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

ИНФОКОММУНИКАЦИИ

МАТЕРИАЛЫ 54-Й НАУЧНОЙ КОНФЕРЕНЦИИ АСПИРАНТОВ, МАГИСТРАНТОВ И СТУДЕНТОВ

(Минск, 23–27 апреля 2018 года)

Минск, БГУИР
2018

Инфокоммуникации:
материалы 54-й научной конференции
аспирантов, магистрантов и студентов
(Минск, 23–27 апреля 2018 г.). – Минск:
БГУИР, 2018. – 144 с.

В сборник включены лучшие доклады, которые были представлены на 54-й научной конференции аспирантов, магистрантов и студентов БГУИР, отобранные по следующим направлениям: системы телекоммуникаций; системы распределения мультимедийной информации; защита информации.

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

СОДЕРЖАНИЕ

СЕТЬ ПЕРЕДАЧИ ДАННЫХ КОМПАНИИ «БЕЛИНФОНЕТ»

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

Червяков А.И.
Зеленин А.С. – ст. преподаватель каф. ИКТ

В соответствии с Государственной программой развития цифровой экономики и информационного общества на 2016-2020 годы большое внимание уделяется развитию современных мультисервисных сетей передачи данных. Таким образом, вопросы, связанные с модернизацией локальной вычислительной сети компании «Белинфонет», являются актуальными. Тем более, что существующая сеть была развернута более 20 лет назад и в настоящее время не соответствует предъявляемым к ней требованиям.

Новая сеть передачи данных проектируется в соответствии с рекомендациями СТБ 2156-2011 и поддерживает скорость передачи данных до 1000 Мбит/с.

Схема подключения сетевого оборудования с указанием моделей представлена на рисунке 1:

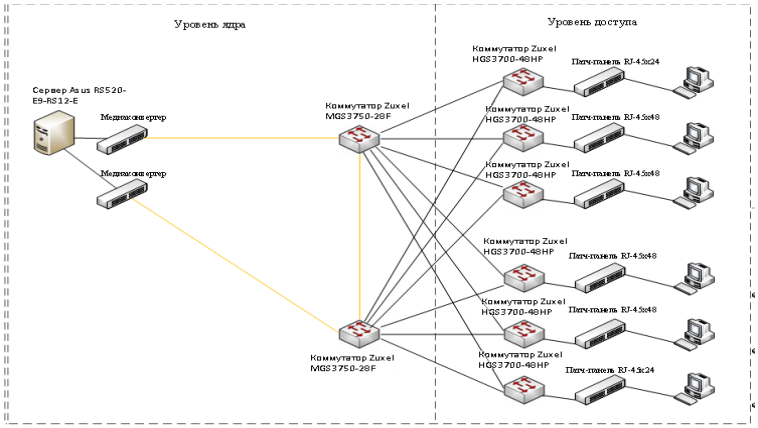


Рис. 1 – Схема подключения сетевого оборудования

Для развертывании сети передачи данных будет использоваться кабель UTP CAT5e.

Пример трассировки линий (4 этаж) представлен на рисунке 2:

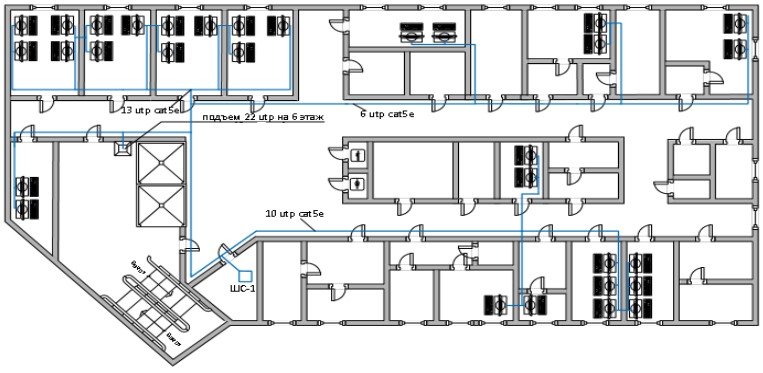


Рис. 2 – Трассировка линий 4-го этажа

Новая сеть передачи данных соответствует топологии "иерархическая звезда", предусматривающей соединение двух уровней коммутаторов: коммутаторов уровня доступа, к которым непосредственно подключаются пользователи, и высокопроизводительных коммутаторов уровня ядра.

Выбранные модели сетевого оборудования обеспечивают высокую производительность и широкие функциональные возможности.

Список использованных источников:

1. Таненбаум Э. Компьютерные сети. 5-е издание / Э. Таненбаум, Д. Уэзеролл - Спб.: Питер, 2012. - 960 с.

2. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации: Учебник для вузов. 4-е издание / В. Л. Бройдо, О. П. Ильина - Спб.: Питер, 2011. - 560 с.

3. Платунова С. М. Технические средства коммутации ZyXEL. Учебное пособие по дисциплине «Корпоративные сети» / С. М. Платунова - Спб.: НИУ ИТМО, 2012. - 59 с.

МОДЕРНИЗАЦИЯ ВНУТРИЗОНОВОЙ СЕТИ СВЯЗИ НА БАЗЕ ТЕХНОЛОГИИ IMS

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

Хацкевич О.А. – к.т.н., доцент

В работе рассмотрена архитектура сети IMS, представлен обзор состояния внутризоновой сети передачи данных и стратегия внедрения новейших телекоммуникационных технологий в Республике Беларусь, дана характеристика объекта модернизации.

Повышение эффективности работы местной сети связи является важной задачей. В настоящее время Министерство Связи РБ реализует проект развития широкополосного доступа в сетях связи.

Основной задачей является строительство на территории страны мультисервисных сетей и использование архитектуру NGNна базе платформы IMS. Концепция IMSпредставляет собой услугу в сетях передачи данных на базе IPпротокола вне зависимости от использования объектов мобильного или стационарного широкополосного доступа.

В качестве объекта применения в работе рассматривается узел связи Витебской области.

В работе предложена замена устаревшей координатной АТС на мультисервисный узел доступа к сети IMS. Это позволит оказывать современные телекоммуникационные услуги концепции TriplePlay – «тройной услуги», которые включают в себя передачу данных (высокоскоростной доступ к сети интернет), передачу видеоизображения (IPTV) и передачу звука (IP-телефония).

В IMS выделяются уровень передачи данных (UserPlane), уровень управления (ControlPlane)и уровень приложений (ApplicationPlane). Рассмотрим каждый из уровней подробнее.

Уровень передачи данных содержит транспортный шлюз TGW который поддерживает взаимодействие IMS-сети с ТфОП ипозволяет устанавливать соединения между пользователями этих сетей. Он в свою очередь состоит изсигнального (SGW – SignalingGateway) для передачи сигнальных сообщений и медиашлюза (MGF – MediaGateway), через который осуществляется передача пользовательской информации. Шлюз безопасности SEG. служит для защиты уровня управления в сети, которая принадлежит одному провайдеру услуг, и в которой действуют единые административные правила и сетевая политика.

Уровень управления состоит из функционального элемента управления сеансами CSCF (CallSessionControlFunction). Он является центральной частью системы IMS, представляет собой SIP-сервер и обрабатывает SIP-сигнализацию в IMS.

Задача передачи телефонных звонков по сетям IP практически разбивается на две фазы: коммутация (маршрутизация) вызовов и передача данных (кодированного голоса). Коммутация вызовов осуществляется передачей сигнальных сообщений, а данный процесс упрощенно называется сигнализацией. Сигнализация решается средствами специальных протоколов. Протоколы обеспечивают регистрацию IP-устройства (шлюз, терминал или IP-телефон) на сервере провайдера, вызов и/или переадресацию вызова, установление голосового или видеосоединения, передачу имени и/или номера абонента. SIP-протокол является основным протоколом сети IMS.

Для взаимодействия с традиционными телефонными сетями, использующими сигнализацию ОКС-7, была разработана модификация протокола SIP для телефонии: SessionInitiationProtocolforTelephones (SIP-T).

Посредник обработки SIP сообщений S-CSCF взаимодействует с сервером домашних абонентов (HSS), получает от последнего данные аутентификации пользователя, пытающегося получить доступ к сети, и данные о профиле пользователя, т. е. перечень доступных ему услуг.

P-CSCF (посредник взаимодействия с абонентским терминалом)– это первая точка взаимодействия (на сигнальном уровне) пользовательского IMS-терминала и IMS-сети. С точки зрения SIP, она является входящим/исходящим прокси-сервером, через который проходят все запросы, исходящие от IMS-терминала или направляемые к нему.

I-CSCF(посредник для взаимодействия с внешними сетями)взаимодействует с сервером домашних абонентов HSS и блоком поиска конкретного абонента SLF, получает от них информацию о местонахождении пользователя и об обслуживающей его S-CSCF. Если никакая функция S-CSCF еще не назначена, функция I-CSCF производит ее назначение.

Каждая IMS-сеть содержит один или более серверов пользовательских баз данных HSS. Сервер HSS представляет собой централизованное хранилище информации об абонентах и услугах. MRF (MediaResourceFunction), является источником медиаинформации, она делится на две части: MRFC – MediaResourceFunctionControllerи MRFP – MediaResourceFunctionProcessor. MRFC находится на сигнальном уровне и взаимодействует с S-CSCF, контроллер MRFC управляет по протоколу Megaco процессором MRFP, находящимся на уровне передачи данных, а тот выполняет все манипуляции с медиаинформацией.

В заключении можно сказать, что рассмотренный проект модернизации сети передачи данных является технически и экономически эффективным иможетреализоваться на практике.

Список использованных источников:

1. IMS [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/IMS.
2. Гольдштейн, Б.С. Протокол SIP: справочник / Б. С. Гольдштейн, А. А. Зарубин, В. В. Саморезов. — СПб. : 2005. – 390 с.
3. Гольдштейн, Б.С. IP-телефония (3-е издание). / М.: Радио и связь, 2006. — 312 с.

МОДЕЛИРОВАНИЕ СИГНАЛОВ НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ ЛАПЛАСА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь
Фам М.Т.
Беленкевич Н.И.- старший преподаватель

В настоящее время в изучении СТК (систем телекоммуникаций) используют различные методы описания сигналов: во временной и частотной областях, а также на комплексной плоскости. Тенденции указывают, что все чаще распространен именно метод описание сигналов на комплексной плоскости с помощью преобразования Лапласа. Это характерно не только для теоретического исследования, но и для программного обеспечения, отвечающего за моделирование.[1]

Преобразование Лапласа- интегральное преобразование, которое связывает функцию комплексного переменного (изображения) с функцией вещественного переменного (оригиналом). Главной из особенностей данного преобразования является то, что большим соотношениям и операциям над оригиналами соответствуют наиболее простые соотношения над их изображениями.[2]

Для преобразования по Лапласу комплекснозначная функция$f(t)$должна удовлетворять условию Гельдера, возрастать не быстрее показательной функции и существовать на положительной временной полуоси. Такую функцию называют функцией-оригиналом.

Прямое преобразование Лапласа ставит в соответствие оригиналу$f(t)$его изображение$F(p)$

$$F(p) = \int_0^\infty f(t)e^{-pt}dt$$

которое является функцией комплексного переменного $p = \sigma + j\omega$.

Обратный переход осуществляется с помощью обратного преобразования Лапласа:

$$f(t) = \frac{1}{2\pi j}\int_{a-j\infty}^{a+j\infty} F(p)e^{pt}dp.$$

При моделировании сигналов на основе преобразования Лапласа в основном применяются следующие свойства [1]:

1) свойство линейности: $f_i(t) \Leftrightarrow F_i(p),\ (i = \overline{1,N})$, то $f(t) = \sum_{i=1}^{N} A_i f_i(t) \Leftrightarrow F(p) = \sum_{i=1}^{N} A_i F_i(p)$, где A_i- постоянные коэффициенты;

2) теорема смещения: $f_1(t) \Leftrightarrow F_1(p)$, то $f_2(t) = f_1(t)e^{p_0 t} \Leftrightarrow F_2(p) = F_1(p - p_0)$;

3) теорема подобия: $f_1(t) \Leftrightarrow F_1(p)$, то $f_2(t) = f_1(nt) \Leftrightarrow F_2(p) = \frac{1}{n}F_1(\frac{p}{n})$;

4) дифференцирование оригинала: $f(t), t \in (0,\infty)$ - дифференцируема и $f_1(t) \Leftrightarrow F_1(p)$, то $f_2(t) == f_1^{(n)}(t) \Leftrightarrow F_2(p) = p^n F_1(p) - p^{n-1}f(0) - p^{n-2}f'(0) - \cdots - f^{n-1}(0)$, где $f^{(k)}(0) = \lim_{t\to 0+0} f^{(k)}(t),\ k == \overline{0,n-1}$;

5) дифференцирование изображения: $F_1(p) \Leftrightarrow f_1(t)$, то$F_2(p) = F_1^{(n)}(p) \Leftrightarrow f_2(t) = (-1)^n t^n f(t)$;

6) интегрирование оригинала: $f_1(t) \Leftrightarrow F_1(p)$, то $f_2(t) = \int_0^t f_1(t)dt \Leftrightarrow F_2(p) = F_1(p)/p$;

7) интегрирование изображения: $F_1(p) \Leftrightarrow f_1(t)$, то $F_2(p) = \int_p^\infty F_1(p)dp \Leftrightarrow f_2(t) = f_1(t)/t$;

8) теорема умножения изображений: $F_1(p) \Leftrightarrow f_1(t)$и $F_2(p) \Leftrightarrow f_2(t)$, $F(p) = F_1(p)F_2(p) \Leftrightarrow f(t) = \int_0^t f_1(\tau)f_2(t-\tau)d\tau$;

9) теорема умножения оригиналов: $f_1(t) \Leftrightarrow F_1(p)$ и $f_2(t) \Leftrightarrow F_2(p)$, то $f(t) = f_1(t)f_2(t) \Leftrightarrow F(p) = \frac{1}{2\pi j}\int_{a-j\infty}^{a+j\infty} F_1(z)F_2(p-z)dz$;

10) теорема запаздывания: $f_1(t) \Leftrightarrow F_1(p),\ t_0 \geq 0,\ f_2(t) = f_1(t-t_0) \Leftrightarrow F_2(p) = F_1(p)e^{-pt_0}$;

11) предельные соотношения: $f(t)$ и ее производная $f'(t)$- оригиналы и $f(t) \Leftrightarrow F(p)$, то $\lim_{p\to\infty} pF(p) = \lim_{t\to 0+0} f(t) = f(0), \lim_{p\to 0} pF(p) = \lim_{t\to\infty} f(t) = f(\infty)$.

Нахождение изображения периодического сигнала на комплексной плоскости является примером эффективного применения свойств преобразования Лапласа, что позволяет намного упростить операции моделирования и обработки инфокоммуникационных сигналов.

Списокиспользованныхисточников:

1.Ильинков, В.А. Моделирование линейных свойств звеньев и сигналов в телекоммуникационных системах : учеб.пособие по дисциплине "Моделирование систем телекоммуникаций" для студентов специальностей "Системы радиосвязи, радиовещания и телевидения", "Многоканальные системы телекоммуникаций" всех форм обучения / В.А. Ильинков, Н.И. Беленкевич, В.Е. Романов. — Мн. : БГУИР, 2005. - 102 с.

2.Труфанова Т.В. Интегральное преобразование Лапласа и Фурье: Учебное пособие / Т.В. Труфанова, Е.М. Салмашова. - Благовещенск: Амурский гос. ун-т, 2006.

СРАВНИТЕЛЬНАЯ ОЦЕНКА ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ С МНОГОПОЗИЦИОННЫМИ ВИДАМИ МОДУЛЯЦИИ

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

Серченя А.А.

ЛипковичЭ.Б. – доцент

Применение помехоустойчивого кодирования с исправлением ошибок в современных системах связи является обязательным. Кодирование информации позволяет, с одной стороны, уменьшить количество ошибок в канале, возникающих из-за влияния частотно-селективных замираний, индустриальных помех и прочих факторов, и тем самым уменьшить общее время неготовности линии связи, и с другой стороны, снизить значение пороговой чувствительности приемника, за счет чего увеличить энергетику линии связи.

В современных системах используют многопозиционные методы модуляции, т.к. они позволяют повысить пропускную способность системы в пределах выделенной полосы частот. Они являются полосносберегающими. Суть выигрыша по скорости передаваемых данных или по используемой полосе частот состоит в том, что радиосимволы, образованные на выходе модулятора с длительностью $T_c = 1/B_c$, переносят несколько бит исходной информации, где B_c – символьная скорость. Различительными признаками состава передаваемых бит в символе являются определенные значения амплитуд, частот и фаз или их комбинаций.

Выбранный метод модуляции не только позволяет повысить пропускную способность, но и влияет на такие характеристики помехоустойчивости системы, как вероятность ошибки и значение отношения несущая/шум (ОНШ).

Для сравнения помехоустойчивого кодирования при использовании разных видов многопозиционной модуляции положим, что имеется цифровая система и используется сверточное кодирование, когерентная демодуляция сигналов КАМ-М, ФМ-М, АМ-М и декодирование по алгоритму Витерби с мягким решением.

Исходным соотношением, увязывающим вероятность ошибки на бит информации с параметрами модуляции и кодирования, является

$$P_{\text{ОШВ}} = C_i \cdot R_{\text{к}} \cdot d_{\text{с}} \cdot \beta \cdot \sqrt{K \cdot q_i} \cdot erfc\,(x); \qquad x = \sqrt{R_{\text{к}} \cdot d_{\text{с}} \cdot \beta \cdot q_i \cdot h_{\text{ок}}}, \tag{1}$$

где C_i, q_i - коэффициенты, зависящие от вида модуляции; d_c - свободное расстояние для сверточного кода.

Чуть подробнее стоит остановиться на коэффициенте q_i. q_i - это квадрат коэффициента помехоустойчивости. Он используется для более полной оценки эффективности многопозиционных видов модуляции и вычисляется по формуле:

$$q_i = d_{0i}^2 / 4E_0 \text{ .} \tag{2}$$

d_{0i} - евклидово расстояние (расстояние между точками сигнального созвездия), которое тем меньше, чем больше кратность модуляции.При его уменьшении уменьшается достоверность приема при наличии шумов и помех в радиотракте. Компенсировать это можно увеличением амплитуд передаваемых сигналов. Для разных видов модуляции евклидово расстояние вычисляется при помощи разных формул.

