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

ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

МАТЕРИАЛЫ 51-Й НАУЧНОЙ КОНФЕРЕНЦИИ АСПИРАНТОВ, МАГИСТРАНТОВ И СТУДЕНТОВ

(Минск, 13–17 апреля 2015 года)

Минск, БГУИР
2015

Телекоммуникационные системы и сети: материалы 51-й научной конференции аспирантов, магистрантов и студентов (Минск, 13 –17 апреля 2015 г.). – Минск: БГУИР, 2015. – 61 с.

В сборник включены лучшие доклады, которые были представлены на 51-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

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК УМНОЖИТЕЛЕЙ ЧАСТОТЫ И СМЕСИТЕЛЯ НА ГАРМОНИКАХ В ДИАПАЗОНЕ ЧАСТОТ 118-178 ГГЦ

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

Копшай А. А.

Гусинский А. В. – канд. техн. наук, доцент

В процессе разработки новых средств измерения в диапазоне частот 118-178 ГГц возникает необходимость создания источников СВЧ сигналов с заданными параметрами. Одним из подходов, позволяющих получить требуемые параметры, является умножение частоты сигнала твердотельного синтезатора частоты. Исследуемые в данной работе устройства предназначены для формирования измерительного сигнала СВЧ, а также переноса сигнала СВЧ на промежуточную частоту.

В рамках разработки и изготовления измерителя комплексных параметров цепей в диапазоне частот 118-178 ГГц возникла необходимость провести измерения характеристик предполагаемых элементов СВЧ тракта данного устройства, в частности умножителей частоты и смесителя на гармониках. Это данные необходимы на этапе синтеза структуры измерителя для оценки метрологических характеристик устройства.

В данной работе рассматриваются следующие устройства: удвоитель частоты в диапазоне частот 110-160 ГГц, удвоитель частоты в диапазоне частот 150-180 ГГц, смеситель на гармониках. Целью исследования является получение амплитудных характеристик данных устройств, а именно, коэффициента передачи и коэффициента стоячей волны (КСВ). В качестве входного сигнала умножителей частоты использованы генераторы сигналов СВЧ Г4-161 (диапазон частот 53-78 ГГц) и Г4-186 (диапазон частот 78-118 ГГц). Для измерения мощности сигналов СВЧ используется измеритель мощности М3-75, для сигналов промежуточной частоты – анализатор спектра Agilent E4407B в режиме измерения мощности. Измерение КСВ производится при помощи блока индикаторного Я2Р-70.

Схема установки для измерения модуля коэффициента передачи и КСВ устройств представлены на рисунках 1 и 2.

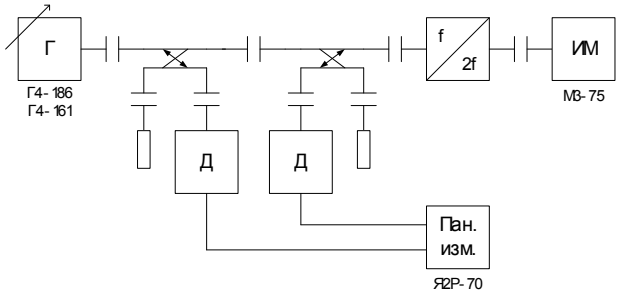

Рисунок 1 – Схема измерения характеристик умножителей частоты

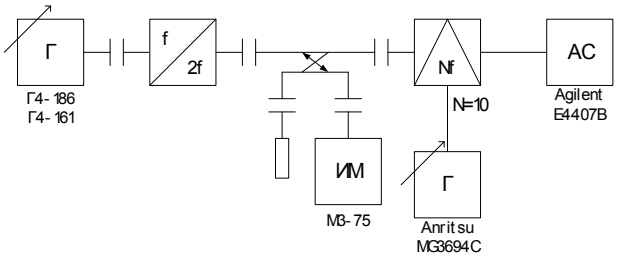

Рисунок 2 – Схема измерения характеристик смесителя на гармониках

В процессе обработки результатов измерений были получены следующие результаты:
– модуль коэффициента передачи умножителя частоты 110-160 ГГц $|S_{21}|$ = (-12,2±1,3) дБ;
– модуль коэффициента стоячей волны умножителя частоты 110-160 ГГц $К_{СВН}$ = (2,6±0,8);
– модуль коэффициента передачи умножителя частоты 150-180 ГГц $|S_{21}|$ = (-22,6±5,4) дБ;
– модуль коэффициента стоячей волны умножителя частоты 150-180 ГГц $К_{СВН}$ = (6,0±0,9);
– модуль коэффициента передачи смесителя на 10-й гармонике $|S_{21}|$ = (-29,7±4,0) дБ.

Также были исследованы зависимости данных параметров устройств от мощности входного сигнала и, в случае смесителя, мощности сигнала гетеродина. Было установлено, что значения модуля коэффициента передачи смесителя на 10-й гармонике существенно зависят от уровня мощности сигнала гетеродина, а именно, имеют локальные максимумы при мощности входного сигнала равной 6,5...7,5 дБм.

Таким образом, в процессе исследований были получены амплитудные характеристики коэффициентов передачи и стоячей волны для трех устройств диапазона частот 118-178 ГГц. Данные характеристики в дальнейшем будут использованы при проектировании и наладке панорамного измерителя параметров цепей данного частотного диапазона.

Список использованных источников:

1. Гусинский, А. В. Векторные анализаторы цепей миллиметровых волн : монография. В 3 ч. Ч. 3 (кн.2) / А. В. Гусинский, Г. А. Шаров, А. М. Кострикин. – Минск: БГУИР, 2008. – с. 474.

КАЛИБРОВКА МНОГОФУНКЦИОНАЛЬНЫХ КАЛИБРАТОРОВ TRANSMILLE СЕРИИ 3000

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

Черношей Е. В.

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

Калибровка - Совокупность операций, устанавливающих соотношение между значением величины, полученным с помощью данного средства измерений и соответствующим значением величины, определенным с помощью эталона с целью определения действительных метрологических характеристик этого средства измерений. В настоящее время на территории РБ начинает активно внедряться процедура калибровки, в связи с чем в данном докладе рассматривается методика калибровки многофункциональных калибраторов Transmille серии 3000.

Калибраторы электрических сигналов Transmille серии 3000 (модели 3010, 3041 и 3050) (далее - калибраторы) предназначены для воспроизведения напряжения и силы постоянного и переменного тока, электрического сопротивления постоянному току, электрической емкости, индуктивности, частоты, электрической мощности, моделирования сигналов термопар и термометров сопротивления. Калибраторы применяются для поверки, калибровки приборов и устройств измерительного типа при разработке, производстве и эксплуатации объектов промышленности. Основные метрологические характеристики калибратора:

- воспроизведение напряжения постоянного тока от 0 В до 1020 В;
- воспроизведение напряжения переменного тока от 0 В до 1020 В;
- сила постоянного тока от 0 А до 30 А;
- сила переменного тока от 0 А до 30 А;
- частотный диапазон от 1 Гц до 10 МГц при точности 28 ppm.

Погрешности воспроизведения тока и напряжения нормируются для каждого поддиапазона в отдельности.
На рисунке 1 отображен внешний вид прибора:

Рисунок 1 – Внешний вид калибратора серии 3000

В данном докладе рассматривается структурная схема приборов, условный принцип их функционирования, а также разрабатывается методика его калибровки по каналам воспроизведения величин постоянного и переменного тока и напряжения

Список использованных источников:

1. Техническая документация фирмы «Transmille Ltd.», Великобритания

КАЛИБРОВКА ВАТТМЕТРОВ-СЧЕТЧИКОВ ЭТАЛОННЫХ МНОГОФУНКЦИОНАЛЬНЫХ ТИПА СЕ 603

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

Арловская Л. С.
Белошицкий А. П. – к-т. техн. наук, доцент

Ценность электроэнергии определяет высокие требования, предъявляемые к точности ее измерения. Своевременная поверка счетчиков электроэнергии позволяет контролировать их соответствие данным требованиям. Для выполнения поверки счетчиков используется специальные установки, а также эталонные ваттметры-счетчики. Для получения точных и качественных измерений эталонные счетчика следует периодически проверять и калибровать. Калибровка проводится по специально разработанным и утвержденным методикам калибровки. В докладе рассматривается методика калибровки ваттметров-счетчиков эталонных многофункциональных типа СЕ 603.

Ваттметры-счетчики эталонные многофункциональные СЕ 603 предназначены для калибровки и определения метрологических характеристик при поверке следующих средств измерений:

электронных и индукционных одно- и трехфазных счетчиков активной и реактивной электрической энергии;

одно- и трехфазных средств измерений активной и реактивной электрической мощности – ваттметров, варметров, преобразователей и калибраторов мощности;

средств измерений напряжения и силы тока – вольтметров, амперметров, преобразователей напряжения и силы тока в промышленном диапазоне частот;

средств измерений и регистрации показателей качества электроэнергии (ПКЭ).

Ваттметр-счетчик обеспечивает контроль режима контролируемой сети и измерение основных показателей качества электрической энергии. На рисунке 1 показан внешний вид прибора всех исполнений:

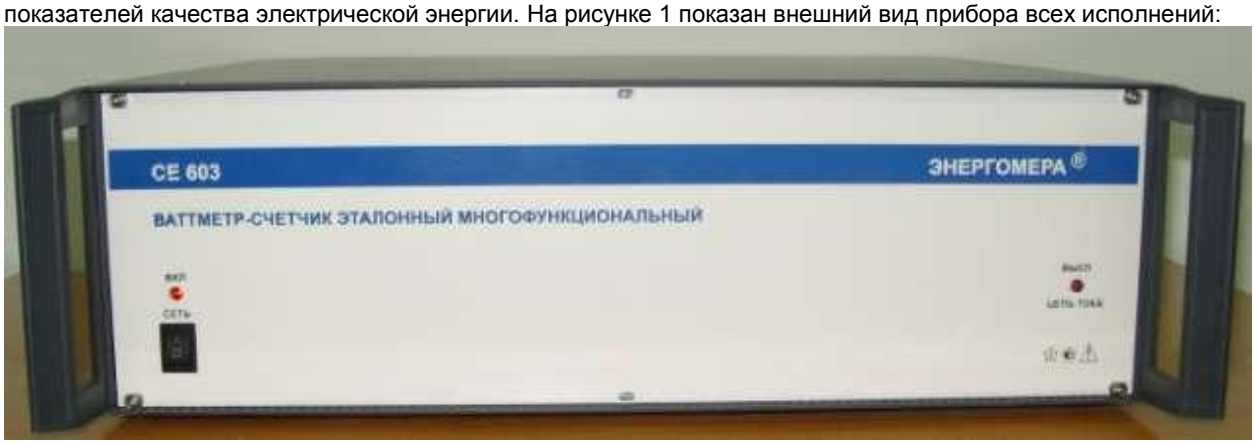

Рисунок 1 – Внешний вид SNA 25-37

Основные характеристики:

1) общий диапазон входных сигналов: напряжение 30-300 В; ток 0,001-120 А.
2) класс точности: 0,2: 0,2S.

Масса прибора составляет не более 17 кг.

Габаритные размеры не более 510*490*145 мм.

Нормальные условия применения:

– температура окружающего воздуха (23±2) ºС;

– относительная влажность воздуха от 30 до 80 %;

– атмосферное давление от 84 до 106 кПа (от 630 до 795 мм рт. ст.);

– допускаемое отклонение частоты тока 5 Гц при питании от сети переменного тока частотой 50 Гц и 6 Гц при питании от сети переменного тока частотой 60 Гц;

– допускаемое отклонение напряжения сети питания переменного тока 22 В.

В докладе рассмотрена структурная схема ваттметра-счетчика, принцип его работы и разработана методика его калибровки. В методике калибровки предусмотрено определение действительных значений и оценка неопределенности измерений мощности (напряжения или тока).

Для оценки неопределенностей выбраны следующая модель измерения:

$Y = U_{\text{изм}} - \delta U_{\text{кв}} - \delta U_0 - \delta U_{\text{к}}$,

где Y – одна из измеряемых величин (мощность, напряжение или ток);

$U_{\text{изм}}$ – действительное значения измеряемой величины;

$\delta U_{\text{кв}}$ – погрешность квантования;

δU_0 – погрешность отклонения от начального значения.

Список использованных источников:

2. Руководство по эксплуатации ваттметра-счетчика эталонного многофункционального типа СЕ 603 ИНЕС.411151.022 РЭ.

ДВУХКООРДИНАТНАЯ ПОЗИЦИОНИРУЮЩАЯ СИСТЕМА ДЛЯ ПРОВЕДЕНИЯ ИЗМЕРЕНИЙ РАСПРЕДЕЛЕНИЯ ПОЛЯ В БЛИЖНЕЙ ЗОНЕ АНТЕННОЙ РЕШЕТКИ

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

Ю. С. Алькевич
В. А. Симоненко

Ревин В. Т. – к. техн. наук, доцент

В статье приведены результаты разработки двухкоординатной позиционирующей системы для проведения измерений распределения поля в ближней зоне антенной решетки

Ключевые слова: *компьютерно-измерительная система, позиционирующая система, автоматизация измерений, фазированная антенная решетка.*

При появлении нежелательных искажений в диаграмме направленности фазированных антенных решеток (ФАР) необходимо в первую очередь установить причину их возникновения. Это можно сделать, если, например, удастся найти распределение амплитуд и фаз поля на раскрыве решетки. Для этого может быть использован зондовый метод, в котором измерительная антенна перемещается параллельно раскрыву решетки в непосредственной близости от излучателей.

Для решения данной задачи необходимо осуществлять точное и плавное движение измерительной антенны по требуемым траекториям. Задачу можно решить простыми средствами, применение которых и технически, и экономически оказывается оправданным. В этом случае речь идёт о координатных столах. Координатный стол представляет собой мехатронную производственную установку, оснащается приводами, информационно-измерительными устройствами и компьютерной системой управления и предназначен для точного перемещения рабочего органа относительно некоторого объекта в процессе выполнения той или иной технологической операции.

С помощью среды графического программирования *LabVIEW* в Научно-исследовательской части Белорусского государственного университета информатики и радиоэлектроники, в Центре 1.6 "Научно-конструкторский центр перспективных радиоэлектронных систем сантиметрового и миллиметрового диапазонов длин волн" была разработана система позиционирования зонда для измерения распределения поля в ближней зоне. Было использовано следующее оборудование:

– координатная система 2*D*-1200-700, технические характеристики:
  количество осей – 2;
  скорость перемещения – 50 мм / с;
  привод – ременно-шаговый;
  перемещение по оси X –1200 мм;
  перемещение по оси Y – 700 мм;
  погрешность установки – ± 0,1 мм.
– шаговые двигатели модели *MS*160, технические характеристики:
  номинальный ток – 2.7 А;
  количество фаз – 2;
  количество полных шагов на оборот – 200;
  напряжение питания – не более 70 В.
– драйвер шагового двигателя *STB*57-3 трехканальный, технические характеристики:
  напряжение питания – 20 .. 40 В;
  ток фазы – до 4 А;
  частота входного сигнала – до 200 кГц.
– плата сбора данных и управления National Instruments *PCI*-6115;
– коннекторный блок *SCB*-68;
– среда разработки и платформа для выполнения программ *LabVIEW* 2009.

Контрольно измерительный стенд, изображенный на рисунке 1, представляет собой двухкоординатную систему управления шаговыми двигателями, которая обеспечивает управление по двум независимым каналам X и Y (используется два шаговых двигателя с ременной передачей). Один из шаговых двигателей перемещает вдоль оси Y второй шаговый двигатель, закрепленный на оси X. Система содержит ограничительные концевики (датчики крайнего положения) по краям осей, сообщающие о достижении крайнего положения перемещения вдоль той или иной оси.

Для предотвращения переотражений поля, стенд покрыт радиопоглощающим материалом.

Управление стендом осуществляется через плату сбора данных *National Instruments PCI*-6115. Данная плата имеет 4 высокоскоростных аналого-цифровых преобразователя с частотой дискретизации до 10 МГц, 2 цифро-аналоговых преобразователя, 8 цифровых входов-выходов и 2 24-битных счетчика-таймера. С платы на драйвер подается тактовый сигнал, задающий скорость переключения управляющих комбинаций шаговых двигателей. Тактовый сигнал формируется за счет применения внутреннего счетчика-таймера платы.

Сигналы управления передаются от ПЭВМ через коннекторный блок *SCB*-68 параллельно на каналы *X* и *Y* трехканального драйвера шагового двигателя *STB*57-3. Драйвер преобразует логические сигналы *STEP* (шаг) / *DIR* (направление) в управляющие сигналы шаговых двигателей в микрошаговом режиме. Происходит перемещение измерительного зонда, согласно заданной программе. Датчики-концевики системы, подключенные к коннекторному блоку *SCB*-68, служат для калибровки начала координат и сообщают о достижении пределов перемещения.

Интерфейс программы управления координатным стендом представлен на рисунке 2.

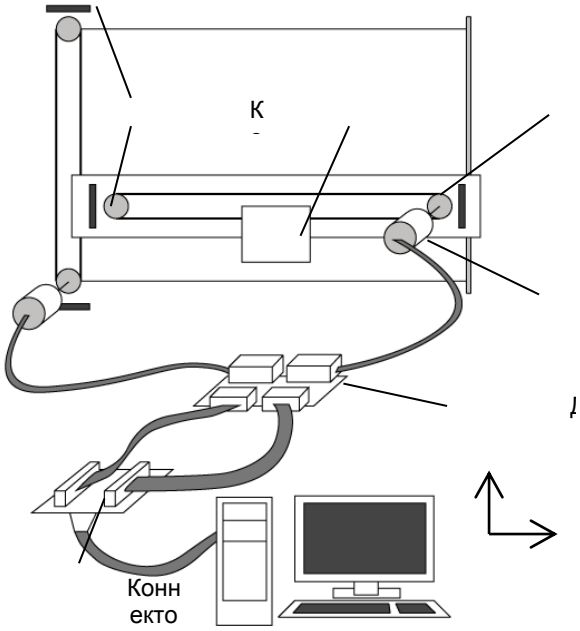

Рисунок 1 – Схематическое изображение стенда

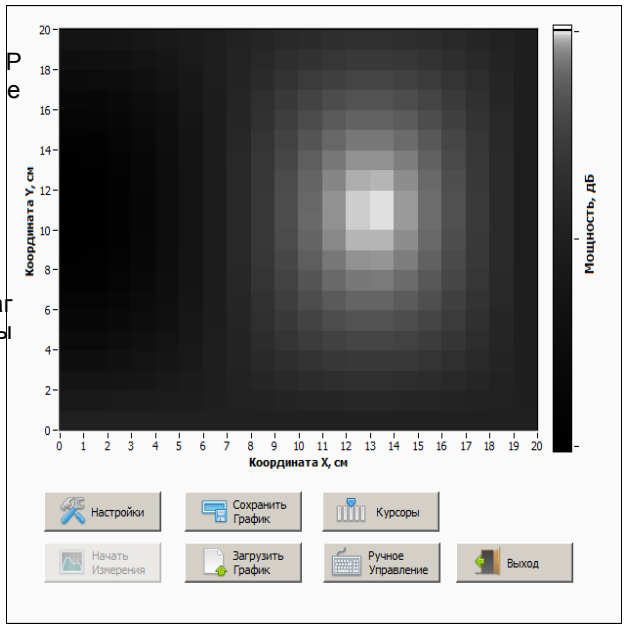

Рисунок 2 – Интерфейс программы управления стендом

Пункты меню программы позволяют выполнять следующие функции:

– «Настройки» – задание начальных и конечных координат перемещения зонда;

– «Начать измерения» – запуск измерений и вывод подробной информации о ходе измерений;

– «Сохранить график» и «Загрузить график» – сохранение или загрузка результатов измерения в файл для последующего воспроизведения;

– «Курсоры» – включение курсоров для измерения уровня мощности в определенной точке плоскости;

– «Ручное управление» – перемещение зонда путем управления шаговыми двигателями с клавиатуры и получение значения мощности в необходимой точке плоскости.

Исходный код управляющей программы в среде *LabVIEW*. Управляющая программа построена с использованием шаблона проектирования – конечный автомат. Это позволяет формировать необходимую пользователю последовательность операций во время исполнения скомпилированного исходного кода и дающего возможность легкого масштабирования функционала программы при дальнейшей разработке. Исходный код построен на двух циклах: главный цикл программы отвечает за реализацию механизма конечного автомата и формирует последовательность операций, таких как:

– инициализация координатного стенда, в которой происходит перемещение измерительного зонда в начальное положение и калибровка координат по концевикам;

– установка координат – перемещение измерительного зонда в необходимую пользователю точку;

– задание области и маршрута измерений;

– операции измерения;

– сохранение и загрузка полученных графиков.

Таким образом, была разработана двухкоординатная позиционирующая система для проведения измерений распределения поля в ближней зоне антенной решетки, удовлетворяющая поставленным требованиям. Основное преимущество использования платы сбора данных и управления National Instruments и среды разработки *LabVIEW* заключается в возможности объединения систем управления и измерения в одной программе, а так же легкого масштабирования необходимого функционала системы.

Список использованных источников:

1. Захарьев Л. Н.. Методы измерения характеристик антенн СВЧ / Л.Н. Захарьев, А. А. Леманский – Москва: Радио и связь, 1985. – 368 с.
2. Блюм П. *LabVIEW*: Стиль программирования / П. Блюм – Москва: ДМК Пресс, 2008. – 400 с.

КАЛИБРОВКА СКАЛЯРНОГО АНАЛИЗАТОРА ЦЕПЕЙ SNA 25-37 В ДИАПАЗОНЕ ЧАСТОТ 25-37 ГГц

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

Вертинский П.И.

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

При проведении измерений главной задачей является получение точных данных об измеряемой величине. Любое СИ следует периодически калибровать или подвергать поверке. Калибровка СИ проводится по специально разработанным и утвержденным методикам калибровки. В докладе рассматривается методика калибровки скалярного анализатора цепей SNA 25-37.

Измеритель SNA 25-37 предназначен для автоматизированного исследования волноводных СВЧ устройств, работающих в частотном диапазоне от 25,95 до 37,50 ГГц и измерения их параметров – модулей коэффициентов передачи и отражения, с цифровым отсчетом измеряемых величин и воспроизведением их частотных характеристик в декартовой системе координат на экране монитора. Объектами измерения (ОИ) могут быть двухполюсники (ДП) – устройства оконечного типа и четырехполюсники (ЧП) – устройства проходного типа.

Основные метрологические характеристики анализатора:

- рабочий диапазон частот анализатора от 25,95 до 37,50 ГГц. Запас по краям диапазона не менее 1 % от значений номинальных граничных частот;
- пределы допускаемой относительной погрешности установки частоты ± 0,002 % от установленной частоты;
- диапазон измерения модулей коэффициентов отражения от 0 до минус 32 дБ;
- диапазон индикации КСВН от 1,05 до 5;
- пределы допускаемой основной погрешности измерения модуля коэффициента отражения $|S_{11}|$ не более $\pm(0{,}2 + 0{,}03|S_{11}|)$ дБ;
- диапазон измерения модулей коэффициентов передачи от 0 до минус 40 дБ.

На рисунке 1 показан внешний вид прибора :

Рис. 1 – Внешний вид SNA 25-37

В докладе рассмотрена структурная схема анализатора, принцип его работы и разработанная методика его калибровки. В методике калибровки предусмотрено определение действительных значений и оценка неопределенности измерений КСВН, ослабления, а также точности отсчета частоты. Описываемые процедуры измерений при калибровке анализатора по указанным выше параметрам, а также методики оценивания неопределенностей.

Для оценки неопределенностей выбраны следующие модели измерения.

Для оценивания неопределенности установки и отсчета частоты.

Модель измерения:

$f = f_{\text{И}} + \Delta f_{\text{Ч}} + \Delta f_{\text{Д}}$,

$f_{\text{и}}$ - показания калибруемого анализатора, ГГц;

$f_{\text{ч}}$ - поправка на неточность эталонного частотомера, ГГц;

$f_{\text{и}}$ - поправка, обусловленная дискретностью калибруемого анализатора, ГГц.

Для оценивания неопределенности измерения КСВН.
Модель измерения:

$K_{CTU} = K_{CTU\text{и}} + \Delta K_{\text{CTUд}} + \Delta K_{\text{CTUэ}} + \Delta K_{\text{CTUр}}$,

$K_{CTU\text{и}}$ - измеренное значение КСВН;

$\Delta K_{\text{CTUд}}$ - поправка на дискретность измерителя;

$\Delta K_{\text{CTUэ}}$ - поправка, обусловленная неидеальностью эталонной нагрузки;

$\Delta K_{\text{CTUр}}$ - поправка на рассогласование узлов СВЧ тракта анализатора.

Для оценивания неопределенности измерения ослабления.
Модель измерения:

$A = A_{\text{и}} + \Delta A_{\text{д}} + \Delta A_{\text{э}} + \Delta A_{p}$,

A_{u} - измеренное значение ослабления;

$\Delta A_{\text{д}}$ - поправка на дискретность измерителя;

$\Delta A_{\text{э}}$ - поправка, обусловленная неидеальностью эталонной нагрузки;

ΔA_{p} - поправка на рассогласование узлов СВЧ тракта анализатора.

Список использованных источников:

1. Руководство по эксплуатации измерителя панорамного КСВН и ослабления ГЛЮИ.411228.009. – Минск, БГУИР 2015. – 45 с.
2. Гусинский А.В., Векторные анализаторы цепей миллиметровых волн: монография. В 3 ч., книга 1.Принципы построения и анализ схем векторных анализаторов цпей / А.В. Гусинский, Г.А. Шаров, А.М. Кострикин. - Минск, 2008. - 240 с.
3. Гусинский А.В., Векторные анализаторы цепей миллиметровых волн: монография. В 3 ч., книга 2.Принципы построения и анализ схем векторных анализаторов цпей / А.В. Гусинский, Г.А. Шаров, А.М. Кострикин. - Минск, 2008. - 241-507 с.

ОЦЕНКА ВЛИЯНИЯ ИНТЕРГАРМОНИК НА КАЧЕСТВО ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ

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

Янченко В. С.

Белошицкий А. П. кандидат технических наук, доцент

В настоящее время большое внимание уделяется качеству электрической энергии. Оценка качества осуществляется посредством контроля нормируемых параметров. Одним из параметров является коэффициент n-ных гармонических составляющих. Гармониками являются токи или напряжения, имеющие частоту, кратную основной частоте переменного тока. В свою очередь, интергармониками или промежуточными гармониками называются токи или напряжения, не являющиеся кратными основной частоте переменного тока. Таким образом, в амплитудно-частотном спектре интергармоники находятся между каноническими. При анализе формы синусоиды переменного тока гармоники и интергармоники определяются как компоненты спектра в квазиустойчивом состоянии в определенном диапазоне частот.

Полного понимания природы электромагнитных возмущений, ассоциирующихся с интергармониками, еще нет, и в настоящее время к этому явлению возникает повышенный интерес. Интергармоники всегда присутствуют в системе электроснабжения, и в последнее время с резким увеличением силовых электронных систем их практическое влияние стало более ощутимым.

Два механизма приводят к появлению интергармоник. Первый заключается в возникновении составляющих в частоте питающего напряжения и его гармониках в результате изменения их амплитуд и/или углов фаз. Это вызывается быстрым изменением значений тока в электроустановках и оборудовании, которые могут быть причиной перепада напряжения. Возмущения вызываются нагрузками в переходных режимах постоянно или временно или во многих случаях при возникновении модуляции токов и напряжений. Эти возмущения носят случайный характер и зависят от оборудования и действующих процессов.

