамках анализируется не информация, а ее атрибуты, такие как тип файла, его размер, время создания или имя владельца. Другим примером контекстной фильтрации является использование специальных меток конфиденциальности, которые инкапсулируются в каждый защищаемый документ.

Необходимо также разделять комплексные DLP-системы и отдельные DLP-функции других систем безопасности. В частности, комплексная DLP-система должна поддерживать все основные исходящие коммуникационные каналы, иметь централизованную консоль управления и настройки политик, а также предоставлять возможность блокирования нежелательных перемещений информации. Это означает, что многие системы, использующие анализ контента, DLP-системами не являются, поскольку указанные функции представляют собой лишь одну из реализованных возможностей.

Одним из главных аспектов выбора и внедрения DLP-системы является ее совместимость с принципами и требованиями работы всей компании, ведь она имеет свои собственные стандарты безопасности, организацию работы IT-структуры, свои собственные, часто уникальные принципы ведения бизнеса. Всю информацию, имеющуюся в сети компании, можно подразделить на несколько типов:

– неклассифицированная;
– общедоступная информация;
– конфиденциальная, но не критичная;
– строго конфиденциальная информация.

Информация каждого из указанных типов требует определенных методов обработки и защиты.

Список использованных источников:

1. Tadviser [Электронный ресурс]. – Электронные данные. – Режим доступа : http://www.tadviser.ru/.
2. InfoWatch [Электронный ресурс]. – Электронные данные. – Режим доступа : www.infowatch.ru.
3. Softline [Электронный ресурс]. – Электронные данные. – Режим доступа : http://softline.ru/.
4. SolarSecurity [Электронный ресурс]. – Электронные данные. – Режим доступа : http://solarsecurity.ru/.

# КВАНТОВЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Жукевич А.Ф., Колесова Т.Р.*

*Бойправ О.В. – м.т.н., ассистент*

Письма по электронной почте, конфиденциальная информация, персональные данные – секреты, которые нужно знать только некоторым лицам, особенно в политике, экономике или банковской сфере. Но, если их узнал посторонний, это может стать роковой ошибкой. Риск есть всегда, даже если информация зашифрована. Однако скоро это может остаться в прошлом. Все спецслужбы, политики и просто важные люди будут в восторге и в тоже время в полном разочаровании. Во-первых, будет невозможно украсть передаваемые секретные данные, во-вторых, это преимущество будет доступно и другим спецслужбам, что полностью исключает возможность кражи данных.

В квантовом мире ключ не может быть украден не замечено и никому не под силу взломать квантовый ключ, т.к. он был сгенерирован не математическим алгоритмом, а самой настоящей случайностью.

Носителями информации в квантовой криптографии являются фотоны, поляризованные под углами 0, 45, 90, 135 градусов. В соответствии с законами квантовой физики, с помощью измерения можно различить лишь два ортогональных состояния: если известно, что фотон поляризован либо вертикально, либо горизонтально, то путем измерения, можно установить — как именно; то же самое можно утверждать относительно поляризации под углами 45 и 135 градусов. Однако с достоверностью отличить вертикально поляризованный фотон от фотона, поляризованного под углом 45 градусов, невозможно.

Эти особенности поведения квантовых объектов легли в основу протокола квантового распространения ключа. Чтобы обменяться ключом, отправитель и получатель предпринимают следующие действия:

Отправитель посылает получателю фотон в одном из поляризованных состояний (0, 45, 90, 135 градусов) и записывает угол поляризации. Отсчет углов ведется от направления "вертикально вверх" по часовой стрелке. Получатель располагает двумя анализаторами: один распознает вертикально-горизонтальную поляризацию, другой — диагональную. Для каждого фотона получатель случайно выбирает один из анализаторов и записывает тип анализатора и результат измерений. По общедоступному каналу связи получатель сообщает отправителю, какие анализаторы использовались, но не сообщает, какие результаты были получены. Отправитель по общедоступному каналу связи сообщает получателю, какие анализаторы он выбрал правильно. Те фотоны, для которых получатель неверно выбрал анализатор, отбрасываются.

| Последовательность фотонов Алисы | \| | / | / | — | \ | \| | \| | — | — |
|---|---|---|---|---|---|---|---|---|---|
| Последовательность анализаторов Боба | + | x | + | + | x | x | x | + | x |
| Результаты измерений Боба | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| Анализаторы выбраны верно | + | + | | + | + | | | + | |
| Ключ | 0 | 0 | | 1 | 1 | | | 1 | |

***Условные обозначения:***

***Поляризация фотонов:*** *| - вертикальная, — - горизонтальная, / - под угром 45, \ - под углом 135.*

***Анализаторы:*** *+ - прямоугольный, x - диагональный*

Значения разрядов ключа получаются следующим образом: в случае вертикально-горизонтальной ("прямоугольной") поляризации вертикально-поляризованный фотон означает 0, горизонтально-поляризованный — 1; в случае диагональной поляризации фотон, поляризованный под углом 45 градусов -- 0, 135 градусов -- 1.