E_0 - это энергия, требуемая для передачи одного бита информации.

Чем больше значение q_i, тем выше эффективность выбранного вида модуляции и ниже требуемое пороговое отношение $h_0 = E_0 / N_0$ для обеспечения необходимой достоверности приема.

Выразим из формулы (1) значение порогового отношения сигнал/шум (ОСШ) $h_{0к}$:

$$h_{0к} = 10 \cdot \lg\left[\frac{2.3 \cdot (D_i - 0.5 D_i \cdot 2.3)}{q_i \cdot \beta \cdot d_c \cdot R_к}\right], \text{ дБ} \tag{3}$$

Если принять $R_к$, d_c, β, K равными единице, то расчетное соотношение (3) переходит к формуле без кодирования.

Требуемое ОНШ при наличии сверточного кодирования для обеспечения заданной достоверности приема определяется по формуле

$$\rho_{0к} = h_{0к} + 10 \lg \gamma_0 + \Delta\rho_{\Sigma}, \text{ дБ.} \quad (4)$$

Эффективность кодирования в цифровых системах определяется величиной выигрыша от кодирования при сохранении выбранного типа модуляций и величины ошибок:

$$\Delta G_к = h_0 - h_{0к} = \rho_0 - \rho_{0к} - 10 \lg R_к = 10 \lg R_к \cdot d_c \cdot \beta \cdot \xi \quad (5)$$

$$\xi = \frac{A_i - 0.5 \lg A_i \cdot 2.3}{D_i - 0.5 \lg D_i \cdot 2.3}. \quad 6)$$

Величина $\Delta G_к$ зависит от свойств корректирующего кода и алгоритма кодирования. Чем выше $\Delta G_к$, тем выше исправляющая способность выбранных кодов и их сочетаний.

В технике цифровой связи методы модуляции играют весьма значительную роль. Помимо своей основной функции – преобразования символ–сигнал – процесс модуляции является составной частью общего процесса согласования сигнала с характеристиками канала.Теоремы Шеннона для канала с шумами связывают пропускную способность канала передачи информации и существование кода, который возможно использовать для передачи информации по каналу с ошибкой, стремящейся к нулю (при увеличении длины блока).Практически важный вывод работ Шеннона состоит в том, что если скорость передачи информации меньше пропускной способности канала, то с использованием кодов, исправляющих ошибки, можно создать систему связи со сколь угодно малой вероятностью ошибки на выходе декодера канала. При этом адекватная система без корректирующего кодирования будет более сложной, дорогой и энергоемкой. Отсюда вывод: система, не имеющая корректирующего кодирования и работающая без ошибок, - это крайне неэффективная система. Наоборот, эффективная система должна иметь возможность работы в режиме с достаточно высокой частотой ошибок в потоке на входе декодера, а сам декодированный поток должен иметь крайне малую вероятность ошибки на бит.

Таким образом, современные методы многопозиционной модуляции в полном соответствии с теоремой Шеннона могут рассматриваться и как способ кодирования данных сообщений в символы канала.

Список использованных источников:

1.Липкович, Э. Б. Цифровые системы радиосвязи и радиовещания : электронный ресурс по учебной дисциплине / Э. Б. Липкович [Электронный ресурс]. – Минск : БГУИР, 2016. – Режим доступа: http://www.bsuir.by/

2. Золотарёв, В.В., Овечкин, Г.В. Помехоустойчивое кодирование. Методы и алгоритмы : Справочник / Ю.Б. Зубарев, – М.: Горячая линия-Телеком, 2004. – 126 с.

3. Методы модуляции в цифровых ТВ системах [Электронный ресурс]. Режим доступа: http://www.konturm.ru/newsprint.php?id=help/stat290805

CDMA-PON

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

Сергеев Н.Н.

Урядов В.Н. – к.т.н.,доцент

Требования абонентов к телекоммуникационным услугам, как к скорости так и к качеству интенсивно растут. Поэтому необходимо искать альтернативы существующей традиционной концепции TDM-PON. Так была предложена концепция CDMA-PON.

.

Новым направлением развития сетей является третье направление развития пассивных волоконно-оптических сетей PON – множественный доступ с кодовым разделением каналов CDMA-PON (рисунок 1)[1] .

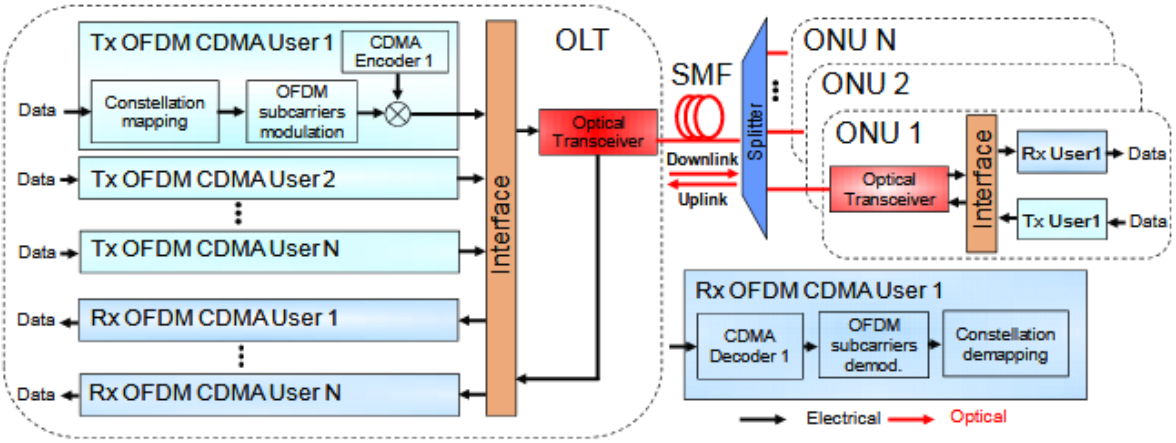


Рис.1. Архитектура OFDM-CDMA PON

Несколько пользователей могут одновременно передавать информацию по одному и тому же ка налу, используя различные кодовые последовательности для передачи логических нулей и единиц. Каждый передатчик кодирует определенным кодом последовательность битов, подлежащих передаче, умножая все разряды расширяющей последовательности на значение информационного бита. На приемной стороне каждый разряд суммарного сигнала умножается на соответствующий разряд расширяющей последовательности данного канала, после чего полученные результаты суммируются в пределах первого периода последовательности. В зависимости от этого вычисляется исходный [2] символ.

Выделим основные преимущества использования технологии CDMA в волоконно-оптических сетях доступа:

- возможность организации гибкого метода множественного доступа для передачи асинхронного трафика: в зависимости от веса и длины выбранного кода можно варьировать количество пользователей сети доступа;
- необходимую величину значения вероятности ошибок либо битовой скорости можно получить перебором используемых кодов;
- отсутствие необходимости строгого управления длинами волн как в WDM-PON [3];
- самомаршрутизация по кодовой последовательности: в матрице используемых в технологии CDMA кодов все строки равноудалены друг от друга в том смысле, что кодовые расстояния между ними (то есть число несовпадающих битов при сопоставлении кодов) одинаковы. Это свойство позволяет нейтрализовать чужеродные сигналы при получении результата своеобразным сравнением в приемнике;
- эффективное использование полосы пропускания;
- повышенная защищенность информации от несанкционированного доступа за счет передачи по линии связи псевдошумоподобного широкополосного сигнала.

Список использованных источников:

1. CDMA-PON Security Issues: Upstream Encryption is Needed / Dovid Gutierrez. Jinwoo Cho, Leonid G. Kozovsky // Optical Fiber Communication and the National Fiber Optic Engineers Conference. Анахайм, Калифорния, США, 25-29 Марта 2007.
2. 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.
3. Рекомендация МСЭ-Т G.983.1. Широкополосные оптические сети доступа на базе пассивных оптических сетей

АНАЛИЗ ЧУВСТВИТЕЛЬНОСТИ ПРИЕМНОГО ОПТИЧЕСКОГО МОДУЛЯ С P-I-N ФОТОДЕТЕКТОРОМ

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

Сергеев Н.Н.

Урядов В.Н. – к.т.н.,доцент

В существующих оптических системах передачи широко используются различные приемные модули, одним из основных модулей приема является приемный оптический модуль с p-i-n фотодетектором. Для корректной работы системы, необходимо, чтобы уровень сигнала был в рамках чувствительности приёмного оптического модуля[1]. Позволит ли порог чувствительности приемного оптического модуля принять информацию используя отражённый сигнал от оветвителя? Для ответа на этот вопрос произведём анализ чувствительности приёмного оптического модуля[2].

.

Одним из модулей приема является приемный оптический модуль с p-i-n фотодетектором. Произведя расчет чувствительности оптического приемного модуля с оптическим предусилителем, учитывая, что мощность шума i^2 p-i-n фотодиода уменьшается в G^2 раз (где G – коэффициент усиления оптического усилителя), при следующих параметрах: η_m =0,8; A_λ=4,8 Вт/А; C_Σ =0,5 пФ (кривая 1), C_Σ =1 пФ (кривая 2); In_2 =0,55, In_3 =0,085; *Sm*=35· 10^{-3} *См*; *Fn*=1.5, с учетом того, что полоса спектра сигнала одного канала $\Delta\nu$ для системы со скоростью В Мбит/с примерно равна $\Delta\nu$=2В, [3] зависимость чувствительности оптического приемника от скорости передачи при k_1 =0.5 будет иметь следующий вид (рисунок 1).

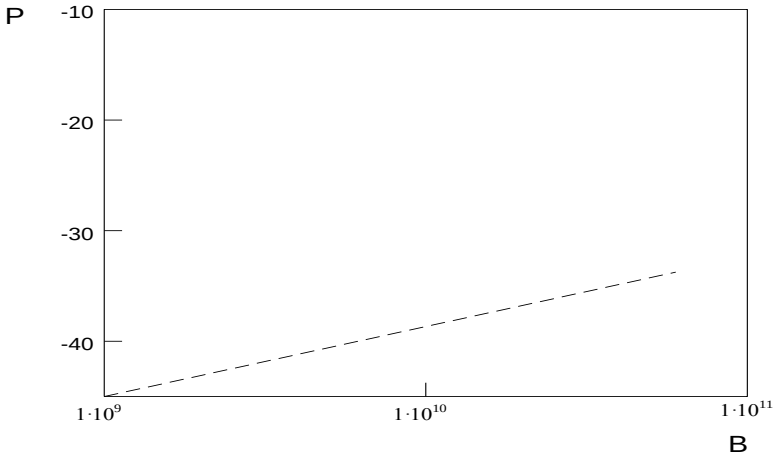


Рисунок 1 – Зависимость чувствительности оптического приемника с p-i-n фотодиодом от скорости передачи при k_1 =0.5

Чувствительность оптического приемника с увеличением скорости передачи информации быстро уменьшается, что приводит к уменьшению бюджета системы, который равен разности уровней передающего оптического модуля и чувствительности оптического премного устройства.

Сравнение оптических приемников различного типа показывает, что приемник с оптическим предусилителем с типичным коэффициентом усиления 20 дБ обеспечивает выигрыш в чувствительности примерно на 7 дБ по сравнению с приемником, использующим лавинный фотодиод и 15 дБ с p-i-n фотодиодом[4].

Чувствительность для скорости 2,5 Гбит/с составила -49дБм., что положительно подтверждает возможность несанкционированного доступа к восходящему потоку с абонентской розетки. Однако, качество приема сигналов будет с большей вероятностью ошибки ~ 10^{-6} .

Список использованных источников:

4. TDM-PON Security Issues: Upstream Encryption is Needed / Dovid Gutierrez. Jinwoo Cho, Leonid G. Kozovsky // Optical Fiber Communication and the National Fiber Optic Engineers Conference. Анахайм, Калифорния, США, 25-29 Марта 2007.
5. Булавкин И.А. Вопросы информационной безопасности сетей PON // Технологии и средства связи — 2006. - IW2. - С. 104-108.
6. Рекомендация МСЭ-Т G.983.1. Широкополосные оптические сети доступа на базе пассивных оптических сетей
7. 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.

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

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

Мурашко Е.А, Марычев Д.В, Петкевич Д.А.

Вишняков В.А., д.т.н., профессор

Системы обнаружения сетевых вторжений и выявления признаков атак на информационные системы уже достаточно длительное время используются как одно из необходимых средств защиты информационных систем.Поскольку количество различных типов и способов организации несанкционированных проникновений в чужие сети за последние годы значительно увеличилось, системы обнаружения атак (СОА) стали необходимым компонентом инфраструктуры большинства организаций. Использование виртуальной инфраструктуры для построения системы обнаружения вторжений позволяет обеспечить как более рациональное распределение и использование физических ресурсов, так и упрощает администрирование всех компонентов системы защиты. В качестве средства обнаружения и предотвращения вторжений используется IDS/IPSSnort.

Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS)) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть. СОВ всё чаще становятся необходимым дополнением инфраструктуры сетевой безопасности.В дополнение к межсетевым экранам (firewall), работа которых происходит на основе политики безопасности, СОВ служат механизмами мониторинга и наблюдения подозрительной активности.Архитектура СОВ включает:

1) Сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы;
2) Подсистему анализа, предназначенную для выявления сетевых атак и подозрительных действий;
3) Хранилище, в котором накапливаются первичные события и результаты анализа;
4) Консоль управления, позволяющая конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты.

Пример реализации СОВ с использованием виртуальной инфраструктуры представлен на рисунке 1:

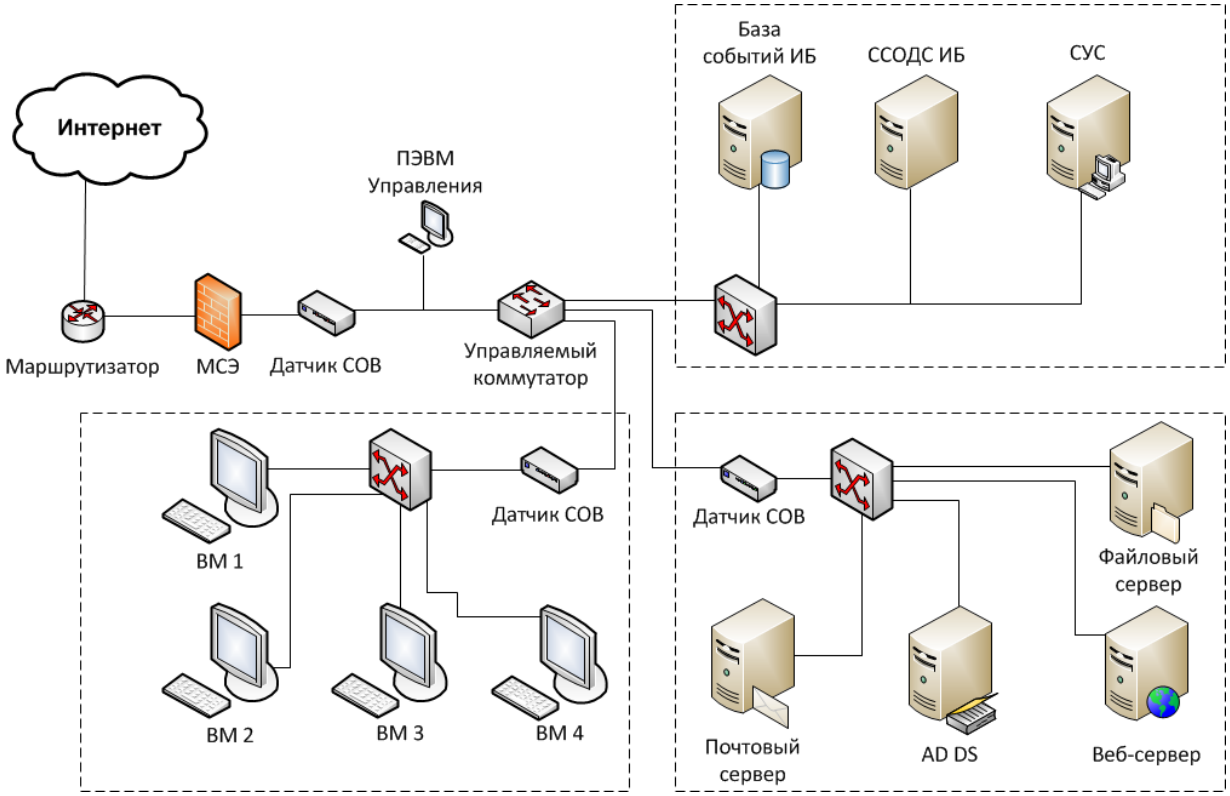


Рисунок 1 – Упрощённая структура сети с виртуальными и физическими СОВ

Штриховыми областями на схеме обозначены сервера виртуализации, на которых развёрнуты

датчики сети, виртуальные коммутаторы, различные сервера и виртуальные рабочие станции.

Созданная виртуальная инфраструктура обладает следующими особенностями:

а) события с датчиков СОВ собираются в базу данных на выделенном виртуальном сервере;

б) для упрощения работы и анализа событий, принятых от датчиков сети, развёрнута виртуальная система сбора и обработки данных о событиях информационной безопасности (ССОДС ИБ).

Основные преимущества использования виртуальной инфраструктуры:

- возможность быстрой миграции виртуальных машин и создания резервных копий;
- возможность перераспределения используемых виртуальными машинами ресурсов;
- уменьшение количества используемого физического оборудования;
- упрощение администрирования и реконфигурации сети;
- упрощение добавления новых рабочих мест и серверов.

Основные недостатки применения виртуализации:

- высокая стоимость серверов и корпоративных лицензий для использования виртуальных гипервизоров;
- необходимость повышения квалификации администраторов и пользователей для работы с виртуальной инфраструктурой;
- риск потери данных и увеличение времени простоя виртуальных серверов или рабочих станций при выходе из строй одного из серверов виртуализации.

Эволюция технологий виртуализации открывает новые возможности для обеспечения оптимальной и максимально удобной организации любых современных локальных сетей. Неизбежный рост сетевой инфраструктуры способствует всё большей популяризации использования средств виртуализации как для простых объектов, как-то рабочие места сотрудников предприятий, так и более сложных и комплексных информационных систем. Переход от исключительно физической инфраструктуры сети к комбинированной с виртуальной является залогом успешного развития локальных и глобальных сетей.

Список использованных источников:

1. Вишняков, В. А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения / В. А. Вишняков. – Минск : Белорусская государственная академия связи, 2016. – 276 с.