Вторым механизмом является асинхронное переключение (т. е. несинхронизированное с частотой питания) полупроводниковых устройств статических преобразователей. Типичным примером являются преобразователи частоты и устройства с широтно-импульсной модуляцией. Производимые ими интергармоники можно обнаружить практически в любой части спектра питания.

В некоторых изделиях имеют место оба механизма появления интергармоник.

Интергармоники могут появляться при любых значениях напряжения и перетекать из одних систем в другие. Так, интергармоники, образовавшиеся в сетях высокого и среднего напряжения, переходят в сети низкого напряжения и наоборот. Амплитуда интергармоник редко превышает 0,5 % значения амплитуды основной частоты, но в условиях резонанса могут возникнуть и большие значения.

Основные источники возмущений включают:

- дуговые нагрузки;
- электроприводы с переменной нагрузкой;
- статические преобразователи, в частности преобразователи частот с прямым и косвенным управлением;
- устройства управления фазами.

Интергармоники могут также вызываться колебательными явлениями, возникающими, например, в системах с сериями или параллельно установленными конденсаторами, или специфическими режимами работы силовых трансформаторов.

Последствия от появления в питающей сети интергармоник могут быть самые разнообразные. Интергармонические токи вызывают искажение напряжения. Степень искажения напрямую зависит от величины тока и импеданса на частоте каждой интергармоники. Чем больше диапазон составляющих тока, тем выше риск возникновения нежелательных резонансных явлений, которые увеличивают искажения напряжения и могут привести к перегрузке или нарушению в работе оборудования и установок. Кроме искажения напряжения, присутствует риск избыточных тепловых эффектов, появления низкочастотных колебаний, фликера, а также перегрузки пассивных параллельных фильтров высокого порядка. На практике, работа любого оборудования, которое синхронизировано с частотой питающей сети, может быть нарушена.

Наличие данной проблемы подтверждает статистические данные пятилетнего исследования Electric Power Research Institute, которые показывают по причине какого несоответствующего нормам параметра качества электрической энергии или наличия неисправности в сети выходит из строя оборудование.

Некачественная энергия, а именно наличие нежелательных гармонических составляющих в питающей сети, наносит экономический ущерб. Как правило, гармоники в сети вызывают три типа проблем:

дополнительные потери энергии (в трансформаторах, соединительных кабелях, электродвигателях, нейтральных проводниках и т.д.);

преждевременное старение устройства;

сбои в работе или неправильная работа устройства.

По оценкам Institute of Electrical and Electronics Engineers, в случае использования нагрузки мощностью 60 кВт, (что примерно равняется потреблению только компьютеров в офисном здании) подключенной к сети питания 12 часов в сутки на протяжении 365 дней в году, потери по вине наличия гармонических составляющих составят 21,9 МВт/ч, что эквивалентно 8 % затрат на электроэнергию. При анализе высокотехнологичной промышленности цифры оказываются куда более значительными, ввиду того, что ущерб от нарушения или остановки технологического процесса может измеряется в млрд. бел. рублей.

Резюмируя все вышесказанное, можно сделать вывод, что в большинстве случаев, появление интергармоник токов и напряжений зависит от многочисленных сложных процессов в электросетях и носит стохастических характер. В настоящее время, в Республики Беларусь отсутствуют нормы, регламентирующие допускаемые уровни интергармоник, однако, принимая во внимание существующие энергетические, производственные, а следовательно и экономические потери, есть практическая необходимость в исследовании и нормировании.

Список использованных источников:

1. Copper Development Association//Power Quality Application Guide, 3.1.1
2. S. Bhattacharyya, S. Cobben. Consequences of Poor Power Quality – An Overview. – Technical University of Eindhoven.
3. Key, T.S.; & Lai, J.S. (1996). Costs and benefits of harmonic current reduction for switch-mode power supplies in a commercial office building. IEEE Transactions on Industry Applications, vol. 32, no. 5.
4. ТКП 183.1-2009 Методические указания по контролю и анализу качества электрической энергии в системах электроснабжения общего назначения. Часть 1.Контроль качества электрической энергии.
5. ТКП 183.2-2009 Методические указания по контролю и анализу качества электрической энергии в системах электроснабжения общего назначения. Часть 2. Анализ качества электрической энергии.
6. ГОСТ 13109-97 – Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения.

МЕРОПРИЯТИЯ, СПОСОБСТВУЮЩИЕ ПОВЫШЕНИЮ КОНКУРЕНТОСПОСОБНОСТИ ПРЕДПРИЯТИЯ

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

Максименко М.М, ПарфенкоЕ.Н.

Певнева Н.А – ассистент каф. МиС

Главным фактором успеха в условиях рыночных отношений является конкурентоспособность. Конкурентоспособность может рассматриваться относительно таких объектов, как товар, предприятие, отрасль, регион, страна в целом. Важную роль в формировании конкурентоспособности страны играет конкурентоспособность отдельно взятых предприятий. Известно, что уровень конкурентоспособности определяется большим числом факторов, соответственно, могут быть выделены и различные направления в решении этой задачи.

Для того чтобы стать конкурентоспособной компанией необходимо:

— обеспечить конкурентоспособность выпускаемой продукции в целевых сегментах рынка. Под конкурентоспособностью товара подразумевается оцененное потребителем свойство объекта превосходить в определенный момент времени по качественным и ценовым характеристикам аналоги в конкретном сегменте рынка без ущерба для производителя.

— поднять потенциал конкурентоспособности предприятия, а следовательно и его подразделений, до уровня мировых производителей в данной отрасли.

Высокая конкурентоспособность предприятия обусловливается наличием следующих трех признаков:

1) потребители довольны и готовы купить повторно продукцию этой фирмы (потребители возвращаются, а товары нет);

2) общество, акционеры, партнеры не имеют претензий к фирме;

3) работники гордятся своим участием в деятельности фирмы, а посторонние считают за честь трудиться в этой компании.

Факторы, влияющие на конкурентоспособность:

1) размер рынка — чем больше, тем сильнее конкуренты;

2) темпы роста рынка — быстрый рост облегчает проникновение на рынок;

3) мощности — излишние мощности приводят к падению цен;

4) препятствия для входа или выхода из рынка защищают позицию фирмы, их отсутствие делает рынки уязвимыми для проникновения туда неконкурентных новичков;

5) цена;

6) уровень стандартизации товаров — покупатели имеют преимущество, так как им легко переключиться с одного товара на другой;

7) мобильные технологические модули;

8) требования к размерам необходимых капитальных вложений — жесткие требования повышают риск, создают дополнительные барьеры входа — выхода;

9) вертикальная интеграция повышает требования к размерам капитала, приводит к сильным различиям в конкурентоспособности и затратах на производство интегрированных, частично интегрированных и неинтегрированных фирм;

10) экономия на масштабе – увеличивает долю рынка, необходимую для достижения конкурентоспособности товара;

11) быстрое обновление ассортимента продукции.

Стремление к повышению конкурентоспособности ориентирует на увеличение объема производства и сбыта продукции, нужной потребителю, снижение затрат на транспортировку. При развитой конкуренции этим достигается не только цель предпринимательства, но и удовлетворение общественных потребностей

Список использованных источников:

1. Аристо О.В. Конкуренция и конкурентоспособность: Учеб.пособие/О.В.Аристов-М: Финстатанфорум, 1999.

2. Богомолова И.П. Анализ формирования категории «конкурентоспособность», как фактора рыночного превосходства экономических объектов [Электронный ресурс] / И.П. Богомолова, Е.В. Хохлов // http://www.dis.ru/ im/article.shtml?id=3548.

ЗАВИСИМОСТЬ МЕНЕДЖМЕНТА КАЧЕСТВА ОТ МЕНТАЛИТЕТА

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

Гаричкина А. А.

Певнева Н.А – ассистент каф. МиС

Для практики менеджмента важно обладать знаниями о национально-исторических особенностях, чтобы определить их влияние на культуру организации, оценить возможность слияния элементов различных национальных культур в рамках одной организации.

Менталитет — подсознательная социально-психологическая «программа» действий и поведения отдельных людей, нации в целом, проявляемая в сознании и в практической деятельности людей. Источником ее формирования выступает совокупность психологических, социально-экономических, природно-климатических явлений, действующих на протяжении длительной эволюции стран.

Культурное разнообразие не что-то такое, что завтра исчезнет, дав нам возможность строить планы, исходя из допущения, что мы понимаем друг друга. Само по себе это явление таит богатства, изучение которых может принести неизмеримую пользу не только тем, что расширит наш кругозор, но и тем, что повысит эффективность наших стратегий деловой деятельности. Люди разных культур пользуются одними и теми же основными понятиями, но вкладывают в них разный смысл. Это определяет особенности их поведения, которое часто представляется нам иррациональным и противоположным тому, что мы считаем очевидным.

Внимание к культурным корням и национальным особенностям других людей, как в обществе, так и в сфере бизнеса позволит нам предвидеть и удивительно точно просчитать то, как они будут реагировать на наши предложения. Более того, мы сможем в определенной степени предсказывать их отношение к нам. Практическое знание базовых черт других культур (как и своей собственной) сведет к минимуму неприятные сюрпризы, даст нам необходимое понимание, которое позволит преодолеть былые трудности общения с представителями других стран.

В настоящие время общепризнанно, что национальный и региональный менталитеты – важнейший фактор, влияющий на формы, функции и структуру управления. Однако констатации этого факта еще недостаточно. Между менеджментом и менталитетом существует более глубокая сущностная взаимосвязь. Преобладание трудолюбия, бережливости, пунктуальности и т.д. также будут определять формы и методы управления, пронизывать поведение, действия управленцев.

Итак, «менталитет-менеджмент», их соотношение, соответствие и противоречие выступает как содержание и форма, как сущность и явление. Они находятся в неразрывной объективно обусловленной, постоянно повторяющейся взаимосвязи, которую можно квалифицировать как «*закон соответствия менталитета и менеджмента*». Соответствие между менеджментом и менталитетом обуславливает относительно устойчивую систему производства, сглаживает противоречия между управляемыми и управляющими, способствует преодолению кризисных ситуаций. Соответствие между менеджментом и менталитетом – одна из основополагающих черт равновесия социальных систем, характеризуемых отсутствием социальных конфликтов. Закон соответствия менеджмента менталитету означает, что определенной ментальности, каждой конкретной черте национального характера, стороне менталитета в целом соответствуют адекватные формы, виды, системы менеджмента.

В мире существуют различные модели менеджмента, учитывающие национальную специфику той или иной страны. В первую очередь это связано с особенностями корпоративной культуры разных народов. Как известно, характер деловых взаимоотношений людей — главное в менеджменте.

В настоящее время под менеджментом понимают прежде всего управление в социальной сфере, а именно, управление организациями, их звеньями и работниками. Необходимость теоретических исследований по менеджменту не подлежит сомнению, ведь вся наша жизнь связана с организациями, занимающимися управленческой деятельностью, от которой зависит не только благосостояние, но и состояние духа в стране. В то же время существует большое количество подходов, школ и направлений в менеджменте, которые имеют различные трактовки управленческой деятельности и различную «окраску» в зависимости от менталитета.

На сегодняшний день очень важно учитывать национальные особенности, потому что учет характеристик менталитета позволяет определить политику государства в области менеджмента: разработку концепции развития отечественного менеджмента, выбор направления прикладных исследований и заимствования управленческого опыта, определение механизмов конкуренции и сотрудничества с фирмами других стран, разработку программ профессионального обучении менеджеров.

Список использованных источников:
1. Льюис Р. Д., Деловые культуры в международном бизнесе. От столкновения к взаимопониманию / Р. Д. Льюис – Москва, 1999.
2. Картавый М. А., Нехашкин А. Н., Методологические принципы формирования российского менеджмента / М. А. Картавый, А. Н. Нехашкин // Менеджмент в России и за рубежом – 1999. – №3.

МОДЕРНИЗАЦИЯ КАБЕЛЬНОЙ СЕТИ ПО ТЕХНОЛОГИИ FTTH

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

Шершнев А. О.

Мищенко В. Н. – к-т. техн. наук, доцент

В Беларуси наметилась тенденция перехода от электрических линейно-кабельных сооружений связи к оптическим. Рост покупательской способности населения Республики Беларусь, повышение интереса к сети интернет, IP-приложениям, мультимедийным услугам обусловливают развитие сети доступа в направлении расширения полосы пропускания. Оптическое волокно практически не имеет ограничений по полосе пропускания, многократно превосходит медную пару по дальности связи и не оказывает влияния на соседние волокна.

В настоящее время оптоволоконные сети доступа строятся исходя из различных концепций FTTx . Fiber To The Building (FTTB) – оптоволоконный кабель ведется в здание; Fiber To The Curb (FTTC) – оптика до группы домов; Fiber To The Home (FTTH) – оптоволоконный кабель проводится в частный дом или квартиру. В первых двух случаях приходит витая пара или коаксиальный кабель, а в узле сопряжения оптического и медножильного кабеля стоит активное оборудование. В случае же FTTH оптоволокно подводится непосредственно к абонентской розетке. Концепция FTTH на данный момент является самой перспективной и позволит удовлетворять растущие запросы абонентов еще долгое время. Одним из возможных решений может стать технология построения пассивных оптических сетей PON. PON – это семейство быстроразвивающихся, наиболее перспективных технологий широкополосного мультисервисного множественного доступа по оптическому волокну. Суть технологии пассивных оптических сетей, вытекающая из ее названия, состоит в том, что ее распределительная сеть строится без каких-либо активных компонентов: разветвление оптического сигнала осуществляется с помощью пассивных делителей оптической мощности – сплиттеров. Следствием этого являются снижение стоимости системы доступа, уменьшение объема необходимого сетевого управления, высокая дальность передачи и отсутствие необходимости в последующей модернизации распределительной сети.

Технология пассивных оптических сетей (PON) также позиционируется производителями как экономичная и способная обеспечить широкополосную передачу мультимедийного трафика в структуре ATM (BPON), SDH (GPON), Ethernet (EPON).

Основными элементами сети PON являются: центральный узел (OLT) (OLT – Optical Line Terminal); пассивные оптические разветвители; оконечное оптическое оборудование (ONU) (ONU – Optical Network Unit). Между центральным узлом и оконечным оптическим оборудованием (ONU) размещается один или несколько пассивных оптических разветвителей, обеспечивающих распределение оптического сигнала от OLT к нескольким ONU. Для нисходящего канала от OLT к ONT (ONT – Optical Network Terminal) используется длина волны 1490 нм, а для восходящего канала от ONT к OLT – длина волны 1310 нм (длина волны 1550 нм используется обычно для передачи сигналов кабельного телевидения). Прямой поток на уровне оптических сигналов является широковещательным. Каждый абонентский узел ONT, читая адресные поля, выделяет из общего потока предназначенную только ему часть информации. Для того чтобы исключить возможность пересечения сигналов от разных ONT, для каждого из них устанавливается свое индивидуальное расписание по передаче данных с учетом поправки на задержку, связанную с удалением данного ONT от центрального узла OLT. Главным достоинством сетей GPON является возможность оказания множества услуг, например Triple Play, с гарантированным качеством обслуживания абонентов (QoS). Это достигается за счет того, что для передачи чувствительного к задержкам и их вариациям трафика (например, голос или видео) может использоваться протокол ATM, а для передачи данных – протокол Ethernet. В оборудовании GPON также имеется возможность организации TDM каналов, что дает возможность пользоваться традиционной телефонией, а также предоставлять потоки E1 операторам сотовой подвижной электросвязи.

Детально было рассмотрено построение абонентского участка, который предназначен для персональной абонентской разводки одноволоконных кабелей (реже двухволоконных) от элементов общих распределительных устройств до оптической розетки и активного оборудования ONT в квартире абонента или до группового сетевого узла ONU, смонтированного в офисе корпоративного клиента. Отработаны варианты построения станционных участков, которые включают в себя оборудование OLT и оптического кросса высокой плотности ODF (ODF – Optical Distribution Frame).

Был выполнен проект модернизации кабельной оптической сети для микрорайона Зеленый луг 6, г. Минск, состоящей из десяти панельных домов. При этом учитывалось реальное количество абонентов, которым необходим весь спектр услуг современных телекоммуникационных сетей с высокой скоростью передачи.

РАДИОРЕЛЕЙНАЯ СИСТЕМА ПЕРЕДАЧИ ДЛЯ СОТОВЫХ СЕТЕЙ РАДИОСВЯЗИ

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

Омелюсик В. Л.

Мищенко В. Н. – к-т. техн. наук, доцент

Радиорелейные линии связи занимают одно из важнейших мест в системах средств передачи информации. Быстрое развитие технологии открывает новые возможности в этой области. Потребность в недорогих и надежных цифровых радиорелейных системах передачи (ЦРРСП) с относительно небольшой протяженностью и емкостью стремительно возрастает. Для частот выше 10 ГГц разработано и имеется на рынке большое количество типов аппаратуры как отечественного, так и зарубежного производства.

Конструктивно, такая аппаратура часто выполняется в виде моноблоков, когда приемопередающее оборудование и антенна составляют единое целое. Это дает возможность строить на линиях связи простые необслуживаемые промежуточные станции с относительно недорогими антенными опорами. Многие системы полностью автоматизированы, и управляются микропроцессорными или компьютерными устройствами, имеют гибкую структуру и обеспечивают реализацию различных конфигураций сетей.

Подобная аппаратура может применяться для организации: линий связи между населенными пунктами; телекоммуникационных сетей связи; технологических линий и сетей связи для железнодорожного транспорта, энергосистем, газо- и нефтепроводов; связи между компьютерными и офисными центрами; соединительных линий для базовых станций сотовой подвижной связи; микроволновых систем распределения информации; временных линий и сетей связи для проведения массовых мероприятий или аварийно-спасательных работ; линий и сетей связи для производственных объединений; сетей связи для крупных производственных предприятий .

Рабочие частоты радиорелейного оборудования обычно находятся в диапазоне от 2 до 40 ГГц и жестко регламентируются внутри каждой полосы рекомендациями ITU (Международного союза электросвязи). На частотах выше 10 ГГЦ уменьшается допустимое расстояние между станциями из-за роста затухания радиоволн в атмосфере и значительных замираний при осадках. На частотах 60 ГГц наблюдается полная непрозрачность атмосферы из-за поглощения радиоволн в атомах кислорода.

Радиорелейное оборудование в настоящее время широко используется для построения соединительных линий между базовыми станциями и контроллером базовых станций сотовых систем связи. Использование радиорелейных линий целесообразно в условиях густонаселенных городских районов, где прокладка оптического кабеля практически нереальна. Архитектура сети радиодоступа стандарта сотовой связи UMTS предназначена для объединения режимов передачи данных с коммутацией каналов и коммутацией пакетов. Основное отличие стандарта UMTS состоит в использовании широкополосных сигналов в диапазоне 2 ГГц, позволяющее добиться более высокого по сравнению с GSM качества обслуживания. В последнее время были внедрены более скоростные режимы передачи информации - режимы HSPA и HSPA+. Известно, что максимальная пропускная способность сети UMTS в режиме HSPA с использованием одной несущей равняется 14,4 Мбит/с, в режиме HSPA+ - до 21 Мбит/с. Все перечисленные обстоятельства сетей сотовой связи накладывают определенные условия на параметры сигналов, которые передаются через соединительные РРСП в сети сотовой связи стандарта UMTS.

Выполнен анализ структурных схем современной аппаратуры ЦРРСП. На основании результатов этого анализа была разработана структурная схема, объединяющая в себе инженерные решения, которые целесообразно применить при построении аппаратуры ЦРРСП.

Использована методика расчёта ЦРРСП, учитывающая технические характеристики передающего и приемного оборудования, а также условия и принципы распространения электромагнитных волн в свободном пространстве.

Выполнен расчёт цифровой радиорелейной линии прямой видимости. Расчет энергетических параметров радиорелейной линии выполнялся для следующих параметров: диапазон частот, ГГц – 17,5 – 18,35; типовая длина интервала, км – 15; скорость передачи (основной поток), Мбит/с – 21; минимально допустимый уровень сигнала на входе приёмника (чувствительность), дБм, при BER = 10^{-6} – минус 80; вид модуляции – 64 QAM; выходная мощность, дБВт – 2,5; диаметр приемных и передающих параболических антенн, м – 0,6; ослабление сигнала в фидерных линиях, дБ – 0,5. Определялась величина одного из важнейших параметров для расчета цифровой системы радиосвязи – запаса на замирания, который представляет собой разницу между уровнями сигнала на входе приемника в отсутствии замираний и пороговым уровнем, при котором коэффициент ошибок составляет определенную величину.

Был выполнен выбор трассы радиорелейной линии путем подбора на топографической карте позиций развертывания станций. Выбор мест расположения радиорелейных станций для организации системы сети стандарта UMTS производился для города Бреста и его окрестностей. В процессе проектирования с использованием программы ГИС MapInfo выбиралось расположение станций РРСП, что позволило учесть структуру рельефа местности и корректно определить основные особенности построения профилей интервалов линии радиосвязи.

КАЧЕСТВО ГОЛОСОВОЙ СВЯЗИ, МОДЕЛЬ РЕАЛИЗАЦИИ В СЕТЯХ НА ОСНОВЕ ОБОРУДОВАНИЯ CISCO

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

Пышненко В. И.

Неборский С.Н – канд. техн. наук, доцент

Предлагается модель качества программных средств голосовой связи в сетях CISCO. Модель основана на стандартах качества группы ISO/IEC 25nnn и включает характеристики: надежность, эффективность, функциональность и сопровождаемост

С ростом комплексных потребностей в области интегрированных услуг по передаче голоса качество обслуживания (QoS), стало ключевым фактором сервисов с жесткими гарантиями качества обслуживания.

VoIP (Voice over IP) стремительно изменяет облик современной телефонии. Термин "Voice over IP" подразумевает под собой VoIP-сети, включая потоковые и сигнальные протоколы, а также кодеки.

Для оценки качества программных средств VoIP предлагается следующая модель качества:

$$Q = \{F, R, E, M\},$$

где F – множество подхарактеристик функциональности, R – множество подхарактеристик надежности, E – множество подхарактеристик эффективности, M – множество подхарактеристик сопровождаемости.

Данная модель основана на стандарте ISO/IEC 25010:2011 Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models [1].

Для внедрения VoIP-решений требуется тщательный анализ сетевых требований и текущих условий с целью обеспечения качества звонка, сопоставимого с аналоговой средой (PSTN - Public Switched Telephone Network). Cisco является одной из компаний, работающих в области создания технологий и протоколов, повышающих качество передачи голоса в сетях IP.

Определяя требования функций качества обслуживания корпоративного трафика IP-телефонии, рекомендуется придерживаться следующих правил:

- Голосовой трафик должен быть промаркирован как DSCP EF, в соответствии с "Базовыми Основами QoS" и RFC 3246.
- Сигнализация должна быть промаркирована как CS3, в соответствии с "Базовыми Основами QoS" (во время миграции можно использовать AF31).
- Потери пакетов в магистралях спроектированных для предоставления VoIP сервиса высокого качества не должны превышать 0.25 процентов.
- Односторонняя задержка не должна превышать 150ms, в соответствии со International Telecommunication Union (ITU – Международный Союз Электросвязи) G.114.
- Колебания задержки (jitter) должны быть менее 10 мсек.
- Для каждого разговора (в зависимости от частоты квантирования, кодека и заголовка второго уровня) требуется 21-106 kbps гарантированной приоритетной полосы пропускания.
- Для трафика сигнализации требуется 150 bps (плюс заголовок второго уровня) гарантированной полосы пропускания.

На качество голосовой связи напрямую влияют все три фактора качества QoS:

- Потери пакетов;
- Задержка;
- Вариации задержки;

Также для обеспечения QoS в Cisco IOS поддерживаются следующие протоколы [2]:

- WFQ - протокол взвешенной справедливой очередности (Weighted Fair Queuing) .
- Протокол приоритетной очередности и обычной очередности (Priority Queuing and Custom Queuing).
- WRED - протокол взвешенного случайного раннего обнаружения (Weighted Random Early Detection).
- Коммутация по меткам (Tag Switching) / многопротокольная коммутация по меткам (MPLS)

Потери пакетов вызывают кратковременные пробелы в разговоре. Стандартные алгоритмы кодирования, используемые в Cisco Digital Signal Processor (DSP), с помощью алгоритмов маскирования могут восстановить потери до 30 мсек. Таким образом, потери двух и более последовательных 20 мсек сэмплов приведут к заметной деградации качества голоса.

В стандарте Международного Союза Электросвязи для технологии VoIP (G.114) говорится, что задержка величиной в 150 мсек в одном направлении является приемлемой для качество голосовой связи. Было продемонстрировано, что разница в качестве голоса между сетями с задержкой в 150 мсек и 200 мсек является незначительной и практически незаметной для пользователя. Cisco рекомендует ориентироваться на ITU стандарт 150 мсек, но если существуют ограничения не позволяющие добиться такого бюджета, то размер задержки может быть увеличен до 200 мсек без значительной деградации качества связи.

Что же касается колебаний задержки, то для их выравнивания в устройствах Cisco для IP-телефонии

используются адаптивные буферы. Однако они могут компенсировать колебания задержки лишь в пределах от 20 до 50 мсек. При централизованной обработке вызовов IP-телефоны используют контрольные каналы TCP для связи с Cisco CallManager.

Качество голосовой связи во многом зависит от обработки голоса на шлюзе. Шлюз Cisco поддерживает множество средств кодирования и декодирования (CODEC). Для обеспечения высокой устойчивости к неблагоприятным условиям окружающей среды и шлюзы могут устанавливаться на платформах, отвечающих стандарту NEBS (Network Equipment-Building System – Система создания сетевого оборудования). Этот стандарт используется региональными операторами (Regional Bell Operating Companies - RBOC), чтобы гарантировать устойчивость оборудования к экстремальным температурам, высокой влажности, условиям высокогорья, пожарам, землетрясениям, повышенной вибрации, всплескам напряжения в сети питания, прекращению подачи электричества и электромагнитным помехам.

При проектировании сети операторы должны учитывать требования к качеству обслуживания, предъявляемые корпоративными клиентами. Общая проблема операторов и корпоративных клиентов заключается в богатстве QoS функциональности Cisco iOS и, как следствие, мириады вариантов реализации и комбинаций. Практически каждый опытный инженер имеет свой собственный взгляд на их применение. Для того, чтобы дать некоторые общие рекомендации по реализации качества обслуживания, Cisco воплотила новую инициативу, под названием "Базовые Основы QoS", целью которой является унификация решений на платформах оборудования Cisco. В "Базовых Основах QoS" [3] специфицирована маркировка и правила обработки до 11 классов сервиса в корпоративных сетях. Важно отметить, что "Базовые Основы QoS" не диктуют каждому корпоративному клиенту немедленно внедрить 11 классов трафика, а скорее учитывают существующие и будущие потребности в поддержке QoS. Даже если корпоративному клиенту сейчас нужна только часть из этих 11 классов, то следование рекомендациям "Базовых Основ QoS" позволит им в будущем плавно мигрировать на расширение количества поддерживаемых классов в будущем.

Список использованных источников:

1. ISO/IEC 25010:2011 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models. – 2011.

2. Yen, Y.S, Nat. Dong Hwa, Chen, W. Sliding weighted fair queueing scheme for real-time applications// Communications, IEE Proceedings. – 2005.-№152.- P. 320 – 326.