Рисунок 1 – Пример шифрования по протоколу BB84

Злоумышленник может попытаться перехватить ключ в ходе передачи потока квантов, но тогда они делятся надвое и уже не передают существенно важной информации. При подобном перехвате данных сразу станет заметным, что кто-то пытается их украсть. И даже если хакер попытается украсть само письмо в бинарном коде, у него все равно ничего не выйдет, ведь сам ключ был сгенерирован настоящей случайностью.

А это означает, что ученые нашли способ сгенерировать не взламываемый код, с которым можно быть на 100 процентов уверенными, что ваше письмо точно не будет украдено. Однако, чтобы использовать такую передачу данным по всему миру, понадобиться создать полноценную инфраструктуру.

Квантовые ключи могут быть переданы через оптоволокно на расстояние до 200 км, и сейчас некоторые банки уже используют эту функцию, а если расстояние слишком большое, то сигнал будет слабее и этот метод уже бездейственен. Для передачи данных на большие расстояния, эта система может работать исключительно через систему спутников.

Сделать специальное оборудование для спутника не самая сложная задача, но до них квантовым состояниям придется преодолеть очень большое расстояние. Главными проблемами на пути передачи фотонов являются два фактора: солнечный свет и турбулентность.

Ученым удалось передать квантовые состояния по воздуху в дневное время суток, с помощью лазерных вспышек. Сигнальные лазерные вспышки и их световые волны являются носителями сигналов, они крепко держатся против дневного света, таким образом ученые сохраняют требуемый квантовый сигнал.

Остается только одна проблема: турбулентность. Передаче квантовых состояний по воздуху могут мешать деревья, здания, горячие дроги.

Ученые открыли, что для поляризации турбулентность не играет никакой роли, это направление вибрации электрического поля электромагнитной волны. Когда свет распространяется в одну сторону, то он может это делать по горизонтальным направлениям или вертикальным, эти два вида движения света не искривляются при встрече с турбулентностью. Благодаря этому, ученым удалось передать лазерную вспышку на расстояние 1,6 км.

Проводятся эксперименты с геостационарными спутниками, если эти эксперименты пройдут успешно, то квантовая коммуникация станет для нас повседневностью, а хакерам придется из-за этого очень нелегко.

Список использованных источников:

Е. А. Павельева, А. С. Крылов, Поиск и анализ ключевых точек радужной оболочки глаза методом преобразования Эрмита, Информ. и ее примен., 2010, том 4, выпуск 1, 79–82

Е.А. Павельева, А.С. Крылов, Алгоритм сравнения изображений радужной оболочки глаза на основе ключевых точек, Информатика и ее применения, 2011. Т.5. Вып. 1 С. 68-72 -

# ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНОЙ СТРАНИЦЫ ИНТЕРНЕТ - САЙТА МАГИСТРАТУРЫ ОТ WEB - АТАК

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Кухарчик Е.И., Конопелько И.А.*

*Казека А.А. – канд. техн. наук, доцент*

Интернет сегодня – это то, без чего не может прожить подавляющая часть населения. Сегодня Интернет открывает для людей безграничные возможности. Для кого-то – это просто развлечение, а для других – это работа и учеба. Изначально, интернет – сайты представляли собой совокупность статичных документов, но в настоящее время большинству из них свойственна динамичность и интерактивность. В связи с этим, в интернет-пространстве начало увеличиваться количество персональных страниц пользователей интернет- ресурсов. Для быстрого поиска необходимой информации студентам и магистрантам на интернет-портале университета, предлагается создание такой страницы обучающегося.

Персональная страница обучающегося – это дополнительные возможности интернет-портала, которые позволяют:

1. Получать актуальную информацию.
2. Отправлять сообщения (заявления, предложения и т.д.).
3. Оперативно менять свои контактные данные.
4. Посмотреть расписание занятий.
5. Проверить отметки в электронной зачётке.
6. Посмотреть свой учебный план.
7. Посмотреть информацию об оплате за обучение.

Не смотря на все удобство использования персональной страницы она содержит конфиденциальную информацию обучающегося, которая может попасть в руки злоумышленника. Одни из самых распространенных способов заполучить конфиденциальную информацию [1]:

1. Подбор – подбор имени пользователя и пароля.
2. Небезопасное восстановление паролей (Weak Password Recovery Validation).

Основные методы противодействия злоумышленникам заключаются в уменьшении количества попыток ввода не правильного пароля. При восстановлении пароля использовать электронную почту, или мобильный телефон, указанный при регистрации. Кроме того, следует учитывать о нарушение доступности Web сервера (ddos attack), переполнение базы данных интернет-роботами (Insufficient Anti-automation), рассылка спама, внедрение вредоносного кода.

Чтобы не стать жертвой злоумышленника, нужно тщательно продумывать план защиты интернет-портала или и персональной страницы на стадии разработки. А для дальнейшей поддержки безопасности, требуется проводить аудит информационной безопасности. [2]

Аудит информационной безопасности позволяет получить наиболее полную и объективную оценку защищенности информационной системы, локализовать имеющиеся проблемы и разработать эффективную программу построения системы обеспечения информационной безопасности организации.