2. Национальный открытый университет [Электронный ресурс]. – Режим доступа : http://www.intuit.ru/.

3. Таненбаум, Э. Компьютерные сети. Пятое издание. / Э. Таненбаум, Д. Уэзеролл – Санкт-Петербург. : Питер, 2012. – 960 с.

4. Dave Mishchenko. VMware ESXi: Planning, Implementation, and Security.

5. David Chisnall, The definitive guide to the Xen hypervisor. ISBN-13: 978-0-13-234971-0.

6. Бэйкер, Э. Р. Snort IDS and IPS Toolkit. / Э. Р. Бэйкер, Дж. Эслер. – Берлингтон : Syngress, 2007. – 766 с.

ВИДЕОКОНФЕРЕНЦСВЯЗЬ В IP-СЕТЯХ

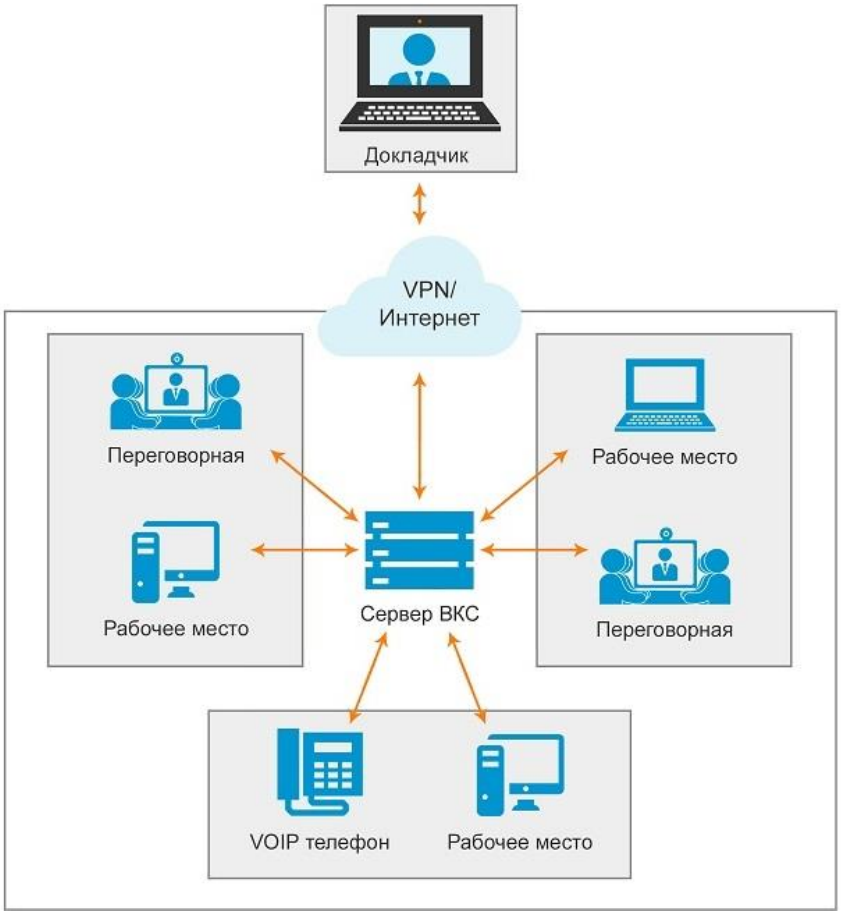
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Масько В.С.

Лагутин А. Е.

Современный мир сегодня невозможно представить без сервисов и услуг, предоставляемых информационными технологиями и телекоммуникациями. Появляется необходимость не отставать от прогресса в сфере информационных технологий. Важно знать и уметь применять новые услуги, решения и научные достижения. Их оптимальное использование позволяет по-новому подойти к решению старых задач, а также сформировать оригинальное решение для задач, ранее неразрешимых. При этом достигается снижение трудозатрат, экономия времени и сокращение денежных расходов. Одной из таких современных технологий является групповая (многоточечная) видеоконференцсвязь.

Групповая видеоконференцсвязь — это технология, которая позволяет нескольким удаленным участникам (трем и более) интерактивно взаимодействовать друг с другом, используя аудио- и видеосвязь. Во время сеанса происходит передача аудио- и видеоданных в режиме реального времени, обмен файлами и их совместная обработка. Эта технология призвана упростить взаимное общение участников, находящихся на расстоянии друг от друга, но испытывающих необходимость в коллективном, одновременном общении друг с другом лицом к лицу.



На данный момент существует множество фирм-производителей систем видеосвязи, а так же сервисы и программное обеспечение как Skype и Google Hangouts, каждые из которых подходят для решения определённых задач.

Список использованных источников:

1. Олифер В.Г. Олифер Н.А. Компьютерные сети изд. 5
2. Системы компьютерной видеоконференцсвязи - Синепол В.С.
3. Протоколы организации видеоконференцсвязи - https://sites.google.com/site/videoconfsys/home/protocol

ПРИМЕНЕНИЕ ОПТИЧЕСКИХ МОДУЛЕЙ С АДАПТИВНЫМ ПОРОГОМ ПРИНЯТИЯ РЕШЕНИЙ

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

Латушкин К.Ю.

Урядов В.Н. – к.т.н.,доцент

В настоящее время в связи с постоянно увеличивающимися потребностями абонентов в пропускной способности широкое применение нашли сетиPON. Однако внедрение данного вида сетей приводит к необходимости решения ряда проблем, одной из которых является крайне широкий диапазон уровней сигналов передаваемых в сети. Решением данной проблемы стало использование оптических модулей с адаптивным порогом принятия решений.

PON(PassiveOpticalNetwork, пассивнаяоптическаясеть) – технологии широкополосного мультисервисного доступа по оптическому волокну. Особенность технологии заключается в том, что ее распределительная сеть (преимущественно древовидной топологии) строится без использования активных компонентов: разветвление оптического по линии связи осуществляется с помощью пассивных разветвителей оптической мощности – сплиттеров.

Второй особенностью идеи PON является то, что инфраструктура работает на базе одного модуля - трансивера, который отвечает за функции приема и передачи данных. Располагается этот компонент в центральном узле системы OLT и позволяет обслуживать информационными потоками множество абонентов. Конечным приемником выступает устройство ONT, которое, в свою очередь, также выступает передатчиком. - Поскольку ONT удалены на разные расстояния от OLT, то и вносимые потери в оптические сигналы, при распространении по дереву PON будут разными. Это может привести к нарушению работы фотоприемников из-за слабости сигнала либо из-за перегрузки [1].

Сейчас наиболее популярным стандартом сменных оптических трансиверов стали SFP модули (SmallForm-factorPluggable). Они представляют собой малогабаритные конструкции в металлическом корпусе (для механической защиты и электромагнитного экранирования) с выводами для подключения к слотам активного оборудования. Также в модуле имеется два оптических порта: излучателя (Tx) и фотоприемника (Rx) для работы в двухволоконном режиме. На плате модуля кроме, собственно, излучателя и фотодетектора находятся схемы обеспечения тока накачки излучателя, преобразования в линейный код, смещения на фотодетекторе, термостабилизации[2].

Принцип реализации приемной части оптического модуля с адаптивным порогом принятия решений представлен на рисунке 1:

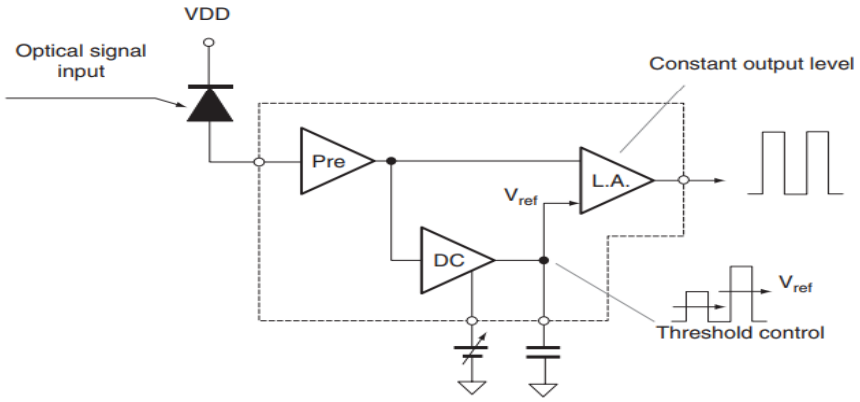


Рисунок 1 – Структура приемной части оптического модуля с адаптивным порогом принятия решений

Принцип работы следующий: полученный сигнал усиливается предварительным усилителем, а затем разделяется на две ветви. Первая ветвь подключается непосредственно к дифференциальному усилителю, вторая ветвь подключается к пиковому детектору для определения амплитуды поступающего сигнала. После определения амплитуды сигнала,перед дифференциальным усилителем происходят адаптивная подстройка порога с помощью делителя напряжения. На выходе дифференциального усилителя, восстановленный сигнал готов для дальнейшей обработки.

Использование данного метода приема сигналов стало одним из залогов эффективного использования сетей PON.

Списокиспользованныхисточников:
1. Cedric F. Lam, Passive Optical Networks. Principles and Practice
2. Основные параметры и сертификация оптических SFP модулей // www.habrahabr.ru

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОГРАММ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ СИГНАЛОВ, ФУНКЦИОНАЛЬНЫХ ЗВЕНЬЕВ И РЕАКЦИЙ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

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

Кухмар Д.А.

Ильинков В.А. – к.т.н.,доцент

Важнейшим этапом проектирования инфокоммуникационных систем является математическое моделирование сигналов, функциональных звеньев и реакций последних. Оно реализуется с помощью программ (пакетов программ) структурнотехнического и схемотехнического моделирования. При этом применяются моделирующие программы как общего применения, так и специализированные. Компьютерные технологии предлагают целый ряд разнообразных средств моделирования, позволяющих не только проектировать сложные системы, но и проводить с ними различного рода эксперименты. Результаты таких экспериментов представляются преимущественно в визуальной форме, более наглядной для человека. Такой подход позволяет значительно ускорить процесс моделирования систем инфокоммуникаций.

На сегодняшний день существует большое число различных программных комплексов математического моделирования. Они обладают рядом определенных особенностей и преимуществ, а именно:

– ускорение процессов анализа и синтеза;

– снижение материальных, интеллектуальных и временных затрат на создание сложных систем (устройств) инфокоммуникаций;

– повышение качества моделирования;

– представление результатов моделирования в визуальной форме;

– поддержка технологии объектно-ориентированного моделирования;

– возможность кастомизации библиотек блоков и элементов.

Проведенный сравнительный анализ также позволил установить, что применительно к задаче моделирования сигналов, звеньев и реакций известные программные комплексы обладают следующими существенными недостатками:

– большой объем черновой и подготовительной работы;

– значительное время моделирования (несмотря на использование производительных вычислительных систем);

– ограничения на редактируемость моделей, их низкая гибкость;

– требование знаний в других областях, не связанных с предметом моделирования;

– отсутствие развитых библиотек;

– стоимость программных комплексов.

Известные программы (программные комплексы) структурнотехнического и схемотехнического моделирования можно разделить на две категории:

1) общего применения, подходящие для моделирования задач и приложений в различных областях науки и техники;
2) специализированные, предназначенные для моделирования систем и устройств радиоэлектроники и телекоммуникаций на функциональном и схемотехническом уровнях.

Наиболее известными программами общего применения являются MathCAD и Mathematica. Они обеспечивают достаточно широкий комплекс возможностей выполнения сложных научно-технических расчетов применительно к различным областям науки и техники, включая также системы инфокоммуникаций.

Вторую группу составляют специализированные моделирующие программы. Применительно к области инфокоммуникаций, радиоэлектроники и радиофизики широкое применение получил, например, программный пакет MATLAB, который является средой визуального моделирования, позволяющий пользователю решать разнообразный спектр задач с помощью широкого набора подсистем и библиотек. Например, подсистема Simulink включает в себя обширные библиотеки элементов и блоков, которые можно использовать для графической сборки систем, а также позволяет пользователю самому создавать новые элементы, блоки и их библиотеки. Ко второй категории моделирующих программ также можно отнести пакеты Scilab, GNU Octave и Sage, которые предоставляют похожий функционал, однако являются полностью либо частично бесплатными.

Ко второй категории программных комплексов моделирования относится и пакет OrCAD – интегрированный программный комплекс для сквозного проектирования аналоговых, цифровых и смешанных аналого-цифровых устройств, синтеза устройств программируемой логики и аналоговых фильтров. Также к данной категории следует отнести программы Electronics Workbench и System View, позволяющие моделировать структурные и функциональные схемы устройств, а также проводить над ними эксперименты и анализировать результаты.

К категории специализированных программ относится также моделирующий пакет Micro-Cap, предназначенный для схемотехнического моделирования электронных устройств – она позволяет создавать и редактировать принципиальные схемы с помощью большой библиотеки элементов и

встроенного редактора, а также анализировать параметры созданных схем.

Несмотря на все особенности и достоинства проанализированных комплексов, они серьезно усложняют процедуру математического моделирования, требуют от исследователя, помимо хорошего знания физических процессов в моделируемой системе, также глубоких знаний по математике, теории цепей и сигналов, программированию, другим дисциплинам, что возможно в редких случаях. Учитывая это, актуальной является разработка многофункциональной программы, пригодной для математического моделирования различных систем инфокоммуникаций, не требующих от пользователя глубоких знаний по совокупности дисциплин. Весьма эффективно применение многофункциональной программы математического моделирования сигналов, функциональных звеньев и реакций в учебном процессе подготовки специалистов телекоммуникационного профиля.

Список использованных источников:

1. Беленкевич Н.И., Ильинков В.А. Совместное математическое описание сигналов, линейных звеньев и реакций систем телекоммуникаций и радиоэлектроники // Известия Национальной академии наук Беларуси. Серия физико-технических наук. – 2017. – №4. – С.93–104.

2. Половко А.М. MATLAB для студента /Половко А.М., Бутусов П.Н.– СПб.: БВХ-Петебург, 2005. – 320 с.: ил.

3. Болотовский Ю. И. OrCad. Моделирование. «Поваренная» книга / Болотовский Ю. И., Таназлы Г. И.– М.: СОЛОН-Пресс, 2005. – 200 с.

МУЛЬТИМЕДИЙНАЯ СПУТНИКОВАЯ СИСТЕМА ОБМЕНА ИНФОРМАЦИЕЙ КА-ДИАПАЗОНА ЧАСТОТ

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

Липкович Э.Б. – доцент

Спутниковый обмен информацией и высокоскоростной доступ к мультимедийным ресурсам считается одним из перспективных трендов в спутниковой отрасли. К настоящему времени созданы специализированные высокоинформативные спутниковые сети (Ka-Sat, Astra2Connect, HughesNet, ViaSat и др.) и выведено на орбиту достаточно большое число спутников с радиостволами мультимедийных услуг, включая российские спутники Экспресс-АМ5/АТ2 (140° в. д.), Экспресс-АМ6 (53° в. д.), Экспресс-АМ8 (14° з. д.). В значительной части этих спутников используются радиостволы Ка-диапазона частот (27,5...31,0 ГГц на линии «вверх» и 17,7...21,2 ГГц на линии «вниз»), что объясняется их широкополосностью (полоса частот 150...400 МГц) и высокой энергетической эффективностью благодаря высокой допустимой плотности потока мощности у поверхности Земли в этом диапазоне[1].

Спутниковые системы Ка-диапазона частот направлены на обеспечение большому числу пользователей, независимо от мест их размещения, доступ к мультимедиа ресурсам. При этом в распоряжении пользователей находится малогабаритная станция типа VSAT, обеспечивающая высокоскоростной обмен информацией. Построение и характеристики станции связаны с использованием передовых телекоммуникационных технологий, основанных на полосносберегающих видах модуляции, помехоустойчивом кодировании, адаптивном изменении параметров, высокой надежности связи и простом обслуживании.

Ка-диапазон устраняет проблему нехватки спутникового сегмента, которая сдерживала развитие спутниковой связи в последние несколько лет в Ku-диапазоне. Появление спутников Ка-диапазона в сочетании с многолучевой технологией обеспечило этой отрасли дополнительный частотный ресурс, использование которого обходится значительно дешевле, чем использование аналогичной емкости Ku- или С-диапазонов в традиционном использовании.

Спутники Ku- и С-диапазонов обычно используют широкие лучи, охватывающие целый континент или крупную страну, такую, например, как Россия. При этом передаваемые по этому лучу данные могут приниматься в любой точке этой зоны. Широкая зона обслуживания является преимуществом для корпоративных приложений или телевизионного вещания, но неэффективна для доступа в Интернет.

Спутники Ка-диапазона работают по другому принципу: они используют много точечных лучей, каждый из которых покрывает заданный регион. Благодаря этому, используя один и тот же спектр, спутник Ка-диапазона способен передавать принципиально больше данных, чем традиционный спутник Ku-диапазона с широким контурным лучом. Примерно пропорционально числу лучей, умноженному на полосу частот, поддерживаемую в одном луче. И хотя спутники Ка-диапазона дороже в 2-3 раза, общая стоимость передачи данных в расчете на один бит информации для них оказывается значительно ниже, чем для спутников Ku-диапазона. Поэтому эта архитектура идеально подходит для обеспечения доступа в сеть Интернет.

Таким образом, при меньшей стоимости за один бит информации и большей пропускной способности, чем в случае спутников Ku-диапазона, спутники Ка-диапазона открывают новые возможности для развития отрасли спутниковых коммуникаций[2].

Ка-диапазон дает три основных преимущества:

– основным достоинством Ка-диапазона является то, что он позволяет обеспечить всем желающим доступный высокоскоростной широкополосный доступ в Интернет, сравнимый по цене и качеству с перспективными наземными сетями. Люди, живущие за пределами мегаполисов, автоматически оказываются в невыгодном положении. Обычно они не могут получить доступ в Интернет на тех же скоростях, что и жители крупных городов. Кроме того, даже более медленный доступ в Интернет обычно обходится им дороже;

– отсутствие высокоскоростного доступа затрагивает не только частных граждан, но и государственные и общественные учреждения, возникает проблема организации государственных электронных услуг. Применение Ка-диапазона позволит обеспечить широкополосный доступ школам и правительственным учреждения. В качестве примеров возможного применения Ка-диапазона можно назвать общегосударственные программы, потоковую передачу видео в учебных целях, общественные точки доступа по технологии Wi-Fi и высококачественные услуги электронного правительства;

– одним из достоинств Ка-диапазона является возможность его применения для обеспечения мобильного широкополосного доступа в Интернет. Ка-диапазон позволяет налаживать высокоскоростной доступ в поездах, автобусах и на самолетах. Возможность обеспечения высокоскоростной широкополосной связи на мобильных платформах также важна для вооруженных сил, служб экстренного реагирования и аварийно-спасательных операций.