3. How QoS Mechanisms Affect VoIP QoS Metrics// IDE1070. – 2010.

ВЗАИМОСВЯЗЬ СКОРОСТИ ЦИФРОВОГО ПОТОКА И ПРОПУСКНОЙ СПОСОБНОСТИ КАНАЛА

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

Сазанов А.С., Джумаева А.А

Ткаченко А.П. – канд. техн. наук, доцент

В системах цифрового ТВ вещания ЦТВ важное значение придается их эффективности - спектральной $\gamma_{сэ}$ и энергетической $\gamma_{ээ}$

Сопоставляются удельная скорость цифрового потока, удельная пропускная способность канала (бит/с·Гц) и $\gamma_{ээ}$, как отношение энергии, приходящейся на бит $E_б$, Вт/Гц, к спектральной плотности мощности шума N_0,Вт/Гц, для определения путей их повышения.

Обобщенная структурная схема системы ЦТВ представлена на рис.1. Она включает три фундаментальных процесса: кодирование – декодирование (на передающей и приёмной сторонах соответственно) источника, кодирование – декодирование канала и модуляцию – демодуляцию.

Рис. 1 – Обобщённая структурная схема цифровой системы передачи ТВ изображений

На передающей стороне все виды обработки сообщений в блоках 2 – 6 служат цели преобразования их в такие сигналы, которые наиболее подходят для передачи по каналу конкретного типа – по свободному пространству (радио- или атмосферному оптическому каналу), либо по направляющей среде (кабелю металлическому или световодному, т.е. волоконно-оптическому).

В кодере источника 4 осуществляются: ограничение полосы частот сигналов значением высшей частоты $F_В$, аналого-цифровое преобразование (АЦП) и существенное уменьшение избыточности, а в кодере канала 5 – помехоустойчивое кодирование, преимущественно каскадное с относительной скоростью $R_К$, сопровождающееся перемежением битов, байтов и символов. Завершается процесс многопозиционной модуляцией в блоке 6.

При передаче изображений источником сообщений являются объекты, оптическое изображение которых нужно ещё построить. Эту задачу выполняет оптическая система 2, которая на светочувствительной поверхности передающей трубки 3 (в общем случае выполняющей роль оптико-электронного преобразователя – ОЭП) строит плоское оптическое изображение $L_{ОИ}(x, y, t)$. В цветном телевидении отражённый от объекта световой поток сначала расщепляется светоделительной оптикой на три цветоделённых потока $L_{ОИ.R}(x, y, t)$, $L_{ОИ.G}(x, y, t)$, $L_{ОИ.B}(x, y, t)$, которые и поступают на три передающие трубки.

Таким образом, оптическое изображение является многомерной пространственно-временной функцией (ПВФ), которая в ТВ камере преобразуется в одномерный ТВ сигнал: сначала оптическое изображение преобразуется в электронное (рельеф зарядов, фотопроводимостей или потенциальных ям в зависимости от типа ОЭП: электровакуумные передающие трубки, ПЗС- или КМОП – матрицы), а затем с помощью электронной развёртки ПВФ преобразуется в сугубо временную и формируются видеосигналы $U(t)$ - три сигнала основных цветов.

На приёмной стороне в блоках 8 – 11 производятся обратные операции для восстановления информации в исходном виде с минимально возможными искажениями. Принятый сигнал $\tilde{U}(t)$ на входе электронно-оптического преобразователя – ЭОП 11 всегда будет отличаться от переданного. Объясняется это неизбежными искажениями информации ввиду не идеальности процессов её прямого и обратного преобразования, отличием характеристик тракта от идеальных, а также системными ограничениями и действием внутренних и внешних помех. В каждом конкретном случае в зависимости от вида передаваемой информации нормируются допустимые искажения сигнала или вероятность ошибок.

Случайный характер сообщений, сигналов и помех обусловил важнейшее значение теории вероятностей в теории связи и вещания .Вероятностные свойства сигналов и сообщений , а также среды , в которой передается сигнал , позволяют определить количество передаваемой информации и ее потери.

Скорость цифрового потока$B_{ИНФ}$.,бит/с на выходе АЦП пропорциональна частоте дискредитации $F_Д$и разрядности двоичного кодирования m:

$$B_{ИНФ} = f_Д \cdot \log_2 N_{КВ} = f_Д \cdot m, \quad (1)$$

где $N_{КВ}$– количество уровней квантования, $N_{КВ} = 2^m$. При выборе значения $f_Д$ учитываются требования теоремы отсчетов

$$f_Д \geq 2F_В, \quad (2)$$

и ряд дополнительных, специфичных для ТВ [1, 4]. Условие (2) является достаточным всегда и одновременно необходимым, если обеспечивается условие

$$F_В/F_Н \geq 2, \quad (3)$$

где $F_Н$ – низшая частота спектра аналогового сигнала. В ТВ сигнале условие (3) выполняется.

Для полосовых сигналов, у которых

$$F_В/F_Н < 2, \quad (4)$$

необходимым значением $f_Д$ является

$$f_Д' = 2(F_В+F_Н) / (2n+1), \quad (5)$$

где n = 1, 2, … , при наименьшем n.

При этом $f_Д' < f_Д$ и поэтому уменьшается как скорость (1) цифрового потока, так и требуемая полоса канала. Для восстановления аналогового сигнала на выходе ЦАП в этом случае нужно применить ПФ вместо ФНЧ.

Скорость $B_{КК}$, бит/с и $B_{СИМВ}$, симв/с на выходах блоков 5 и 6 соответственно имеют вид

$$B_{КК} = B_{ИНФ.СЖ} / R_К, \qquad B_{СИМВ} = F_К / b_Р = B_{КК} / \log_2 M,$$

где $B_{ИНФ.СЖ} = B_0$ – скорость цифрового сигнала с учетом сжатия, $F_К$ – полоса частот канала, $b_Р$ – коэффициент расширения полосы, M – количество амплитуд и фаз или только фаз, которые принимает несущая при многопозиционной модуляции.

Дополнительным свойством сложных (многопозиционных) видов модуляции является более плотная упаковка данных в частотной области, когда на единицу полосы пропускания приходится больше передаваемой информации.

Учитывая изложенное, можно записать выражение для определения максимально допустимой скорости цифрового потока B_0 на выходе блока 4, которую можно “вписать” в канал с шириной полосы $F_К$

$$B_0 = B_{КК}R_К = B_{СИМВ}R_К\log_2 M = (F_К R_К / b_Р)\log_2 M, \quad (6)$$

и выражение для пропускной способности канала $C_К$ в соответствии с формулой Шеннона:

$$C_К = F_К\log_2 (1+P_С / P_Ш) = F_К\log_2 [1+(E_b / N_0) \cdot (B_0 / F_К)]. \quad (7)$$

В выражения (7) учтена зависимость между отношением средних мощности сигнала и шума $P_С / P_Ш$ и отношением E_b / N_0 [2]. При анализе $\gamma_{с.э}$ и $\gamma_{э.э}$ необходимо перейти к удельным скорости $B_0 / F_К$ и пропускной способности $C_К / F_К$. После деления выражений (6) и (7) на $F_К$, приравняем правые их части:

$$(R_К / b_Р) \log_2 M = \log_2 (1+P_С / P_Ш) = \log_2 [1+(E_b / N_0) \cdot (B_0 / F_К)]. \quad (8)$$

При использовании многочастотной схемы модуляции COFDM в (8) нужно учесть и относительную длительность защитного интервала. Наличие в (6) и (8) относительной скорости помехоустойчивости кодирования $R_К$ не позволяет судить об энергетическом выигрыше от кодирования. Так, напр., при сверточном кодировании (СК) с $R_к$ = 1/2 выигрыш будет максимальным, но различным в зависимости от типа СК. Однако, при фиксированной после $F_к$ и скорости $B_{кк}$ (для выбранного вида модуляции) необходимо при этом уменьшать информационную скорость B_0. Ряд выражений для оценки выигрыша от кодирования получен в работе [3]. Анализ выражения (8) показывает на некоторые пути осуществления обменных операций между $\gamma_{с.э}$ и $\gamma_{э.э}$ и возможные варианты их одновременного увеличения, что во многом обеспечивается в системах ЦТВ DVB второго поколения.

Список использованных источников:
1. Зубарев, Ю. Б. Цифровое телевизионное вещание. Основы, методы, системы / Ю. Б. Зубарев, М. И. Кривошеев, И. Н. Красносельский. – НИИР, 2001. – 568с.
2. Ткаченко, А. П. Тенденции развития систем цифрового телевизионного вещания / А. П. Ткаченко, М. И. Зорько, Д. А. Хатьков // международная научно – техническая конференция, приуроченная к 50 – летию МРТИ – БГУИР (Минск, 18-19 марта 2014 года): материалы конф. В 2 ч. Ч.1. – Минск: БГУИР, 2014. - 539с. (С. 261-263).
3. Липкович, Э. Б. Системы наземного цифрового телевизионного вещания: метод. пособие / Э. Б. Липкович. – Минск: БГУИР, 2006. – 84с.
4. Ткаченко, А. П. Цифровое представление сигналов изображения и звукового сопровождения: учеб. пособие / А. П. Ткаченко, П.А. Капуро, А. Л. Хоминич. – Минск: БГУИР, 2003. – 56с.

РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ

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

Ярук А.М., Киевец Н.Г.

Корзун А.И. - кандидат технических наук, доцент

Представлены результаты тестирования случайных последовательностей по тестам FIPS-140-2 при различных программных реализациях.

Одним из основных элементов систем криптографической защиты информации является криптографический ключ. Ключи, как правило, формируются с помощью генераторов случайных последовательностей (ГСП). Ключи, отвечающие высоким требованиям к равномерности распределения вероятностей случайных чисел, должны быть получены от качественных генераторов. Качество генератора определяется путем его тестирования. Вследствие этого представляет интерес разработка инструментальных средств тестирования ГСП.

Существуют инструментальные средства тестирования ГСП. Недостатки их следующие: 1- необходимость получения результатов тестирования на промежуточных этапах, 2 – сложное теоретическое обоснование, 3 – ограниченность интервалов и промежутков тестирования. [1]

В докладе приводятся результаты тестирования, полученные с помощью программ, написанных на языках программирования вычислительной системы Matlab и JavaScript.

В качестве системы тестирования выбраны тесты стандарта FIPS-140-2, который имеет подробное теоретическое описание алгоритмов тестирования. Стандарт FIPS 140-2 является единственным стандартом, включающим статистические тесты. Стандартом рекомендованы следующие статистические тесты:

– монобитный тест (The Monobit Test);
– тест покера (The Poker Test);
– тест на подпоследовательности одинаковых бит (The RunsTest);
– тест на длинные подпоследовательности одинаковых бит (The LongRunTest). [2]

В качестве инструментальных сред выбраны два языка программирования: язык вычислительной системы Matlab и язык JavaScript. В каждой из сред на основе теоретического описания созданы алгоритмы тестирования с использованием выбранных языков программирования.

Программа Matlab [3] использована потому, что она представляет собой удобную интерактивную среду для разработки алгоритмов, визуализации и анализа данных, числовых расчетов с возможностью вывода промежуточных результатов для проверки вычислений на каждом из этапов тестирования.

JavaScript - прототипно-ориентированный сценарный язык программирования высокого уровня, позволяющий получить собственный программный продукт тестирования и разместить программу в интернете, например в «облаке» для терминального доступа.

Для каждого из означенных выше языков были составлены алгоритмы, написаны программы тестирования и выполнено тестирование в соответствии с методологией FIPS 140-2.

В качестве объекта сравнения результатов тестирования выступало время тестирования при условии задания одинаковой точности вычислений.

Результаты тестирования представлены в таблице

Таблица – Сравнение результатов тестирования

№	Тест	Время тестирования (Matlab),с	Время тестирования (JavaScript),с
1	Монобитный тест (The Monobit Test)	0,29	0,004
2	Тест покера (The Poker Test)	0,28	0,005
3	Тест на подпоследовательности одинаковых бит (The RunsTest)	0,35	0,006
4	Тест на длинные подпоследовательности одинаковых бит (The LongRunTest)	0,30	0,005
Суммарное время расчетов		1,22	0,02

Таким образом, созданы программы тестирования по FIPS 140-2 в системе Matlab и с помощью JavaScript. Суммарное время, затраченное на тестирование в программе, написанной на JavaScript примерно в 60 раз меньше, чем в Matlab. Также целесообразно использовать программу, написанную на JavaScript, при необходимости организации удаленного тестирования.

Список использованных источников:
1. FIPS 140-2 (Change Notice 1) Random Number Tests//FDK Corporstion [Electronic resource]. – 2003. – Mode of access: http://www.fdk.com/cyber-e/pdf/HM-RAE103.pdf – Date of access: 30.06.2014.
2. Н.Ф. Казакова. «Поэтапное тестирование и подбор составных элементов генераторов псевдослучайных последовательностей» - Украина: 2010 г. Журнал «Восточно-Европейский журнал передовых технологий».
3. Бондаренко, В. Ф. MatLab. Основы работы и программирования, компьютерная математика / В. Ф. Бондаренко, В. Д. Дубовец – Минск: Харвест, 2010. – 256 с.

ТЕХНОЛОГИИ БЛИЖНЕЙ БЕСКОНТАКТНОЙ СВЯЗИ И ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

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

Сабериан М.А..

Утин Л. Л. – к.т.н, доцент

В последние годы наблюдается устойчивая тенденция развития технологий ближней бесконтактной связи NFC. Известно, что внедрение новых средств связи способствует появлению дополнительных угроз нарушения конфиденциальности, целостности, доступности, сохранности и подлинности информационных ресурсов. В докладе предлагаются к обсуждению проблемные вопросы в области защиты информации при применении технологий NFC.

Технологии ближней бесконтактной связи являются одним из альтернативных решений передачи данных с мобильного телефона к приемному устройству. NFC — технология с открытой платформой, стандартизированная в ECMA-340 и ISO/IEC 18092.Эта технология может применяться:

для обмена файлами между телефонами (отдельно либо в сочетании с каналом Bluetooth);

эмуляции смарт-карт;

в качестве средства оплаты за проезд в общественном транспорте;

для открытия электронных замков в квартиру или машину;

в качестве удостоверения личности, страховой карты и т.д.

Достоинствами данной технологии является низкое время установления связи (менее 0,1 с. (для сравнения в технологии Bluetooth данный параметр равен 6 с)), сложность перехвата электромагнитного излучения злоумышленником из-за малого радиуса действия (менее 20 см), простота реализации и ряд других.

Следует отметить, что не смотря на достоинства данной технологии ей присущи определенные недостатки:

до настоящего времени существует потенциальная опасность заражения банковской системы вирусами, которая может осуществиться при использовании мобильного телефона в качестве средства по оплате платежей;

использование средств постановки помех в диапазоне 13,56 МГц приводит к срыву сеансов связи с использованием технологии NFC;

потенциальная возможность утечки персональных данных при осуществлении связи.

Для защиты от утечки применяют различные методы шифрования, антивирусные программы. Проведенный анализ показал, что в настоящее время подходы к шифрованию данных в мобильной связи меняются. Так в дополнение к шести основным принципам Керкгоффса ужесточаются требования к пропускной способности, объему оперативной памяти. В докладе предлагается к обсуждению полученные результаты исследований возможностей различных криптографических алгоритмов шифрования, которые могут быть использованы для шифрования информации с использованием технологий NFC/

СИСТЕМА СИТУАЦИОННОГО УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ИНФОРМАЦИОННОГО ПЕРИМЕТРА

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

Судакевич А. А.

Утин Л. Л. – к.т.н, доцент

Безопасность информационного периметра отдельных организаций обеспечивается множеством межсетевых экранов, систем обнаружения вторжений и антивирусных средств. Однако в подавляющем большинстве случаев множество проблем информационной безопасности остаются нерешенными. Использование системы управления и мониторинга информационной безопасности с возможностью анализа информационных событий является одним из направлений решения отдельных аспектов информационной безопасности.

В настоящее время все больше внимания уделяется повышению эффективности системы управления информационной безопасностью. Это обусловлено тем, что применение для защиты информационного периметра отдельных организаций только межсетевых экранов, систем обнаружения вторжений и антивирусных средств уже не гарантирует обеспечение сохранности, целостности, конфиденциальности и доступности информационных систем. Увеличение количества устройств защиты при отсутствии программно-технических решений по их управлению или мониторингу и корреляции событий от установленных технических средств, может приводить к конфигурационным ошибкам, снижению возможности по проведению анализа информационных потоков и ослаблению уровня защиты всей системы.

Умение распознавать определенные типы поведения, выраженные сотрудниками, которые готовятся к информационной атаке, может помочь предотвратить потенциальную угрозу. Согласно исследованиям [1] большинство атак планируется заранее, а, следовательно, шаги потенциальных нарушителей могут быть предотвращены:

- у 80% нарушителей, которые совершали нападения на свои компании, было негативное поведение до инцидента;
- 92% нарушителей сталкивались с негативом на работе, например, понижение в должности или предупреждение об увольнении;
- 57% нарушителей были восприняты другими как недовольные;
- для выполнения большинства нападений использовался удаленный доступ;
- наиболее распространенным мотивом была месть.

Информационная безопасность компании обычно строится не только на использовании технологических средств защиты, но использует и организационно-юридические возможности. При этом общие принципы обеспечения безопасности остаются неизменны и должны учитывать разграничение прав доступа и контроль за соответствием служебных обязанностей сотрудников и доступной им информации.

Инфраструктура современных корпоративных информационных систем постоянно развивается, становится все более сложной и разнообразной и приобретает распределенный характер. Внутри такой распределенной системы, состоящей из серверов приложений, сетевого оборудования, средств и систем безопасности, пользователи корпоративной сети ежедневно генерируют миллионы событий. В таких условиях остро встает вопрос контроля текущего состояния и обеспечения информационной безопасности.

Системы мониторинга и управления информационной безопасностью осуществляют сбор и анализ событий от разнородных приложений, операционных систем, сетевых устройств, телекоммуникационного оборудования. Их обычно разделяют на три класса решений:

- Security Information Management (SIM) – системы, которые в первую очередь ориентированы на сбор, анализ и долгосрочное хранение событий безопасности от приложений, операционных систем, баз данных и в меньшей степени на сбор данных от сетевого и серверного оборудования
- Security Event Management (SEM) – системы, которые в первую очередь ориентированы на сбор и анализ событий аудита от телекоммуникационного оборудования и в меньшей мере на сбор данных от пользовательских и серверных приложений
- Security Information and Event Management (SIEM) – системы, сочетающие в себе функционал и SIM, и SEM решений

В настоящее время на рынке систем мониторинга и управления информационной безопасностью преобладают SIEM решения, предназначенные для решения следующих задач:

- оперативное обнаружение нарушений политики информационной безопасности;
- мониторинг, выявление и приоритезация в режиме реального времени событий от разных устройств и инцидентов информационной безопасности;
- автоматическое реагирование на инциденты информационной безопасности;
- формирование базы знаний по инцидентам информационной безопасности;
- проведение расследований инцидентов информационной безопасности.

Системы мониторинга, анализа и управления информационной безопасностью, разворачиваемые поверх корпоративной сети, в общем случае состоят из менеджеров событий, управляющего сервера и базы данных, рисунок 1. Менеджеры событий осуществляют сбор событий информационной безопасности и

выполняют их первоначальную обработку и фильтрацию, после чего передают на анализ серверу приложений, который является основой системы. Сервер приложений анализирует собранную с помощью агентов информацию и преобразует ее в более высокоуровневое и удобное для анализа представление. Вся информация, собранная агентами, а также результаты анализа ее сервером приложений сохраняются в базе данных. Для обработки и анализа событий информационной безопасности можно использовать механизмы нормализации, фильтрации, классификации, агрегации, корреляции и приоритезации событий.

Внедрение системы мониторинга событий информационной безопасности позволяет обеспечить централизованное управление, увеличить скорость выявления, расследования и реагирования на инциденты информационной безопасности, а также повысить эффективность управления рисками информационной безопасности

Список использованных источников:

3. Яфизов Р. А. Защита от внутренних угроз // Information Security/ Информационная безопасность – 2008 – Номер 1.
4. Башлыков М. А. Предотвращение утечки конфиденциальной информации // Information Security/ Информационная безопасность – 2010 – Номер 3.
5. Поспелов Д .А. Ситуационное управление. Теория и практика / Д. А. Поспелов. – Москава: Наука, 1986 – 285 с.

ФАКТОРЫ, ВЛИЯЮЩИЕ НА ЗАЩИТУ ИНФОРМАЦИИ ПРИ ПРОЕКТИРОВАНИИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ

Государственное учреждение
«Научно-исследовательский институт Вооруженных Сил Республики Беларусь»
г. Минск, Республика Беларусь

Яковцев П.А.

Утин Л. Л. – к-т техн. наук, доцент

Переход от единичных мэйнфреймов до корпоративных информационных сетей (КИС) позволило расширить возможности по информационному обмену внутри организации, повысить ее управляемость. Однако, с преимуществами, связанными с обработкой информации в КИС, появляются и сложности, связанные с защитой информации. Чем совершеннее, становятся информационные технологии - тем сложнее процесс обеспечения защиты информации. Учитывать эти вопросы целесообразно на этапе проектирования КИС.

В ходе анализа были выявлены основные факторы проектирования КИС, влияющие на защищенность информации:

1. Территориальный фактор.

Если раньше объектом защиты являлись отдельные компьютеры, по возможности объединённые в локально вычислительную сеть, то сейчас это совокупность разнесенных территориально сетей, которые имеют ряд особенностей:

увеличение зоны контроля (специалисту необходимо контролировать работу пользователей вне зоны его досягаемости);

в состав общей системы включаются комбинации различных аппаратно-программных средств (система настроенная на обеспечение безопасности информации может не сработать на удаленную систему, отсюда рост уязвимостей);

увеличение количества точек атаки (увеличение элементов КИС, а соответственно и промежуточных узлов передачи информации, каждый из которых является источником угрозы);

снижение контроля периметра (высокая расширяемость сетей ведет к тому, что становится сложно определить границы сети: один и тот же узел может быть доступен различным сетям);

снижение управляемости и контроля доступа к системе (возникает возможность атаки без получения физического доступа к определенному узлу).

2. Программный фактор.

Применение стороннего программного обеспечения, вызывает необходимость в:

выборе программного обеспечения (различное программное обеспечение, или даже различные версии одного и того же программного обеспечения, ведет к затруднению обеспечения безопасности КИС, так как у каждого программного продукта свой набор уязвимостей);

выборе средств защиты (отсутствие универсальных средств защиты, вынуждает организацию постоянно обновлять возможности средств защиты, вплоть до полной замены при модернизации программного обеспечения КИС, что вызывает рост расходов на систему информационной безопасности).

3. Организационный фактор.

Рост количества узлов КИС неизбежно вызовет необходимость в росте количества обслуживающего персонала, что вызовет **рост риска преднамеренных и непреднамеренных инсайдерских атак.**

4. Фактор принадлежности КИС.

Если КИС проектирует для себя коммерческая организация, то ее в первую очередь будет интересовать конфиденциальность информации циркулирующей в сети. В случае проектирования КИС для силовых структур их в «особый» период будет больше интересовать доступность информации.

5. Временной фактор.

При проектировании КИС организация заинтересована в как можно большем жизненном цикле создаваемой сети. При этом необходимо учитывать **длительную поддержку и сопровождение внедряемых средств защиты**;

6. Фактор кодирования.

При увеличении количества пользователей и плеча передачи информации растет роль средств криптозащиты.

7. Фактор управления.

В настоящее время особое внимание уделяется автоматизации управления существующими и перспективными средствами защиты, например путем введения АСУ защитой информации КИС.

8. Финансовый фактор.

Система защиты требует больших материальных затрат, в частности на:

программную составляющую КИС (новое ПО, поддержка старого ПО и т.д.);

техническую составляющую КИС (сетевое оборудование, серверы, постройка или аренда линий связи и т.д.);

организационную составляющую (найм или содержание штатных программистов, системных администраторов, проведение аудита безопасности и защищенности КИС и т.д.).

Таким образом, рассматривая вопросы создания КИС, специалистам следует учитывать вышеизложенные факторы, влияющие на ее безопасность.

ПРОБЛЕМНЫЕ ВОПРОСЫ КОНТРОЛЯ ЭФФЕКТИВНОСТИ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ И ПУТИ ИХ РЕШЕНИЯ

Государственное учреждение
«Научно-исследовательский институт Вооруженных Сил Республики Беларусь»
г. Минск, Республика Беларусь

Федорцов А. В.

Утин Л. Л. – к-т техн. наук, доцент

В государственных информационных системах обработка данных должна осуществляться после реализации установленных законодательством мер, с применением системы защиты информации [1]. Данная система представляет собой совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами в области защиты информации [2]. Для повышения эффективности применения мер защиты информации на ОИ СВТ должен осуществляется контроль действий пользователей.

Имеется множество подходов к классификации контроля. Различают контроль по:

целям (соответствие требованиям законодательства, эффективность мероприятий по обеспечению безопасности информации);

используемым средствам (экспертный, комплексный, инструментальный);

периодичности (внезапный, непрерывный, периодический);

степени охвата (сплошной, выборочный);

динамике (динамический, статический);

принадлежности специалистов (внешний, внутренний);

степени осведомленности сотрудников (гласный, негласный);

характеру связи с объектом (дистанционный, встроенный).

Деятельность в области контроля основывается на следующих основных принципах:

законность действий контролирующих специалистов;

регулярность;

действенность;

независимость контролирующих специалистов от руководящего персонала;

гласность результатов;

расследование нарушений требований законодательства Республики Беларусь.

Результаты комплексного контроля, с соблюдением основных принципов, должны позволять оценивать полноту и качество проведенных мероприятий.

На практике, при осуществлении контроля эффективности мероприятий по защите информации возникает ряд проблем, основными из которых являются:

недостаточная оснащенность структурных подразделений по защите информации программно-техническими средствами;

привлечение к оценке эффективности мер защиты информации неквалифицированных должностных лиц (нештатных специалистов), не имеющих достаточных навыков и опыта;

отсутствие общепринятой методики контроля.

Обеспечение программно-техническими средствами и разработка методики являются первоочередными задачами на пути повышения эффективности контроля. В результате их решения персонал, ответственный за обеспечение защиты информации, получает инструмент для качественной оценки результативности проведенных мероприятий по заданным направлениям контроля, снижения ресурсоемкости (временных затрат, количества участвующих в контроле специалистов и т.д.) процесса оценки, повышения оперативности в представлении результатов (отчетов, анализов и т.д.) и своевременном реагировании на возникшие инциденты (угрозы для системы), принятии управленческих решений. Применение программно-технических средств позволяет снизить влияние «человеческого фактора» на полученные результаты и расширить границы контроля.

Вместе с тем, разработке программно-технических средств контроля предшествует этап исследований математического аппарата оценки эффективности мер защиты информации. В докладе предложен к обсуждению разработанный подход, реализация которого позволит частично устранить рассмотренные проблемные вопросы.

Список использованных источников:

1. Об информации, информатизации и защите информации, Закон Респ. Беларусь от 10.11.2008 № 455-З, текст по состоянию на 1.03.2015. – Минск – 21 с.

2. Защита информации Основные термины и определения, СТБ ГОСТ Р 50922-2000: - Введ. 22.05.2000 – Минск: Государственное проектное и научно-исследовательское предприятие «Гипросвязь», 2000. – 6 с.

ПРЕИМУЩЕСТВА ПРИМЕНЕНИЯ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СЕТЯХ

Государственное учреждение
«Научно-исследовательский институт Вооруженных Сил Республики Беларусь»
г. Минск, Республика Беларусь

Мацылевич А. Р.

Утин Л.Л. – к-т. техн. наук, доцент

Субъективные факторы являются одними из наиболее опасных факторов, влияющих на защиту информации, особенно в системах управления процессами обеспечения информационной безопасности. Максимально возможное исключение человека из контура управления защитой информации требует определения обоснованных путей его реализации, одним из которых является разработка и применение в информационных сетях программно-технических средств управления защитой информации.