Аудит безопасности сайта осуществляется путем тестирования на устойчивость сайта к комбинированным методам и техникам взлома. В случаях использования популярной CMS (Битрикс, NetCat, WordPress, Joomla!, Drupal и т.д.) [3], дополнительно проводится проверка устойчивости системы к известным эксплойтам. По завершению тестирования на проникновения составляется подробный отчет, содержащий обнаруженные уязвимости, способы их эксплуатации, а также рекомендации по их устранению.

Список использованных источников:

1. Жуков Ю. В. – Основы веб-хакинга. Нападение и защита (2-е изд.) – 2012 г.
2. Ярочкин В. И. – Информационная безопасность: учеб. для вузов. (2-е изд.) – 2005 г.
3. Система управления содержимым [Электронный ресурс] https://ru.wikipedia.org/wiki/Content_Management_System
4. Обзор эксплойтов [Электронный ресурс] https://xakep.ru/2011/07/04/57578/

# ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕМЕДИЦИНСКИХ СИСТЕМАХ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Саракуца И. М., Мальцева Е. С.*

*Бойправ О. В. – м.т.н.*

В настоящее время активно создаются виртуальные инфраструктуры здравоохранения, объединяющие на базе единого информационного пространства (ЕИП) все составляющие элементы системы охраны здоровья населения. Создаваемые виртуальные инфраструктуры позволяют решить актуальную задачу дистанционного мониторинга состояния здоровья населения. При этом остро стоит вопрос с обеспечением информационной безопасности передаваемых физиологических данных.

Телемедицина – это отрасль медицины, которая использует телекоммуникационные и электронные информационные технологии для обеспечения медицинской помощи на расстоянии. Предмет телемедицины - передача посредством телекоммуникаций и компьютерных технологий всех видов медицинской информации между отдаленными друг от друга пунктами.

Телемедицину можно разделить на две части: локальная телемедицина (в рамках одного медицинского учреждения) и глобальная телемедицина (между различными медицинскими учреждениями). Локальная ТМ создаётся на базе уже действующей в клинике системы взаимоотношений между администрацией, врачами и пациентами. Глобальная ТМ создается при взаимодействии специалистов двух или нескольких медицинских учреждений.

В состав ТМ консультативно-диагностических системах входят следующие подсистемы:

- подсистема консультативно-диагностических пунктов (КДП);
- подсистема консультативно-диагностических центров (КДЦ);
- подсистема координационно-технического центра.

ТМКДС имеет структуру "клиент-сервер" и состоит из двух независимых частей - "клиента" и «сервера». В роли клиента выступают подсистема КДП и подсистема КДЦ. Приложение-сервер инициализируется при запуске и далее ожидает поступления запросов от клиентов: передачи телемедицинских запросов, ответов консультантов, информации о прохождении запроса и т. п.

Приложение-клиент посылает запрос на соединение с сервером, а также выполняет передачу телемедицинских запросов, ответов консультантов, информации о прохождении запроса и т.д. в зависимости от типа клиента (КДП или КДЦ).

Основная база данных ТМКДС находится на сервере. В БД хранятся консультационные запросы, полученные от удаленных пунктов, заключения консультантов, полученные от консультационных центров, информация о пользователях системы.

В качестве протокола обмена данными в системе используется TCP/IP, являющийся стандартным протоколом для обмена данными в сетях типа Интернет и интранет. В сетях на базе TCP/IP в наши дни наиболее широко используется интерфейс, основанный на сокетах.

В качестве структурной основы для хранения и передачи информации в системе используется распределенная БД. При этом клиент и сервер имеют независимые БД, информация в которых может дублироваться с целью сокращения трафика и повышения эффективности работы системы.

Связь между ТМ пунктами и ТМ центрами организуется по выделенным каналам связи или через Интернет. С экономической точки зрения наиболее выгодным является использование сети Интернет при условии, что провайдер обеспечит гарантированную пропускную способность, необходимую для удовлетворительной работы систем видеоконференцсвязи.

Как и у других телекоммуникационных систем, у телемедицинских систем имеется ряд нерешённых проблем, одной из которых является проблема защиты информации. Анализ ТМКДС позволяет представить их в обобщенном виде как совокупность КДП, КДЦ и узлов коммутации, соединенных между собой каналами связи.

При большом количестве пользователей необходима также защита и от пользователя-нарушителя, являющегося штатным сотрудником или законным абонентом ТМКДС. Кроме того, территориальное распределение средств КДП и КДЦ предполагает реализацию связи на дальние расстояния по кабелю, радиоканала и другим каналам, физически доступным для нарушителя, так как реализовать их охрану и контроль доступа к ним не представляется возможным. Поэтому вполне реальна возможность подключения нарушителя к каналам и линиям связи в виде шлюза, через который может происходить утечка информации, но и её модификация, разрушение, в результате чего могут подвергаться опасности системные отношения и связи между элементами ТМКДС.