Из вышесказанного можно сделать вывод, что будущее спутниковой связи неразрывно связано со спутниками, работающими с Ка-диапазоном частот.

Список использованных источников:

1. Проектирование цифровых систем спутникового мультимедийного вещания и интерактивной связи : учеб.-метод. пособие / Э. Б. Липкович. – Минск : БГУИР, 2017. – 67 с.

2. Анпилогов, В. Р. Спутниковые системы массового обслуживания в Ка-диапазоне / В. Р. Анпилогов // Технологии и средства связи. Спец. вып. «Спутниковая связь и вещание – 2010». – С. 16–21.

ВЫБОР НАЧАЛЬНЫХ ТОЧЕК ВОЛНОВОГО ВЫРАЩИВАНИЯ ОБЛАСТЕЙ ПО ГИСТОГРАММЕ ЯРКОСТИ ИЗОБРАЖЕНИЯ

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

Козак М.В.

Никульшин Б.В. – к.т.н.,доцент

Исследован алгоритм выбора начальных точек для волнового наращивания областей на основе выделения локальных максимумов гистограммы яркости пикселей. Алгоритм позволяет управлять числом сегментов в алгоритме волнового наращивания областей и обеспечивает уменьшение ошибки восстановления сегментированных изображений.

В задачах обработки изображений широко используется сегментация. Она позволяет упростить структуру изображения за счет логического объединения близких по яркости смежных пикселей. Современные методы сегментации берут начало от четырех базовых методов, основанных на формировании областей с использованием водораздела [1, 2, 3, 4], квантовании по гистограмме, разделении и слиянии областей с использованием квадра-дерева, выращивании областей.

Метод выращивания областей является самым быстрым и представляет наибольший интерес для задач обработки изображений в реальном масштабе времени на базе универсального компьютера.

Исследованн алгоритм выбора начальных точек для волнового наращивания областей на основе выделения локальных максимумов гистограммы яркости пикселей реализованный в среде Matlab. Для оценки его эффективности использовались алгоритмы периодического и случайного выбора начальных точек волнового наращивания областей. Сравнение данных алгоритмов произведено по значениям среднеквадратической ошибки MSE, вычисляемых для исходного и восстановленных после сегментации изображений.

На рис. 1 представлено тестовое полутоновое изображение.

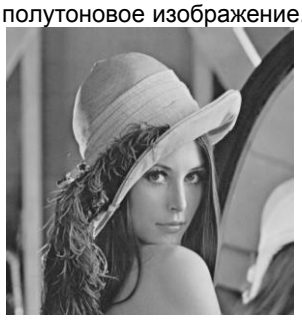


Рисунок 1 – Тестовое изображение Lena

В табл. 1 для тестового изображения и изображений, восстановленных после сегментации волновым методом со случайным и периодическим выбором начальных точек роста, приведены значения MSE.

Таблица 1 – Значения среднеквадратической ошибки MSE для исходного и восстановленных после сегментации волновым методом изображений

Тестовые изображения	Число K начальных точек роста	Значения среднеквадратической ошибки MSE при различных алгоритмах выбора начальных точек волнового выращивания областей		
		Выбор по гистограмме яркости	Периодический выбор	Случайный выбор
Lena	48	0,81	1	2,8
	30	1,1	3,9	4,4
	13	3,7	7,48	7,4
	11	4,2	7,5	6,5

Как следует из табл.1, среднеквадратическая ошибка восстановления изображений увеличивается с уменьшением числа начальных точек роста областей. Алгоритм выбора начальных точек волнового выращивания областей по гистограмме яркости изображения обеспечивает минимальную по сравнению с другими алгоритмами среднеквадратическую ошибку для всех типов тестовых изображений и при любом числе начальных точек роста.

Список использованных источников:

1. Lalitha M., Kiruthiga M., Loganathan C. // International Journal of Science and Research (IJSR). 2013. Vol. 2. №. 2. P. 348–358.

2. Gauch J.M. // IEEE TRANSACTIONS ON IMAGE PROCESSING. 1999. Vol. 8. №. 1. P. 69–79.

3. Альмияхи О.М., Цветков В.Ю., Конопелько В.К. // Доклады БГУИР. – 2016. – № 8 (102). – С. 82–88.

ОСОБЕННОСТИ ТЕХНОЛОГИЙ РАСШИРИТЕЛЬНОГО СТАНДАРТА DVB-S2X

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

Грабун Е. А.

Липкович Э.Б. – к.т.н.,доцент

В конце 2014 года на рынок вышел новый стандарт, а точнее, расширение существующего спутникового стандарта цифрового вещания DVB-S2X. На фоне оптимистичных заявлений об увеличении скорости передачи в канале от 20% до 50% также прозвучала информация об отсутствии обратной совместимости с приемниками стандарта DVB-S2, что потребует обновления оборудования при переходе на новый стандарт.

Стандарт DVB-S2X по сути является расширением стандарта DVB-S2 и добавляет в него дополнительные технологические возможности и функции. DVB-S2X был официально выпущен как ETSI EN 302 307, часть вторая, первой частью которого является DVB-S2. Уже тот факт, что новый стандарт назван расширением существующего, говорит о том, что коренных изменений в его спецификацию не вносилось, а были добавлены лишь новые опции и улучшения.

Внесенные изменения изображены на рисунке 1, на котором продемонстрировано сравнение спектральной эффективности новой (DVB-S2X) и старой (DVB-S2) версий стандарта. На этом рисунке параметр «спектральная эффективность» использован для удобства сравнения их эффективности, так как этот параметр не зависит от полосы транспондера. При этом его легко конвертировать в пропускную способность канала, просто умножив на полосу транспондера.

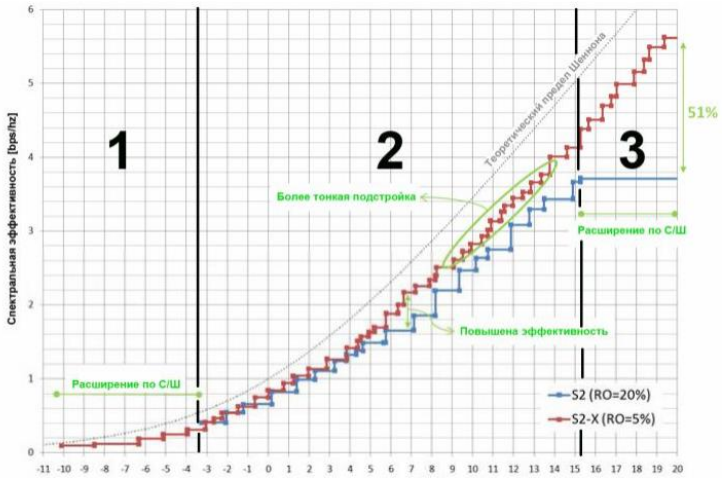


Рисунок 1- Отношение сигнал/шум [dB]

Рисунок условно разбит на три зоны: первая зона — сверхнизких отношений сигнал/шум, вторая — нормальных отношений сигнал/шум, зона 3 — высоких отношений сигнал/шум.

Учитывая, что практически все новые спутниковые DVB-приемники, выпущенные после 2014 года, поддерживают как DVB-S2, так и DVB-S2X, при создании новых спутниковых сетей практически безальтернативно использование нового стандарта. Однако уже существующим спутниковым операторам новый стандарт не предоставляет настолько существенных преимуществ, чтобы сподвигнуть их перейти на него и заменить все приемное оборудование у абонентов.

Новая спецификация стандарта DVB-S2X в области массового применения для DTH-систем имеет определенные преимущества, особенно для сервисов нового поколения (UHD, HEVC), что делает привлекательным его использование при реализации новых спутниковых проектов.

Список использованных источников:

1. Диденко, М. Datum взял лучшее от DVB-S2X // Технологии и средства связи/ специальный выпуск «Спутниковая связь и вещание− 2018». С. 36-37.

2. Быструшкин К. Второе дыхание DVB // «Телеспутник− 2017». С. 58-60.

3. Чулков В. DVB-S2X – теория и практика // «Телеспутник− 2017». С. 54-57.

ОСОБЕННОСТИ ТЕХНОЛОГИЙ ЦИФРОВОГО НАЗЕМНОГО ВЕЩАНИЯ ATSC 3.0

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

Галуза А.В.

Липкович Э.Б.. – к.т.н.,доцент

Организация ATSC (Advanced Televisions Systems Committee, Комитет передовых телевизионных систем) представила окончательную версию стандарта ATSC 3.0, применяемого для распространения программ наземного эфирного телевидения.

Новый стандарт должен обеспечить внедрение новых служб интерактивного телевидения на основе IP—технологий, развитие UHD-контента, персонализированных служб и служб экстренного информирования, а также доставку контента на различные устройства.

«С началом нового 2018 года для ATSC делает важный шаг на пути к внедрению платформы телевидения нового поколения, представляя набор стандартов ATSC 3.0, делающих возможным внедрение целого ряда продуктов и услуг. Первая в мире система телерадиовещания, основанная на использовании интернет—протокола, становится реальностью», — говорит президент ATSC Марк Ричер.

Основной целью физического уровня ATSC 3.0 является создание стандарта, дающего возможность передавать ТВ-контент на устройства как фиксированного, так и мобильного приёма. Приоритетными задачами также являются эффективное использование частотного спектра и повышение надёжности предоставляемых услуг. Так же приоритетными вопросами является поддержка высоких скоростей передачи данных, необходимых для предоставления услуг в новых стандартах – таких, как Ultra HD.

В настоящее время в перечне согласованных следующие базовые функции:

1) Модуляция на основе OFDM, с широким спектром защитных интервалов для смягчения многолучевости.
2) Коррекция ошибок (FEC) на основе LDPC с широким выбором скоростей кодирования в двух вариантах длины кода (поддерживает мобильный и фиксированный приём).
3) Широкий выбор размеров «созвездий».

Физический уровень ATSC 3.0 обеспечит широкий выбор возможных точек работы для передатчиков, каждая из которых – крайне близка к пределу Шеннона (теоретический предел, обуславливающий то, сколько информации можно передавать через канал с зашумлением), как показано ниже на Рисунке 1. Базовые эксплуатационные компромиссы включают в себя выбор меньшего количества передаваемых данных, большей надёжности услуги и/или большего количества передаваемых данных, меньшей надёжности услуги, либо промежуточного уровня.

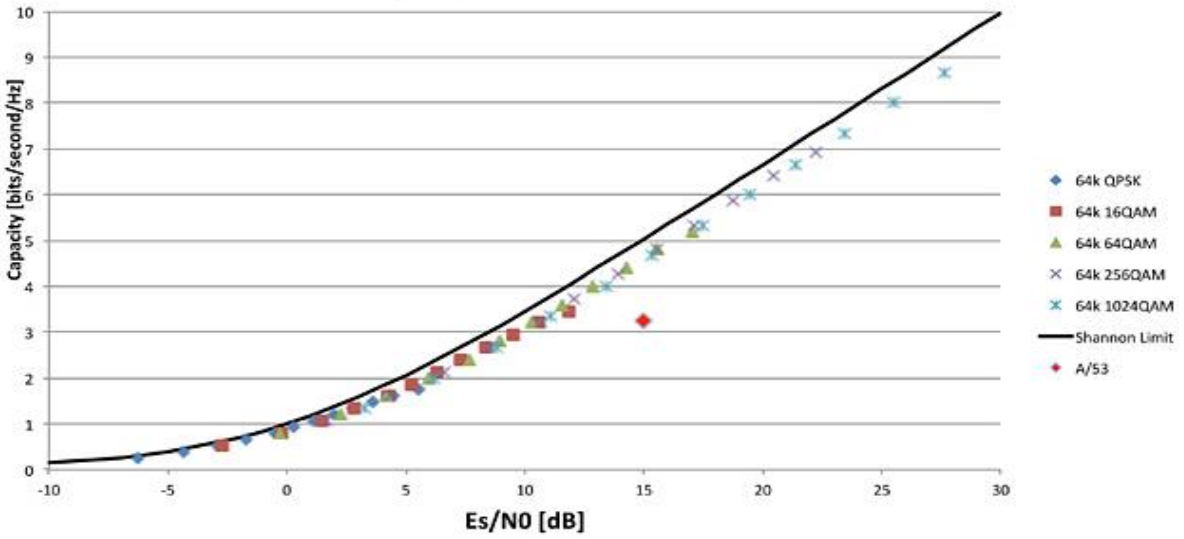


Рис. 2 – Пример кривой мощности для физического уровня ATSC 3.0

Передатчики имеют возможность выбирать рабочие точки и модуляции. Используя различные каналы физического уровня (PLP), можно одновременно использовать различные рабочие точки – к примеру, выделять часть пропускной полосы в передаваемом сигнале для нужд UHD, а остаток – для мобильных служб.

Краеугольным камнем системы цифрового вещания нового поколения – ATSC 3.0 DTV – стала гибкость в выборе услуг, включая возможность бесшовно для эфирных вещателей отправлять гибридный контент на мобильные и фиксированные приёмные устройства – объединяя таким образом в одно целое

эфирную трансляцию и передачу через широкополосные сети. Такие опции, как «мультипросмотр» и «многоэкранность» также являются чрезвычайно важными, как и опция выбора между стандартами разрешения – SD, HD и Ultra HD.

Использование в качестве транспорта IP-протокола (вместо MPEG-2, который использовался в предыдущих системах цифрового телевидения), обеспечивает широкую степень унификации с прочими механизмами доставки. Потоковый контент будет передаваться в виде пакетов (используя ISOBMFF в качестве формата контента), а не в виде непрерывного потока фрагментов.

На Рисунке 2 ниже можно увидеть пример стека протоколов для ATSC 3.0. В системе наблюдается унификация способов доставки через эфир и через широкополосные сети, особенно выше уровня протокола доставки, с полным слиянием на уровне приложений.

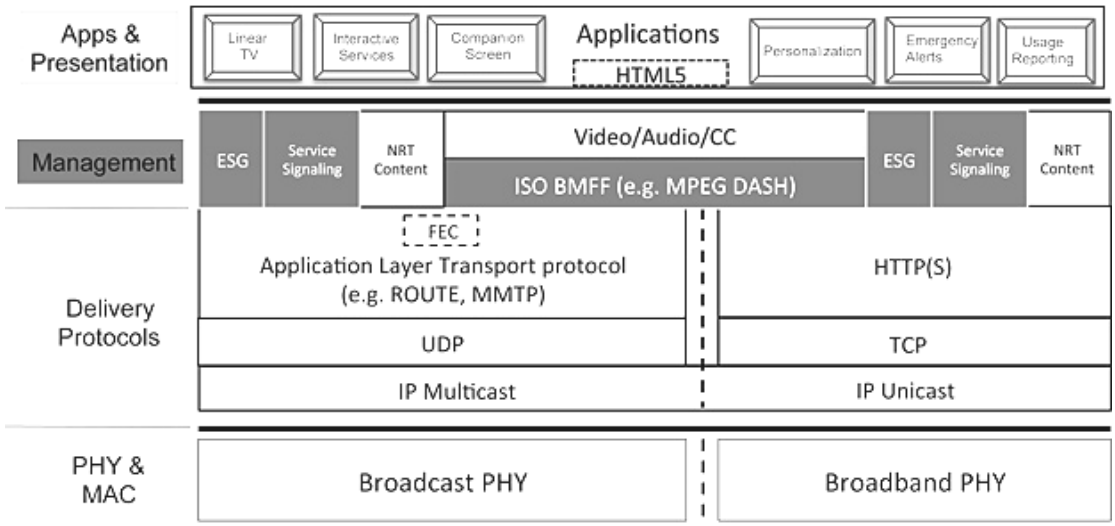


Рис. 3 – Пример модели стека протоколов для ATSC 3.0

В ряде ситуаций приемник может иметь доступ исключительно к не компрессированному аудио и видео; к примеру, через HDMI, подключённый к модему пользователя. Система автоматического распознавания контента (ACR) позволит ресиверу определить, что именно просматривается. Среди методов, применяемых в ACR, – системы «отпечатков пальцев» и «водяных знаков». ACR-совместимые приемники с широкополосным подключением могут запрашивать и получать через широкополосные каналы дополнительный контент из Интернета.

Для систем кодирования видео первоочередной задачей является создание систем работы с UHD и HD, с изначальной поддержкой 4K и возможностью поддержки 8K в будущем, через реализацию расширения. Кодек HEVC (H.265) был выбран в качестве основного кодека видео. Для кодирования аудио предлагаются к обсуждению новые функции, которые включают управление диалогом, использование альтернативных звуковых дорожек, а также смешивание вспомогательных аудио-служб, диалогов на другом языке, спецэффектов, комментариев и музыки. Кроме того, ожидается нормализация громкости контента и контуров динамического диапазона, основанная на специальных возможностях пользовательских устройств для мобильного или фиксированного приёма и уникальной звуковой среды. Рассматривается возможность внедрения функций, дающих большее ощущение погружения, с более высоким пространственным разрешением в локализации источников звука (азимут, подъём, расстояние), для увеличения ощущения от звукового окружения.

В целом, по энергетической эффективности для гауссовского канала, стандарт ATSC 3.0 превосходит DVB-T. Этот показатель очень существенный и обеспечивает запас для надёжного приёма ТВ программ. Несмотря на то что стандарт ATSC разработан под полосу частот 6 МГц, он легко модифицируется для полосы 7 и 8 МГц без изменения алгоритмов канального кодирования. В этой связи следует всесторонне изучить возможности стандарта ATSC для условий приема в Республике Беларусь и обратить внимание на опыт адаптации стандарта в Канаде, где частотное планирование ведётся на основе, близкой к европейской райсовской модели многолучевого сигнала.

Список использованных источников:

1. ATSC 3.0, Standard “ATSC 3.0 SYSTEM”.
2. Rich Chernock, “top 5” new features of ATSC 3.0.
3. ATSC Document A/53. ATSC Digital Television Standart.
4. ATSC Document A/54.Guide to the Use of the ATSC Digital Television Standard.
5. Dr. Yiyan Wu. “Performance Comparison of ATSC 8-VSB and DVB-T COFDM Transmission Systems for Digital Television Terrestrial Broadcasting.” Communications Research Centre Canada.