Используемые в настоящее время информационные сети для обеспечения деятельности органов государственного управления, субъектов экономики государства являются сложными организационно-техническими системами. С одной стороны, внедрение цифровых информационных технологий обеспечивает повышение эффективности управления подчиненными силами и средствами, с другой стороны, их использование привело к появлению принципиально новых угроз защищенности информации, ущерб от воздействия которых может снизить эффективность управления, вплоть до его срыва. Решение этого противоречия в процессе информатизации общества является и будет являться наиболее актуальным.

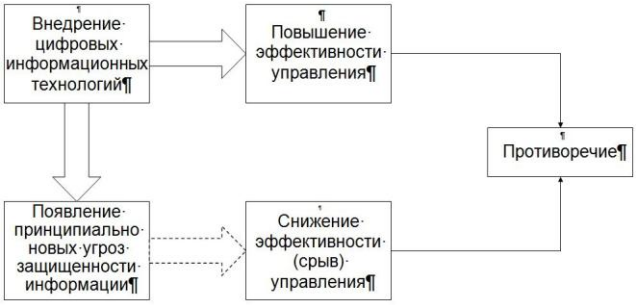

Рис. 1 – Структурная схема выявленного противоречия в защите информации

Вышеуказанные угрозы имеют техногенную природу, вследствие чего, человек, в силу своих психофизиологических возможностей, не в состоянии своевременно и адекватно на них реагировать (противодействовать).

В целях защиты информации в информационных сетях применяются разноплановые технические средства защиты информации, непосредственное управление которыми человеком не обеспечивает оперативность реагирования на возникающие угрозы защищенности информации. Это вызвано необходимостью использования ресурсоемких интерфейсов. Кроме того, эффективность выявления угроз защищенности информации и выработки рациональных способов их нейтрализации находится в зависимости от таких свойств человека как мотивация, профессиональная подготовленность, усталость, отвлеченность, эмоциональность и других, что в некоторых случаях может привести к блокированию работы системы защиты информации в информационной сети.

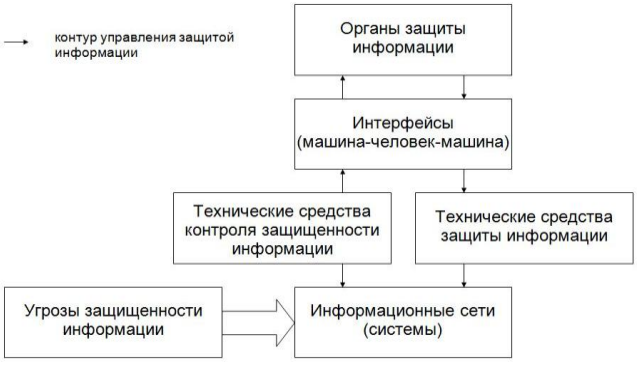

Рис. 2 – Структурная схема существующей системы управления защитой информации

Максимально возможное исключение антропогенного фактора из процессов управления защитой информации возможно путем передачи части функций управления защитой информации на программно-технический уровень, посредством применения программно-технических средств, реализующих функции управления защитой информации. Это позволит наиболее эффективно решать задачи единого управления защиты информационных ресурсов, распределенных в информационных сетях. При этом максимально исключив из контура управления защитой информации «человеческий фактор». В перспективе такие средства целесообразно интегрировать в существующие системы защиты информации информационных сетей.

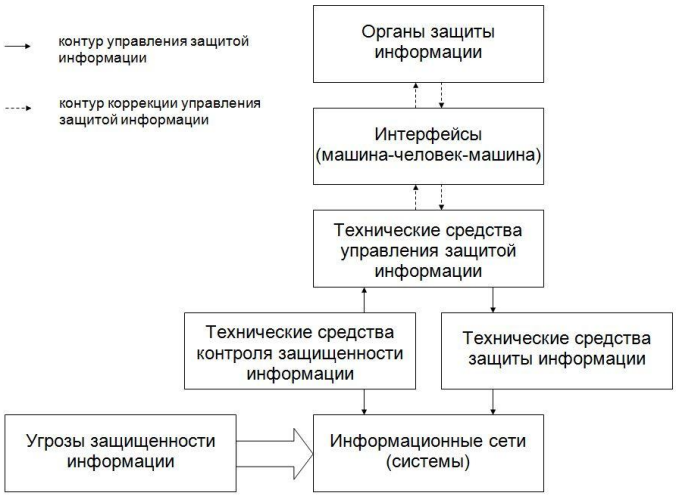

Рис. 3 – Предлагаемый подход к разрешению выявленных противоречий

Определение наиболее эффективных способов применения программно-технических средств, реализующих функции управления защитой информации в информационных сетях, является актуальным.

Достигнуть этого предлагается путем решения ряда научных задач:

разработать методику управления защитой информации в информационных сетях посредством применения программно-технических средств;

определить способы применения программно-технических средств управления защитой информации в информационных сетях;

оценить эффективность способов применения программно-технических средств управления защитой информации в информационной сети;

разработать рекомендации по созданию и применению программно-технических средств управления защитой информации в информационных сетях.

Список использованных источников:

1. Об информации, информатизации и защите информации, Закон Респ. Беларусь от 10.11.2008 № 455-З, текст по состоянию на 1.03.2015. – Минск – 21 с.
2. Защита информации Основные термины и определения, СТБ ГОСТ Р 50922-2000: - Введ. 22.05.2000 – Минск: Государственное проектное и научно-исследовательское предприятие «Гипросвязь», 2000. – 6 с.

ЗАЩИТА ДАННЫХ В СЕТИ DEEPNET

ГУ НИИ ВС РБ

г. Минск, Республика Беларусь

Мастыкин А.Л.

Утин Л.Л. –к-т техн. наук, доцент

Известно, что при обеспечении безопасности сети Интернет возникает множество проблем. Специалисты в области защиты информации по-разному подходят к приоритетности вопросов обеспечения безопасности информационных ресурсов сети (далее ресурсов) и безопасности пользователя данными ресурсами.

При обеспечении безопасности ресурсов сети основными направлениями являются сохранение конфиденциальности личных регистрационных данных пользователей защищаемого ресурса, сохранение в неизменном состоянии структуры и содержания ресурса, размещенного пользователями с соответствующими правами доступа. Кроме того, должны быть предусмотрены меры по недопущению модификаций, разработанных алгоритмов работы ресурсов, таких как внедрение программ для рассылки спама.

Безопасность ресурса сети основана на комплексе мер защиты предпринятых как разработчиками, так и администраторами сайтов и серверов на которых эти ресурсы размещены. К основным из них относятся:

подтверждение того, что пользователей ресурсов не является роботизированной программой;

регистрация новых пользователей ресурса;

идентификация и аутентификация пользователей;

ограничение количества запросов пользователя;

ограничение количества пользователей одновременно обращающихся к ресурсу сети.

Безопасность пользователя ресурсами в основном зависит от его действий, а также используемого программного обеспечения, установленного на ПЭВМ.

Необходимо заметить, что то информационное пространство, доступное через такие современные браузеры как «Opera», «Internet Explorer», «Google Chrome», «Fire Fox», «Safari» и т.д. (назовем его «видимый Интернет») представляет собой лишь, небольшую, видимую часть, огромной, многоуровневой информационной структуры, которая постоянно разрастается. В «Видимом Интернете» предпринимаются попытки контроля контента на предмет легальности и именно в нем проводит время среднестатистический пользователь. Вместе с тем известна часть Интернета, содержащая информацию, предназначенную для определенного кругов пользователей («Deepnet», «DarkNet», «DeepWeb», «Глубокий интернет», «Invisible Web» и т.д.)

Эта информация может быть:

-недоступной тому, кто не знает что конкретно ему нужно, и где это находится;

-спрятана за паролями;

-находится в архивах;

-не подключена к интернету, но является частью сети;

-на неиндексируемых страницах;

- на заброшенных форумах

- огромных объемов не всегда легального контента.

Например, Darknet знаменит тем, что является местом, где многие посетители получают на свои устройства специализированное программное обеспечение даже не подозревая, что стали жертвами кибермошенничества. Успешное противодействие данным угрозам возможно при наличии у пользователей специализированных знаний в области информационных технологий и противодействия компьютерным преступлениям.

Следовательно, для относительно безопасного посещения «Темной сети» должны использоваться компьютерные программы позволяющие:

- обеспечить защиту приватности и анонимности в сети;

- шифровать текст (включая электронную почту) и файлы;

Более эффективно применение сложных и дорогостоящих технических решений, включающих собственные серверы , wifi роутеры (или другое аналогичное оборудование дальнего радиуса действия), обеспечивающее доступ в интернет. Такой подход актуален для держателей своих ресурсов в «Invisible Web». Однако для осуществления этого решения необходимы не только средства на приобретение вышеуказанного оборудования, но и соответствующая техническая подготовка. В докладе предлагается к обсуждению некоторые проблемные вопросы защиты информации в сети Deepnet.

Список использованных источников:

1. C. Sherman, G. Price: The Invisible Web: Uncovering Information Sources Search Engines Can’t See. CyberAge Books, 2001.

СЕТЬ РАДИОДОСТУПА МОБИЛЬНОГО ОПЕРАТОРА СТАНДАРТА UMTS

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

Корбут А. Л.

Мищенко В. Н. – к-т. техн. наук, доцент

Мобильная сотовая связь является самой быстроразвивающейся отраслью телекоммуникационного рынка. История сотовых мобильных сетей берёт своё начало с 80-ых годов 20 века, когда услуги мобильной связи были доступны ограниченному количеству пользователей, из-за высокой стоимости и небольшой зоны покрытия. По мере развития сотовых систем, они становились доступны всё большему количеству пользователей. Согласно данным компании Ericsson, на конец 2014 года, общее число абонентов мобильной связи в мире приближается к семи миллиардам. С поправкой на то, что некоторые пользователи имеют более одного сотового телефона, эта цифра снижается до пяти миллиардов человек. Таким образом, около 70% жителей планеты имеют как минимум один мобильный телефон. Появление сотовых мобильных систем было обусловлено потребностью в голосовых мобильных услугах. Со временем появлялось множество дополнительных сервисов и услуг, основной из которых является передача данных. В настоящее время акцент в развитии сотовых систем делается на повышении скорости передачи данных. Это стало возможным благодаря внедрению систем сотовой связи 3-его поколения.

В республике Беларусь в настоящее время услугами сотовой подвижной электросвязи охвачено более 98,8% территории республики, на которой проживает 99,8% населения. Уровень проникновения сотовой связи в республике составляет приблизительно 113 абонентов на 100 жителей республики.

Первая сеть 3-его поколения в республике была введена в эксплуатацию в июне 2006 года (технология CDMA-2000 EV-DO). Первая же сеть 3G стандарта UMTS была введена в коммерческую эксплуатацию в ноябре 2009 года.

По сравнению с GSM и другими широко распространенными стандартами цифровых сотовых мобильных систем связи стандарт UMTS обеспечивает: лучшие энергетические характеристики; более высокую скорость передачи данных; поддержка услуг с различными требованиями к качеству обслуживания; совместимость систем второго и третьего поколения в части межсистемной эстафетной передачи управления (межсистемных хэндоверов) для увеличения зон охвата и перераспределения нагрузки; поддержку возможности ассиметричной загрузки восходящей и нисходящей линий; высокую эффективность использования спектра; безопасность связи и ее конфиденциальность.

Архитектура сети стандарта UMTS предоставляет максимальную унификацию для режимов передачи данных с коммутацией каналов и коммутацией пакетов. В качестве способа передачи данных через воздушное пространство используется радиоинтерфейс WCDMA, стандартизованный в соответствии с проектом 3GPP. Сети радиодоступа этой системы связи на начальных этапах развития обеспечивали скорости передачи данных до 144 Кбит/с для абонентов с высокой мобильностью (скорость движения до 120 км/ч), 384 Кбит/с для абонентов с низкой мобильностью (скорость до 3 км/ч), 2,048 Мбит/с для стационарных абонентов (Release 99), до 14,4 Мбит/с для стационарных абонентов (Release 6). Сети UMTS создаются на основе популярного стандарта GSM и инвестиций в инфраструктуру, производимых существующими операторами сотовой связи. Основное отличие UMTS состоит в использовании широкополосных сигналов в диапазоне 2 ГГц, позволяющее добиться более высокого по сравнению с GSM качества обслуживания. С появлением данной системы появилась возможность предоставлять мультимедийные широкополосные услуги, такие как видеовызов, высокоскоростная передача данных и другие. В последующем были внедрены более скоростные режимы передачи информации - режимы HSPA и HSPA+. Максимальная пропускная способность сети UMTS в режиме HSPA с использованием одной несущей равняется 14,4 Мбит/с, в режиме HSPA+ - до 21 Мбит/с. Имеется возможность для дальнейшего повышения пропускной способности при использовании режима с несколькими несущими и технологии MIMO.

Проектирование сетей радиодоступа на начальном этапе планирования представляет собой приблизительную оценку требуемого числа базовых станций и соответствующую емкость передаваемой информации. Данный этап включает в себя расчет бюджета радиолинии, оценку емкости сети, анализ покрытия. Распределение нагрузки сети по различным сервисам, распределение трафика по территории и требования к качеству обслуживания определяет исходные данные для расчета.

Для проектирования сети радиодоступа произведён расчёт максимальных допустимых потерь для нисходящего и восходящего каналов для режима скорости передачи 384 кбит/с. Выполнен расчёт максимальной дальности радиосвязи до границы сотовой ячейки, а также количества базовых станций, необходимых для покрытия региона общей площадью приблизительно 200 км^2 вблизи города Червень, Республика Беларусь. Расчёт покрытия базовых станций произведён в программе Mentum Planet. Обработка результатов осуществлялась в программе ГИС MapInfo, что позволило в наглядной форме представить полученные данные для исследуемого района местности.

ИССЛЕДОВАНИЕ СВОЙСТВ АНТЕННЫХ РЕШЁТОК МИЛЛИМЕТРОВОГО ДИАПАЗОНА

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

Гостинщиков А. В.

Печень Т. М. – ассистент каф. СТК

Применение в современных инфокоммуникационных технологиях фазированных антенных решёток (ФАР) с цифровым диаграммообразованием (ЦДО) позволяет повысить помехоустойчивость аппаратуры и увеличить пропускную способность системы связи в миллиметровом диапазоне длин волн.

В задачах связи это позволяет динамически оптимизировать обслуживаемую зону покрытия, оперативно перенацеливая цифровые приемопередающие лучи в зависимости от территориального распределения абонентов. Созвездие лучей, синтезируемое, например, по алгоритмам быстрого преобразования Фурье является, по сути, совокупностью пространственно-частотных фильтров, каждый из которых селектирует строго определенный набор сигналов и подавляет остальные, воспринимаемые как помеховые.

В решетке с цифровым формированием лучей диаграммы направленности (ДН) принятые сигналы преобразовываются в приемном устройстве в цифровую форму на уровне элементарной антенны, а затем обрабатывается в специальном процессоре для формирования требуемой диаграммы направленности антенны. Такой подход сохраняет полную информацию, имеющуюся в апертуре (т.е. N индивидуальных сигналов $\{x_1, x_2 \dots x_n\}$ в противоположность аналоговому способу формирования ДН, который приводит лишь к взвешенной сумме этих сигналов и поэтому уменьшается размерность сигналов от N до 1 [1].

Современные методы обработки в раскрывах ФАР рассчитаны в основном (и даже почти исключительно) на цифровую реализацию, при этом имеется в виду обработка сигналов, и в первую очередь – радиолокационные приложения, хотя область их применений гораздо шире.

Применение цифрового диаграммообразования обладает важными преимуществами по сравнению с традиционными аналоговыми решетками, а именно: стабильность параметров; изменение параметров за счет изменения программного обеспечения без замены аппаратной части; многоканальность с идентичными характеристиками каналов; возможность корректировки амплитудного распределения с более высокой точностью при амплитудном диаграммообразование фазового распределения, чем при амплитудном диаграммообразование; обеспечение более высокого динамического диапазона за счет цифрового суммирования сигналов от составных частей антенны (по сравнению с аналого-цифровым преобразованием) на выходе устройства аналогового диаграммообразования; процесс калибровки ФАР с ЦДО существенно проще, чем аналоговых ФАР и может быть выполнен с большей точностью (это весомый аргумент в пользу перехода к цифровой обработке для больших решеток); выигрыш по объемам аппаратуры при одновременном формирование большого числа лучей на прием [2].

Среди проектов ЦДО в системах мобильной сотовой связи прежде всего отметим TSUNAMI (Technology in Smart Antennas for Universal Advanced Mobile Infrastructure) и RDRN (Rapidly Deployable Radio Network). компания ERA Technology инициировала новый, более продвинутый проект «Солнечный луч» – SUNBEAM (Smart UNiversal BEAMforming).

Стремление выжить в конкурентной борьбе вынуждает отдельных участников SUNBEAM проводить собственные проекты по освоению технологии ЦДО. Так, Antenna Processing Laboratory – подразделение французской компании Thomson CSF Communications – в кооперации с другими европейскими фирмами разрабатывает адаптивную цифровую антенную решетку для мобильной связи в рамках двухлетнего проекта ADAMO (Adaptive Antenna for MObils). В качестве антенной решетки для базовой станции в системе ADAMO создается шестипанельная ЦАР с четырьмя вертикально расположенными элементами в каждой панели. Ширина луча в азимутальной плоскости – 70° по уровню 3 дБ, коэффициент усиления четырехэлементной панели 30 дБ, уровень первых боковых лепестков не превышает 12 дБ. Уступая по масштабности проекту SUNBEAM, ADAMO ориентирован на более продвинутые стандарты связи HIPERLAN (High Perfomance Radio Local Area Network) с полосой пропускания 23,5 Мбит/с на канал и центральными несущими 5,2 ГГц (Hiperlan/1) или 17,2 ГГц (Hiperlan/2), которым отводится роль будущего европейского стандарта для высокопроизводительных локальных радиосетей. По сравнению с SUNBEAM, ADAMO создает задел на более отдаленную перспективу, поэтому их нельзя противопоставлять друг другу.

Таким образом, в рассмотренных системах с цифровыми антенными решетками различными способами обеспечивается управление фазой и амплитудой в антенных апертурах, а также необходимо отметить, что методы сверхразрешения чрезвычайно актуальны в системах телекоммуникациях.

Список использованных источников:

1. Григорьев, Л. Н. Цифровое формирование диаграммы направленности в фазированных антенных решетках/ Л. Н. Григорьев. – М: Радиотехника, 2010.

2. Пархоменко, Н. Г. Быстрый поляризационно-независимый синтез пеленгационного рельефа для многоэлементных антенных решеток // Антенны. № 10. – 2010. С. 44 – 50.

МОДЕРНИЗАЦИЯ ONU GPON СЕТИ

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

Былинович А.С.

Хацкевич О.А. – к.т.н., доцент

Унификация систем связи и интеграция сервисов в единую сеть является одним из наиболее важных вопросов в современном мире телекоммуникаций. Это стимулирует производителей создавать системы связи, способные взаимодействовать с множеством других технических решений.

Технология PON показала себя как наиболее эффективное и перспективное решение проблемы «последней мили». Развитие техники и совершенствование методов передачи данных с каждым годом провоцирует рост объемов передаваемой информации. В данный момент в Республике Беларусь идет активное развертывание GPON сети с целью предоставления абонентам услуги Triple-play [1]. Услуга Triple-play, как наиболее востребованная, занимает подавляющий сегмент в области предоставления услуг массовому пользователю. Однако многим организациям необходим более широкий спектр услуг, таких как видеонаблюдение, видеоконференция, система контроля и управления доступом (СКУД), и при этом построение каждой системы в отдельности требует немалых средств на монтаж и последующее обслуживание, а территориальная рассредоточенность филиалов компании не позволяет унифицировать одну систему в нескольких филиалах.

В данном докладе рассмотрены вопросы интеграции сервисов в единую сеть, обмен данными с помощью рядового GPON соединения с провайдером и внутрисетевой обмен данными. Абонентские модули ONU каждого филиала компании соединяются с провайдером услуг посредством рядового GPON подключения. Таким образом, филиалы компании имеют виртуальное соединение посредством выделенного туннеля передачи данных, обеспечиваемого провайдером услуг. ONU является концентратором и коммутатором всех предоставляемых услуг: пакет triple-play, а также видеонаблюдение, видеоконференция, система контроля и управления доступом и других систем, адаптированных для подключения к модулю, и использующих PON в качестве транспортной сети.

Модернизация ONU GPON сети позволяет получить следующие дополнительные услуги:

- Модуль IP-телефонии позволяет без выхода в телефонную сеть общего пользования коммутировать вызовы между абонентами одного филиала и через выделенный виртуальный туннель с абонентами других филиалов.
- Модуль Ethernet обеспечивает создание локальной вычислительной сети внутри филиала с общим для всех абонентов каналом связи с провайдером.
- Для системы видеонаблюдения ONU имеет порты для подключения внешнего запоминающего устройства и IP видеокамер. Система видеоконференции интегрирована в сеть видеонаблюдения и позволяет программно настраивать список камер, какие будут участвовать в конференции.
- С целью объединения нескольких систем СКУД и обеспечения администрирования системы предусмотрен порт для подключения центрального блока системы. Центральные блоки систем разных филиалов образуют единую систему контроля и управления доступом.
- С целью экономии ресурса полосы пропускания и уменьшения избыточности передаваемой информации по заброску от абонента передается только один канал IPTV. Блок управления системой IPTV обеспечивает коммутацию запрошенных каналов разными абонентам.

Для обеспечения корректной работы, мониторинга и внесения изменений в конфигурацию системы предусмотрен порт для подключения ПК администратора.

Проведенные расчеты показали, что предлагаемая концепция модернизации может быть реализована на базе существующих GPON сетей. Основной сложностью при создании системы стало распределение трафика между службами и адресация его к провайдеру и между внутрисетевыми абонентами.

Разработаны принципы формирования пакетов данных, алгоритм распределения трафика внутри сегмента сети и передачи провайдеру. Проведена комплексная оценка внедрения данного решения в филиалы организаций различного размера и территориального расположения.

Практическая ценность работы состоит в унификации среды передачи множества сервисов, возможности обработки и обмена данными без выхода к провайдеру и использовании одного рядового GPON соединения для всего офиса или филиала компании.

Предлагаемая концепция модернизации сети PON обладает следующими достоинствами: используется одна транспортная сеть для передачи данных разных сервисов, одна служба для обслуживания всех сервисов, адаптация системы для офисного пользователя с использованием одного GPON соединения.

Список использованных источников:

6. Recommendations ITU-T G.984.x-series, Gigabit-capable passive optical networks (G-PON).

ПРИМЕНЕНИЕ СПИРАЛЬНЫХ АНТЕНН В ИНФОКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЯХ

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

Кравченя П. Н.

Печень Т. М. – ассистент каф. СТК

В современных системах радиолокации широко применяются спиральные антенны. Они характеризуются диапазонам частот с перекрытием до пяти октав, широким сектором углов одновременного обзора, слабонаправленностью и управляемой эллиптической поляризацией, а также имеют небольшие габариты и массу.

Принято спиральные антенны подразделять на пространственные (винтообразные) и плоские. По принципу работы пространственные антенны бывают: с поперечным излучением (NMHA − Normal-Mode Helical Antenna) и с осевым излучением (AMHA − Axial-Mode Helical Antenna). Для работы в режиме поперечного излучения диаметр витков спирали должен быть гораздо меньше длины волны. Диаграмма направленности аналогична обычному несимметричному вибратору. Данный тип антенн широко используется в портативных радиокоммуникационных устройствах, в том числе в мобильных телефонах.

Для работы в осевом режиме диаметр витков спирали должен быть порядка длины волны. Винтообразные антенны в осевом режиме предназначены для излучения и приёма электромагнитных волн с круговой поляризацией. Правая круговая поляризация используется для радиосвязи практически на всех орбитальных спутниках. Направление поляризации определяется направлением намотки спирали.

Плоская спиральная антенна обычно состоит из двух спиралей, выполненных из проволоки или из фольги (например, по микрополосковой технологии), и расположенных центральносимметрично в плоскости антенны. Фидер подключают к этим плечам, аналогично подключению к симметричному вибратору. Рабочий диапазон антенны может превышать декаду.

Спиральная антенна характеризуется количеством витков *N*, диаметром витков *D* и шагом спирали *d*. В принципе, чем больше витков содержит антенна, тем выше коэффициент усиления. При этом радиус витка обычно выбирается исходя из условия, чтобы длина витка соответствовала длине волны излучения λ, то есть: $\lambda = 2\pi R$, а шаг спирали должен быть равен четверти длины волны излучения: $d = \lambda / 4$ [1].

Размер рефлектора, который устанавливается перпендикулярно оси спирали и может иметь форму диска или квадрата, должен быть не меньше длины волны излучения. При длине волны излучения 123 мм (частота 2,437 ГГц) получим, что диаметр витка должен быть равен примерно 40 мм, а шаг спирали – 30 мм.

Спиральная антенна может быть описана как пружина с количеством витков N с отражателем. Окружность (*C*) витка составляет приблизительно длину волны (λ), а расстояние (d) между витками составляет приблизительно 0,25*C*. Размер отражателя (*R*) составляет *C* или λ и может иметь форму круга или квадрата. Конструкция излучающего элемента вызывает круговую поляризацию (КП), которая может быть как право-, так и левосторонней (П и Л соответственно), в зависимости от того, как намотана спираль. Для того, чтобы передать максимум энергии, обе стороны соединения должны иметь одинаковую направленность поляризации, кроме случаев, когда используется пассивный отражатель радиоволн на пути передачи сигнала.

Усиление (*G*) антенны относительно изотропии рассчитывается по следующей формуле:

$$G = 11{,}8 + 10 \cdot \lg\left[\left(\frac{C}{\lambda}\right)^2 \cdot N \cdot d\right] \quad (1)$$

В соответствии с выводами Даррела Эмерсона из Национальной Радиоастрономической Обсерватории, результат вычисления по формуле (1), также известной как формула Крауса, усиление *G* составляет 4 … 5 дБ [2].

Таким образом, спиральную антенну, изобретенную в конце сороковых Джоном Краусом, можно назвать самой простой реализацией антенны, которую можно представить, в особенности для частот в диапазоне 2−5 ГГц. Эта конструкция является очень простой, практичной и при этом надежной. В технической литературе можно встретить статьи как самостоятельно сделать спиральную антенну для частот 2,4 ГГц которая может быть использована, например, для высокоскоростных радиочастотных (S5-PSK, 1,288 Мбит/с), 2,4 ГГц беспроводных сетей и любительских спутниковых (AO40). Развитие оборудования беспроводных сетей позволяет легко получить высокоскоростной радиодоступ с использованием стандарта IEEE 802.11b (Wi-Fi).

Список использованных источников:

1. Юрцев, О.А. Антенны бегущей волны, антенные решетки, антенны коротких, средних и длинных волн / О. А. Юрцев. // Методическое пособие по курсу "Антенны и устройства СВЧ" для студентов специальности "Радиотехника ". В 3 ч. – Ч.3: – Минск, 2001. – 72 с.

2. Emerson, D. T. The Gain of the Axial-Mode Helix Antenna / D.T. Emerson // Antenna Compendium. – ARRL, Vol. 4, 1995. – pp 64 – 68.

МЕЖСАЙТОВАЯ АТАКА С ВНЕДРЕНИЕМ СЦЕНАРИЯ

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

Каленик К.Г.