Возможными каналами НСД для ТМКДС являются:

- штатные средства, при их использовании законными пользователями не по назначению и за пределами своих полномочий, а также посторонними лицами;
- технологические пульты и средства управления;
- побочное эми информации с аппаратуры технических средств;

- побочные наводки информации по сети электропитания, на вспомогательных и посторонних коммуникациях, сервисном оборудовании;
- изменение удаление, задержка, переупорядочивание, дублирование и посылка ложных сообщений;
- воспрепятствование передаче сообщений;
- осуществление ложных соединений;
- анализ трафика и id-ров абонентской сети;
- повторы сообщений, передача различного рода «информационного мусора» и т. д.

В зависимости от ожидаемой модели нарушителя этот перечень может быть до определённой степени сокращён. Нарушителем может быть человек: посторонний; законный пользователь или из числа лиц обслуживающего персонала. Квалификация его также может быть различной. Он может обладать или не обладать определенным набором технических средств, работать в комфортных условиях риска; быть единственным или в составе организованной группы. Круг доверенных лиц зависит от важности обрабатываемой информации и выполняемых задач. Такими лицами должны быть, по меньшей мере, администраторы, руководители работ и должностные лица службы безопасности.

Рекомендуемые средства защиты информации ТМКДС в соответствии с возможными несанкционированными действиями представлены в табл. 1.

Табл. 1 – Рекомендуемые средства защиты информации ТМКДС в соответствии с возможными несанкционированными действиями

| № п/п | Возможные несанкционированные действия | Средства защиты информации ТМКДС |
|---|---|---|
| 1. | Устройства ввода-вывода информации | - Средства контроля и разграничения доступа в помещения.<br>- Программа контроля и разграничения доступа к ПО и информации.<br>- Антивирусные средства. |
| 2. | Машинные носители информации | - Учет и разграничение доступа к носителям.<br>- Электронная идентификация носителей.<br>- Шифрование информации |
| 3. | Носители ПО | -Учет, регистрация и разграничение доступа к носителям ПО.<br>- Верификация и контроль целостности ПО.<br>- Резервирование ПО с контролем доступа к его копии. |
| 4. | Средства загрузки ПО | - Средства контроля и разграничения доступа в помещениях.<br>- Антивирусные средства. |
| 5. | Технологические пульты и органы управления, внутренний монтаж аппаратуры | - Средства контроля и разграничения доступа в помещения.<br>- Система контроля вскрытия аппаратуры. |
| 6. | Побочное электромагнитное излучение и наводки информации | - Средства снижения и зашумления уровня излучения и наводок информации на границе контролируемой зоны объекта автоматизации. |
| 7. | Мусорная корзина | - Средства уничтожения носителей закрытой информации. |
| 8. | Анализ трафика и идентификаторов получателей сообщений | - Специальные средства заполнения потока.<br>- Линейное шифрование. |
| 9. | Посылка ложного сообщения | - Цифровая подпись содержательной части сообщения. |
| 10. | Задержка и удаление сообщений | - Подтверждение получения сообщений.<br>- Введение контрольного интервала времени ответа.<br>- Дублирование соединения или маршрута. |
| 11. | Отказ отправителя от переданного, получателя – от принятого сообщения | - Центр контроля и управления безопасностью информации. |

Список использованных источников:

1. Наумов В.Б., Савельев Д. А. Правовые аспекты телемедицины. – СПб.: Издательство "Анатолия", 2002. – 107 с.
2. Мельников В.В. Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.
3. Галатенко В.А. Основы информационной безопасности. – М.: ИНТУИТ.РУ «Интернет-университет информационных технологий», 2006. – 208 с.
4. Казаков В.Н., Климовицкий В.Г., Владзимирский А.В. Телемедицина. - Донецк: Типография ООО «Норд», 2002. – 100 с.

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ КОНСТРУКЦИЙ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

*Белорусский государственный университет информатики и радиоэлектроники*
*Минск, Республика Беларусь*

*Сухоницкая Е. В., Шараев Н. П.*

*Позняк А. А. – канд. физ.-мат. наук, доцент*

**Одной из важных технических проблем современного мира является подавление нежелательных электромагнитных излучений, возникающих из-за несовершенства конструкций излучающих блоков. Такие излучения могут оказывать влияние на организм человека, а также быть причиной образования электромагнитного канала утечки информации. В связи с этим разработка высокоэффективных, широкополосных, технологичных и удобных в эксплуатации экранирующих и радиопоглощающих материалов является актуальной.**

## Введение

При разработке конструкций экранов электромагнитного излучения (ЭМИ) или поглотителей электромагнитных волн, в настоящее время, используются различные материалы, обладающие способностью отражать или поглощать это излучение в определенном диапазоне частот. В природе не существует ни идеально отражающих, ни идеально поглощающих электромагнитную энергию материалов, поэтому подавление ЭМИ чаще всего обеспечивается за счет их комбинирования [1]. Из этого следует, что важную роль при создании экрана электромагнитного излучения играет сама его конструкция. В современном мире существует большое количество экранов ЭМИ. Сферой же их применения, в основном, является защита информации и подавления излучений, вредных для живых организмов и человека, в частности.