ОПТИМИЗАЦИЯ СЕТИ МОБИЛЬНОЙ СВЯЗИ

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

Хацкевич О.А. – к.т.н.,доцент

Повышение эффективности работы сети мобильного оператора связи является важной задачей при планировании, построении и дальнейшей модернизации сети. Актуальность данной работы заключается в первую очередь связана с тем, что в настоящее время в сетях сотовой мобильной связи Республики Беларусь возникает проблема перегрузки существующих ресурсов и оптимального распределения трафика, что вызвано постоянным ростом числа активных абонентов и увеличением перечня услуг, предоставляемых сотовыми операторами.

Следует отметить, что даже в настоящее время, несмотря на сформировавшееся разделение потребительского рынка между операторами мобильной подвижной связи, все равно между ними наблюдается довольно жесткая конкуренция и определенный процент абонентов постоянно "мигрирует" между поставщиками услуг сотовой связи. В следствии чего одним из критериев при выборе оператора мобильной связи является качество предоставляемых услуг. Качество обслуживания – комплексный показатель, который формируется путем оценки ряда статистических параметров, отражающих некоторые особенности эксплуатации сети при установлении соединения при входящем или исходящем вызовах, а также в процессе самого разговора между абонентами или использования той или иной неголосовой услуги. С точки зрения абонента наиболее существенны такие показатели, как доступность свободных каналов при дозвоне, качество передачи голоса на протяжении разговора, а также скорость передачи данных при использовании услуг передачи данных.

Одной из основных проблем распределения трафика является не только нехватка существующих ресурсов (каналов, приемопередатчиков базовых станций, потоков между базовыми станциями и коммутаторами), но и их неоптимальное использование, вследствие некорректной настройки эксплуатационных параметров оборудования, а также стремлением поставщиков услуг минимизировать издержки на расстановку и содержание необходимого количества базовых станций при обеспечении требуемого уровня сигнал/шум в пределах зоны покрытия.

Обеспечить качественную радиосвязь можно только при условии эффективного планирования, которое невозможно без использования многокритериальной оптимизации с учетом совокупности показателей качества. Во время создания и совершенствования сети мобильной связи решаются две неразрывно связанные задачи: планирование сети и оптимизация сети (перепланирование по результатам эксплуатации с целью повышения эффективности сети).

Планирование ССС включает три основных этапа:

– предварительное планирование;

– детальное планирование;

– планирование сотовой транспортной сети (трансмиссии).

На всех этапах планирования ССС необходимо принимать во внимание совокупность противоречивых требований к сети, которые можно строго учитывать, используя методы многокритериальной оптимизации.

На основе предварительных расчетов осуществляется непосредственно выбор позиций базовых стаций. В работе предлагается использовать стохастический подход для рационального выбора позиций. Целесообразность этого подхода обусловлена большим количеством случайных неконтролируемых факторов, влияющих на отношение сигнал/шум в точке приема. Для реализации метода была использована существующая сеть мобильной связи одного из городов брестской области.

Характеристику алгоритмов управления радиоресурсами и их параметры можно анализировать, используя основные рабочие показатели. В алгоритмы управления радиоресурсами входят хэндоверы, управление мощностью, планирование передачи пакетов, управление доступом и нагрузкой. Анализ работы сети производился с помощь программного обеспечения ZTE Netnumen. При расчёте основных технических параметров сети использовался алгоритм Окамура-Хата.

В работе рассмотрена общая методология многокритериальной оптимизации систем как взаимосвязанную совокупность методов формирования множества допустимых проектных решений, выбора подмножества Парето-оптимальных решений и сужения его до единственного проектного решения. Решение задачи выбора оптимального проектного варианта системы включает формирование множества допустимых вариантов системы, определение совокупности показателей качества, задание критерия оптимальности системы, а также выбор вариантов системы, оптимальных по заданному критерию оптимальности.

В ходе работы проведена комплексная отработка и оценка научно-технических решений для улучшения показателей сети. А также показано, что существующая схема, применяемая сотовыми операторами, является не самой удачной при оценке времени, затраченного на все этапы оптимизации. Результатом работы является законченная топология сети мобильного оператора, изменены показатели существующих базовых станций: углы направления секторов, значение мощностей радиопередатчиков, увеличения числа радиоканалов, а также перерассмотрен вопрос повторного использования частоты.

Список использованных источников:

1. Amaldi E., Capone A., Malucelli F. Radio planning and coverage optimization of 3G cellular networks. Wireless Networks, 2008, vol. 14, no. 4, pp. 435–447. doi:

2. Тихвинский В.О., Терентьев С.В. Управление и качество услуг в сетях GPRS/UMTS. – М:Эко-Трендз, 2007. – 400с.

54-я научная конференция аспирантов, магистрантов и студентов БГУИР, 2018 г

ВНЕДРЕНИЕ ТЕХНОЛОГИИ ПЕРЕДАЧИ ДАННЫХ ПО ЭЛЕКТРИЧЕСКОЙ СЕТИ 220 В 50 ГЦ HOMEPLUGAV (AV2)

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

Валицкая Е. Ю., Сакович Д. А.

Чепикова В. В. –ассистент

Стандарт HomePlug AV дает возможность передавать данные по электропроводке. С помощью специальных Powerline-адаптеров, мы можем построить сеть, в которой будут обмениваться данными разные устройства. Так же, как по Wi-Fi, или по сетевому кабелю. Только для передачи информации в Powerline сети используется электропроводка, которая есть в каждой квартире, доме, или офисе. В итоге, мы получаем подключение к интернету из розетки, по всему дому.

В 2000 году группа сетевых и электронных фирм, создали альянс HomePlug Powerline Alliance с целью стандартизировать powerline технологии для домашних сетей. Эта группа подготовила ряд технических стандартов названых «HomePlug». Первое поколение HomePlug 1.0, была завершена в 2001 году обеспечивала пиковую скорость 14 Мбит/с, стандарт второго поколения получил имя HomePlugAV, был введен в августе 2005 года, обеспечивал достаточную высокую пропускную способность для приложений, таких как HDTV и VoIP . HomePlug AV предлагает пиковую скорость передачи данных 200 - 500 Мбит/с. Спецификация HomePlugAV2 была введена в январе 2012 года, она совместим с HomePlug AV и поддерживает скорость до 1 Гбит/с.

В основе передачи информации по электропроводке лежит принцип частотного разделения сигнала (представлено на рисунке 1): высокоскоростной поток данных разбивается на несколько более медленных потоков, каждый из которых передается в отдельной полосе частот, накладываясь на несущую частоту 50 Гц (в США 60 Гц), и на другом конце линии объединяется в общий сигнал.

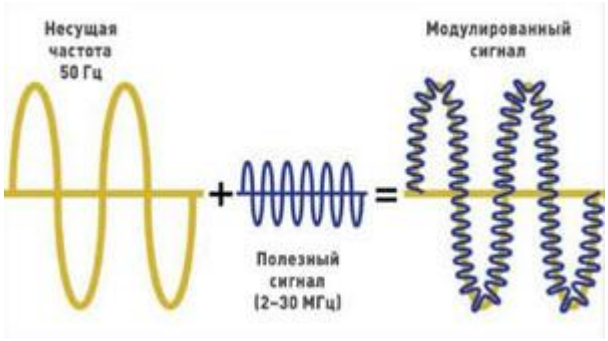


Рис. 1 –Частотное разделение сигнала

Для передачи данных выделена полоса частот, далеко отстоящая от 50 Гц, - частоты электротока. Чтобы обеспечить высокую скорость передачи данных используется широкий высокочастотный спектр: 4,3…20,9 МГц. Применяемый способ передачи данных – OFDM (orthogonal frequency division multiplexing). Он обеспечивает разделение большого потока данных на более мелкие и передачу каждого из них на своей частоте. Для повышения достоверности передачи используется избыточное кодирование. Сначала формируется спектр (комплексный) OFDM символа, потом при помощи обратного быстрого преобразования Фурье (ОБПФ) формируется его временная реализация. Между OFDM символами вставляется специальный защитный символ, который служит для предотвращения межсимвольной интерференции, возникающей из-за непостоянства канала по частоте. Для расшифровки сообщения, на приёмном конце используется соответственно прямое быстрое преобразование Фурье (БПФ). Используемый тип модуляции - дифференциальная квадратурная фазовая модуляция со сдвигом (DQPSK). Протокол доступа к среде (MAC) основан на базе метода коллективного доступа с обнаружением несущей и избежанием коллизий (CSMA/CA), - аналогично принятому в Ethernet[1].

Стандарт HomePlug подразумевает наличие двух и более powerline-адаптеров.Каждый адаптер HomePlug AV подключается к розетке, к нему с помощью сетевого кабеля Ethernet подключаются сетевые устройства (например: роутер, точка доступа, компьютер, ноутбук, телевизор). Если в доме/офисе используется сетевой маршрутизатор/роутер, один HomePlug адаптер может быть подключен к маршрутизатору, чтобы все устройства подключенные к HomePlug AV получили доступ в Интернет.

Для поддержки мобильных устройств, таких как ноутбуки, планшеты и смартфоны, некоторые адаптеры HomePlug, имеют Wi-Fi адаптер, таким образом ими можно расширить зону покрытия Wi-Fi сети[2].

Принцип построения сети по стандарту HomePlug AV отображен на рисунке 2:

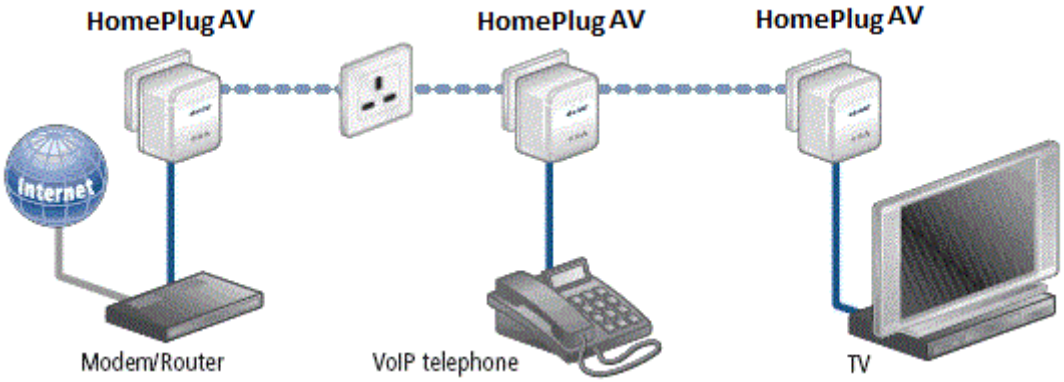


Рис. 2 – Построение сети через адаптерыHomePlug

Применение современных методов обработки сигналов и кодирования данных, которые давно и успешно используются в широкополосных беспроводных и проводных технологиях позволило достичь в технологии PLC**HomePlugAV** высокой скорости и достоверности передачи данных. Учитывая широкое распространение низковольтных электрических сетей, технология PLC**HomePlugAV** особенно привлекательна для использования в домашних сетях и небольших офисах[3].

Список использованных источников:

Технология HomePlug сетей и переспективы её развития [Электронный ресурс]. – Электронные данные. – Режим доступа: http://kunegin.com/ref6/hp/2.htm

Интернет/ локальная домашняя сеть через розетку. Технология HomePlug AV[Электронный ресурс]. – Электронные данные. – Режим доступа: http://pk-help.com/network/homeplug-av/

PLC-технологии. Часть 2[Электронный ресурс]. – Электронные данные. – Режим доступа:http://www.russianelectronics.ru/developer-r/review/2191/doc/47934/

КОМПЛЕКСНАЯ СИСТЕМА МОНИТОРИНГА И ХРАНЕНИЯ ИНФОРМАЦИИ О СОСТОЯНИИ ПАЦИЕНТОВ НА ОСНОВЕ ВИРТУАЛЬНОЙ ПЛАТФОРМЫ

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

Юницкая А.А.

Смирнов Ю.В. – ассистент

Мониторинг в реальном масштабе времени жизненно важных параметровимеет огромное значение для эффективного контроля состояния его здоровья и предупреждения болезней. Неоспоримые преимущества имеет лечение пациентов в домашних условиях, с одной стороны это выгодно государству, так как больной не находится в стационаре и соответственно не расходуются деньги на его содержание, с другой стороны пациенты находятся дома в привычной обстановке и ведут более активный образ жизни.

Система мониторинга и хранения информации о состоянии здоровья пациентов представляет собой информационную беспроводную систему, имеющую интерфейсы для сбора показателей здоровья пациента и передачи данных лечащему врачу в режиме реального времени для оперативного контроля физического состояния пациента. На теле человека устанавливается датчик, измеряющий положение и движения пациента, и устройства, измеряющие медицинские показатели (например, датчик измерения температуры тела, пульса, частоты дыхания и т.д.). Каждый из этих устройств имеет Bluetooth-интерфейс, по которому информация передаётся на смартфон. Эта информация передаётся в базу данных, доступ к которой врач может получить через веб-интерфейс.

Эти устройства становятся незаменимыми в случае неожиданного ухудшения состояния, вызванного, например, осложнениями в послеоперационном или реабилитационном периодах. При необходимости, персональные устройства связи могут быть оснащены системой для определения местоположения, что позволяет вместе с информацией о состоянии передавать медицинскому персоналу точные координаты пациента.

Области применения:

1. Долечивание – каждодневное измерение жизненно важных показателей для стабилизации здоровья;
2. Реабилитация – поддержание здоровья в домашних условиях в процессе или после лечения;
3. Хронические заболевания – самостоятельный контроль течения болезни и консультация в случае необходимости с врачом.

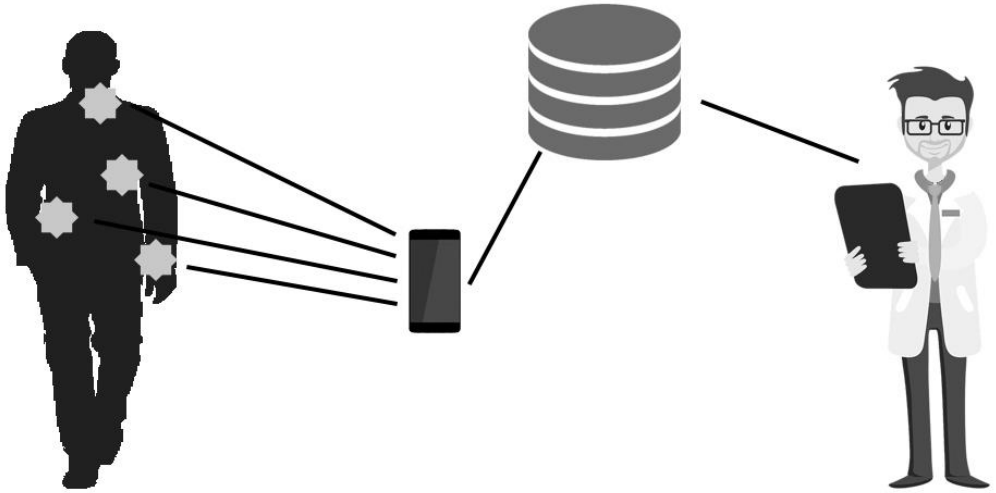


Рис. 1 – Схема передачи данных о состоянии пациента врачу

Преимущества такой системы:

– Получение объективных данных от пациента. Многие пациенты склонны переоценивать свое состояние в ответ на традиционный вопрос «Как Вы себя чувствуете?», в то время как автоматические сенсоры способны предоставить наиболее точную и объективную информацию;

- Обнаружение проблем со здоровьем на более раннем этапе;
- Снижение затрат на лечение несвоевременно диагностированных заболеваний;
- Непрерывный мониторинг — лечащий врач получает более подробные данные о состоянии пациента;
- Снижение нагрузки на медперсонал за счёт сокращения времени сбора информации о состоянии пациента;
- Возможность наблюдения за пациентом вне стационара, благодаря чему снижается стоимость обслуживания пациента;
- Уменьшение количества немотивированных визитов в поликлинику, вызовов врача на дом;
- Удобство для пациентов, проживающих далеко от медучреждения;
- Повышение трудового потенциала населения.

Основной недостаток — необходимость в приобретении дополнительных устройств, однако затраты на их покупку компенсируются за счёт исключения издержек, связанных с госпитализацией (нахождение в стационаре, транспортные расходы и т.п.). Также существует потенциал радиопомех (из-за погоды, других беспроводных устройств, или препятствий,таких как стены).

Применяя систему дистанционного наблюдения за больными, появляется возможность обнаружить нарушения в работе организма на более раннем этапе и появляется больше времени на анализ состояния пациента, благодаря чему повышается уровень качества оказания медицинских услуг. Благодаря уменьшению числа госпитализаций пациентов с хроническими заболеваниями, увеличивается качество их жизни. Процесс выздоровления проходит в домашних условиях, так же сохранение привычного образа жизни позволяет пройти обследование, либо реабилитацию тем, кто в обычных условиях отказался бы от этого.

Список использованных источников:

1. Морозова Е. В., Данилова Е. О. Дистанционный мониторинг за состоянием здоровья пациентов на базе беспроводной системы браслета ПКИД // Молодой ученый. — 2017. — №14. — С. 247-249.

Персональный телемониторинг в медицине [Электронный ресурс]. Режим доступа : http://sci-article.ru/stat.php?i=1394014915

АППАРАТНАЯ РЕАЛИЗАЦИЯ КОДЕКА КОДА РИДА-СОЛОМОНА

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

Дворников В.Д. – к.т.н.,доцент

Современные технологии хранения и передачи данных невозможны без эффективных средств их защиты от потерь. Одним из путей повышения помехоустойчивости систем передачи и обработай данных является использование помехоустойчивого кодирования и в частности циклического кода Рида-Соломона.

Коды Рида-Соломона (РС-коды) – недвоичные циклические коды, позволяющие исправлять ошибки в блоках данных. Применение РС-кодов при проектировании кодеков положительно влияет качественные характеристики устройства. Основой сложностью при проектировании кодека, является декодирование РС-кодов. Декодирование представляет собой решение сложной неоднородной математической задачи с применением нестандартной арифметики полей Галуа. В результате этого, программная реализация декодера РС-кода, как правило, имеет низкую скорость реализации. Поэтому в подавляющем числе случаев такой декодер реализован аппаратно в виде спецвычислителя. С развитием технологий в области цифровых интегральных схем, появилась возможность реализации РС-кодека с помощью программируемых логических интегральных схем (ПЛИС).