Новиков В.И. – кандидат техн. наук, доцент, УО"ВГКС"

Межсайтовая атака с внедрением сценария (XSS) на текущий день является одной из самых распространенных атак на уровне приложения, которые хакеры используют для незаконного проникновения в Web-приложения. XSS – это атака, направленная не на сервер или сайт напрямую, а на клиентов этого сайта и их конфиденциальную информацию.

Важно отметить, что XSS сама по себе не является уязвимостью, а XSS лишь одним из возможных способов эксплуатации уязвимости определенного класса.

Целью такой атаки могут быть cookies, или другая информация, идентифицирующая пользователя. Располагая регистрационными данными легитимного клиента, атакующий получает возможность действовать от его имени при работе с сайтом, что наверняка приведёт к взлому всей системы безопасности с похищением или фальсификацией данных о пользователе.

Для получения cookie злоумышленник, после выявления XSS уязвимостей, создает ссылку с вредоносным кодом. В этом коде данные из куков передаются на сторонний сервер, на котором обрабатываются и сохраняются, затем пользователь перенаправляется на страницу обратно. Все это происходит незаметно для человеческого глаза, и поэтому атака остается необнаруженной.

Атаки, построенные по принципу межсайтингового скриптинга, можно разделить на два типа:

Активные XSS атаки – подразумевают внедрение ссылки в саму страницу ресурса.

Пассивные XSS атаки – пользователь сам должен вставить ссылку в адресную строку или просто кликнуть по ней.

Всё это осуществляются через браузер жертвы: атакующий старается заставить пользователя перейти по злонамеренной ссылке. Это может быть реализовано многими способами от размещения ссылки на изображении до отправки электронного сообщения.

Самый простой пример XSS атаки можно представить запросом:

http://index.php?name=guest<script>alert('XSS')</script>

Чаще всего в современные браузеры по умолчанию встроена система безопасности, предотвращающая такие атаки. Они защищают от XSS прямого действия, но могут пропустить более сложные, например хранимые XSS и основанные на DOM XSS атаки. Одна из брешей в системе защиты браузера основана на «доверительной» политике доменов.

До того как фильтр XSS в браузере обработает исходящий HTTP запрос, он проверит, откуда этот запрос отправлен. Считается, что системе нет смысла рассматривать запросы, отправленные с того же домена, т.к. это простая трата ресурсов. Однако XSS может прихоть от любого источника. Злоумышленник может просто применить отраженную XSS атаку, и перенаправить запрос на «доверенный» домен средствами JavaScript.

Для борьбы с самой атакой может быть достаточно экранирования всех строк, попадающие в HTML-документ. Однако устранять необходимо не XSS, а уязвимость её породившую, что влечёт за собой необходимость защищенной обработки данных. Такую обработку можно реализовать при помощи определения степени доверия к данным, типизации и валидации всей входящей информации, а также приведение выходных данных к виду, безопасному для принимающей стороны.

Предположим, на сайте есть форма для размещения комментариев, которые будут отображаться сразу же после добавления. Злоумышленник может попытаться разместить комментарий, содержащий JavaScript код. После отправки формы, все данные переправляются на сервер и сохраняются в базе данных. После этого информация извлекаются из базы и новый комментарий отображается на HTML странице, вместе с внедрённым вредоносным кодом. Он может перенаправлять пользователя на какую-то вредоносную страницу или на фишинговый сайт.

Для защиты приложений, можно пропустить входной поток данных через функцию strip_tags(), которая удалит все присутствующие теги. Тогда при отображении данных в браузере, используется функция htmlentities(), преобразующая все возможные символы в соответствующие HTML-сущности.

Эти правила актуальны для любых атак, обусловленных уязвимостью этого класса. Например, для SQL-инъекций, внедрений команд и т.д. И, хотя эти атаки давно известны, и разработчики давно знают, что данным, поступающим на сервер от клиента доверять нельзя, они зачастую не задумываются о том, что обратное также верно, причем по тем же самым причинам. Тем не менее, если бы защищенная обработка данных была реализована и на стороне клиента, это позволило бы свести к минимуму риски клиентских атак, связанные с эксплуатацией уязвимостей на сервере.

Список использованных источников:

1. XSS: the easiest way to hack your website in 2014 [Электронный ресурс] – электронные данные – Switzerland: 2014. – Режим доступа: https://www.htbridge.com/blog/xss_the_easiest_way_to_hack_your_website_in_2014.html, свободный.
2. Sebastian Lekies, Ben Stock, Martin Johns. A tale of the weaknesses of current client-side XSS filtering [Текст]: доклад / конф. Black Hat USA 2014.

РЕКУРРЕНТНОЕ БЛОЧНОЕ КОДИРОВАНИЕ В МОДУЛЬНОЙ АРИФМЕТИКЕ

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

Дикевич Д. В.

Овсянников В. А. – кандидат физ.-мат. наук, доцент кафедры СТК

При передаче цифровых данных по каналу всегда существует вероятность того, что принятые данные будут содержать ошибки. Если частота ошибок превышает некоторый уровень, то можно использовать кодирование с исправлением ошибок, которое позволяет уменьшить частоту ошибок до приемлемой. Кодирующие устройства сложны, однако рекуррентное кодирование позволяет построить более простые кодирующие и декодирующие устройства по сравнению с другими методами.

Рекуррентное кодирование позволяет строить блочные коды. Представим исходный алгоритм в модульной арифметике:

$$C_n = \sum_{k=0}^{m-1} C_k \delta(n-k) + h(n-m) \sum_{k=1}^{m} \alpha_k C_{n-k} \ , \ \mathrm{mod}\ p \ ,$$

где C_k - информационный символ, C_{n-k} - проверочные символы.

Наличие периодичности позволяет записать системную функцию генератора одного периода последовательности C_n в виде:

$$D(z) = (1 - z^{-N}) \frac{\sum_{n=0}^{m-1} U_n z^{-n}}{1 - \sum_{k=1}^{m} \alpha_k z^{-k}} \ , \ \mathrm{mod}\ p \ ,$$

$$U_n = C_n - h(n-1) \sum_{k=1}^{m} (p - \alpha_k) C_{n-k} \ , \ n = 0(1)m-1 , \ \mathrm{mod}\ p \ .$$

Все действия (сложение, деление, умножение) выполняются с поправкой на модульную арифметику.

Алгоритм и системная функция дают правило формирования блочного кода (N, m) длиною в N позиций, из которых первые m позиций (стартовые) представляют информационную часть, а $N - m = r$ – проверочную. Каждая позиция может принимать значения $0,1,..., p-1$, где p – простое число.

Процесс определения кодового слова по полученному набору длины N, т.е. декодирование, осуществляется в 2 этапа. Декодером вычисляется синдром полученного слова. Затем по синдрому определяется, в каком символе произошла ошибка, после чего она исправляется.

Разработаны схемы кодирующего и декодирующего устройств. На рисунках 1 и 2 представлены схемы для кода (7,3), используя образующий полином $1 + z^{-2} + z^{-3}$.

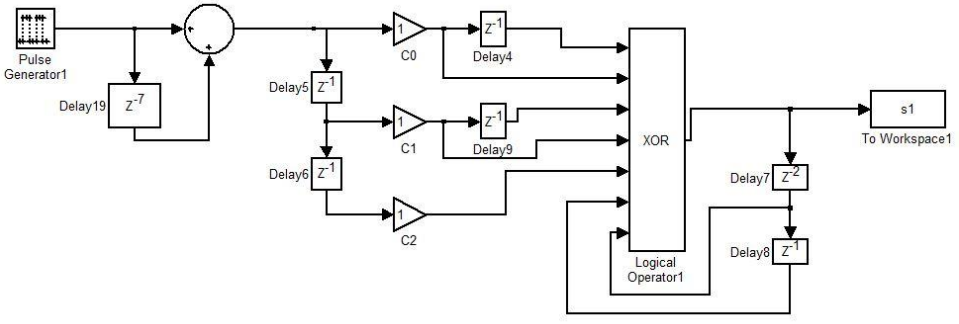

Рис. 1 – Структурная схема кодирующего устройства (7,3)

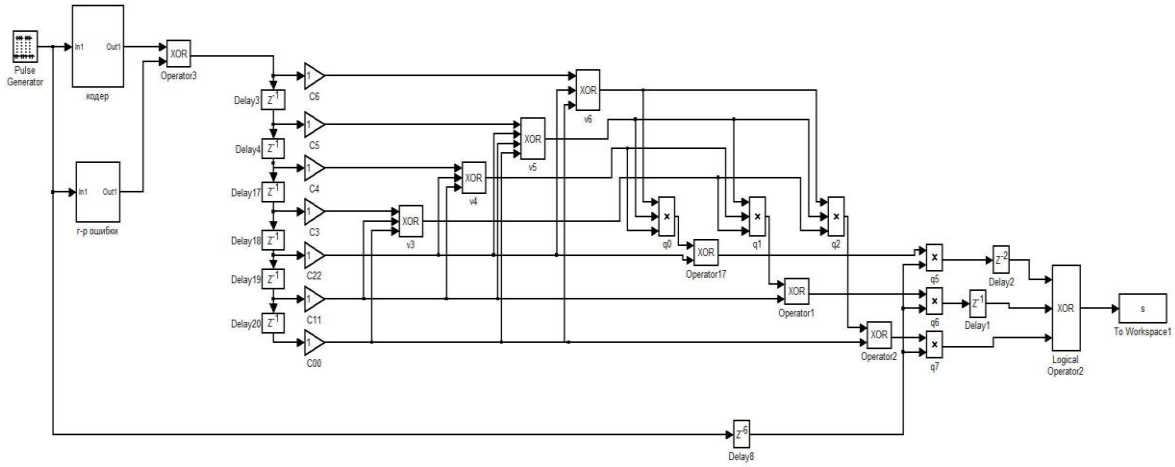

Рис. 2 – Структурная схема декодирующего устройства (7,3)

Для создания моделей была использована встроенная в MatLab система динамического моделирования Simulink.

Таким образом, были разработаны схемы кодирования и декодирования рекуррентных блочных кодов, которые позволяют находить и исправлять ошибки. Блочное кодирование обеспечивает высокую верность передачи и имеет определенное преимущество при построении декодеров.

Список использованных источников:

1. Прокис, Дж. Цифровая связь. Пер. с англ. /Под ред. Д.Д. Кловского. – М.: Радио и связь. 2000. – 800 с.: ил.
2. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. – М.: Связь, 1979. – 744., ил.
3. Кларк Дж., мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. – М.: Радио и связь, 1987. – 392 с.: ил. – (Стат. теория связи).
4. Лидр Р., Нидеррйтер Г. Конечные поля: В 2-х т. Т. 1. Пер. с англ. – М.: Мир, 1988. – 430 с.
5. Овсянников В.А. Методы формирования и цифровой обработки сигналов: Учеб. пособие для студ. спец. «Многоканальные системы телекоммуникаций» и «Системы радиосвязи, радиовещания и телевидения» всех форм обуч. /В.А. Овсянников. – Мн.: БГУИР, 2005. – 91 с.: ил.

ФУНКЦИОНАЛЬНАЯ МОДЕЛЬ ЦЕНТРАЛЬНОЙ СТАНЦИИ СОПРЯЖЕНИЯ ИНТЕРАКТИВНОЙ СПУТНИКОВОЙ СЕТИ

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

Акуционок В. В., Джафаров Ф.

Липкович Э. Б. – д-р. доцент

В современных интерактивных спутниковых сетях одной из главных задач является предоставление широкого спектра услуг. Это обязывает к применению сложного оборудования, одним из которых является центральная станция сопряжения.

Центральная станция сопряжения (ЦСС) интерактивной спутниковой сети располагается в местах с насыщенной телекоммуникационной инфраструктурой или в точках сопряжения с высокоскоростными оптическими каналами и сетями ведущих поставщиков информационных услуг. Она осуществляет подготовку и передачу данных, прием запросов, идентификацию и сетевую синхронизацию спутниковых интерактивных терминалов (СИТ), находящихся в зоне обслуживания, а также цифровую обработку сигналов.

В состав ЦСС (рис. 1) входят: тракты приема и передачи, блок контроля и управления системой (БКУС), модуль контроля качества обслуживания (МККО), маршрутизатор, Ethernet-коммутатор, подсистема технических средств доставки данных и центр управления системой.

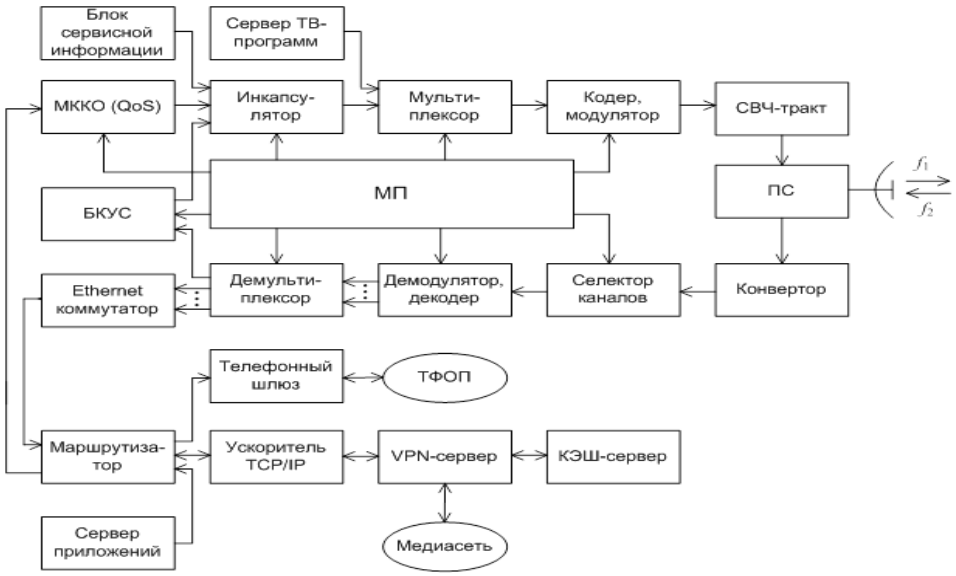

Рисунок 1 – Структурная схема центральной станции сопряжения

Основные функции БКУС заключаются в управлении доступом абонентских терминалов к ИСЗ, назначении каждому периферийному СИТ динамических или статических IP-адресов, установлении параметров прямого и обратного каналов (значения частот, длины временных окон, кодозащита и др.), синхронизации периферийных терминалов, сборе и обработке, поступивших с СИТ данных. В целях избирательного функционирования отдельных служб для них могут устанавливаться приоритеты, как на уровне устройств, так и приложений. Приоритеты распределяются на основе IP-адресов и номеров портов источника и получателя информации.

Структура построения приемопередающего тракта станции основывается на положениях стандартов DVB-S/ DVB-S2 [1]. В тракте передачи пришедшие на вход инкапсулятора потоки информационных данных в протоколе TCP/IP (UDP, ICMP) преобразуются вместе с сигналами контроля, управления и сигнализации в транспортный поток данных стандарта MPEG-2. Преобразование IP-дейтаграмм в пакеты по 188 байт осуществляется в соответствии с процедурой многопротокольной инкапсуляции (МПИ), которая управляется транспортным протоколом DSM-CC (Digital Stronge Media – Command and Control – средства цифровой записи – управления и контроля). В процессе инкапсуляции генерируется и вносится в транспортные пакеты сервисная информация, идентификационные номера (PID) основных и дополнительных сообщений, метки времени, максимальные и текущие значения скоростей передаваемых данных и IP адреса каждого пользователя. В инкапсуляторе производится также обработка адресов потокового вещания в режиме

Multicast, ограничение скорости передачи данных для исключения переполнения буферной памяти, расстановка приоритетов по значимости компонент транспортного потока и др.

Образованный поток данных, адресованный большому числу пользователей, поступает на мультиплексор, в котором при необходимости происходит его объединение с цифровыми сигналами ТВ-вещания. В модуляторе осуществляется помехоустойчивое двухступенчатое канальное кодирование, перемежение бит и QPSK (8-ФМ, 16-APSK или 32-APSK) модуляция несущей на промежуточной частоте. Последующее преобразование фазомодулированного радиосигнала на частоту передачи и его усиление осуществляется в СВЧ блоке. Выходная мощность передатчика 250…400 Вт.

Для компенсации дополнительных потерь, возникших на спутниковой радиолинии вследствие осадков, в модуляторе ЦСС стандарта DVB-S2 предусмотрено адаптивное изменение параметров кодирования и формата модуляции (ACM). Изменение параметров ведется по пакетам, адресованным соответствующим СИТ под действием управляющих сигналов, поступающих по обратным каналам от СИТ. Условием формирования управляющих сигналов является снижение величины ОНШ на входе СИТ, при котором падает достоверность приема ниже допустимого значения.

В тракте приёма ЦСС осуществляется конвертация принятых спутниковых сигналов в более низкий частотный диапазон (например, в диапазон 0,95-2,15 ГГц), канальная селекция, многоканальная демодуляция, декодирование и демультиплексирование субпотоков. В демультиплексоре производится выделение вспомогательных сигналов, содержащих сведения о характеристиках СИТ, неточностях в значениях фаз, частот и синхронизации, а также сведения для регистрации СИТ и предоставления им рабочих и временных окон. Вспомогательные сигналы поступают на блок контроля и управления сетью, где на их основании формируется информация для коррекции характеристик СИТ. Субпотоки с запросными данными направляются через Ethernet-коммутатор и маршрутизатор на VPN- сервер. При отключении АИТ от сети, процессор БКУС перераспределяет освободившиеся полосы частот другим АИТ и отправляет IP-адреса неработающих терминалов на хранение.

Список использованных источников:

1. Липкович, Э. Б. Проектирование и расчёт систем цифрового спутникового вещания / Э. Б. Липкович, Д.В. Кисель // Уч. метод. пособие. – Мнинск: БГУИР, 2006. – 135 с.

ПРИНЦИПЫ ВЫСОКОСКОРОСТНОГО ОБМЕНА ИНФОРМАЦИЕЙ В СПУТНИКОВЫХ СЕТЯХ

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

Пытель А. Н., Джафаров Ф. Р.

Липкович Э. Б. – доцент кафедры СТК

В настоящее время приобрели широкое развитие спутниковые технологии высокоскоростного обмена информацией между оборудованием потребителей услуг и опорными телекоммуникационными сетями наземного сегмента. Для реализации данной технологии операторы спутниковых сетей выделяют группу радиостволов или весь ресурс многофункциональных космических аппаратов, через которые организуется широкополосный доступ в интернет, видеоконференцсвязь, дистанционное обучение, репортажи с мест событий, удаленное видеонаблюдение и др.

В течение последних пяти лет в мире развернуто свыше десятка интерактивных высокоскоростных сетей, базирующихся на спутниках нового поколения HTS (High Throughput Satellites) с многолучевыми антеннами, сотовым покрытием территории и процессорной обработкой сигналов на борту. В результате принятых решений многократно увеличилась пропускная способность и энергетическая эффективность сетей. Вместо пропускной способности, характерной для традиционных спутников в 2…4 Гбит/с, спутники нового поколения за счет широкой полосы радиоканалов (250…450 МГц) обеспечивают 50..70 Гбит/с в Ка-диапазоне частот. Кроме того в этом диапазоне допускается высокая плотность потока мощности спутникового сигнала у поверхности Земли (от -115 до -105 дБВт/м^2 для углов мест приема от 0º до 90º), что позволяет реализовать высокий уровень эквивалентной изотропно -- излучаемой мощности (до 65 дБВт) при соблюдении требований на электромагнитную совместимость спутниковых и наземных средств. Несмотря на усложнение высокоинформативных спутников и рост их стоимости более чем в два раза (до $450 млн.) благодаря их высокой пропускной способности снижены затраты на эквивалентную полосу, размеры приемных антенн и увеличена скорость доставляемых данных (4…8 Мбит/с) в адрес абонентов сети.

Технология высокоскоростного доступа к информационным ресурсам посредством использования обратного спутникового канала определена принятым ETSI стандартом DVB-RCS (Return Channel Satellite). Эта технология отвечает требованиям масштабируемости и гибкости построения и особенно удобна для обмена информацией между центром и филиалами. В прямом широкополосном канале предусмотрена высокая энергетическая и спектральная эффективности передачи данных на периферийные терминалы за счет использования современных методов канального помехоустойчивого кодирования, полососберегающих методов модуляции и многолучевых антенн с «сотовым» способом покрытия территории обслуживания. Согласно этому способу в разнесенных по пространству спутниковых лучах одинаковые значения несущих частот могут многократно повторяться. Большое число узких лучей, создаваемых антенной, (их число может превышать 50) позволяет повысить энергетику на радиолинии и эффективность частотного ресурса. В обратных запросных каналах используются разные способы передачи данных с их упаковкой в ATM или MPEG-2 пакеты, разные методы многостанционного доступа к спутниковому сегменту, а также разные типы протоколов (IP; 10/100 Base –T/ L 2; TCP/IP) для подключения терминалов пользователей к локальным компьютерным и телефонным сетям.

Абонентский интерактивный терминал RCS-T (Return Channel Satellite Terminal) относится к классу станций региональной спутниковой связи VSAT (Very Small Aperture Terminal) и строится на принципах стандартов DVB-S/DVB-S2 и DVB-RCS. Основными потребителями терминального оборудования DVB-RCS являются государственные учреждения, нефте-газодобывающие и бизнес-компании, энергетики, торговые сети, структуры оперативного сбора и распределения новостной информации, службы подвижных средств, корпоративные и индивидуальные пользователи.

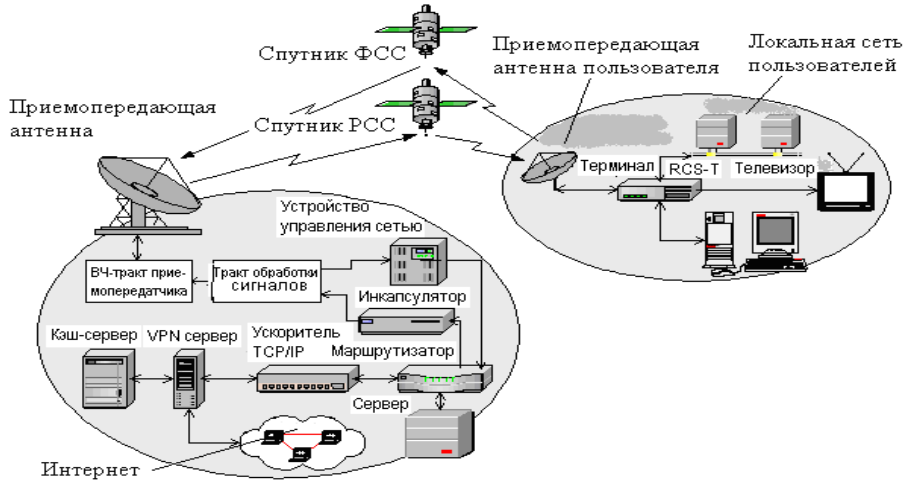

Рисунок 1 – Концепция построения интерактивной спутниковой сети

Система двустороннего спутникового обмена информацией может строиться на базе одного или двух близкорасположенных на ГО спутников (рисунок 1). Обычно запросные каналы организуются через ИСЗ фиксированной спутниковой службы (ФСС), поскольку ретрансляторы этой службы работают в квазилинейном режиме (ниже уровня насыщения передатчика на 4..6 дБ) и допускают одновременное усиление большого числа сигналов без заметного роста искажений. Доставка широкополосной информации к пользователям организуется через тот же ИСЗ ФСС или ИСЗ радиовещательной спутниковой службы (РСС). Последний имеет худшую линейность передающего тракта, но обладает более высоким значением ЭИИМ, что позволяет снизить размеры приемных антенн АИТ. Однако аренда ретрансляторов РСС дороже. Работа в двухспутниковой сети предполагает использование антенн с двумя облучателями. Каждый облучатель служит для связи с соответствующими ИСЗ, расположенными на разных позициях ГО. Поляризация сигналов на прием и передачу чаще всего выбирается разной.

Стандартом DVB-RCS рабочий диапазон сети не регламентирован, поэтому могут использоваться полосы частот C-, Ku-, Ka-диапазонов. Например, доставка данных с ИСЗ на АИТ организуется в полосе Ku-диапазона (14/11 ГГц), а отправка данных на ИСЗ в Ka-диапазоне (30/20 ГГц). Реализация этого варианта возможна через спутники, содержащие стволы Ku- и Ka-диапазонов (Astra 1-H, Eutelsat W6, Hot Bird-7 и др.).

Важным функциональным показателем системы является используемый способ множественного доступа удаленных терминалов к ИСЗ. Выбор конкретного варианта зависит от загрузки сети, объемов и видов предоставляемых услуг, активности работы пользователей в сети и др. Распространенными способами множественного доступа терминалов к ИСЗ являются: PAMA (Pre-assigned Multiple Access) – предоставление спутникового ресурса на постоянной основе; DAMA (Demand Assigned Multiple Access) – предоставление спутникового ресурса на время сеанса связи по требованию; SCPC (Single Channel Per Burst) – передача данных по каналу связи на одной несущей, MCPC (Multiple Channel Per Carrier) –передача объединенной группы данных пользователей на одной несущей; MF-TDMA (Multiple Frievanci – Time Division Multiple Access) – частотно-временное разделение каналов. Множественный доступ MF-TDMA основан на динамическом назначении удаленным терминалам конкретных частот, временных сегментов и полос пропускания в соответствии с запросом. Сформированные с помощью АИТ пакеты запросных данных переносятся на несущую передачи и поступают на спутник в определенные интервалы времени по сигналам синхронизации со стороны центральной станции.

В соответствии с принятой для DVB-RCS топологией сети типа “звезда” (star) осуществить обмен информацией между удаленными АИТ возможно только в два “скачка”, т. е. сигналы проходят через ИСЗ дважды. В результате возникает существенная задержка сигналов (в 0,6 с) и усложняются проблемы организации телефонной связи. Поэтому телефонная связь часто реализуется по упрощенной схеме, т.е. напрямую между АИТ и телефонной сетью общего пользования (ТфСОП). Для организации телефонной связи между каждым АИТ (по полносвязной схеме) необходимо, чтобы эту технологию поддерживала ЦСС и ретранслятор ИСЗ или чтобы один из терминалов был ведущим и обладал функциями узловой станции.

В более расширенной сети DVB-RCS может присутствовать несколько узловых станций (шлюзов), которые обслуживают региональные подсети. Каждая узловая станция имеет свой спутниковый сегмент и набор частот несущих, а также собственную IP-адресацию, устройства сетеобразования и управления качеством обслуживания. Благодаря наличию шлюзов в сети возможна прямая взаимосвязь между АИТ разных подсетей.

Для эффективной работы интерактивной системы в ее состав входит центр управления сетью NCC (Network Control Center). Он осуществляет контроль параметров системы DVB-RCS, управление работой региональных станций, перераспределение ресурсов полосы пропускания, выявляет и устраняет отказы, ведет учет и управление базами данных. К числу достоинств данной технологии следует отнести:

– возможность отправки запроса для получения информации с территорий, на которых отсутствуют наземные каналы связи;

– возможность доступа к информационным ресурсам с подвижных сухопутных, морских и воздушных средств;

– быстрая установка и настройка терминалов для работы в сети;

– высокая эксплуатационная надежность системы;

– универсальность каналов сети для передачи разных видов информации;

–фиксированные затраты на реализацию доступа к спутниковой сети независимо от местоположения абонента.

Список использованных источников:

1 Липкович Э.Б., Кисель Д. В. Проектирование и расчет систем цифрового спутникового вещания. // Учебное пособие для студентов специальностей «Многоканальные системы телекоммуникаций», «Системы радиосвязи, радиовещания и телевидения» всех форм обучения – Минск, 2014. – 266с.