## I. Конструкции экранов электромагнитного излучения

Все конструкции экранов электромагнитного излучения можно разделить на 4 категории: однослойные, многослойные, со структурной неоднородностью, комбинированные.

**Однослойные конструкции экранов ЭМИ.** Такие конструкции выполняются листовой формы и в виде сеток из разнообразных материалов (сталь, медь, алюминий, цинк, латунь). Наиболее технологичными являются конструкции экранов из стали, так как при их изготовлении и монтаже можно использовать сварку. Применение сетчатых экранов ЭМИ обеспечивает снижение их материалоемкости. В случае, когда расстояние между микропроводом сетчатого экрана соответствует λ/2, он по своим экранирующим свойствам эквивалентен сплошному металлическому листу [2]. Сравнительные характеристики эффективности сетчатых и металлических экранов представлены в таблице 1 [3].

Табл. 1 – Сравнительные характеристики эффективности экранирования (дБ), сетчатых и металлических экранов с различными параметрами

| Вид экрана | Материал экрана | Частота, кГц | | | | |
|---|---|---|---|---|---|---|
| | | 10 | 100 | 1000 | 10000 | 100000 |
| Металлические листы толщиной 0,5 мм | Сталь | 64 | 87 | 120 | 120 | 120 |
| | Медь | 67 | 70 | 88 | 120 | 120 |
| | Алюминий | 65 | 66 | 80 | 120 | 120 |
| Металлические сетки | Медь, проволока диаметром 0,1 мм ячейки размером 1×1 мм$^2$ | 65 | 55 | 50 | 42 | 32 |
| | Сталь, проволока диаметром 0,1 мм ячейки размером 1×1 мм$^2$ | 48 | 47 | 42 | 36 | 29,5 |

**Многослойные конструкции.** Одним из способов повышения эффективности поглощения электромагнитных волн (ЭМВ) является использование конструктивно выполненного четвертьволнового поглотителя, в котором радиопоглощающий материал (РПМ) находится на некотором расстоянии от отражающей ЭМВ поверхности. Поглощение достигает максимального значения на частоте, соответствующей длине волны, четверть которой равна расстоянию между верхней поверхностью поглощающего материала и отражающей поверхностью (рис. 1), а также на всех ее высших нечетных гармониках (интерференционная конструкция) [4].

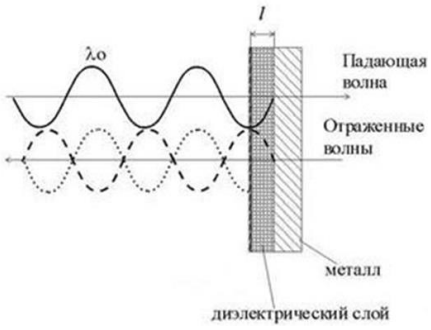
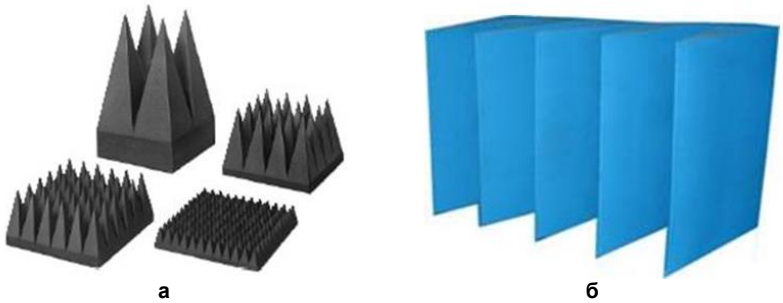



Рис. 1 – Схема взаимодействия ЭМИ с четвертьволновой конструкцией экрана

Также повысить эффективность экранов ЭМИ можно с помощью конструкций, представляющих собой либо симметричные структуры, полученные чередованием слоев с одинаковыми электромагнитными характеристиками, либо градиентные материалы, в которых слои располагаются с увеличением электрических и магнитных потерь по мере удаления от границы раздела экрана. В симметричных многослойных

материалах подавление волны происходит за счет многократного переотражения ЭМИ внутри экрана. Градиентные материалы могут быть выполнены в виде или многослойных структур, или с непрерывным изменением параметров материала по глубине, причем параметры обращенной к источнику ЭМИ поверхности экрана подбираются таким образом, чтобы обеспечить необходимые отражающие характеристики, а общая эффективность определяется в основном свойствами материала внутри экрана.