Принцип реализации декодера РС-кода представлен на рисунке 1:

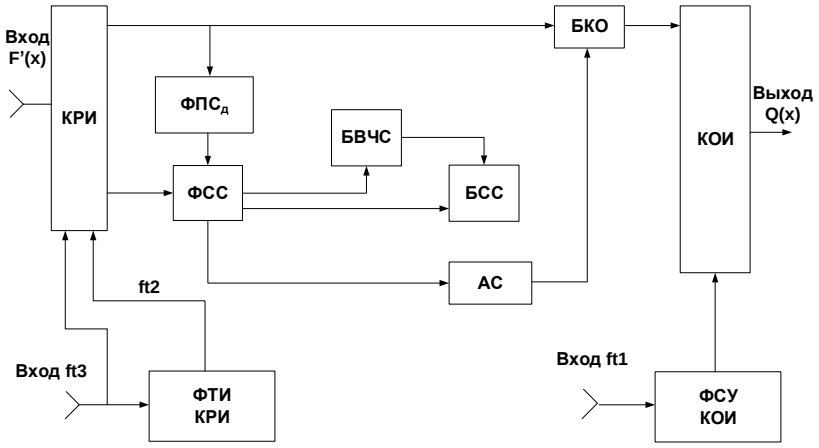


Рисунок 1. Структурная схема декодера РС-кода

Декодер состоит из следующих функциональных блоков:

- КРИ – коммутатор распределения информации на n параллельных подпотоков. Выполняется в виде последовательного и параллельного регистров сдвига;
- КОИ – коммутатор объединения информации параллельных подпотоков в последовательный поток. Выполняется в виде синхронного мультиплексора;
- ФПСд – формирователь проверочных символов декодера. Выполняется в виде совокупности сумматоров по модулю два, входы которых подключаются к информационным цепям в соответствии с проверочной матрицей;
- ФСУ – формирователь сигналов управления и ФТИ (формирователь тактовых импульсов (КРИ строятся из кольцевого двоичного счетчика;
- ФСС/ БВЧС – формирователь синдромных символов и блок вычисления частных синдромов. Выполняются в виде схем контроля четности;
- БКО – блок коррекции ошибок. Выполняется в виде сумматоров по модулю 2;
- БСС – блок сравнения синдромных символов и символов частных синдромов. Состоит из схем контроля четности и логических элементов И-НЕ;
- АС – анализатор синдрома. Формирует вектор коррекции модуля ошибок.

Реализация рассмотренной схемы декодера с помощью ПЛИС, позволит решить проблемы присущие кодерам реализованным программным методом. Основным достоинством данного метода реализации является существенное повышение быстродействия роботы кодека. А также появляется возможность перенастройки алгоритма работы устройства, уже после введения в эксплуатацию.

Список использованных источников:

1.Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. – М.: Техносфера, 2006. – 320 с.

2.Золотарев В.В., Овечкин Г.В. Помехоустойчивое кодирование. Методы и алгоритмы / под ред. чл.-кор. РАН Ю.Б. Зубарева. – М.: Горячая линия – Телеком, 2004. – 126 с.

АНАЛИЗ МЕТОДОВ СЕГМЕНТАЦИИ

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

Ермак А.В.

Лагутин А.Е. – к.т.н.,доцент

В настоящее время наблюдается бурное развитие систем автоматической обработки изображений, требующие применения новейших методов обработки, включая предварительную обработку изображений. К методам, используемых в таких системах, предъявляются требования по степени автоматизации, качеству и, особенно, скорости обработки, т.к. большинство таких систем работают в режиме реального времени. Разработка эффективных методов предварительной обработки изображений является актуальной проблемой, которая способствует появлению более совершенных систем мониторинга, охранного телевидения, видеонаблюдения, медико-биологических и других систем.

Предварительным этапом любой системы анализа и обработки изображений является сегментация изображений. Она позволяет оперативно выделить интересующие объекты на изображении от фона и других объектов, определить размер, форму, положение объекта, преобразовать изображение к виду, удобному для дальнейшей обработки автоматическими системами и эффективного решения задач более высокого уровня, таких как распознавание образов и анализ сцен. Неточная, недостаточная или избыточная сегментация может привести к возникновению ошибок на следующих этапах обработки изображения.

Метод выделения контуров

При таком способе сегментации объекты представляются их границами. Граничными принято считать точки резкого перепада функции яркости. Для нахождения граничных точек используется численное дифференцирование. Наиболее распространенным является градиентный метод. Применяя маску (фильтр) к изображению, получают так называемое изображение градиентов. Оно отличается от исходного подчеркнутыми перепадами яркости. Точка (i,j) принадлежит контуру, если яркость изображения градиентов превышает некий порог, который может определиться по гистограммам.

Пороговый метод.

Пусть задано изображение B(i,j), s=1 (один объект), яркость точек находится в пределах $[T_1, T_2]$, а яркости точек фона в этот отрезок не входят. Если $B(i,j) \in [T_1, T_2]$, то точку (i,j) считаем принадлежащей области объекта, в противном случае — области фона. В случае s>1 должны быть известны отрезки $[T^k_1, T^k_2]$, в пределах которых находятся яркости k-х объектов. Эти отрезки не должны пересекаться. Разметка точек осуществляется с помощью отображения. Проблемой является определение пороговых величин. Для этого производится анализ гистограммы яркостей. В случае с одним объектом (s=1) на гистограмме должно быть два максимума. Порог выбирается между этими двумя максимумами. На практике применяются более сложные методы построения и анализа гистограммы.

Волновой метод.

После выбора стартовых точек проводится процесс, состоящий из итераций. На каждой из итерации рассматриваются точки множеств S_i, кроме тех, что были включены в S_i на данной итерации. для точки (i,j) рассматриваются её соседние точки. Одной из них может быть присвоена метка 8_i. После того как анализ выполнен для всех точек множества S_i, кроме тех, что были добавлены на данной итерации, производится анализ точек из S_{i+1}. Точки множества S_i добавленные на k-й итерации, называются фронтом $F_k(8_i)$, объединение $\cup F_k(8_i)$ называется волной. 1

Слияние - расщепление.

Метод состоит в разбиении изображения на квадраты некоторым образом. Затем проводится анализ однородности этих квадратов, чаще всего анализируется однородность яркостей. Если квадрат не удовлетворяет условию однородности, то он заменяется четырьмя подквадратами. Если же участок из четырёх соседних квадратов оказывается таким, что для него выполняется условие однородности, то эти четыре квадрата объединяются в один. Результатом слиянии - расщепления может служить некоторая структура с информацией о квадратах, чаще всего - граф, может быть и изображение, в котором все пиксели внутри однородной области имеют одинаковую яркость.

Критерии оценки результатов.

Оценивать методы с точки зрения их применения в системах компьютерного зрения можно по качеству подавления фона и выделения объектов в виде связных областей. Поскольку понятие "объект" в общем случае формализовано не до конца и априорная информация минимальна, то нельзя требовать точного выделения объекта, состоящего из нескольких частей разной яркости как одной связной области. Должны быть выделены по крайней мере ключевые части объекта, необходимые для его распознавания.

Список использованных источников:

1. Сравнительный анализ методов сегментации. [Электронный ресурс]. – Режим доступа: http://www.docme.ru/doc/1459014/2230.sravnitel._nyj-analiz-metodov-segmentacii-izobrazhenij/.
2. Панченко Д.С. Сравнительный анализ методов сегментации изображений // Д. С. Панченко, Е.П. Путятин // Радиоэлектроника и информатика. – 1999. – №4. – С.109–114.
3. Сравнительный анализ методов сегментации изображений [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-metodov-segmentatsii-izobrazheniy/.

ЭФФЕКТИВНОЕ КОДИРОВАНИЕ ГИПЕРСПЕКТРАЛЬНЫХ ИЗОБРАЖЕНИЙ

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

Мирончик Д.Ю.
Новицкий В.В. – инж.-констр. 2-й кат. ОАО «Пеленг»

Дистанционное зондирование Земли (ДЗЗ), т.е. наблюдение поверхности Земли авиационными и космическими средствами, представляет собой незаменимый инструмент, применяемый в сельском, лесном, водном хозяйствах, экологии и геологии. Более того, система ДЗЗ – это пример сети с ограниченной пропускной способностью, требующей алгоритм сжатия изображений, который обладал бы высоким коэффициентом сжатия.

Гиперспектральная съёмка – это весьма перспективный метод ДЗЗ. Её целью является определение спектральных характеристик объектов земной поверхности за счёт их отражающей способности. Результатом такой съёмки является гиперспектральное изображение (ГСИ), называемое также «гиперкубом». «Слои» ГСИ представляют собой изображение одного и того же участка земной поверхности в различных узких участках спектра.

Современные гиперспектральные системы могут фиксировать несколько сотен спектральных каналов (в данном конкретном случае их 224), расположенных в широком диапазоне, который включает как видимую область, так и инфракрасную, а количество строк в получаемых изображениях может достигать нескольких тысяч. Как следствие, полный объём ГСИ измеряется в гигабайтах, что обуславливает необходимость их сжатия ещё на борту носителя, до передачи на Землю.

Стандартные алгоритмы сжатия изображений рассчитаны на двумерные, привычные нам изображения. С помощью таких алгоритмов вполне возможно сжать и ГСИ, рассматривая его как набор из 224-ёх различных изображений, сжимаемых независимо друг от друга, но такой подход не учитывает целостность гиперкуба как трёхмерного массива данных.

Таким образом, очевидной становится задача распространения двумерных алгоритмов сжатия изображений на трёхмерный случай и проверки предположения о том, что таким образом можно заметно повысить коэффициент сжатия.

Изображения как структуры данных обладают двумя типами избыточности: психовизуальной и статистической. Первая принимается во внимание при сжатии с потерями – в этом случае пренебрегают той частью информации, отсутствие которой попросту не будет заметно для человека. Но так как сжатие с потерями не является предметом рассмотрения данной работы, следует сосредоточиться на втором типе избыточности.

Статистическая избыточность обусловлена коррелированностью смежных пикселей изображения – соседние пиксели с большой долей вероятности имеют либо одинаковые, либо близкие уровни яркости. Её резкие скачки наблюдаются только вблизи контуров, границ.

Очевидно, что для сжатия изображений первым делом необходимо разрушить эту избыточность, т.е. произвести т.н. декорреляцию его пикселей, для чего применяется дискретное вейвлет-преобразование (ДВП). А так как ГСИ являются трехмерными массивами данных, они имеют (по сравнению с обычными изображениями) дополнительное, третье измерение избыточности. Как следствие, применять следует именно трёхмерное ДВП – это первое изменение, которое необходимо внести в стандартные алгоритмы.

Прочие изменения касаются специфических особенностей конкретных алгоритмов. SPECK3D, в отличие от классического SPECK, оперирует трёхмерными множествами S. Для FBQT3D был разработан трёхмерный вариант Z-развёртки, а для JPEG2000-3D – развёртка трёхмерного блока данных в двумерный.

В рамках данного исследования проводилось сжатие небольших фрагментов ГСИ размером 256x256x224 (см. рис. 1) как двумерными, так и трёхмерными алгоритмами.

Рис. 1 – RGB-представление ГСИ Clinton и Maui

Итогом всей работы является заметное повышение коэффициента сжатия (CR) и подтверждение исходного предположения.

Таблица 1 – Полученные результаты

ДВП	Двумерное ДВП пятого уровня каждого спектрального канала			Трёхмерное ДВП пятого уровня по всему объёму куба		
Алгоритм	SPECK	FBQT	JPEG2000	SPECK3D	FBQT3D	JPEG2000-3D
Clinton, CR	1.79	1.84	1.82	2.09	2.19	2.29
Maui, CR	2.81	2.92	2.94	3.07	3.34	3.47

Список использованных источников:

1. Гиперспектральное дистанционное зондирование в геологическом картировании / В. Л. Щербаков [и др.]. – Москва : Физматлит, 2014. - 134 с.

2. Гонсалес Р. Цифровая обработка изображений. / Р. Гонсалес, Р. Вудс. – Пер. с англ. − Москва. – Техносфера, – 2006. − 1072 с.

3. Сэломон, Д. Сжатие данных, изображений и звука / Д. Сэломон. − Москва: Техносфера, 2004. – 368с.

4. Новицкий В.В., Цветков В.Ю. Сжатие полутоновых изображений на основе кластеризации и прогрессивного вложенного кодирования вейвлет коэффициентов / В.В. Новицкий, В.Ю. Цветков // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы междунар. научно-технич. семинара. Минск, апрель–декабрь 2015 г. – Мн.: БГУИР, 2015. – С. 45-51.

CASCADED CLASSIFIER FOR LICENSE PLATE DETECTION

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Losiukov L.N.

Volkov K.A. – PhD, docent

License Plate Recognition (LPR) has found numerous applications in various areas. It can be used for automatically identifying vehicles in a car park, for vehicle access control in a restricted area and for detecting and verifying stolen vehicles. A LPR system consists of two major components: license plate detection and character recognition. The first step of license plate detection is classifier training at which a six-layer cascade classifier is constructed.

As shown in [1], the basic idea of the detection algorithm is to use a variable scanning window moving around on the input vehicle image. At each position, the image area covered by the scanning window is classified using a pre-trained classifier as either a license-plate area (a positive decision) or a non-license-plate area (a negative decision). The classifier used in this algorithm is a significant extension of Viola and Jones' work shown in [2] to license plate detection.

In this algorithm, a six-layer cascaded classifier is constructed to increase the detection speed, in which the first two layers are based on global features and the last four layers are based on local Haar-like features. The classification process can be taken as a degenerate decision tree containing multi-layer classifiers as shown in Fig. 1. A positive result from the first classifier triggers the evaluation of a second classifier. A positive result from the second classifier triggers a third classifier, and so on. A negative outcome at any layer leads to the immediate rejection of the image region (block). In other words, those image regions that are not rejected by the initial classifier will be processed by a sequence of classifiers. If any classifier rejects a selected image region, no further processing will be performed for this region. It is commonly seen that, for a given vehicle image, the majority of evaluated image regions are negative. Therefore, the cascaded classifier shown in Fig. 1 attempts to reject as many negatives as possible at the earlier stages. As its consequence, this cascaded classifier leads to fast license plate detection. It is also worth to note that the detection algorithm (classifier) acts on the vertical edge maps of input vehicle images rather than on the raw image intensity values. This further enhances the efficiency of the cascaded classifier.

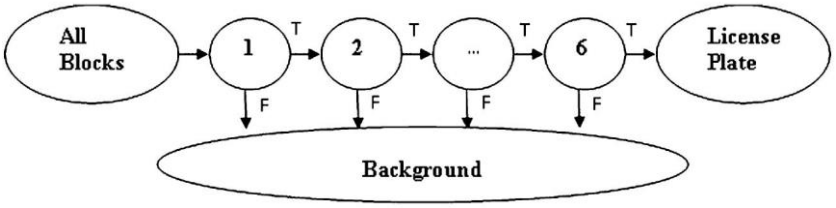


Fig. 1 - Process of constructing a cascaded classifier

In the following, the algorithm is described in two aspects: training and testing. Training is a process that the classifier is learning to make correct decisions using pre-classified samples. Testing is a process to use the pre-trained classifier to classify individual image blocks.

To obtain the cascaded classifier which can make correct decisions, pre-classified positive samples (images containing license plates) and negative samples (images containing non-number-plates) are selected for training.

The individual classifiers that together construct the cascaded classifier are trained independently. Recall that the classifiers on the first two layers are based on global features, and the classifiers on the other four layers are based on local Haar-like features.

To train the classifier on the first layer, the value of the first global feature, called Edge Density, is computed for each input sample. Statistical methods are used to select a threshold that can correctly classify all positive samples (i.e., using the selected threshold, the edge densities of all positive samples are on the "positive" side). Note that the threshold is not unique. Also note that, for a given threshold, some negative samples may be wrongly classified as "positive", i.e., some non-number-plate blocks may be classified as a "license plate". These are referred as false positives. Hence, a threshold which can correctly classify all positive samples and produce the least number of false positives is selected.

For the second layer classifier, another global feature is employed. It is called the Edge Density Variance. All input samples used to train the classifier on the second layer are from "positive" classification outcomes using the first classifier after training. Since the false positive rate of the first classifier is usually non-zero, samples which are classified as "positive" by the first classifier contain both real positive samples and some negative samples. By properly selecting another threshold based on the second global feature, we can classify all positive samples as "positive" and produce minimum false positives. The classifier on the second layer based on the second global feature is thus obtained. Again, the training of the second classifier is implemented using statistical methods similar to those used for the first classifier.

Similarly, the samples used to train the classifier on the third layer are those samples which are filtered as "positive" by the classifiers on the first two layers. Unlike the first two layers, which are both based on global

features, the classifiers on the third through sixth layers are all based on local Haar-like features. We will find that, within any image area (region), the total number of Haar-like features is very large and much larger than the total number of pixels within the area. To ensure fast classification, the AdaBoost learning algorithm is used to select best-performing classifiers (called weak classifiers), each based on a Haar-like feature, and to combine these multiple weak classifiers to construct one classifier (referred as strong classifier). This procedure is completed in multiple rounds. In each round, an optimal weak classifier is selected. The AdaBoost algorithm introduces a weight for each sample. Through continuously increasing the weights of “hard” samples in each round and selecting the corresponding best-performing weak classifiers until the constructed strong classifier meets the predefined accuracy requirement, a strong classifier is then constructed and the training on this layer is finished.

Similarly, the samples classified as positive ones by the third layer are input to the fourth layer, and so forth. Finally, a six-layer cascade classifier is constructed.

Since both global and local features in this algorithm are generated from vertical edge maps of input images, the vertical edge maps of images are computed first before any feature is extracted.

References:

1. Huaifeng Zhang, Wenjing Jia, Xiangjian He, Qiang Wu, Learning-based license plate detection using global and local features, in: Proceedings of the 18th International Conference on Pattern Recognition (ICPR 2006), vol. 2, 2006, pp. 1102-1105.

2. Paul Viola, Michael J. Jones, Robust real-time face detection, Int. J. Comput. Vis. 57 (2004) 137-154, http://dx.doi.org/10.1023/B:VISI.0000013087.49260.fb.

IP-ТЕЛЕФОНИЯ НА ОСНОВЕ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ СП «МАЗ-МАН»

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

Корякина О.С.