МЕТОДЫ СИНХРОНИЗАЦИИ В СВЕРХШИРОКОПОЛОСНЫХ СИСТЕМАХ СВЯЗИ

Полоцкий государственный университет, г. Новополоцк, Республика Беларусь

Иванов М.М., Кременя К.И., Андреев Ю.А.

Чертков В.М. – м.т.н.

Представлены основные методы синхронизации для сверхширокополосных систем связи, пояснен принцип действия каждого метода с целью выявления их недостатков и сформированы требования для проектирования высокостабильной сверхширокополосной системы телекоммуникаций.

Тенденции развития сверхширокополосных (СШП) систем связи обусловлены наличием у них ряда преимущественных факторов перед узкополосными системами телекоммуникаций. Среди достоинств необходимо отметить следующие: высокая скрытность канала связи, (благодаря низкому уровню мощности спектральной плотности СШП сигнала), высокая абонентская емкость, возможность достижения высоких скоростей передачи данных, хорошая помехоустойчивость [1-2]. Кроме того, вследствие широкополосности затухание короткоимпульсного сигнала в различных средах достаточно мало [2].

Важным фактором, обеспечивающим корректную работу СШП системы, является синхронизация передатчика и приемника. В устройствах СШП радиолокации задача синхронизации не представляет собой технической сложности, так как структура таких систем предполагает, как правило, размещение передатчика и приемника в пределах одного общего корпуса или шасси, в зависимости от конструктива. Передача синхросигнала в таком случае обеспечивается с помощью стандартной проводной линии связи. Но в системах телекоммуникаций приемник и передатчик удалены друг от друга на некоторое расстояние. Возникает необходимость в синхронизации с помощью беспроводного канала связи. На сегодняшний день существует несколько путей решения данной проблемы. При этом появляется потребность в анализе известных подходов с целью формирования оптимальных критериев для получения высокоточной и стабильной синхронизации при построении СШП систем связи.

Использование двух независимых каналов (рисунок 1)**.** Сущность способа вхождения в синхронизм состоит в использовании двух независимых радиоканалов - СШП радиоканал и широкополосный (ШП) радиоканал с частотно- (ЧМ) и фазомодулированными (ФМ) радиосигналами, по которым одновременно распространяется, например, кодовая последовательность синхросигнала. Моменты изменения фазы или частоты ШП радиосигнала соответствуют временным окнам с импульсами СШП радиосигнала в центре каждого временного окна. Вхождение в синхронизм и поддержание его через определенные промежутки времени, в течение которых СШП радиосигнал не должен выйти за пределы временного окна при всех дестабилизирующих факторах, обеспечивается ШП радиоканалом. В промежутках между синхросигналами ШП радиоканал может передавать другую информацию. Выделение моментов изменения фазы или частоты ШП радиосигнала осуществляются в процессах его усиления, преобразования на промежуточную частоту и в цифровую форму с помощью аналого-цифрового преобразователя (АЦП) и последующей обработки вейвлет-фильтром [3].

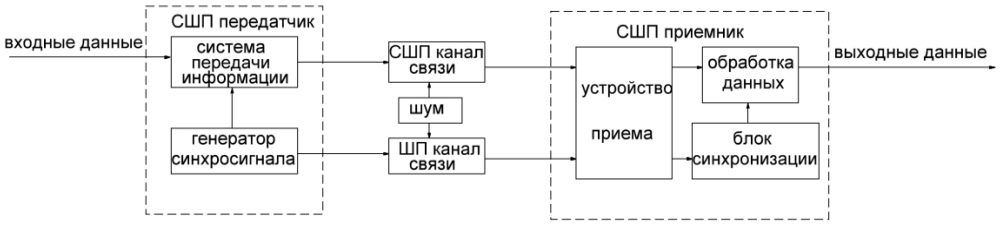

Рис.1 – Обобщенная структурная схема СШП системы связи с двумя каналами передачи

Недостатком данной системы является работоспособность только при отсутствии многолучевости в ШП радиоканале [4].

Корреляционная обработка кодовой последовательности при многолучевом распространении. В отличие от предыдущего метода в данной системе используется один общий сверхширокополосный канал связи для синхронизации и передачи данных. Сущность способа вхождения в синхронизм заключается в использовании любой части многолучевого распространения кодовой последовательности сверхширокополосного сигнала [5]. За счет увеличенного импульсного потока многолучевого сигнала проводится операция корреляционной обработки с образцовым импульсным потоком и в случае их совпадения система входит в синхронизм. При пороговой обработке, по крайней мере, одной отраженной части многолучевости после проверки на синхронизм система осуществляет быстрый захват. Таким образом, способ синхронизации заключается в приеме импульсного сигнала, измерении образцового (копии) импульсного потока, поиске импульсного сигнала за счет сдвига копии импульсного потока до момента их совпадения.

К недостатку данной системы следует отнести неработоспособность в мобильном исполнении, так как условие многолучевости непредвиденно изменяется в зависимости от дальности и относительного положения приемника и передатчика [3].

Метод быстрой синхронизации. Способ идентификации фазы входного СШП сигнала включает в себя несколько этапов: прием входных импульсов СШП сигнала, соседние импульсы которого поступают в фиксированные интервалы; генерация локальных импульсов в СШП приемнике; корреляция локальных импульсов с входными импульсами и получение корреляционной функции; определение максимума корреляционной функции при каждом смещении локальных импульсов в СШП приемнике, содержащее определение первого максимума на первом фазовом интервале, анализа корреляционной функции для нахождения второго импульса, который превышает первый максимум; поиск интервалов вокруг второго максимума около второго фазового интервала и определение является ли второй максимум действительно максимумом [3, 6].

Метод быстрой синхронизации с плавающим порогом. Метод заключается в приеме входного СШП сигнала, формировании его копии в СШП приемнике, анализе входного СШП сигнала и сравнении с его копией с заранее определенным порогом, получении результата сравнения, сдвиге копии входного сигнала, когда результат анализа превышает заранее определенный порог, изменении величины порога, повторении указанных операций сравнения, сдвиге копии входного сигнала[3,7].

Недостаток вышеприведенных двух методов заключается в эффективности системы только при большом отношении сигнал/шум на входе приемника.

Синхронизация с повышенной точностью и стабильностью синхронизации (Рисунок 2)**.** Структура данной систем включает в себя, как минимум, две радиостанции, каждая из которых имеет общую, передающую (ПРД) и приемную (ПРМ) части. Передатчик первой радиостанции излучает в каждом интервале ПРД синхроимпульсы и информационные сигналы, а приемник второй радиостанции принимает эти сигналы и с помощью местного цифрового синтезатора частот (ЦСЧ) на основе системы импульсно-фазовой автоподстройки частоты (ИФАПЧ) подстраивает и синхронизирует свои интервалы ПРМ с интервалами от ПРД первой радиостанции с точностью до фазы. Повышенная точность обеспечивается благодаря тому, что передатчик первой радиостанции и приемник второй радиостанции начинают работать от одного опорного генератора в первой радиостанции. Аналогично передатчик второй радиостанции излучает в каждом интервале ПРД синхроимпульсы и информационные сигналы, а приемник первой радиостанции принимает эти сигналы и с помощью ЦСЧ первой радиостанции синхронизирует свои интервалы ПРМ с интервалами от ПРД второй радиостанции с точностью до фазы. В результате образуются две синхронные системы ИФАПЧ, работающие каждая от своего опорного генератора. Синхронизация сохраняется при всех дестабилизирующих факторах и в скоростных мобильных устройствах [4].

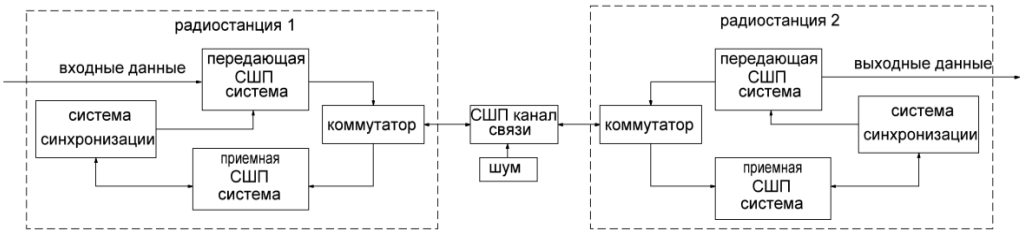

Рис.2 – Обобщенная структурная схема СШП системы связи с повышенной точностью и стабильностью синхронизации

В качестве недостатка данного метода можно выделить повышенные затраты на время вхождения в синхронизм.

В результате анализа рассмотренных методов сформированы общие требования к устройству синхронизации при проектировании высокостабильной СШП системы связи: возможность работы в мобильном исполнении при многолучевом распространении сигнала, малая вероятность рассинхронизации, высокая помехоустойчивость, высокая степень точности синхронизации (до фазы) для минимизации потерь данных на приемной стороне и обеспечение минимального времени вхождения в синхронизм.

Список использованных источников:

1. Дмитриев В. Технология передачи сигналов с использованием сверхширокополосных сигналов (UWB) / В. Дмитриев // Компоненты и технологии – 2004 – №1.

2. Шахнович И. В. Современные технологии беспроводной связи / И. В. Шахнович. – 2-е изд. – Москва: Техносфера, 2006. – 288с.

3. Способ и система связи с быстрым вхождением в синхронизм сверхширокополосными сигналами: пат. 2354048 RU. МПК H04B7/00 / Г.А. Кыштымов, В.В. Бондаренко, С.Г. Кыштымов; заявитель ОАО "Концерн "Созвездие". - № 2007144256/09; заявл. 28.11.07; опубл. 27.04.09.

4. Система связи сверхширокополосными сигналами с повышенной точностью и стабильностью синхронизации: пат. 2441320 RU. МПК H04B7/00/ Г.А. Кыштымов, С.Г. Кыштымов, Е. И. Стецура, И. П. Усачев; заявитель ОАО "Концерн "Созвездие". - № 2010119288/08; заявл. 13.05.10; опубл. 27.01.12.

5.Method and system for fast acquisition of ultra-wideband signals: US 6925109. Int. cl. H04B 1/69 / James L. Richards, Mark D. Roberts; Assignee: Alereon Inc., Austin, TX - Appl. No.: 10/356'995; filed Feb.3.2003; data of patent Aug. 2, 2005.

6. Ultrawide bandwidth system and method for fast synchronization: US 6925108. Int. cl. H04B 1/69 / Timothy R. Miller, Martin Rofhear; Assignee: Freescale Semiconductor, Inc., Austin,Tx - Appl. No.: 09/685,195; filed Oct. 10, 2000; data of patent Aug. 2, 2005.

7.Ultrawide bandwidth system and method for fast synchronization using sub-code spins: US 6967993. Int. cl. H04B 1/707/ Timothy R. Miller; Assignee: Freescale Semiconductor, Inc., Austin,Tx - Appl. No.: 09/684,401; filed Oct. 10, 2000; data of patent Nov. 22, 2005.

WDM PON КАК СЛЕДУЮЩЕЕ ПОКОЛЕНИЕ ПАСИВНЫХ ОПТИЧЕСКИХ СЕТЕЙ

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

Сергеев Н.Н., Белятко А.Л.

Урядов В.Н. – к.т.н.,доцент

В настоящее время потребности абонентов к пропускной способности сети электросвязи растут с каждым днём, так стараясь удовлетворить эти потребности, национальный оператор электросвязи РУП «Белтелеком» ведёт активное внедрение GPON сети, однако с таким темпом роста уже очевидно, что сеть GPON не сможет в полной мере удовлетворить потребителя в будущем, а разделив каждого абонента по длине волны, можно существенно увеличить пропускную способность оптических сетей.

WDM-PON (Wavelength division multiplexing passive optical network) – пассивная оптическая сеть со спектральным разделением каналов. Такая сеть подразумевает присвоение каждому абоненту своей длинны волны. Есть две вариации построения сети WDM-PON:

1) с присвоение каждому абоненту по две длинны волны (одну на приём и одну на передачу)[1];
2) с присвоением абоненту только одной длинны волны (в этом случае можно вдвое увеличить количество абонентов работающих в такой сети)[2,3].

Принцип реализации WDM-PON представлен на рисунке 1:

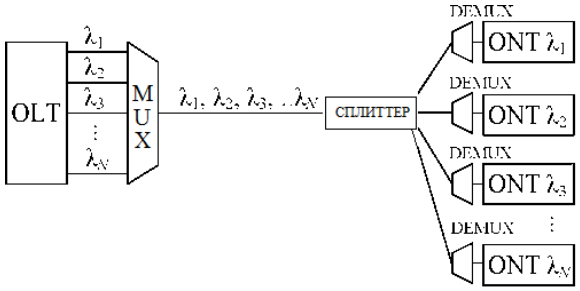

Рис. 1 - Структура сети WDM-PON

На схеме видно, что каждому терминалу ONT выделена своя длина волны λ_1, λ_2, λ_3, ... λ_N,

Сеть WDM-PON обладает следующими особенностями:

а) среднее время задержки передачи пакетов приблизительно в 20 раз ниже, чем для GPON;

б) влияние разброса длин линий на среднее время задержки передачи пакетов не возрастает с ростом числа абонентов, включенных в сегмент WDM-PON, так как отсутствует временное разделение доступа;

в) наименьшее влияние коэффициента вариации интервала обслуживания на среднее время задержки передачи пакетов (кадров) в обратном канале достигается при использовании технологии WDM-PON в виду отсутствия длительного процесса доступа и малой величины интервала обслуживания.

Основные преимущества WDM-PON:

– пользователю предоставляется выделенная полоса (нет распределения на конкурентной основе);
– при увеличении количества абонентов затухание в WDM-мультиплексоре растёт в меньшей степени чем в оптическом сплиттере;
– сигналы абонентов физически изолированы;
– эффективно используется волокно (до 64 абонентов на волокно, как и в GPON);

Основной недостаток WDM-PON — высокая стоимость, так как требуются узкополосные передатчики, излучающие на заданной длине волны. Это особенно критично для абонентских устройств ONT, так как их стоимость напрямую влияет на стоимость абонентской линии. С одной стороны проблема частично решается за счет унификации и уменьшения типов аппаратных компонент в оконечных устройствах (например, использование настраиваемых на заданную волну лазеров), с другой — не без оснований можно надеяться, что через несколько лет к моменту выхода стандарта стоимость оптических компонент для WDM-PON будет значительно ниже нынешнего уровня.

Переход от TDM-PON к WDM-PON является залогом успешного будущего оптических сетей доступа.

Список использованных источников:

1. Kyeong-Eun Han, Design of AWG-based WDM-PON Architecture with Multicast Capability

2. Урядов В.Н., Глущенко Д.В. Использование технологии WDM для повышения эффективности пассивных оптических сетей // Международная научно-техническая конференция, посвященная 45-летию МРТИ-БГУИР : тез. докл. Междунар. науч.-техн. конф., Минск, 19 марта 2009. – Минск : БГУИР, 2009. – 19с.

3. Урядов В.Н., Глущенко Д.В. Коллективная пассивная WDM сеть с независимым доступом к оптической среде передачи // Современные средства связи : материалы XIV Междунар. науч.-техн. конф., 29 сент.-1 окт. 2009 года, Минск, Респ. Беларусь. – Минск : ВГКС, 2009. – 23с.

ОХРАННЫЕ СИСТЕМЫ РАЗНЕСЕННЫХ ОБЪЕКТОВ НА ОСНОВЕ ВОЛОКОННО-ОПТИЧЕСКИХ ТЕХНОЛОГИЙ

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

Глебович Д.Ч.

Урядов В.Н. – к.т.н.,доцент

На сегодняшний день системы охранной сигнализации — это одно из наиболее эффективных решений, позволяющих обеспечить безопасность и неприкосновенность различного рода имущества и объектов.

Охранные системы на основе волоконно-оптических технологий не имеют равной альтернативы на объектах с большой протяженностью, таких как: пункты пропуска на границе, крупные режимные предприятия и объекты, тюрьмы, колонии, военные склады, подстанции, объекты нефтеперерабатывающей промышленности (нефтебазы, нефтехранилища, нефтепроводы), аэропорты, АЭС и т.д.

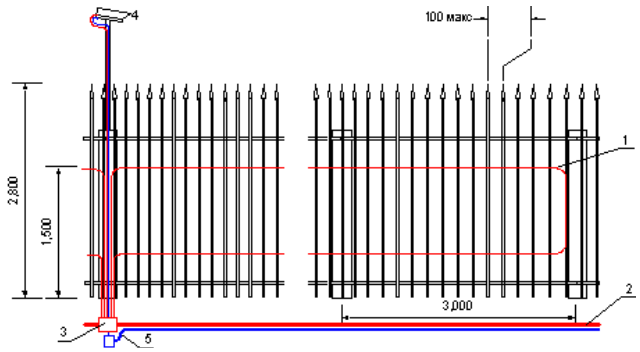

Рис.1. Фрагмент охранной сигнализации периметра: 1 – сенсорное оптическое волокно; 2 – магистральный ВОК; 3 – муфта; 4 – ТВ камера; 5 – магистральный кабель электропитания ТВ камер

При построении волоконно-оптических охранных систем применяются следующие технологии:

1) Технология основанная на методе регистрации межмодовой интерференции.

Полупроводниковый лазер обычно генерирует несколько десятков близких по частоте мод (спектральных линий) с определенным распределением энергии по спектру излучения. Если много-модовый оптоволоконный кабель подвергается механическим воздействиям, то на его выходе спектр излучения претерпевает изменения, что позволяет обнаруживать деформации или вибрации кабеля.

2) Технология использующая принцип двухлучевой интерферометрии.

Луч лазера расщепляется на два и направляется в два идентичных одномодовых оптических волокна. На приемном конце оба луча образуют интерференционную картину. Механические воздействия на чувствительный кабель приводят к изменениям интерференционной картины, которые и регистрируются фотоприемником.

3) Технология оптической рефлектометрии во временном диапазоне.

Данная технология использует явления обратного рассеяния света в волокне и отражения света от скачков показателя преломления. Измерения с помощью оптического рефлектометра основано на анализе отражённых оптических импульсов, излучаемых рефлектометром в оптическое волокно. Импульсы света, распространяясь по линии, испытывают отражения и затухания на неоднородностях линии и вследствие поглощения в среде.

4) Технология основанная на методе регистрации спекл-структуры.

На выходе многомодового оптоволокна наблюдается так называемая «спекл-структура», представляющая собой нерегулярную систему светлых и темных пятен. При деформациях или вибрациях волокна спекл-структура излучения претерпевает изменения.

Основные преимущества волоконно-оптических охранных систем:

- невосприимчивость сенсоров к электромагнитным излучениям и электробезопасность;
- волоконные датчики, построенные из диэлектрических элементов, применяются на металлических оградах, тяжелых жестких стенах, а также под землей и под водой и на взрывоопасных объектах;
- максимальная длина одной зоны охраны может достигать десятков километров;
- высокая надежность, большой срок службы, неприхотливость в эксплуатации.

Недостатком является то, что применение таких систем для периметров небольшой протяженности, к примеру, частных домовладений, неоправданно дорого.

Список использованных источников:

1. Урядов В.Н. Волоконно-оптические системы передачи// Электронный учебно-методический комплекс по дисциплине «волоконно-оптические системы передачи» (теория) для студентов специальностей I-45 01 01 «многоканальные системы телекоммуникаций». Минск: БГУИР, 2008. – 229 с.

2. Э. Удда. Волоконно-оптические датчики. Вводный курс для инженеров и научных работников. Москва: Техносфера, 2008, 520 с.

ПРИМЕНЕНИЕ ОПТОВОЛОКНА ДЛЯ РАСПРЕДЕЛЕННОГО КОНТРОЛЯ ТЕМПЕРАТУРЫ

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

Белятко А.Л., Сергеев Н.Н.

Урядов В.Н. – к.т.н., доцент

В современном мире оптические волокна (ОВ) нашли широкое применение в устройствах контроля и измерения физических параметров окружающей среды, таких как температура, натяжение, давление и т.п. Достоинствами датчиков на основе ОВ являются устойчивость к агрессивным воздействиям среды, пожаробезопасность, иммунитет к электромагнитному излучению. Самым главным достоинством, с точки зрения измерений и получения информации, является возможность проведения распределенных измерений, когда значение исследуемого параметра считывается по всей длине ОВ.

Внутримолекулярные вибрации, возникающие в ОВ под влиянием температуры, давления или растягивающих усилий, могут локально изменять характеристики пропускания света.

Внешние факторы вызывают колебания в кристаллической решетке твердого тела. Когда свет действует на эти колебания молекул, то частицы света (фотоны) взаимодействуют с электронами молекул, вызывая в оптическом волокне рассеяние света, состоящее из нескольких спектральных компонент: релеевского рассеяния, рамановского рассеяния и бриллюэновского рассеяния.

Для определения температуры наиболее важным параметром является рамановское рассеяние, которое в свою очередь имеет стоксовую и антистоксовую компоненты, спектрально сдвинутые на величину, эквивалентную резонансной частоте колебаний молекулярной решетки (рисунок 1).

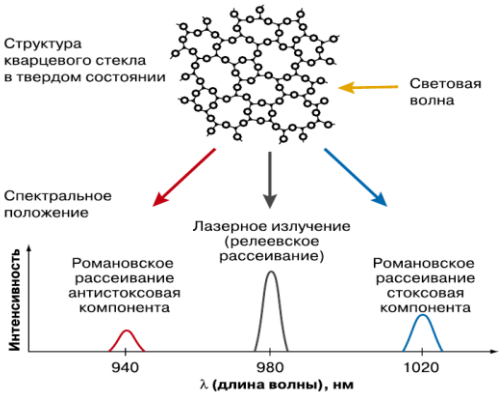

Рис. 1 – Спектр рамановского рассеяния

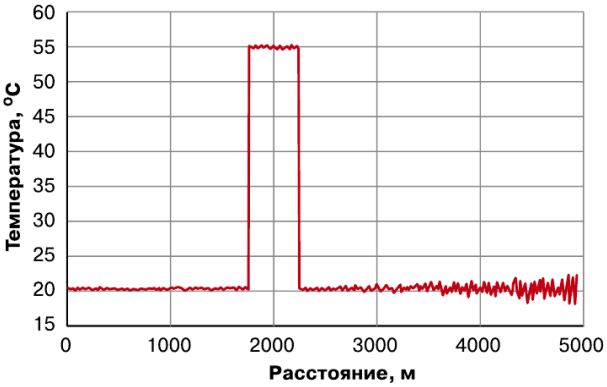

Рис. 2 – Расчет температуры линии

Зная скорость распространения света (основного сигнала с несущей частотой) в однородном кварцевом стекловолокне, а также математическую зависимость его затухания во времени (интенсивность отраженного пучка света уменьшается во времени по экспоненциальному закону) можно определить температуру в любой точке кабельной линии. Значение температуры и место рассчитывается из соотношений между интенсивностями основного сигнала, антистоксовых и стоксовых компонент света. Визуальное отображение окончательного расчета температуры линии показано на рисунке 2.

Рамановское излучение возникает при взаимодействии падающего (стимулирующего) излучения с температурной вибрацией молекул вещества среды распространения. Имеют место две линии рамановского сигнала – стоксова, расположенная правее по шкале длин волн от стимулирующего сигнала, и антистоксова – слева. Максимум интенсивности стоксовой (СЛ) и антистоксовой (АСЛ) линий для оптического волокна на основе кварца находится примерно на расстоянии ±440 1/см. [1]

При этом уровень мощности рамановских линий на 20-30 дБ ниже уровня рэлеевского сигнала. Отношение интенсивностей АСЛ и СЛ определяется из выражения (1): [2]

$$\frac{I_a}{I_s} = \frac{\lambda_s^4}{\lambda_a^4} \cdot \exp\left(\frac{-hc\nu}{kT}\right), \quad (1)$$

где I_a, I_s, λ_a, λ_s – интенсиность и длина волны СЛ и АСЛ; h – постоянная Планка; c – скорость света; k - постоянная Больцмана, T – абсолютная температура, ν – расстояние от стимулирующего излучения до рамановских линий. Таким образом, для измерения температуры T достаточно знать отношение интенсивностей СЛ и АСЛ.

Распределение обратнорассеянного сигнала СЛ и АСЛ можно измерить с помощью оптического рефлектометра, а затем рассчитать температуру в каждой точке проложенного оптического волокна. На рисунке 3 представлена упрощенная структурная схема такого устройства. Устройство измерения температуры отличается от обычного OTDR (оптическая рефлектометрия во временной области) лишь наличием волоконно-оптического фильтра, выделяющего из общего обратнорассеянного сигнала сигналы СЛ и АСЛ, и оптического коммутатора, направляющего эти сигналы поочередно на фотодиод. На схеме обозначены: ОР — разветвитель; ОВ — оптическое волокно; ВОФ – волоконно-оптический фильтр;ОК – оптический коммутатор; ФД – фотодиод; У — усилитель; АЦП — аналого-цифровой преобразователь; ЦСП — цифровой сигнальный процессор; РС — компьютер.

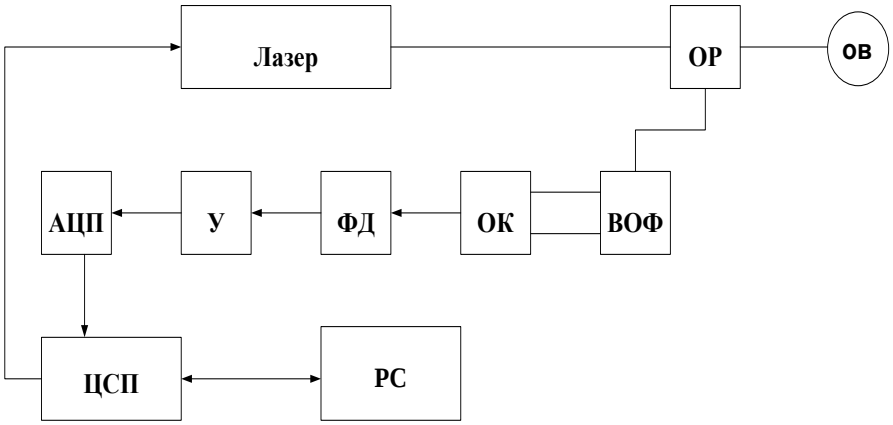

Рис. 3 - Схема системы контроля на основе рамановского излучения

Использование данного метода позволяет проводить непрерывный контроль температуры и целостности ОВ. Основные преимущества метода — это возможность использования обычных с примесью германия телекоммуникационных градиентных волокон, распределенный контроль в агрессивных средах и труднодоступных местах.

Список использованных источников:

1.ФОТОН-ЭКСПРЕСС, Научно-технический журнал №5(45) сентябрь 2005. -56 с.

2.Волоконно-оптические датчики. Вводный курс для инженеров и научных работников. Под ред. Э.Удда М.: «Техносфера», 2008. – 520 с

3. Новости электротехники №2(50) 2008.

СПОСОБЫ ОПОВЕЩЕНИЯ О ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ ЧЕРЕЗ СОТОВУЮ СЕТЬ

УП «Велком», Республика Беларусь

Матвеев Д.Н.

Мельниченко Д.А. – к.т.н., доцент

SMS и прочие варианты мобильных уведомлений никогда не рассматривались спецслужбами как основные инструменты оповещения населения. Таковыми по-прежнему остаются телевидение, радио и уличные громкоговорители. Тем не менее, МЧС всегда было заинтересовано в расширении своего инструментария, именно поэтому системы оповещения о чрезвычайных ситуациях с помощью сотовых сетей имеют место быть в разных странах. В значительной степени они универсальны и в свое время создавались для предупреждения о природных и техногенных катастрофах. Они постоянно развиваются, используя достижения современной техники.