а б

Рис. 2 – Внешний вид фрагментов конструкций экранов ЭМИ с геометрическими неоднородностями

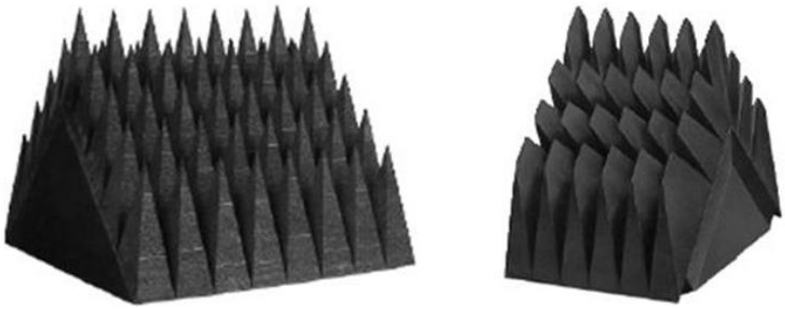


Рис. 3 – Внешний вид фрагментов конструкций экранов ЭМИ со сложной формой волноведущей поверхности

**Конструкции со структурно неоднородной поверхностью.** Формирование геометрических неоднородностей на поверхности экрана ЭМИ (пирамидальной (рис. 2, а), клиновидной (рис. 2, б) формы позволяет обеспечить широкодиапазонность характеристик отражения. Самым эффективным диапазоном подавления ЭМИ является 3…12 ГГц [5]. Взаимодействие с ЭМВ подобных конструкций обусловлено не только параметрами материала, из которого она изготовлена, но и формой волноведущей поверхности (рис. 3). В таких конструкциях падающая ЭМВ преобразуется в поверхностную и по мере переотражения от неоднородностей поверхности ее энергия уменьшается.

**Комбинированные конструкции.** Такие конструкции имеют, как правило, многослойную структуру и выполняются с учетом принципов построения рассмотренных выше конструкций. Основная проблема экранов подобного типа заключается в том, что они являются громоздкими и, как следствие, редко применяются (рис. 4). Исследование в данной области направлены на создание более гибких и легких экранов ЭМИ.

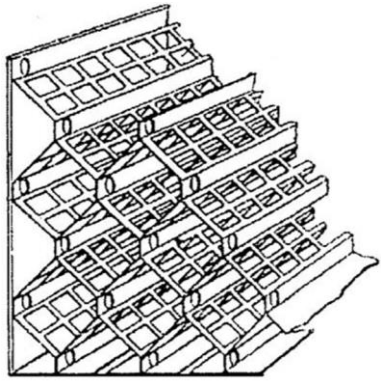


Рис. 4 – Схема защитного экрана,

## II. Сравнительная характеристика конструкций экранов электромагнитного излучения

Дать объективную оценку экранам ЭМИ и установить, какой из них является наиболее эффективным, сложно, так как часто приходится учитывать не только его характеристики ослабления и отражения ЭМИ, но и форм-факторы (объем, массу, прочность и т. д.). Так, напри-

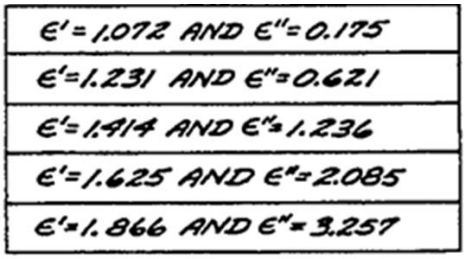



Рис. 5 – Схематичное изображение градиентного экрана ЭМИ

мер, из-за большой массы листовые экраны применятся редко. В многослойных конструкциях, состоящих из металлов с различными характеристиками, эффективность экранирования выше, чем в однослойных материалах эквивалентной толщины. Экранирующий эффект обусловлен процессами поглощения энергии в объеме и отражения энергии на границах раздела сред. В многослойных структурах роль эффекта отражения возрастает с увеличением количества слоев и различия характеристических сопротивлений среды (рис. 5) [6]. Из этого следует, что многослойная конструкция является более эффективной, по сравнению с однослойных, но требует гораздо большего объема.

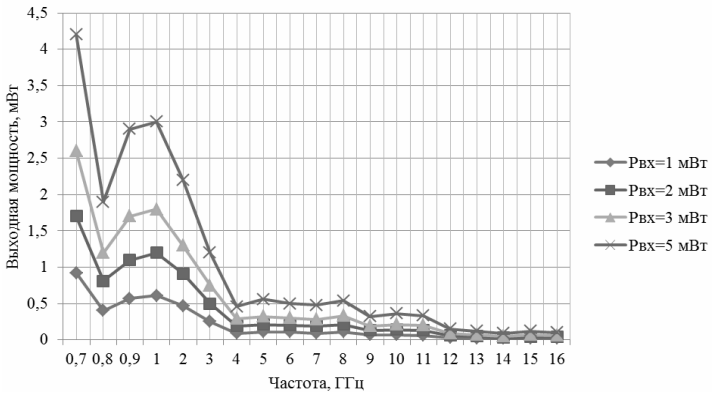



Рис. 6 – Частотные зависимости уровня прошедшей мощности ЭМИ при разных уровнях мощности падающего ЭМИ для экрана с пирамидальной поверхностью, изготовленного на основе смеси бетона и шунгита

Кроме того, в мире часто применяются конструкции со структурно неоднородной поверхностью. Рассмотрим данную конструкцию на конкретном примере – образце с пирамидальной поверхностью, изготовленного на основе смеси бетона и шунгита. На рис. 6 приведен график частотной зависимости уровня прошедшей мощности ЭМИ при разных уровнях мощности падающего ЭМИ.