Курилович А.В. - ст. преподаватель

В настоящее время IP-телефония всё больше и больше распространяется, постепенно вытесняя традиционную телефонию, так же как когда-то мобильный телефоны вытеснили стационарные. IP-телефония помогает существенно сократить расходы на связь, что не мало важно для бизнеса на начальном этапе. Но если дело касается готового бизнеса и существующей телефонной сети предприятия, стоит ли переходить на IP-телефонию? Давайте разбираться.

Итак, IP-телефония — телефонная связь по протоколу IP. Под IP-телефонией подразумевается набор коммуникационных протоколов, технологий и методов, обеспечивающих традиционные для телефонии набор номера, дозвон и двустороннее голосовое общение, а также видеообщение по сети Интернет или любым другим IP-сетям [1].

Достоинства использования IP-телефонии [2]:

1) Низкая стоимость эксплуатации;
2) Универсальность;
3) Расширяемость;
4) Масштабируемость;
5) Гибкость;
6) Мобильность.

Недостатки IP-телефонии [2]:

1) Дорогое оборудование, если АТС физическая;
2) Возможны сбои в работе программы, если АТС программная;
3) Сложность (отсюда и высокая цена) первоначальной настройки АТС;

Как видно из изложенного выше материала, достоинств несомненно больше, поэтому нет ничего удивительного в том, что предприятия охотно переходят с традиционной (аналоговой) телефонии на цифровую. Когда дело касается уже существующей ЛВС поверх, которой будет идти IP-телефония, нет необходимости закладывать дополнительные розетки для IP-телефонов, их можно включить в сеть между компьютером и розеткой, через которую компьютер связан с локальной сетью (рисунок 1а), если есть свободные розетки, то можно телефон и компьютер подключить в разные (рисунок 1б).

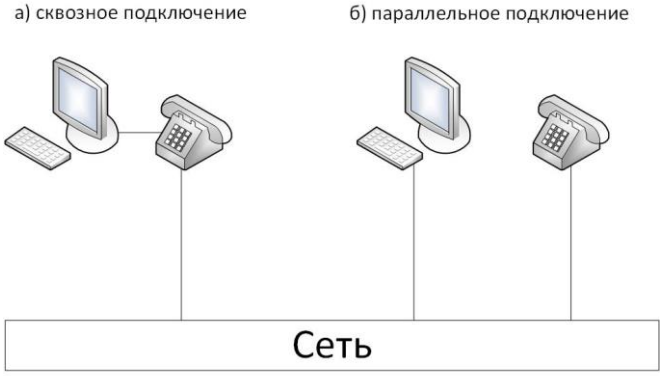


Рис 1 – Схемы подключения IP-телефонов в сеть

При сквозном подключении необходимо учитывать максимальную скорость соединения, которую может поддерживать телефон, чтобы он не стал «бутылочным горлышком» и не уменьшил скорость обмена данными компьютера и локальной сети. Также на компьютер необходимо установить программу, которая позволит телефону и компьютеру иметь один и тот же IP-адрес. Также при такой схеме в случае сбоя или выхода из строя какого-либо из элементов, сеть перестанет видеть всю ветку, при параллельном подключении таких проблем не возникнет, но в этом случае необходимо, чтобы были две розетки.

Из всего выше сказанного, делаем вывод, что IP-телефония достойная замена аналоговой, но это не значит, что стоит аналоговые АТС отправить на покой. У аналоговой АТС есть преимущество перед цифровыми: для поддержания работоспособности аналоговой телефонной сети в случае отключения электричества, источник бесперебойного питания надо ставить только на АТС, при IP-станции – на каждый элемент сети. Каждая из систем имеет свои преимущества и недостатки – значит каждая из них имеет право на существование.

Список использованных источников:

1. IP-телефония [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/IP-телефония
2. Преимущества IP телефонии [Электронный ресурс]. Режим доступа:http://linux.mixed-spb.ru/asterisk/ip_telephony_advantages.php

АВТОМАТИЗАЦИЯ ТЕСТИРОВАНИЯ WEB-ПРИЛОЖЕНИЙ НА ОСНОВЕ СРЕДСТВ КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИИ И НЕПРЕРЫВНОЙ ИНТЕГРАЦИИ

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

Бобов М.Н. – д.т.н.,профессор

В настоящее время каждый день появляются новые web-приложения, которые построены на различных платформах и написаны на разнообразных языках программирования. Вместе с этим растут требования, предъявляемые к приложениям и всё большую роль, играет обеспечение качества для каждой из систем. Наиболее важным направлением здесь является внедрение различных систем автоматизированного тестирования. Получающие всё большее распространение технологии контейнерной виртуализации и непрерывной интеграции в разработке ПО требуют от систем автоматизированного тестирования соответствующей эволюции, которая бы позволила в кратчайшие сроки наладить процесс тестирования ПО.

Автоматизация тестирования – использование программного обеспечения для осуществления или помощи в проведении определенных тестовых процессов, например, управление тестированием, проектирование тестов, выполнение тестов и проверка результатов [1].

Непрерывная интеграция (англ. Continuous Integration) — это практика разработки программного обеспечения, которая заключается в выполнении частых автоматизированных сборок проекта для скорейшего выявления и решения интеграционных проблем [2].

Контейнеризация — это подход к разработке программного обеспечения, при котором приложение или служба, их зависимости и конфигурация (абстрактные файлы манифеста развертывания) упаковываются вместе в образ контейнера. Контейнерное приложение может тестироваться как единое целое и развертываться как экземпляр образа контейнера в операционной системе узла [3].

Для эффективной реализации автоматизированного тестирования создаются тестовые фреймворки, представляющие собой наборы библиотек и готовых программных модулей, полностью определяющий внутреннюю структуру разрабатываемого приложения [4]. Фреймворк позволяет автоматизировать рутинные операции, связывать между собой различные части системы и разные приложения. Внутрь контейнера помещается сервер непрерывной интеграции и окружение для тестирования (например, браузеры). Общая схема такого подхода представлена на рисунке 1.

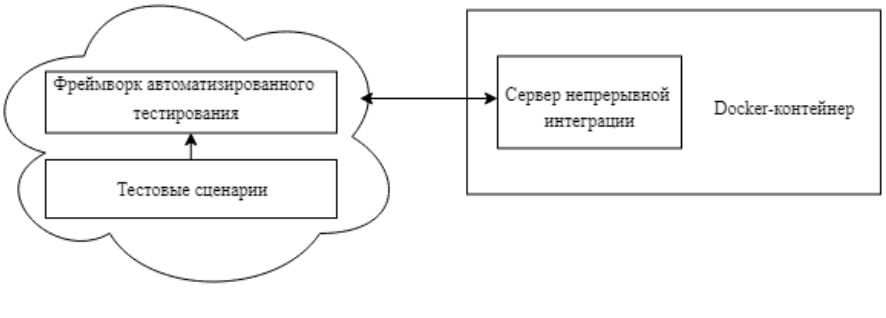


Рис. 1 – Система автоматизированного тестирования на основе средств контейнерной виртуализации и непрерывной интеграции

Реализация такой схемы предоставляет такие преимущества, как изоляция, переносимость, гибкость, масштабируемость и контроль, на протяжении всего жизненного цикла приложения. Самым важным преимуществом является изоляция среды разработки от среды тестирования и возможность запуска тестов на удаленном сервере.

Обычно, автоматизированное тестирование учитывает следующие особенности web-приложений: – кроссплатформенность, т.е. работа их на таких платформах как Windows, macOS, Android, iOS; – кроссбраузерность, т.е. работа приложений в различных браузерах (Chrome, Mozilla Firefox, Internet Explorer, Safari, Egde); – многокомпонентость, т.е. web-приложения состоят из множества компонентов, таких как серверы баз данных, серверы приложений, web-серверы [5]. Исходя из поставленных задач, для хранения фреймворка и сценариев могут использоваться различные системы контроля версий (Git, SVN, Mercurial). В качестве сервера непрерыной интеграции можно использовать Jenkins, TeamCity, Travis CI и др. Docker используется для для автоматизации развёртывания и управления приложениями в среде виртуализации на уровне операционной системы. Позволяет «упаковать» приложение со всем его окружением и зависимостями в контейнер.

Список использованных источников:

1. Автоматизированное тестирование программного обеспечения. Внедрение, управление и эксплуатация. // Д. Рэшка, Д. Пол, Э. Дастин М: ЛОРИ, 2003 – 576с.
2. Jenkins Continuous Integration Cookbook – Second Edition // Alan Mark – Packt Publishing Ltd, 2015 – 408 с.
3. Использование Docker // Эдриен Моуэт – O'Reilly Media, 2017 – 354 с.
4. TestNG Beginner's Guide. // Varun Menon –Packt Publishing Ltd, 2013 – 276 с.
5. Куликов, С. С. Тестирование программного обеспечения. Базовый курс : практ. пособие. // С. С. Куликов. – Минск: Четыре четверти, 2015. — 294 с

ПРИМЕНЕНИЕ ПРОТОКОЛА IPSEC ДЛЯ ЗАЩИТЫ СЕТЕВОГО ТРАФИКА

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

Сороко М.В.

Астровский И.И. – к.т.н., доцент

Обеспечение информационной безопасности компьютерных сетей возможно при создании системы защиты не для отдельных классов приложений, а для сети в целом. Применительно к компьютерным сетям это означает, что системы защиты должны действовать на сетевом уровне модели открытых систем. Преимущество такого выбора заключается в том очевидном факте, что в компьютерных сетях именно сетевой уровень отличается наибольшей гомогенностью: независимо от вышележащих протоколов, физической среды передачи и технологии канального уровня, транспортировка данных по сети не может быть произведена в обход протокола IP. Для этих целей в компьютерных сетях принято использовать протокол IPSec. Впервые протокол официально стандартизирован Целевой группой Internet Engineering Task Force (IETF) в 1995 году и по-прежнему используется в корпоративных сетях, благодаря гибкой настройке и управлению политиками.

Благодаря реализации протокола обеспечивается конфиденциальность и целостность информации. IPSec включает протоколы для установления взаимной аутентификации между агентами в начале сеанса и согласование криптографических ключей, которые будут использоваться во время сеанса. IPsec может использоваться для защиты потоков данных между двумя хостами (хост-хост), между двумя шлюзами безопасности (сеть-сеть) или между шлюзом безопасности и хостом (от сети к хосту). IPsec использует криптографические алгоритмы безопасности для защиты соединения по сетям IP, поддерживает аутентификацию источника данных, целостность данных, конфиденциальность данных.

Протокол поддерживает сквозную схему безопасности, работая на сетевом уровне, в то время как другие системы безопасности в Интернете, такие как Transport Layer Security (TLS) и Secure shell (SSH), работают в верхних слоях на транспортном уровне и прикладном уровне соответственно. Следовательно, только IPsec защищает весь трафик приложений по IP-сети [1].

IPSec использует фильтрацию IP для определения того, какой трафик должен быть защищен. Специальный тип действия фильтра указывает на разрешение трафика. IP-фильтры представляют политику безопасности, указывая трафик, требующий шифрования. Фильтры также используются для определения исходящей ассоциации безопасности IPSec и для проверки того, что входящий трафик получен с использованием правильной ассоциации безопасности [2].

Большинство реализаций протокола IPSec имеют несколько компонентов. Основной протокол IPSec реализует протоколы аутентификации (Authentication Header, AH), шифрования (Encapsulated Security Payload, ESP), отвечающим за шифрование содержимого отдельных пакетов, протоколы обмена ключами (Internet Key Exchange, IKE), предназначенные для согласования используемых алгоритмов аутентификации и шифрования, ключей и продолжительности их действия, а также для защищенного обмена ключами [3].

Протоколы AH или ESP передают данные в двух режимах: туннельном, при котором IP-пакеты защищаются целиком, включая их заголовки, и транспортном, обеспечивающим защиту только содержимого IP-пакетов. Основным режимом является туннельный. В туннельном режиме исходный пакет помещается в новый IP-пакет, и передача данных по сети выполняется на основании заголовка нового IP-пакета. При работе в этом режиме каждый обычный IP-пакет помещается целиком в шифрованном виде в конверт IPSec, а тот в свою очередь инкапсулируется в другой защищенный IP-пакет.

Реализация комплекса IPSec в компьютерных сетях необходима в следующих вариациях:

-Обеспечение безопасного подключения к интрасети предприятия через Интернет

-Предоставление возможности удаленного доступа через Интернет

-Установление защищенного соединения с партнерами

-Безопасное проведение транзакций в системах электронной коммерции

-Настройка политик безопасности для соединений клиент-сервер

Главная особенность протокола заключается в том, что IPSec способен поддерживать все приложения и может шифровать или аутентифицировать весь трафик на уровне IP. Это обеспечивает безопасность для всех приложений, которые используются в сети ежедневно.

Список использованных источников:

1. IPSec [Электронный ресурс] – Режим доступа: https://www.opennet.ru/docs/RUS/vpn_ipsec/
2. Информационная безопасность и защита // В. Ф. Шаньгин – 2014
3. IP Security (IPsec) and Internet Key Exchange (IKE) // RFC 6071 – 2011

МЕТОДЫ СЕГМЕНТАЦИИ В СИСТЕМАХ РАСПРЕДЕЛЕНИЯ МУЛЬТИМЕДИЙНОЙ ИНФОРМАЦИИ

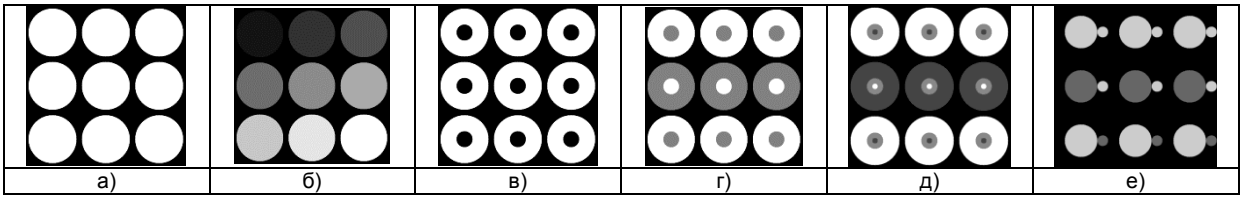
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ловецкий М.Ю.
Рабцевич В.В. — асс. каф. ИКТ

В области атомно-силовой микроскопии очень важной задачей всегда являлась необходимость выделения на изображениях интересующих объектов, что породило необходимость в использовании алгоритмов сегментации изображений, однако существующие сегодня широко распространенные алгоритмы либо допускают весьма заметные ошибки, либо тратят очень много машинного времени на сегментацию, что указывает на необходимость создания новых, более эффективных, алгоритмов сегментации изображений. Одним из таких алгоритмов является алгоритм регрессивного волнового выращивания областей.

Алгоритм регрессивного волнового выращивания областей (РВВО) — алгоритм, разработанный специально для сегментации изображений, полученных с атомно-силового микроскопа, основанный на присоединении к областям новых элементов с учетом их уровня квантования. Работа данного алгоритма сводится к проверке всех возможных уровней изображения на наличие точек и присвоении им номера сегмента, к которому принадлежит точка, основываясь на наличии соседних точек, которым уже присвоен номер.

Данный алгоритм, а также несколько альтернативных алгоритмов, были протестированы на тестовых изображениях, изображенных на рисунке 1. Данное тестирование сводится к определению времени, затраченное на сегментацию, и значений нормированных ошибок сегментации. В качестве альтернативных алгоритмов были выбраны следующие — маркерного водораздела (МВ), выращивания областей (ВО), Винсента-Солли (ВС). Значения нормированных ошибок сегментации получались как отношение количества точек, которые были неправильно различены от подложки к количеству всех точек на изображении. Время, затраченное на сегментацию тестовых изображений, и значения нормированных ошибок сегментации были занесены в таблицу 1 и 2 соответственно.



а) б) в) г) д) е)

Рис. 1. Исходные тестовые изображения

Таблица 1 — Время работы алгоритмов, реализованных в c++

Метод сегментации	Время сегментирования, мс			
	РВВО	МВ	ВО	В-С
$M_T(1)$	6378.000	4790.919	8470.000	1289.000
$M_T(2)$	5716.000	4289.990	7756.000	1492.000
$M_T(3)$	5957.000	4793.635	8196.000	1378.000
$M_T(4)$	7674.000	9291.930	9781.000	1398.000
$M_T(5)$	7824.000	13796.738	9907.000	1344.000
$M_T(6)$	3907.000	9301.518	6988.000	1380.000

Таблица 2 – Значения нормированных ошибок сегментации для тестовых матриц в 10^{-3}

Метод сегментации		Реализация C++			
		РВВО	МВ контроль	ВО	В-С
$M_T(1)$	E_O	0	10.172	0	0.471
	E_I	0	0	55.171	1000.000
	E_S	0	10.172	55.171	1000.471

Метод сегментации		Реализация C++			
		РВВО	МВ контроль	ВО	В-С
$M_T(2)$	E_O	0	10.172	0	0.471
	E_I	0	0	55.171	1000.000
	E_S	0	10.172	55.171	1000.471
$M_T(3)$	E_O	0	94.643	109.590	0.110
	E_I	0	0.528	81.736	0.615
	E_S	0	95.171	191.326	0.725
$M_T(4)$	E_O	0	10.172	0	0.463
	E_I	0	0	73.664	517.115
	E_S	0	10.172	73.664	517.577
$M_T(5)$	E_O	0	10.172	0	0.475
	E_I	0	0	79.930	523.079
	E_S	0	10.172	79.930	523.555
$M_T(6)$	E_O	0	19.853	0	2034.901
	E_I	0	0	96.055	0
	E_S	0	19.853	96.055	2034.901

Как видно из данных, представленных на таблицах 1 и 2, разработанный алгоритм позволяет безошибочно найти границы всех элементов, а время выполнения делает его хорошей альтернативой его аналогам, которые допускали ошибки при их применении.

Список использованных источников:

1. Гонсалес Р., Вудс Р. Цифровая обработка изображений. М. : Техносфера, 2005. [R. Gonzalez, R. Woods, Digital Image Processing, (in Russian). Moscow: Tehnosfera, 2005.]

2. Roerdink J., Meijster A. The Watershed Transform: Definitions, Algorithms and Parallelization Strategies // Fundamenta Informaticae. 2001. Vol. 41. P. 187–228. [J. Roerdink, A. Meijster, “The Watershed Transform: Definitions, Algorithms and Parallelization Strategies,” Fundamenta Informaticae, vol. 41, pp. 187-228, 2001.]