Для оповещения по мобильной сети в РБ прибегают к двум способам:

- Cell Broadcast (CBC)
- SMS-рассылка.

В обоих случаях система автоматически выбирает всех абонентов, находящихся в сети в пределах указанного МЧС радиуса. CBC представляет собой пассивную технологию оповещения: на экране телефона появляется сообщение «МЧС Инфо!****». Таких выделенных коротких номеров у «Сотового оператора» может быть несколько. Позвонив по этому номеру, абонент прослушивает полный текст сообщения о происходящем, предоставленный МЧС (описание произошедшей ситуации, необходимые действия и т.д.). Количеством оповещённых людей считается число позвонивших и прослушавших автоответчик с информацией. CBC применяют при необходимости охватить большое количество зарегистрированных в сети номеров, а SMS эффективнее на относительно небольшом радиусе охвата. Граница пролегает по числу в сто тысяч абонентов.

Плюсы:

- Может вещать на огромную территорию, CBC просто обеспечить, позволяет не перегружать оборудование, не вызывает раздражения при частом использовании при небольших ЧС.

Минусы:

- Не все мобильные телефоны поддерживают эту технологию. (Она работает только в 2G-сети, простые аппараты с ней справляются хорошо, в смартфонах поддержку этой функции владелец должен выставить в настройках самостоятельно. iPhone, например, CBC не поддерживает вообще);
- Требует дополнительного действия – набрать короткий номер для прослушивания сообщения; Так как используется довольно часто в силу частоты природных катаклизмов в этом районе, люди привыкают и не уделяют должного внимания этим сообщениям.

Достоинства SMS-рассылки:

- Есть звуковой сигнал, SMS принимают все телефоны;
- Платформа, рассылающая SMS о чрезвычайных ситуациях, никак не связана с биллингом, поэтому абонент получает сообщение при любом балансе

SMS-рассылка информативнее.

Недостатки:

- Процесс рассылки занимает какое-то время, так как оборудование рассылает SMS в порядке очереди. Как правило, это не занимает более 15-20 минут, но и они могут быть в таких случаях критичны.

В США предложили другую систему CMC-оповещения о чрезвычайных ситуациях под названием “PLAN” (Personal Localized Alerting Network). "Персональная сеть оповещения" способна функционировать даже в режиме перегруженности мобильных сетей, так как технология позволяет сначала передавать оповещения, и только потом личные звонки или прочие CMC. Таким образом, при помощи PLAN абоненты любого мобильного оператора США будут оперативно предупреждены об угрозе терактов, стихийных бедствий, а также об иных ЧС в районе их места нахождения или проживания.

CMC-предупреждения представляют собой обычные текстовые сообщения размером до 90 знаков, отправляются только на телефоны абонентов, находящихся в зоне ЧС. Подразделяются на три группы:

- сообщения от президента;
- предупреждения об угрозе жизни и/или безопасности;
- сообщения в рамках Amber Alert (система поиска похищенных или пропавших детей).

У абонентов будет возможность отключить некоторые группы предупреждений, кроме тех, которые приходят от имени президента США. Сейчас на всех новых телефонах устанавливаются чипы, позволяющие принимать CMC-оповещения о ЧС. Также, в Нью-йоркском метро в течение нескольких лет будут установлены передающие станции мобильной связи, чтобы абоненты могли получать CMC от PLAN даже в подземке. В Израиле и в России также создана система оповещения через мобильные телефоны. Абоненты получают оповещения независимо от сотового оператора, суммы средств на счету. Устройство, обеспечивающее эти преимущества, изначально заложено в SIM-карты или телефоны и активизируется при необходимости.

ПРОГРАММНЫЙ КОМПЛЕКС АУДИТА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ДЛЯ ПРОТИВОДЕЙСТВИЯ АТАКАМ

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

Понамарчук А. И., Вахаб Алаа

Борботько Т. В. – д-р. техн. наук, профессор

Рассмотрен состав и назначение компонентов программного комплекса обеспечивающего моделирование информационных систем, уязвимостей таких систем для оценки возможности их использования при реализации атак.

Современные информационные системы используются для обработки различных сведений, в том числе в банковском секторе. Атаки на подобные системы приносят существенный ущерб банкам и влияют на их репутацию. Одним из способов противодействия таким угрозам является обнаружение уязвимостей в информационной системе и их своевременное устранение. Для практической реализации указанного способа созданы программные средства, которые позволяют обнаруживать уязвимости, а так же проверять возможность их использования при реализации тех или иных атак. Однако существенной проблемой применения таких средств является решение задачи снижения вероятности ложных тревог. Такая задача может быть решена за счет повышения достоверности получаемых сведений, когда события безопасности регистрируются несколькими датчиками и решение о наличии угрозы принимается на основе корреляции таких событий.

Разработанный комплекс основан на использовании программного обеспечения VMware Workstation и включает в себя:

- виртуальные машины с IDS/IPS, HoneyPot и с программным обеспечением для имитации атак;
- интерфейсы настройки HoneyPot, просмотра сообщений о событиях безопасности, управления атаками.

Первая виртуальная машина содержит следующие сервисы:

- системы IDS/IPS и HoneyPot;
- HTTP-сервер и PHP-интерпретатор для интерфейса конфигурирования HoneyPot;
- систему просмотра сообщений безопасности IDS/IPS.

В качестве системы IDS/IPS использовалось программное обеспечение Snort. Система HoneyPot включает в себя подсистемы: honeyd, arpd и набор скриптов. Интерфейс настройки HoneyPot позволяет упростить конфигурирование подсистемы honeyd, за счет исключения необходимости редактирования файла настроек в ручном режиме. Базовая настройка HoneyPot заключается в создании шаблона HoneyPot и его применение.

Интерфейс просмотра сообщений о событиях безопасности реализует процедуры аутентификации пользователей программного комплекса, разграничения прав их доступа к системному журналу, отображения событий с учетом их корреляции по различным критериям в виде графиков и отчетов.

Вторая виртуальная машина обеспечивает функционирование программного комплекса моделирования атак, который выполнен по модульному принципу. Основными компонентами данного комплекса являются:

- консоль управления;
- модуль эксплоитов - для проверки целевой системы на уязвимость, а также выполнение самого кода эксплоита;
- модуль реализующий атаку «отказ в обслуживании» (DoS) – для проверки целевой системы на подверженность DoS атакам;
- модуль реализующий атаку «подмены» (Spoofing) – для проверки целевой системы на возможность такой атаки;
- модуль фаззинга (Fuzzing) - технология тестирования программного обеспечения, когда вместо ожидаемых входных данных программе передаются случайные или специально сформированные данные. В большинстве своем это некорректно составленные данные. Смысл такой проверки сводится к тому, что программист не знает, какие данные будут переданы приложению/протоколу/функции, поэтому его задача предусмотреть и проверить как можно больше вариантов;
- модули нагрузки и кодирования – для возможности установить кодирующее устройство во время выполнения процедуры передачи данных или изменить полезную нагрузку.

Разработанный программный комплекс позволяет оценить защищенность моделируемых информационных систем, выявить уязвимости их различных сервисов, проследить возможные сценарии атак, за счет использования систем-ловушек, проверить корректность работы системы обнаружения атак, за счет реализованной в нем методике, основанной на сравнении информации об атаках получаемых от различных источников.

Список использованных источников:

1. Ограбление по-российски: хакеры Carbanak сумели похитить $1 млрд // Aercom.by. Безопасность в Беларуси [Электронный ресурс]. – 2015. – Режим доступа : http://aercom.by/ograblenie-po-rossijski-xakery-carbanak-sumeli-poxitit-1-mlrd/. – Дата доступа : 12.03.2015.

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ОПТИЧЕСКИМ КАНАЛАМ

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

Алавси Хайдер Али Хуссейн

Борботько Т. В. – д-р. техн. наук, профессор

Скрытие объектов на фоне различных природных сред требует применение средств защиты, которые обладают спектрально-поляризационными характеристиками идентичными таким средам, что обуславливает необходимость оценки эффективности средств защиты информации от утечки по оптическим каналам.

Для обнаружения объектов используются технические средства, которые функционируют в различных диапазонах длин волн, например оптико-электронные системы видимого и ближнего инфракрасного диапазонов. Анализ изображений, получаемых с помощью таких технических средств, включает в себя следующие взаимосвязанные этапы: обнаружение, идентификацию и опознавание объекта наблюдения.

На практике, при обнаружении объекта освещенность местности (фона), где он расположен, может создавать экспозицию (освещенность) фотоприемника выше пороговой, поэтому на первый план выходит задача обнаружения объекта с минимальным контрастом относительно фона. В соответствие с чем, важным показателем является контрастная чувствительность оптико-электронной системы, которая определяется минимально необходимым контрастом объекта наблюдения, который может быть обнаружен при пороговом отношении сигнал/шум фотоприемника оптико-электронной аппаратуры.

Для снижения заметности объекта наблюдения используются различные способы его скрытия, которые реализуются на практике за счет использования средств защиты. Одним из подходов в оценке эффективности средств защиты является их натурные испытания, при которых объект наблюдения скрывается с помощью средства защиты и выполняется процедура его обнаружения с использованием оптико-электронной системы обнаружения. Такой подход требует значительных финансовых и временных затрат, а полученный результат оценки эффективности соответствует тем условиям, при которых проводился такой натурный эксперимент.

Отдельные элементы оптического изображения, получаемого с помощью оптико-электронной системы, могут отличаться по яркости, цвету, размеру, геометрической форме, поэтому условием обнаружения объектов является их контраст по выше перечисленным параметрам. Наиболее важным из которых является контраст по яркости.

Возникновение контраста по яркости между объектом и фоном обусловлено отражением объектом и фоном, на котором он размещается оптического излучения, в результате чего объект может быть темнее или светлее фона. Защита информации от утечки по оптическим каналам обеспечивается с использованием средств защиты (маскировочного окрашивания, оптических искусственных масок и т.д.). Их спектральный коэффициент яркости (СКЯ) должен соответствовать аналогичному параметру окружающего фона, на котором обеспечивается скрытие объекта, что позволит существенно снизить демаскирующие признаки объекта. Для оценки их эффективности предлагается использовать следующую методику.

Исследования КСЯ средств защиты выполняется на лабораторном стенде, который содержит источник оптического излучения видимого и ближнего инфракрасного диапазона длин волн и аппаратуру позволяющую обеспечить регистрацию СКЯ при различных углах падения и отражения оптического излучения источника. В результате первого этапа записываются СКЯ исследуемого средства защиты, обработка которых позволяет рассчитать степень поляризации отраженного оптического излучения средством защиты.

На втором этапе рассчитываются дальности обнаружения, опознавания и идентификации объекта наблюдения, скрытого с помощью исследуемого средства защиты, с учетом возможных погодных условий наблюдения и основных технических характеристик телевизионной техники.

Полученные результаты дают возможность проанализировать эффективность исследуемого средства защиты для выбранного варианта применения и разработать рекомендации по его дальнейшему использованию и совершенствованию.

Список использованных источников:

1. Никитин, В.В. Телевидение в системах физической защиты: учеб. пособие / В.В. Никитин, А.К. Цыкулин. – СПб. : ЛЭТИ, 2001. – 132 с.

2. Лыньков, Л.М. Снижение яркостного контраста наземных объектов / Л.М. Лыньков, Б.И. Беляев, Ю.В. Беляев, Т.В. Борботько, А.В. Хижняк, Хай Нгуен Ван // Сборник научный статей Военной академии Республики Беларусь. – 2005. – № 8. – С. 74–76.

3. Борботько, Т.В. Поглотители электромагнитного излучения. Применение в вооруженных силах / Т.В. Борботько, Н.В. Колбун, Л.М. Лыньков, И.С. Терех, А.В. Хижняк ; под ред. Л.М. Лынькова. – Минск : Бестпринт, 2006. – 228 с.

РАЗРАБОТКА СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

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

Пилипенко Д.А.

Кучинский П.В. – д-р ф-м. наук, профессор

Сегодня уже всем ясно, насколько важна защита информационных ресурсов. Многие также понимают, что система информационной безопасности — это не просто защита от прямых материальных потерь, но и конкурентные преимущества, репутация на рынке и более высокая степень доверия со стороны клиентов и партнеров. Поэтому на данный момент финансовые вложения в защиту своих ресурсов в том или ином объеме сделаны практически во всех компаниях: отдельные средства или комплексные системы безопасности установлены в каждой ИТ-системе.

Основная задача на этапе эксплуатации системы — это поддержание достигнутого уровня безопасности. Данное требование является таким же жестким, как и требование обеспечения отказоустойчивости ИТ-компонентов и непрерывности работы информационной системы в целом.

Современные угрозы безопасности в принципе преодолимы, уязвимости — устранимы, и в целом задача обеспечения защиты ресурсов выполнима. Именно поэтому так необходимо грамотно эксплуатировать и поддерживать систему безопасности предприятия. Это подразумевает проведение целого комплекса непрерывных и периодических работ, таких как техническая поддержка средств защиты, мониторинг и анализ событий безопасности, происходящих в системе, периодический контроль защищенности ресурсов, преодоление нештатных ситуаций и ликвидация последствий.

Для выполнения названных работ, во-первых, требуется соответствующее техническое и программное обеспечение, а во-вторых, нужен персонал необходимой численности, квалификации и имеющий достаточный опыт. Современные технологии безопасности действительно довольно эффективны, но они все равно не заменят человека, его мышление и опыт, особенно в преодолении критических проблем в системе защиты корпоративных ресурсов.

Система информационной безопасности предприятия была разработана на основе следующих принципов:

1) Приоритет мер предупреждения. Содержание этого принципа предполагает своевременное выявление тенденций и предпосылок, способствующих развитию угроз, на основе анализа которых вырабатываются соответствующие профилактические меры по недопущению возникновения реальных угроз.

Тщательная идентификация активов позволяет выявить возможных нарушителей информационной безопасности, определить возможные методы проведения атак, идентифицировать угрозы и, следовательно, определить перечень задач, возлагаемых на систему информационной безопасности.

2) Законность. Меры безопасности предприятия разрабатываются на основе и в рамках действующих правовых актов. Локальные правовые акты предприятия не должны противоречить законам и подзаконным актам.

Работы этапа системы безопасности проводятся и документируются в соответствии с требованиями ГОСТ 34.201-89 «Автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем», СТБ ISO/IEC 27001-2011 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», ISO/IEC 17799:2000(E) «Информационные технологии. Правила управления информационной безопасностью».

3) Комплексное использование сил и средств. Для обеспечения безопасности используются все имеющиеся в распоряжении предприятия силы и средства. Каждый сотрудник должен в рамках своей компетенции участвовать в обеспечении безопасности предприятия. Организационной формой комплексного использования сил и средств является программа обеспечения безопасности предприятия.

Система информационной безопасности создается с учетом особенностей информационных систем и реализуется комплексом согласованных между собой организационных и технических мер, поддерживается соответствующими управленческими решениями. Для создания системы информационной безопасности, в первую очередь, разрабатываются процессы информационной безопасности и только во вторую очередь проектируются и внедряются программно-аппаратные комплексы системы безопасности, служащие для обеспечения процессов информационной безопасности.

4) Координация и взаимодействие внутри и вне предприятия. Меры противодействия угрозам осуществляются на основе взаимодействия и скоординированности усилий всех подразделений, служб предприятия, а также установления необходимых контактов с внешними организациями, способными оказать необходимое содействие в обеспечении безопасности предприятия.

Отдельным компонентом обследования является сбор и анализ всей информации, непосредственным образом связанной с обеспечением информационной безопасности — процессами управления в организации, персоналом, методами и средствами обработки информации.

При проведении исследования допускается использовать различные методы сбора информации, например, интервью, опросные листы, анкетирование. При необходимости используются инструментальные средства — программно-аппаратные сканеры сетевой безопасности.

5) Сочетание гласности с конспирацией. Доведение до сведения персонала предприятия и общественности в допустимых пределах мер безопасности выполняет важнейшую роль — предотвращение потенциальных и реальных угроз. Такая гласность, однако, должна непременно дополняться в оправданных случаях мерами конспиративного характера.

6) Компетентность. Сотрудники и группы сотрудников должны решать вопросы обеспечения безопасности на профессиональном уровне, а в необходимых случаях специализироваться по основным его направлениям.

Специалисты, занимающиеся поддержкой и обслуживанием систем безопасности, должны иметь высокую квалификацию в области информационной безопасности и смежных областях информационных технологий, поскольку набор используемых в большинстве компаний средств защиты довольно широк, а механизмы их работы усложняются год от года. Уровень подготовки персонала, ответственного за корректную и - главное - эффективную работу систем защиты, всегда должен соответствовать таким условиям работы. То есть необходимо обеспечить сотрудникам возможность проходить специализированное обучение по всему набору средств и систем защиты. В больших и сложных информационных системах выполнение этого условия также требует серьезных затрат.

7) Экономическая целесообразность. Стоимость финансовых затрат на обеспечение безопасности не должна превышать тот оптимальный уровень, при котором теряется экономический смысл их применения.

8) Плановая основа деятельности. Деятельность по обеспечению безопасности должна строиться на основе комплексной программы обеспечения безопасности предприятия, подпрограмм обеспечения безопасности по основным его видам (экономическая, научно-техническая, экологическая, технологическая и т.д.)и разрабатываемых для их исполнения планов работы подразделений предприятия и отдельных сотрудников.

9) Системность. Этот принцип предполагает учет всех факторов, оказывающих влияние на безопасность предприятия, включение в деятельность по его обеспечению всех сотрудников подразделений, использование в этой деятельности всех сил и средств.

В зависимости от характера защищаемых активов информационных систем, система информационной безопасности может выполнять функции межсетевого экранирования, антивирусной защиты, обнаружения и предотвращения атак, контроля веб-трафика, защиты электронной почты, беспроводных соединений, информации в каналах связи, противодействия утечке конфиденциальной информации, контроля соответствия установленной политике информационной безопасности, стандарту.

Таким образом, был разработан комплекс мер по обеспечению информационной безопасности предприятия. Данные меры позволяют предприятию, эксплуатирующему защищенные информационные системы, владеть информацией о реальном уровне безопасности (или уязвимости) корпоративных ресурсов и контролировать их. Это означает, кроме прочего, выявлять и пресекать нарушения, контролировать действия персонала (как пользователей, так и администраторов), избегать негативных последствий для бизнеса. В конечном счете, все это является серьезным обоснованием инвестиций в корпоративную безопасность.

Список использованных источников:

1. Захарченко, В. И., Меркулов, Н.Н., Халикян, Н.В Экономическая безопасность бизнеса / В.И. Захарченко, Н.Н. Меркулов, Н.В. Халикян. – О.: Наука и техника, 2009. – 176 с.

2. Мак, В.И. Система безопасности предприятия / В.И. Мак // Best of security. – 2006. - №1

3. Ярочкин, В.И. Информационная безопасность. Учебник для студентов вузов / В.И. Ярочкин 3-е изд. - М.: Академический проект: Трикста, 2005. - 544 с

4. Бевалекс [Электронный ресурс]. – Режим доступа: http://www.bevalex.by/

ОБОРУДОВАНИЯ ДЛЯ WI-FI СЕТЕЙ КЛАССА ENTERPRISE

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

Малько А.А.

Хацкевич О.А. – к.т.н. доцент.

Передача данных осуществляется путем беспроводной передачи данных Wi-Fi с использованием усовершенствованного оборудования WOP-12ac Enterprise класса. Данное оборудование-это новейшее гибкое решение, позволяющее менять зону покрытия сети, тем самым увеличивая количество обсуживаемых мобильных устройств, а также легко и быстро разворачивать беспроводную IT-инфраструктуру. Благодаря поддержке стандарта IEEE 802.11ac оборудование WOP-12ac обеспечивает скорость передачи данных до 1Гбит/с. Использование технологии MiMO и узконаправленных антенн позволяет сделать WOP-12ac универсальным решением для организации общедоступных сетей. Для IT-инфраструктуры предусмотрены современные технологии аутентификации и шифрования, которые обеспечивают защиту персональных данных и безопасность сети. В частности используется динамический ключ, индивидуальный для каждого с WOP мобильного устройства.

На рисунке 1 показана схема сети класса Enterprise с использованием данного оборудования.

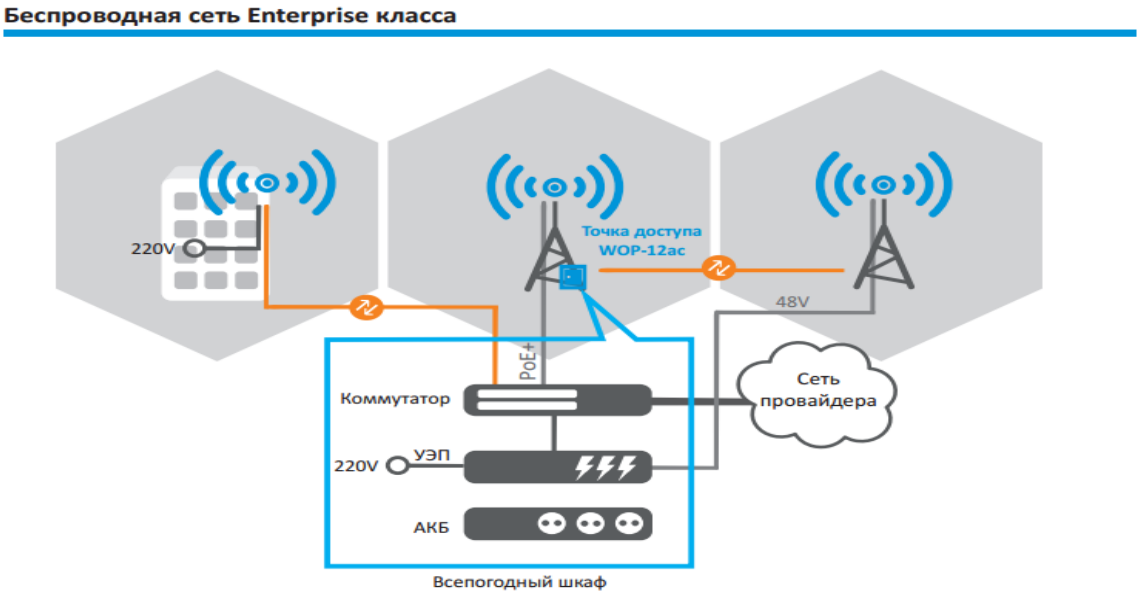

Рис.1 - Сеть Enterprise класса

Для стабильной и непрерывной работы устройства используются высокопроизводительные процессоры Broadcom, позволяющие добиться самых высоких показателей в скорости маршрутизации данных и наилучшей эффективности работы по технологии FBWA.

WOP-12ac обеспечивает высокоскоростную и безопасную беспроводную сеть, которая сочетает в себе множество возможностей и сервисов, необходимых для комфортного доступа в местах с большим скоплением людей. Устройство является незаменимым решением для организации беспроводной сети в различных климатических условиях в широком диапазоне рабочих температур и высокой влажности (парки, заводы, стадионы), а также является идеальной платформой для организации связи в коттеджах поселках и удаленных населенных пунктах.

Список использованных источников:

2. Б.С Гольдштейн, А.Е. Кучерявый Сети связи пост-NGN.

ЭВОЛЮЦИЯ СКОРОСТИ ПЕРЕДАЧИ ДАННЫХ В СЕТЯХ WI-FI

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

Дульский Д.В.

Стандарт WiMAX – Worldwide interoperability for Microwave Access, вышелвконце 2001г. В соответствии с Впервые рабочая группа IEEE 802.11 была анонсирована в 1990 году и вот уже 25 лет идёт непрекращающаяся работа над беспроводными стандартами. Рассмотрению будут подвергнуты стандарты, определяющие физический уровень, из взаимно совместимой линейки a/b/g/n/ac/ad.

Стандарты и описание:

1. 802.11 – первоначальный основополагающий стандарт. Поддерживает передачу данных по радиоканалу со скоростями 1 и 2 (опционально) Мбит/с.
2. 802.11a – высокоскоростной стандарт WLAN. Поддерживает передачу данных со скоростями до 54 Мбит/с по радиоканалу в диапазоне около 5 ГГц.
3. 802.11b – поддерживает передачу данных со скоростями до 11 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц.
4. 802.11g – устанавливает дополнительную технику модуляции для частоты 2,4 ГГц. Предназначен, для обеспечения скоростей передачи данных до 54 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц.
5. 802.11n – самый популярный стандарт, пропускная способность сетей до 600 Мбит/сек.
6. 802.11ac – стандарт IEEE. Скорость передачи данных – до 6,77 Гбит/с для устройств, имеющих 8 антенн. Утвержден в январе 2014 года.
7. 802.11ad – стандарт с дополнительным диапазоном 60 ГГц (частота не требует лицензирования). Скорость передачи данных – до 7 Гбит/с.

Опишем наиболее ожидаемый стандарт 802.11ac: максимальная скорость, предусмотренная стандартом, составляет до 6,93 Гбит/с, однако фактически такая скорость ещё не достигнута ни на одном оборудовании, представленном на рынке. Увеличение скорости достигнуто за счёт увеличения полосы пропускания до 80 и даже до 160 МГц. Такая полоса не может быть предоставлена в диапазоне 2,4 ГГц, поэтому стандарт 802.11ac функционирует только в диапазоне 5 ГГц. Ещё один фактор увеличения скорости – увеличение глубины модуляции до 256 уровней на один символ (8 бит на 1 бод) К сожалению, такая глубина модуляции может быть получена только вблизи точки из-за повышенных требований к соотношению сигнал/шум. Указанные улучшения позволили добиться увеличения скорости до 867 Мбит/с. Остальное увеличение получено за счёт ранее упомянутых потоков MIMO 8x8:8. 867x8=6,93 Гбит/с. Технология MIMO была усовершенствована: впервые в стандарте Wi-Fi информация в одной сети может передаваться двум абонентам одновременно с использованием различных пространственных потоков. В более наглядном виде результаты в таблице:

Параметр	802.11b	802.11a	802.11g	802.11n	802.11ac
Макс. скорость	22	54	54	600	6930
Расширение спектра	DSSS	OFDM	DSSS/ OFDM	OFDM	OFDM
Повышение скорости помехоустойчивого кода	+	+	=	=	=
Увеличение глубины модуляции	+	+	=	=	+
Уменьшение защитного интервала	-	-	-	+	=
Увеличение полосы	-	-	-	+	++
Пространственные каналы	-	-	-	+	+

Рис. 1 – Способы увеличения пропускной способности

В таблице перечислены основные способы увеличения пропускной способности: «-» – метод не применим, «+» – скорость была увеличена за счёт данного фактора, «=» – данный фактор остался без изменений.

Ресурсы уменьшения избыточности уже исчерпаны: максимальная скорость помехоустойчивого кода 5/6 была достигнута в стандарте 802.11a и с тех пор не увеличивалась. Увеличение глубины модуляции теоретически возможно, но следующей ступенью является 1024QAM, которая является очень требовательной к соотношению сигнал/шум, что предельно снизит радиус действия точки доступа на высоких скоростях. При этом возрастут требования к исполнению аппаратной части приёмопередатчиков. Уменьшение межсимвольного защитного интервала также вряд ли будет направлением совершенствования

скорости – его уменьшение грозит увеличением ошибок, вызванных межсимвольной интерференцией. Увеличение полосы канала сверх 160 МГц так же вряд ли возможно, так как возможности по организации непересекающихся сот будут сильно ограничены. Ещё менее реальным выглядит увеличение количества MIMO-каналов: даже 2 канала являются проблемой для мобильных устройств (из-за энергопотребления и габаритов).