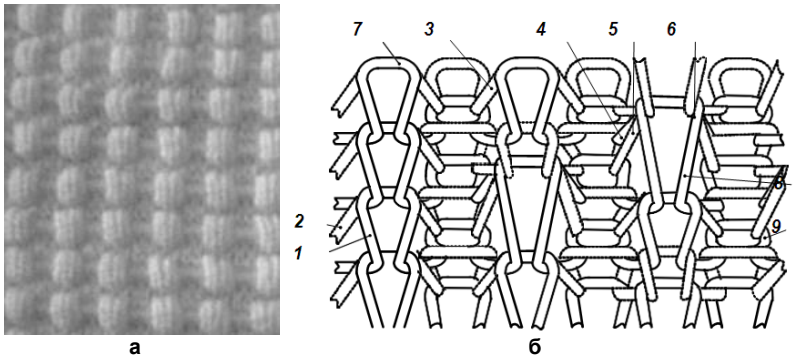



Рис. 7 – Внешний вид (а) и структура (б) полотна
с псевдопирамидальными неоднородностями на лицевой поверхности

Для экрана, изготовленного на основе бетона и шунгита, значение коэффициента отражения в диапазоне частот 3…12 ГГц лежит в пределах –10…–20 дБ [5]. Из этого следует, что благодаря этому они могут вводиться в структуру наружных стен зданий, которые отражают сигналы РЛС и вносят тем самым помехи в работу последних. Кроме того, данные экраны обладают малым весом. Однако в силу их большого объема не являются универсальными.

Что касается комбинированных конструкция, то они являются самыми эффективными из всех выше перечисленных конструкция, но к сожалению, имеют самый большой объем, массу и обладают большой трудоемкостью при их изготовлении. Так, например, на рис. 7 можем увидеть внешний вид (рис. 7, а) и структуру (рис. 7, б) полотна с псевдопирамидальными неоднородностями на лицевой поверхности.

## III. Заключение

Проблема разработки новых материалов и технологий создания гибких и мобильных электромагнитных экранов с повышенной эффективностью и широкополосностью весьма актуальна. В современном мире электромагнитные ресурсы используются широко, число действующих радиоэлектронных средств постоянно увеличивается, разрабатываются новые виды электромагнитного оружия. Это приводит к обострению проблем экологической защиты живых организмов и актуализации разработки и проектирования экранов ЭМИ. На вопрос, касающийся выбора конструкции экрана электромагнитного излучения, однозначного ответа нет. Каждый из типов рассмотренных конструкций характеризуется своими преимуществами и недостатками.

Список использованных источников:

1. Лыньков, Л.М. Гибкие конструкции экранов электромагнитного излучения // Л.М. Лыньков, В.А. Богуш, В.П. Глыбин и др. – Минск: – 2000. – 284 с.

2. Конструкции экранов электромагнитного излучения // Хелпикс.Орг - Интернет помощник [Электронный ресурс]. – Режим доступа: http://www.helpiks.org/5-8074.html. – Дата доступа: 09.04.2016

3. Лыньков, Л.М. Новые материалы для экранов электромагнитного излучения // Л.М. Лыньков, В.А. Богуш, Т.В. Борботько, Е.А. Украинец, Н.В. Колбун. – Минск: –2003. – С. 152–167.

4. Устройство адаптивного управления поляризационными и амплитудно-фазовыми характеристиками рассеяния радиолокационного объекта пат. 2323451 G01S7/38 Российская Федерация. Дата подачи заявки: 29.06.2006. Дата публикации: 27.04.2008. Е.В. Кузнецов, И.В. Ильин, А.И. Семенихин, М.А. Степаненков, А.Н. Хрипков, Б.М. Петров. [Электронный ресурс]. – Режим доступа: http://www.findpatent.ru/patent/232/2323451.html. – Дата доступа: 09.04.2016

5. Бойправ, О.В. Влияние экранов с геометрически неоднородной поверхностью на ослабление мощности электромагнитных излучений // О.В. Бойправ, М.Ш. Махмуд, М.Р. Неамах // Доклады БГУИР. – 2011. – № 3. – С. 5–10.

6. Чернушенко, А.М. Конструкции экранов и СВЧ-устройств: учебник для вузов // А.М. Чернушенко, Б.В. Петров, Л.Г. Малорцкая и др. – М.: Радио и связь. –1990. – С. 61–63.

# МЕТОДЫ И СРЕДСТВА БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ПОПУЛЯРНЫХ СИСТЕМ УПРАВЛЕНИЯ СОДЕРЖИМЫМ ВЕБ-САЙТОВ

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Цалко А. С.*

*Кучинский П. В. – д-р. физ.-мат. наук, профессор*

С каждым годом растет доля сайтов, использующих широко распространенные системы управления содержимым (CMS). В 2016 году из 10 миллионов крупнейших веб-сайтов 26.2% работают на CMS WordPress. Суммарно же доля данной системы составляет 59.3% среди всех используемых CMS [1]. Широкое распространение как данной, так и других популярных систем делает их мишенью для злоумышленников.

Как правило, использование самих CMS не несет угрозы. Однако в декабре 2015 года была найдена критическая уязвимость в системе «Joomla», затрагивающая все использующие данную CMS сайты (около 3 миллионов веб-сайтов) [2]. Основная же опасность использования популярных систем заключается в расширении функционала веб-сайтов с помощью дополнительных модулей (плагинов) от сторонних разработчиков, не уделяющих проблеме безопасности должного внимания.

Исследована безопасность веб-сайтов, написанных на скриптовом языке PHP и обслуживаемых ЦИИР БГУИР. Был проведен поиск вредоносного ПО методами сигнатурного сканирования и эвристического анализа исходных файлов веб-сайтов. В результате на небольшом количестве сайтов (менее 50) было найдено более 200 образцов вредоносного программного обеспечения.

В абсолютном большинстве доступ был получен злоумышленниками через популярные системы управления содержимым веб-сайтов и их модули. Веб-сайты и системы, разработанные ЦИИР БГУИР не были скомпрометированы. При анализе исходных кодов были обнаружены образцы вредоносного ПО различного характера действия и разной степени шифрования.

С каждым днем вредоносный код (веб-шеллы, скрипты для рассылки спама и т.п.) становится более изощренным и сложным в обнаружении. Кроме обфускации идентификаторов и шифрования кода злоумышленники повсеместно начали использовать неявные вызовы функций посредством методов с callable аргументами, handler'ы и косвенные вызовы функций.

Вредоносных скриптов с линейной структурой и статическими переменными и функциями среди найденных образцов практически не было обнаружено. Исходный код стараются замаскировать и сделать как можно более изменчивым, «полиморфным» или наоборот, сделать максимально простым и похожим на обычный скрипт.

Вредоносное ПО размещается не только в новых файлах, а также и в системных файлах CMS, на которой функционирует сайт. В большинстве случаев это не влияет на работу сайтов, либо влияет незначительно, тем самым усложняя обнаружение атаки администраторами.

Зачастую, анализируя вредоносный скрипт, невозможно выделить фиксированный фрагмент, по которому однозначно можно было бы идентифицировать «вредонос». Очевидно, что подобный вредоносный код невозможно найти по простой базе сигнатур (антивирусной базе), которая используется в подавляющем большинстве веб-антивирусов и сканеров исходных кодов. Для эффективного поиска современных «вредоносов» необходимо использовать более сложные методики определения вирусных паттернов, а в некоторых случаях - эвристику.

В качестве минимизации риска сетевых атак на веб-сайты, использующие популярные системы управления содержимым (CMS) предлагается использовать следующие методы и средства:

- Использование сложных паролей к администраторским панелям любых сайтов и систем
- Ограничение доступа к панелям администрирования, ограничение попыток неудачного входа
- Запрещение регистрации пользователей при возможности
- Запрещение прав редактирования системных файлов CMS
- Запрещение возможности выполнения скриптов в тех папках, права на запись в которых невозможно выставить без сохранения функционирования CMS
- Регулярное создание резервных копий файлов и БД, на разных серверах и хранилищах
- Минимизация использования дополнительных модулей от сторонних разработчиков
- Регулярное обновление самих CMS и модулей к ним
- Осуществлять проверку файлов сканерами вредоносного кода (AI-Bolit, maldet, clamav и др.)

Все вышеописанные методы позволяют снизить риск сетевой атаки, но не гарантируют полную безопасность веб-сайтов. Максимально эффективным средством является использование систем обнаружения вторжений (IDS).

Для серверов ЦИИР БГУИР, на которых размещаются сайты, работающие на скриптовом языке PHP была выбрана система OSSEC - хостовая система обнаружения вторжений (Open Source Host-based Intrusion Detection System). Данная система обладает открытым исходным кодом, а значит ее использование безопасно. С ее помощью были решены задачи проверки контроля целостности файлов, логирования

различных действий на серверах, получения событий безопасности (анализ системных журналов) и оповещений об этих событиях.

В результате всех описанных методов и средств удалось существенно повысить безопасность сайтов, использующих популярные системы управления содержимым. Количество успешных сетевых атак злоумышленников значительно снизилось: на том же количестве сайтов за месяц наблюдения не было выявлено успешных атак. Проведенная работа подтверждает актуальность выбранного направления исследования информационной безопасности веб-узлов.

Список использованных источников:

17. W3Techs, Software Quality Management Consulting: [Электронный ресурс]. Режим доступа: http://w3techs.com/technologies/overview/content_management/all (Дата обращения: 11.03.2016).

18. Sucuri Security, Critical 0-day Remote Command Execution Vulnerability in Joomla [Электронный ресурс]. Режим доступа: https://blog.sucuri.net/2015/12/remote-command-execution-vulnerability-in-joomla.html (Дата обращения: 10.03.2016).

19. Wikipedia, OSSEC [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/OSSEC (Дата обращения: 10.03.2016).