Из перечисленных методов увеличения скорости передачи большая часть в качестве расплаты за своё применение забирает полезную площадь покрытия: снижается пропускная способность волн (переход от 2,4 к 5 ГГц) и повышаются требования к соотношению сигнал шум (увеличение глубины модуляции, повышение скорости кода). Поэтому в своём развитии сети Wi-Fi постоянно стремятся к уменьшению площади, обслуживаемой одной точкой в пользу скорости передачи данных.

В качестве доступных направлений совершенствования могут использоваться: динамическое распределение OFDM поднесущих между абонентами в широких каналах, совершенствование алгоритма доступа к среде, направленное на уменьшение служебного траффика и использование техник компенсации помех.

Подводя итог вышесказанному попробуем спрогнозировать тенденции развития сетей Wi-Fi: вряд ли в следующих стандартах удастся серьёзно увеличить скорость передачи данных, если не произойдёт качественного скачка в беспроводных технологиях: почти все возможности количественного роста исчерпаны. Обеспечить растущие потребности пользователей в передаче данных можно будет только за счёт увеличения плотности покрытия (снижения радиуса действия точек за счёт управления мощностью) и за счёт более рационального распределения существующей полосы между абонентами.

Вообще тенденция уменьшения зон обслуживания, похоже, является основным трендом в современных беспроводных коммуникациях. Некоторые специалисты считают, что стандарт LTE достиг пика своей пропускной способности и не сможет далее развиваться по фундаментальным причинам, связанным с ограниченностью частотного ресурса. Поэтому в западных мобильных сетях развиваются технологии оффлоада: при любом удобном случае телефон подключается к Wi-Fi от того же оператора. Это называют одним из основных способов спасения мобильного Интернета. Соответственно роль Wi-Fi сетей с развитием сетей 4G не только не падает, а возрастает. Что ставит перед технологией всё новые и новые скоростные вызовы.

Список литературы:

1. http://www.cisco.com/
2. Олиффер, Компьютерные сети/ В. Олифер, Н. Олифер; под ред. В. Олифер – М.: Питер, 2010. Глава 3

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ VDSL2. ОСНОВНЫЕ СФЕРЫ ПРИМЕНЕНИЯ

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

Парфенюк А. И.

Королев А. И. – к.т.н. доцент.

VDSL (сверхвысокоскоростная цифровая абонентская линия) - технология доступа, использующая для передачи данных медную пару. Технология имеет скорость передачи данных по направлению к пользователю до 52Мбит.с и по направлению к сети до 16Мбит.с. Полоса пропускания технологии 12МГц. Более актуальной на сегодняшний момент стала технология VDSL2. Принципиальное отличие от первой версии состоит в ширине диапазона используемых частот, теперь она стала 30МГц. Это позволило увеличить возможную скорость до 100Мбит.с в обе стороны.

Технический комитет Международного союза электросвязи публикуя стандарт VDSL2 предполагал, что наилучшим применением этой технологии будет предоставление услуг Triple Play для населения. Технология вызвала большой интерес в России где ряд телекоммуникационных операторов начинали коммерческое внедрение этих (телевидение высокой четкости, видео по запросу, видео-конференц-связь, высокоскоростной доступ в Интернет, VoIP) услуг.

С ноября 2010 года по начало 2012 года проходила программа модернизации сетей ЦТК («ЦентрТелеком»). Модернизация происходит за счет внедрения технологии VDSL2.

На сегодняшний день метод доступа VDSL2, весьма подходит для решения задач частного сектора, это обусловлено тем что кабельные операторы не охотно развивают свои услуги в частном секторе, где как правило низкая плотность абонентов и монтаж линий требует высоких трудозатрат. Что касается медных линий, то они могут уже существовать.

В виду того что POTS сеть в наше время имеет весьма развитую инфраструктуру практически во всех местах государства, для средних и мелких предприятий, нуждающихся в высокой скорости доступа к тем или иным ресурсам технология VDSL2 является весьма привлекательной из-за простоты внедрения. Для реализации канала связи необходимо установить конечное оборудование на уже существующую телефонную линию. Для реализации оптического канала связи необходимо строительство лини передачи данных. И при условии низкой плотности потребителей связи строительство как правило не рентабельно.

Также технология VDSL2 применяется в промышленных решениях. Так эта технология была применена весьма интересным образом при строительстве системы охраны периметра на одном из деревообрабатывающих предприятий Брестской области. Для детектирования несанкционированного пересечения охраняемого периметра используются ИК-датчики которые связываются с приёмным оборудованием по средству телефонного кабеля плотностью 30 пар. Для усовершенствования системы охраны по периметру были установлены поворотные IP-камеры, и для связи камер с центральным сервером видеонаблюдения были использованы VDSL модемы ZyXEL P872HA на уже существующих медных линиях, что позволило сильно сэкономить на строительстве оптических линий.

Имеют место быть и сложные единичные решения на различных модификациях технологии, таких как LR-VDSL2. LR-VDSL2 - модификация технологии VDSL2, позволяет увеличить максимальную длину линии до 4,5 км и способна к поддержке скорости приблизительно 1-4 Мбит/с (нисходящий поток) на таком расстоянии. Такие решения как правило используются на отдалённых технических узлах предприятий, на которых существует необходимость наличия связи, но фактор высокой скорости критичным не является.

В целом можно сказать что технология VDSL2 достаточно широко используется в промышленных и бизнес решениях, но для частных пользователей теряет свою актуальность. Это объясняется довольно высокой стоимостью конечного оборудования.

В настоящее время развитие сетей VDSL прекращено в пользу FTTH, в силу наличия протокола IGMP. В связи с усиленным развитием архитектуры FTTH, VDSL2 теряет свою актуальность в массовом использовании, но технологию нельзя списывать со счетов. VDSL2 по-прежнему является весьма подходящим решением для тяжелых технических задач в которых из-за экономических или политических вопросов прокладка оптических линий невозможна.

Список использованных источников:

1. Королев, А. И. Высокоскоростные технологии передачи информации по абонентским и соединительным линиям связи / А. И. Королев // Уч. метод. пособие по дисциплине «Сети телекоммуникаций». – Минск, 2005. – 68 с.

2. Ioannis P. Karamitsos Broadband Access Network / Ioannis P. Karamitsos // Книга. – Изд.LAP Lambert Academic Publishing, 2012. – 100 с.

АКТУАЛЬНОСТЬ ИСПОЛЬЗОВАНИЯ ПРОТОКОЛОВ ДИНАМИЧЕСКОЙ МАРШРУТИЗАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

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

Оксентюк А. И.

Селезнёв И.Л. – к.т.н. доцент.

В последние десятилетия компьютерные сети передачи данных активно внедряются по все сферы человеческой жизни. Именно компьютерные сети сегодня позволяют нам быстро и качественно принимать и передавать огромные объёмы информации. При проектировании сетей передачи данных требуется учитывать многие критерии и факторы, чтобы развернуть качественную и легко расширяемую сетевую инфраструктуру, учитывая топологию, каналы связи, активное оборудование, исследование передаваемого трафика и протоколов маршрутизации. Последнее играет ключевую роль при распределении информационных потоков в каналах связи. Так, при кратковременных отказах некоторых сегментов или расширении существующей компьютерной сети, использование статической маршрутизации не разумно, в виду отсутствия гибкости функционирования, при простоте реализации. Ведь все записи о маршрутах вносятся в память каждого маршрутизатора администратором сети вручную и в случае необходимости требуется срочно внести изменения в соответствующие таблицы, иначе сеть будет работать некорректно. При адаптивной или динамической маршрутизации все изменения конфигурации сети автоматически отображаются в таблицах маршрутизации протоколами маршрутизации. Эти протоколы основаны на сборе информации о топологии связей в сети, что позволяет им оперативно отрабатывать все текущие изменения. Динамическая маршрутизация используется преимущественно в средних и крупных сетях со сложной, часто меняющейся инфраструктурой, где прежде всего важна оперативность отслеживания и устранения проблем связи.

На сегодняшний день в IP-сетях применяются такие протоколы маршрутизации, где маршрут выбирается либо по кротчайшему расстоянию (т.е. по количеству промежуточных устройств при прохождении пакета), либо по показателю номинальной пропускной способности каналов связи между маршрутизаторами, их надёжность и вносимые задержки. Современные протоколы маршрутизации осуществляют согласование таблиц маршрутов между маршрутизаторами, для доставки пакета от источника к получателю за конечное количество шагов. Однако при отказе маршрутизаторов или каналов связи требуется определённое время, называемое временем конвергенции, при котором происходит обмен служебной информации и перестройка таблиц маршрутизации, когда они смогут вновь стать согласованными. В результате маршрутизация в Интернете носит ярко выраженный иерархический характер. Внутри каждой автономной системы может применяться любой из существующих протоколов маршрутизации, в то время как между автономными системами всегда применяется один и тот же протокол. В IP-сетях в качестве внутренних шлюзовых протоколов, то есть протоколов, применяемых внутри автономных систем, сегодня активно используются три протокола - RIP, OSPF и IS-IS (Протокол маршрутизации промежуточных систем). Внешним шлюзовым протоколом, то есть протоколом выбора маршрута между автономными системами, сегодня является протокол BGP (Border Gateway Protocol, протокол граничного шлюза - основной протокол динамической маршрутизации в Интернете).

Использование протоколов динамической маршрутизации значительно сокращает затраты труда системного администратора по обслуживанию сети. Также может уменьшить среднее время нахождения пакета в сети, что позволяет минимизировать затраты на его доставку получателю в сетях с разнородным трафиком. Однако следует принимать во внимание тот факт, что при этом повышается нагрузка на процессоры маршрутизаторов и, как следствие, на сеть в целом. Отчасти данная проблема решается за счет использования динамической балансировки сетевой нагрузки и прописывания статических маршрутов отдельным сегментам сети.

Список использованных источников:

1.Пятибратов А. П., Гудыно Л. П., Кириченко А. А. Вычислительные системы, сети и телекоммуникации. Учебник для вузов под ред. А. П. Пятибратова. Издание 2-е, переработанное и дополненное. — М.: Финансы и статистика, 2001.

2.Куракин Д.В. Маршрутизаторы для глобальных телекоммуникационных сетей и реализуемые в них алгоритмы // Информационные технологии. 1996. №2.

НЕРАВНОМЕРНАЯ ЗАЩИТА ДАННЫХ НА ОСНОВЕ ПЕРФОРИРОВАННЫХ НЕРАВНОМЕРНЫХ СВЕРТОЧНЫХ КОДОВ

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

Волостных Г. А.

Королев А. И. – к.т.н. доцент.

В современных цифровых и телекоммуникационных системах и сетях, в том числе и глобальной сети интернет, постоянно требуется повышение скорости, а так же достоверности передаваемой информации.

В данной статье речь пойдёт о помехоустойчивом кодировании. Широкое распространение получили коды Хемминга, БЧХ-коды, сверточные коды, коды Рида-Соломона, и другие, позволяющие контролировать, корректировать и обнаруживать случайные и зависимые модульные и пакетные ошибки. Контроль ошибок высокой кратности затруднен из-за больших вычислительных затрат, включая аппаратные и временные затраты. Это является проблемой. Так по некоторым оценкам, каждый децибел энергетического выигрыша от кодирования в спутниковых и космических системах связи позволяет уменьшить на один миллион долларов стоимость запуска спутника связи, а в проводных корпоративных, например банковских, сетях связи коррекция одного ошибочного символа снижает финансовые потери более чем на 1500 евро.

В телекоммуникационных сетях с коммутацией пакетов разработаны методы прогрессивной передачи изображений. Эти методы постоянно развиваются. Их суть в передаче информации по изображению в порядке убывания её психовизуальной значимости. Т.е. в первую очередь передаётся информация о расположении яркости и цвете наиболее крупных деталей, затем средних, и далее мелких. Ошибки при восстановлении изображении тем меньше, чем больше значимой информации удалось передать правильно. В настоящее время эффективные кодеки алгоритмов сжатия JPEG2000, MPEG-4 и другие используют преобразования, обеспечивающие прогрессивную неравномерную передачу фрагментов изображений, что осуществляет защиту значимой передаваемой информации, а так же уменьшает информационную избыточность и сложность кодеков. При использовании неравномерной защиты символов от ошибок, передаваемые символы делятся на группы, имеющие разный уровень значимости при восстановлении. Группы более значимых символов кодируются помехоустойчивым кодом высокой исправляющей способности, а группы менее значимых символов соответственно меньшей исправляющей способностью, либо передаются без кодирования.

В беспроводных сетях, в частности мобильных системах связи, неравная защита данных организуется на основе использования либо каскадных кодов, либо канального кодирования данных, реализуемых на основе сверточных турбокодов. Наиболее известными стандартами мобильных сетей связи являются D-AMPS, IS-136, ULTRA-TDD.

В канальном кодеке модема мобильной сетя связи стандарта D-AMPS реализован каскадный метод кодирования значимых информационных символов и передача без помехоустойчивого кодирования менее значимых символов. А в стандарте IS-136 используется метод двухканального кодирования с неравномерной защитой значимых информационных символов, и передача менее значимых по третьему потоку без помехоустойчивости.

Метод неравной защиты информационных символов на основе сверточных кодов с разной корректирующей способностью состоит в следующем: Передающая часть системы – канальный кодер, содержит два канала кодирования информационных символов. В первом канале кодирования используется диффузный сверточный код, обеспечивающий коррекцию одновременно пакетных и независимых ошибок. Во втором канале кодирования используется самоортогональный сверточный код, корректирующий только независимые ошибки. Скорости передачи обоих потоков кодов выбираются равыми. Символы жанный потоков поступают соответственно на выходы первого и второго каналов. На приемной стороне во второй канал декодирования вводится дополнительный буферный регистр, что позволяет обеспечить согласование по задержке значимых и менее значимых информационных символов.

Показано, что при передаче сжатых пакетов данных на основе широко используемых на практике алгоритмов прогрессивного кодирования для уменьшения информационной избыточности и вычислительной сложности следует использовать неравномерное кодирование информации.

Список использованных источников:

1. Королев, А. И. Высокоскоростные технологии передачи информации по абонентским и соединительным линиям связи / А. И. Королев // Уч. метод. пособие по дисциплине «Сети телекоммуникаций». – Минск, 2005. – 68 с.
2. Ioannis P. Karamitsos Broadband Access Network / Ioannis P. Karamitsos // Книга. – Изд.LAP Lambert Academic Publishing, 2012. – 100 с.

ЭТАПЫ РАЗВИТИЯ СТАНДАРТА WiMAX

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

Игнатюк А. А.

Стандарт WiMAX – Worldwide interoperability for Microwave Access, вышелвконце 2001г. В соответствии с иерархией стандартов беспроводного доступа он относится к классу MAN (Metropolitan Area Network). По ряду показателей, таких как пропускная способность, покрытие территории и предоставляемые услуги, WiMAX превосходит стандарт Wi-Fi (IEEE802.11) класса LAN (Local Area Network), позволяя при развитой инфраструктуре строить региональные, национальные и даже глобальные сети.

На физическом уровне в стандарте WiMAX применяют две принципиально разные технологии. Данные можно передавать, модулируя одну несущую частоту (SC – Single Carrier) или множество поднесущих – технология OFDM (Orthogonal Frequency Division Multiplexing) - это механизм мультиплексирования (уплотнения) посредством ортогональных поднесущих.В режиме SC (одной несущей) к радиоканалам предъявляют те же требования, что и в радиорелейных сетях: использование только прямых лучей и применение узконаправленных антенн, подавление всех отраженных лучей с целью устранения межсимвольной интерференции. В связи с этим технологию SC (одной несущей)невозможно использовать в сетях массового пользования с многолучевым распространением радиоволн в каналах связи.

Переход к технологии OFDM произошел в 2004г при появлении нового стандарта WiMAX: 802.16-2004. Данная технология позволяет устранить межсимвольную интерференцию. В следующей версии стандарта были существенно изменены параметры OFDM. В частности, перешли к масштабируемой OFDM: число используемых поднесущих стало зависеть от рабочей полосы (SOFDM), а абоненту стали выделять определенное число подканалов (SOFDMA – Scalable OFDM Access). Также появилась возможность реализации хэндоверов. Данному варианту стандарта WiMAX дали название мобильного WiMAX или стандарта 802.16e. Вариант 802.16e является базовым в действующих сетях WiMAX. Его постоянно усовершенствовали. Например, он был дополнен стандартами 802.16i и 802.16j. Последний позволяет расширять существующие сети, применяя ретрансляторы.

В 2011 году был утвержден новый вариант стандарта WiMAX – 802.16m. Он предназначен для построения сетей с пропускной способностью выше 100 Мбмит/с и для реализации ряда новых перспективных услуг. Он предусматривает ряд изменений, которые позволяют более эффективно использовать частотный диапазон: несколько механизмов управления мощностью и смягчения интерференции на краю соты, 4x4 MIMO (Multiple Input Multiple Output), HARQ (Hybrid automatic repeat request) — механизм, позволяющий отслеживать ошибки и отправляющий запрос на повторную передачу и некоторые другие.

Все эти нововведения дают возможность получения данных до 365 Мбит/сек, а передачи данных – до 376 Мбит/сек. На одной полосе 20 МГц теперь могут одновременно поддерживаться до 80 VoIP соединений. Стандарт 802.16m также включает улучшенный сервис определения местоположения по базовым станциям, расширенные возможности рассылки широковещательных сообщений, более строгие меры безопасности. Теперь услуги Mobile WIMAX можно получить на скоростях до 350 км/час, а в некоторых случая (в зависимости от частотного диапазона) до 500 км/час.

Этапы усовершенствования стандарта WiMAX

Стандарт	**Принят**	**Полосы частот, ГГц**	**Мобильность**	**Технологии**	**Ширина канала, МГц**
802.16	12.2001	11 - 66	нет	Одна несущая (SC)	20, 25, 28
802.16-2004	06.2004	2 - 11	нет	SC или OFDM (256)	1,75; 3,5; 7; 14; 1,25; 5; 10; 15; 8,75
802.16e	12.2005	11 - 66 2 - 11 (фикс.) 2 - 6 (моб.)	есть	SC или OFDM (256), или SOFDM (128, 512, 1024, 2048)	1,25; 5; 10; 20
802.16k	2007	11 - 66 2 – 11 (моб.)	есть	SC или OFDM (256), или SOFDM (128, 512, 1024, 2048)	1,25; 5; 10; 20
802.16-2009	2009	Те же	есть	Те же + 802.16i	Та же
802.16j	2009	Те же	есть	Те же + ретрансляция	Та же
802.16m	2011	Ниже 3,6	есть	SOFDMA	1– 20

WiMAX – стандарт, который занял особое место на рынке современных технологий. Для развития технологий следующих поколений опыт WiMAXнеобходим как пример последовательного и качественного улучшения и совершенствования технологий для улучшения качества, удобства и доступности для пользователя.

Списокисточников:

1. WiMAX Forum Network Architecture. (Stage 2: Architecture Tenets, Reference Model and Reference Points). Release 1, Version 1.2. – WiMAX Forum, January 11, 2008.

ОРГАНИЗАЦИЯ ДИСПЕТЧЕРИЗАЦИИ ЛИФТОВ

ОАО «Беллифт», Республика Беларусь

Урбан А.И.

Мельниченко Д.А. – к.т.н., доцент

Когда родители застревают в лифте с детьми, иногда детям объясняют, что тетя-диспетчер, которой сообщают о поломке, сидит прямо за стенкой. Взрослые знают - связь идет по специальной проводной линии, а "тетя" сидит за несколько километров от лифта.

В Республике Беларусь подключение лифтов осуществлено по специальным проводным линиям. Только в городе Минске в эксплуатации находится около 16 тыс. пассажирских лифтов. Из них 4,1 тыс. выработали нормативный срок службы 25 лет, установленный производителем, и теперь их необходимо заменить. На поддержание в рабочем состоянии изношенного лифтового оборудования затрачиваются большие трудовые и материальные ресурсы. Поэтому ставится задача выводить из эксплуатации морально устаревшие и физически изношенные лифты в жилых домах. Исходя из этого, возникает необходимость диспетчеризации лифтов в части несоответствия устаревшего диспетчерского оборудования требованиям действующих правил (т.к. оконечное оборудование малоинформативное: диспетчер только знает, что с ним связываются и больше никакой информации) и наличия большого числа диспетчерских пунктов с незначительным количеством подключенных к ним лифтов. Каждый лифт в обязательном порядке должен быть связан с диспетчерским пультом, где отображается вся информация о нем: время работы либо простоя лифта, его текущее положение, состояние, наличие неисправности и т.д. Расстояние от пульта до лифта может доходить до 5 километров. Прокладка кабелей и аренда коммуникаций стоит дорого и даже не всегда возможна, поэтому возникла необходимость разработки новых способов связи. Главным недостатком проводных систем является необходимость прокладки проводных линий связи. В первую очередь, данная процедура ведет к усложнению, а значит, и удорожанию монтажных работ. Проводные линии связи следует защищать от возможного механического воздействия, которое может привести к их обрыву или возникновению короткого замыкания между проводами. Наличие проводных линий связи может отрицательно сказываться на эстетичном виде помещения. Проводные линии связи могут ограничивать максимальное расстояние между связываемыми техническими средствами, так как любой кабель имеет собственную погонную емкость и индуктивность. Значительное удлинение проводов приводит к ограничению максимально возможной передаваемой частоты электрического сигнала, снижению его уровня за счет воздействия собственной емкости и индуктивности и, естественно, к искажению сигнала в виде «заваливания» фронтов передаваемых импульсных посылок

Развитие мобильной связи и её широкое распространение среди населения позволит разработать оборудование связи лифта с диспетчерской по сотовому каналу в стандарте GSM через сеть сотовой связи. Преимущество такого метода в гибкости, быстром развертывании и доступности даже там, где прокладка кабеля затруднена, а диспетчерский пункт находится далеко. Вызов диспетчера будет осуществляться так же, как звонок с мобильного аппарата. При этом связь можно организовать не только по звонку, но и с помощью SMS-сообщений. Диспетчеру будут приходить смс-оповещения о неисправности лифта, внезапной потере питания и т.д. Оператор будет видеть не только адрес вызова, но и состояние лифта (на каком этаже лифт, открыты ли двери, есть ли перегрузка), может получать подробную статистику по своему участку, связываться не только с пассажиром лифта, но и с электромехаником, находящимся в машинном помещении.

Терминал будет осуществлять передачу информации в диспетчерский центр по сети сотовой связи стандарта GSM с использованием пакетной передачи данных GPRS. Реализация адаптивного алгоритма работы, позволит гибко и в полном объеме использовать все существующие ресурсы GSM сетей – голосовой канал, канал данных CSD и канал пакетной передачи данных GPRS. Благодаря этому, существует возможность автоматически оптимизировать работу системы в различных режимах использования и в случае перегрузки сети GSM, выбирать каналы в зависимости от их доступности и целесообразности использования того или иного канала для передачи необходимой в данный момент информации.

Основными функциями предлагаемой системы являются: дистанционный сбор и визуализация информации о состоянии технологических объектов лифтового хозяйства в режиме реального времени; обеспечение экстренного канала голосовой связи между диспетчером и кабиной лифта; оперативное управление главным контактором питания станции лифта.

Предполагаемый экономический эффект внедрения системы будет обеспечиваться:

1. наличием информационной обратной связи о включении требуемого режима, что позволяет сократить время реакции диспетчера на нештатную ситуацию;
2. наличием дистанционного управления питанием станции лифта позволяющим исключить выезды, связанные с необходимостью перезапуска оборудования;
3. защитой оборудования станции лифта, в результате контроля состояния питающей сети, сочетания сигналов с датчиков, и принятием решения о прекращении эксплуатации, в случае аварийной ситуации;
4. дистанционным техническим учетом потребляемой энергии, позволяющим сократить рабочее время и транспортные расходы, необходимые при объездах для снятия показаний;
5. простотой монтажа и минимальными требованиями к текущему обслуживанию (приблизительно 1 раз в год).

Защита web-сайта на базе CMS Wordpress от web-атак

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

Новиченко И. В.

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

В последнее время создание и продвижение сайтов является довольно популярным занятием. Над удобством и простотой создания сайтов трудится огромное количество людей. Большим прорывом в технологии создания и разработки современных веб-проектов является создание CMS. Современные системы управления контентом широко используются на просторах сети Интернет при создании проектов любой сложности.

CMS представляет собой программный комплекс, позволяющий автоматизировать процесс управления сайтом в целом и его составляющими: макетами страниц, шаблонами вывода данных, структурой, информационным наполнением, пользователями и правами доступа.

Существуют разнообразные системы управления сайтом, из которых наиболее популярными являются CMS Drupal, Joomla и WordPress.

Важной особенностью Joomla является минимальный набор инструментов при начальной установке, который дополняется по мере необходимости. Это упрощает использование административной панели, а также снижает нагрузку на сервер и экономит место на хостинге. Предусмотрены настраиваемые схемы расположения модулей, включая левый, правый, центральный и любое другое произвольное положения блоков выводимой информации. При желании содержимое модуля можно включить в содержимое материала.

Архитектура Drupal позволяет применять его для построения различных типов сайтов — от блогов и форумов, до информационных архивов или сайтов новостей. Функциональность обеспечивается подключаемыми модулями, обращающимися к общему API Drupal. Стандартный набор модулей включает, например, такие функции как новостная лента, блог, форум, загрузка файлов, сборщик новостей, голосования, поиск и др. Большое количество дополнительных модулей, значительно расширяющих базовые функции можно скачать с официального сайта.

WordPress — это мощная платформа для персонального блоггинга. Она содержит набор возможностей для того, чтобы максимально упростить процесс создания онлайн-публикаций, сделать его легко воспринимаемым и удобным. Платформа для персонального блоггинга с практичными настройками и свойствами по умолчанию и с чрезвычайно гибким и настраиваемым ядром. Отличная особенность – наличие централизованной базы WordPressCodex.

Каждая из рассмотренных CMS – систем имеет свою отличительную особенность: дизайн и гибкость (Drupal), удобство и простор в работе (Joomla), легкий и удобный интерфейс (WordPress). Есть очень важная составляющая в каждой из этих систем – это безопасность администрирования CMS - системы и защита данных пользователей.

Несмотря на свои достоинства, именно CMS часто являются причиной получения несанкционированного доступа к данным. Постоянно публикуются все новые уязвимости популярных CMS, возможность эксплуатации которых ставит под угрозу безопасность всего сервера. Защита системы управления содержимым позволит значительно повысить защищенность сервера от внешних угроз, и наоборот – уязвимости CMS могут свести «на нет» все усилия администратора. Ниже на рисунке 1 представлена статистика уязвимостей CMS WordPress.

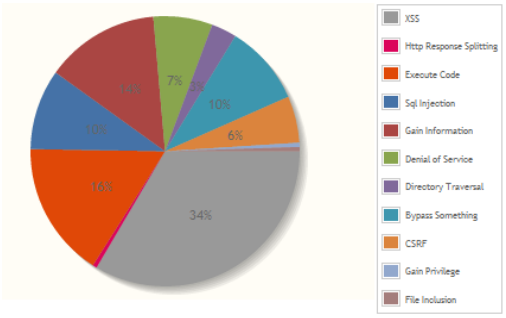

Рис. 1 – Статистика уязвимостей

В ходе выполнения дипломной работы была разработана модель web-сайта на основе системы управления web-содержимым. Проведен анализ защищенности web-ресурса, на основании которого выбрал необходимые средства защиты и разработана защищенная модель. Полученные результаты нашли практическое применение в ОАО «Хоум кредит банк».

Список использованных источников:

1. М.Л. Лопатин, О. Ю. Пескова «АНАЛИЗ ЗАЩИЩЕННОСТИ СОВРЕМЕННЫХ СИСТЕМ УПРАВЛЕНИЯ КОНТЕНТОМ».