3. Moga A., Cramariuc B., Gabbouj M. Parallel watershed transformation algorithms for image segmentation // Parallel Computing. 1998. Vol. 24. P. 1981–2001. [A. Moga, B. Cramariuc, M. Gabbouj, “Parallel watershed transformation algorithms for image segmentation”, Parallel Computing, vol. 24, pp. 1981-2001, 1998.]

АНАЛИЗ РЫНКА ОБЛАЧНЫХ УСЛУГ. МЕТОДЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СЕРВИСОВ

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

Госса А.И.

Лагутин А.Е. – к.т.н.,доцент

Исследования рынка облачных вычислений представлены агенством TAdviser[1].

По форме предоставления услуг на рынке выделяется два сегмента:

- проектные услуги (выбор, внедрение, интеграция, обучение);
- услуги операционного управления (плата за пользование сервисом, включая управление биллингом, учитывающим неравномерность потребления).

Анализ рынка публичных облачных услуг также включает функциональные сегменты:

- приложение как услуга (Software as a Service, SaaS);
- платформа как услуга (Platform as a Service, PaaS);
- инфраструктура как услуга: системное ПО, серверы и СХД (Infrastructure as a Service, IaaS).

По данным исследования, крупный бизнес максимально готов к использованию облачных услуг: в этом сегменте свыше 90% опрошенных знают про облачные услуги, в малом бизнесе – свыше 70%. При этом в крупном бизнесе 54,5% опрошенных пользуется одновременно облачными услугами из 2-х и более категорий, в среднем бизнесе – 50%, в малом – 43%.

Большинство респондентов ассоциируют облачные услуги с виртуальной инфраструктурой (IaaS), хотя сейчас наибольшую долю на рынке занимает модель SaaS — 58,9%. На IaaS и PaaS пока приходится соответственно 37,2% и 3,9% в объеме рынка. По данным исследования доля SaaS к 2020 году увеличится до 62,4%, а IaaS - снизится до 32,3%[1].

Риски использования облачных сервисов

Наиболее полный список угроз облачным сервисам в составе референсной архитектуры информационной безопасности частного облака от Microsoft насчитывает 50 разнообразных угроз на девяти уровнях, полный анализ которых в рамках одной статьи невозможен. Можно выделить ключевые угрозы, представляющие наибольший риск для потребителей облачных сервисов[2]:

- блокировка данных (lock-in) внутри инфраструктуры провайдера из-за отсутствия возможности экспорта данных, хранения в нестандартизированных форматах или потери криптографических ключей для расшифрования данных;
- компрометация административного доступа клиента вследствие успешного перебора паролей или компрометации рабочего места сотрудника клиента;
- потеря контроля над данными вследствие делегирования его провайдеру облачных сервисов, архитектура и организация информационной безопасности которого могут иметь существенные недостатки на уровнях инженерной и ИТ-инфраструктуры, гипервизора и др.;
- неэффективная работа механизмов разграничения доступа между клиентскими данными, обусловленная ошибками в реализации гипервизоров (уязвимостей ПО);
- нарушение нормативных требований по защите данных или обеспечения достоверности финансовой отчетности, что обусловлено передачей данных между юрисдикциями или невыполнением требований по защите чувствительных с точки зрения конфиденциальности/целостности данных;
- утечка клиентских данных, что обусловлено плохой организацией процедуры безопасного удаления данных с мест хранения;
- недоступность облачного сервиса вследствие изменения рыночной стратегии провайдера, покупки провайдера, плохой организации производственного процесса провайдера либо DDoS-атаки;
- непредвиденные затраты недопустимого уровня на оплату облачного ресурса в результате DDoS-атаки против клиента (economical DDoS).

На данную тему произведены исследования, в соответствии с которыми многообразие угроз облачным сервисам не позволяет обеспечить эффективную защиту в разумные сроки и бюджеты. Тем не менее каждая компания может реализовать подходящую ей стратегию информационной безопасности(ИБ) облаков.

Выбор стратегии информационной безопасности облачных сервисов

Специфика обеспечения ИБ облачных сервисов заключается в том, что итоговый уровень информационной безопасности является суммой уровней ИБ провайдера и клиента, из чего следуют два практических тезиса[2]:

- клиент никак не сможет закрыть проблемы в стратегии ИБ провайдера, поэтому выбор провайдера облачных услуг и работа над договором о предоставлении облачных услуг являются наиболее важным элементом;

- не имеющий специалистов и не обладающий ресурсами для обеспечения ИБ клиент может переложить операционные задачи по обеспечению ИБ на провайдера (при этом SaaS дает максимум контроля провайдеру, IaaS, наоборот, клиенту).

Исходя из этого, можно использовать одну из четырех стратегий обеспечения облачной безопасности для бизнеса разных размеров с разными требованиями к конфиденциальности.

Стратегия "Минимум ошибок"

Стратегия предполагает максимальное использование лидирующих SaaS-сервисов не обладающими необходимой экспертизой предприятиями малого бизнеса, поскольку они вряд ли достигнут сравнимого уровня ИБ самостоятельно.

Стратегия "Минимальные усилия"

Стратегия предусматривает максимальное использование лидирующих SaaS-сервисов и дополнительно тщательное изучение и использование доступных встроенных сервисов безопасности, например: двухфакторной аутентификации, защиты паролем загружаемых в Google Drive документов, аккаунта Google на других сайтах ("кустарная" реализация принципа SSO), хранение резервных учетных записей Google и удаление учетных записей сотрудников при их увольнении.

Стратегия "Точечное внимание"

Стратегия заключается в снижении общепризнанных рисков и активном противодействии базовым угрозам. Ключевой посыл - противодействие управляемому количеству угроз, концентрация ресурсов и экспертиз на самых важных направлениях. Как минимум девять указанных угроз ИБ облаков должны быть смягчены, по возможности интегрированы с платформой сервис-провайдера для снижения капитальных и операционных затрат. В случае отсутствия интегрированных мер необходимо внедрение выделенных решений/мер по ИБ облаков. При выборе мер можно использовать как лучшие практики от ENISA, так и описанные ниже продукты ИБ (в том числе интегрированные с платформами сервис-провайдеров).

Стратегия "Многослойная оборона"

Стратегия предполагает разработку целостной комплексной концепции обеспечения облачной безопасности на основе глубокого анализа рисков, тщательного выбора сервис-провайдера, с учетом вопросов обеспечения ИБ и соответствия требованиям законодательства, а также последующего проектирования и внедрения организационных и технических мероприятий по защите информации. Исходя из значимости и количества чувствительной информации, система защиты по возможности должна быть независима от провайдера облачных сервисов. Все средства защиты информации должны быть переданы в промышленную эксплуатацию и эксплуатироваться командой экспертов. В случае отсутствия внутренних ресурсов - сертифицированных специалистов по облачной безопасности, аудиту и контролю ИТ желательно привлекать внешних экспертов на постоянной основе - как через открытие новых позиций, так и путем аутсорсинга или аутстаффинга.

Список используемых источников:

1.Облачные сервисы [Электронный ресурс]. – Режим доступа: http://www.tadviser.ru/index.php/ http://www.tadviser.ru/index.php/Статья:Облачные_сервисы_%28рынок_России%29

2.Защита облачных сервисов: стратегия информационной безопасности и продукты. [Электронный ресурс]. – Режим доступа: http://астерос.рф/press/press/2477/

ОПЕРАЦИОННАЯ СИСТЕМА ANDROID. ANDROID V 8.1

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

Томин В.А.

Лагутин А.Е. – к.т.н.,доцент

Android – операционная система для смартфонов, планшетов, электронных книг, цифровых проигрывателей, наручных часов, фитнес-браслетов и др. Основана на ядре Linux и собственной реализации виртуальной машины Java от Google. Android позволяет создавать Java -приложения, управляющие устройством через разработанные Google библиотеки. Android Native Development Kit позволяет портировать библиотеки и компоненты приложений, написанные на Си и других языках.

Первым устройством, работающим под управлением Android, стал разработанный компанией HTC смартфон HTC Dream, презентация которого состоялась 23 сентября 2008 года. Вскоре последовали многочисленные заявления других производителей смартфонов о намерении выпустить устройства на базе Android.

Приложения под операционную систему Android являются программами в нестандартном байт-коде для виртуальной машины Dalvik, для них был разработан формат установочных пакетов .Apk. Для работы над приложениями доступно множество библиотек Bionic (библиотека стандартных функций, несовместимая с glibc); мультимедийные библиотеки на базе PacketVideo OpenCORE ; SGL (движок двухмерной графики); OpenGL ES 1.0 ES 2.0 (движок трёхмерной графики); Surface Manager (обеспечивает для приложений доступ к 2D/3D); WebKit (готовый движок для веб-бразуера; обрабатывает HTML, JavaScript); FreeType(движок обработки шрифтов); SQLite (легковесная СУБД, доступная для всех приложений); SSL (протокол, обеспечивающий безопасную передачу данных по сети). По сравнению с обычными приложениями Linux приложения Android подчиняются дополнительным правилам: Content Providers — обмен данными между приложениями; Resource Manager — доступ к таким ресурсам, как файлы XML, PNG, JPEG; Notification Manager — доступ к строке состояния; Activity Manager — управление активными приложениями.

Google предлагает для свободного скачивания инструментарий для разработки (Software Development Kit), который предназначен для x86-машин под операционными системами Linux, macOS (10.4.8 или выше), Windows XP, Windows Vista и Windows 7. Для разработки требуется JDK 5 или более новый.

Android 8.1 Oreo привносит поддержку нейронных сетей, повышающих общую производительность совместимых устройств, задействует процессор Visual Core в смартфонах Pixel 2 и Pixel 2 XL, а также активирует функцию безопасного просмотра веб-страниц.

Кроме того, был добавлен индикатор батареи сопряженных Bluetooth-аксессуаров, усовершенствована система автозаполнения, повышена безопасность работы дактилоскопического сканера, а также изменен принцип уведомления пользователей о входящих сообщения, препятствующий зацикливанию звуковых сигналов.

Новая функция автоматического заполнения данных (Autofill) дебютировала в Android 8.0. В обновлении Android 8.1 она получила несколько важных улучшений, которые разработчики могут внедрить в свои приложения.

Пользовательские описания. Добавлена поддержка пользовательских описаний, которые Android отображает в пользовательском интерфейсе автозаполнения, а не в исходном представлении данных. Нововведение придется очень кстати, например, в случае, когда вы хотите замаскировать номер своей кредитной карты и показывать только последние четыре цифры.

Сохранение данных. Разработчик может указать в приложении объект Validator. Он может использоваться приложением, чтобы Android показывал в меню автозаполнения кнопку «сохранить», когда это необходимо. Функциональность обеспечивается методом setValidator() класса SaveInfo.Builder.

Строковые представления данных. Класс BaseAdapter в Android 8.1 Developer Preview включает метод setAutofillOptions(), который реализует строковые представления значений в адаптере. Прежде всего, нововведение будет полезным для элементов управления Spinner, которые динамически генерируют значения в адаптере. Например, можно использовать метод setAutofillOptions() для включения строковых представлений списка годов, которые пользователи выбирают в качестве даты истечения срока действия кредитной карты. Функция автозаполнения может использовать строковое представление для заполнения подобного вида данных.

Список использованных источников:

Licenses Android Open Source Project. Android

Ingraham, Nathan Oreo is officially the next name for Android Engadjet. — «But the company is going all out this year, using the solar eclipse as an opportunity to reveal that Android O will henceforth be referred to as Oreo»

www.android.com

СХЕМА АНАЛИЗА СЕТЕВОГО ТРАФИКА

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

Мухуров Н.И. – д.т.н.,профессор

Задача анализа сетевого трафика в настоящее время становится все более актуальной. Этому способствует не только развитие и внедрение новых сетевых технологий (и ,как следствие, увеличение объёма данных, передаваемых по сети), но и появление большого количества новых сетевых протоколов прикладного уровня. Основными практическими задачами анализа сетевого трафика являются: выявление проблем в работе сети; тестирование (отладка) сетевых протоколов; восстановление потоков данных («прослушивание»); предотвращение сетевых атак; сбор статистики.

Общая схема анализа сетевого трафика состоит из определённой последовательности шагов. Каждый из приведенных ниже шагов приводит к повышению уровня представления объекта анализа.

1.Захват пакетов, проходящих через контролируемое сетевое соединение. Результат шага – получение объекта анализа в виде сетевых пакетов. В зависимости от необходимой точности и скорости последующего анализа, а также доступных вычислительных мощностей могут использоваться различные подходы.

- Слайсинг. При использовании этого подхода анализу подвергаются не всё содержимое пакетов, а только некоторый префикс (n первых байт). В ряде исследований показано, что этот подход хорошо работает для последующей классификации трафика по протоколам.

- Сэмплинг. При использовании этого подхода перехватываются не все пакеты, а только их часть, которая может выбираться по различным критериям, в зависимости от потребностей. В процессе развития технологии было предложено большое число стратегий отбора. Например, для задач мониторинга типов трафика подходит вариант с выбором каждого n-го пакета (uniform sampling), где n может выбираться в зависимости от соотношения ширины канала и пропускной способности системы анализа.

- Для задач, в которых требуется максимально точный анализ трафика, например для систем обеспечения сетевой безопасности, требуется перехватывать все данные всего поступающего трафика без потерь – для обозначения этого подхода используется термин lossless capture или deep packet capture (DPC).

2. Агрегирование пакетов в потоки по некоторым адресным признакам (flow generaion), получение нового объекта для анализа – сетевого потока. Если при этом данные пакетов в дальнейшем анализе не учитываются, то такой вид анализа называется «анализ потоков» - flow based analysis (в отличие от packet-based анализа, при котором анализируются данные пакетов). Flow-based анализ широко используется в силу значительно меньших требований к мощности вычислителя и пропускной способности, за счёт значительного снижения объёма данных для обработки. Такой вид анализа может выполняться и локально, и удалённо от точки сбора данных. Для передачи собранных данных от точки сбора до точки анализа используется большое число протоколов, часть из которых стандартизирована в виде IPFIX. IP Flow Information Export – стандарт, современный вариант модели сетевых потоков netflow, который обеспечивает компактное и универсальное представление информации о сетевом трафике. Другая часть разработана отдельными производителями – Cisco NetFlow, Juniper Jflow. В рамках подхода записи, описывающие поток, могут содержать различный набор данных. Наиболее общим набором таких данных является: IP адреса источника и адресата, протокол транспортного уровня, в случае протоколов TCP/UDP – номера портов источника/адресата, набор счётчиков: количество переданных пакетов и байт, время создания и завершения потока.

Данный метод действительно значительно снижает требования к анализатору, тем не менее, он не является достаточно гибким, так как в отличие от слайсинга и сэмплинга не позволяет варьировать количество поступающих данных (зависит от входных данных).

3. Выполнение классификации по протоколу прикладного уровня или конкретному сетевому приложению. Результатом данного шага является получение нового объекта для анализа – сетевого потока конкретного протокола или приложения (в этом случае связанных потоков может быть несколько, например, в случае VoIP приложения это потоки SIP и RTP). После выполнения данной операции возможна следующая дополнительная обработка полученного объекта, конкретный вид которой зависит от решаемой прикладной задачи:

- разбор полей протокола (protocol parsing),
- сборка сессии протокола для протоколов с установлением соединения,
- извлечение данных приложения (content extraction) – страниц сайтов (HTML), файлов различных типов (исполняемые, изображения, текстовые документы, и т.д.), электронных писем, аудио-видео потоков
- разбор данных приложения (application content parsing).

Анализ сетевого трафика актуален из-за быстрого совершенствования сетевой отрасли. Он также жизненно важен для эффективного управления сетью, по результатам которого можно судить о качественных и количественных характеристиках работоспособности сети или её отдельных компонентов.

Список использованных источников:

1. Гетьман А. И., Евстропов Е.Ф., Маркин Ю. В. Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений // Препринт ИСП РАН №28, 2015. – 16с.

2. Маркин Ю. В., Санаров А.С. Обзор современных инструментов анализа сетевого трафика // Препринт ИСП РАН №27, 2014.

ШИФРОВАНИЕ МУЛЬТИМЕДИЙНЫХ ДАННЫХ С СОВМЕСТНЫМ РАНДОМИЗИРОВАННЫМ ЭНТРОПИЙНЫМ КОДИРОВАНИЕМ И ВРАЩЕНИЕМ В РАЗБИТОМ БИТОВОМ ПОТОКЕ

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

Мельничук О.В.

Борискевич А.А – д.т.н., профессор.

В современном обществе успех любого вида деятельности сильно зависит от обладания определенными сведениями (информацией) и от отсутствия их (ее) у конкурентов. Чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере и тем больше потребность в защите информации. Одним словом, возникновение индустрии обработки информации привело к возникновению индустрии средств ее защиты и к актуализации самой проблемы защиты информации, проблемы информационной безопасности.

Одна из наиболее важных задач – задача кодирования сообщений и шифрования информации.

В данной работе, проблемы мультимедийного шифрования исследуется под новым углом зрения. Если тщательного сравнивать между мультимедийными процессами сжатия и шифрования с точки зрения теории информации, отметим, что оба могут в целом рассматривается как процесс удаления избыточности, содержащейся во входных данных. Основное различие между ними состоит в том, что секретный ключ контролирует операции шифрования, в то время как все операции по сжатию осуществляются в соответствии с некоторыми стандартами. Новый подход шифрования состоит из двух этапов. Первый этап называется рандомизированное энтропийное кодирование (РЭК). Основная идея РЭК заключается в использовании нескольких энтропийных параметров кодирования или параметров соответствующих случайной последовательности внутри энтропийного кодера. Второй называется вращение в разделенных битовых потоках (ВРБП), которая дополнительно выполняет случайные вращения на выходе стадии РЭК для получения окончательного битового потока. [1]

Алгоритм метода шифрования состоит из следующих шагов:

1. Рандомизированное энтропийное кодирование исходной последовательности символов. Рассмотрим шифрование источника информации I на основе рандомизированных таблиц Хаффмана. В начале генерируется $M = 2^m$ различных кодовых таблиц Хаффмана, пронумерованных от 0 до $M - 1$. Данные таблицы могут быть обнародованы. Далее выбирается криптографически безопасный ПБГ (Псевдослучайный битовый генератор). Генерируется случайное число z, которое и является ключом шифрования РТХ. $z \leftarrow$ первый результат генератора ПБГ. Затем идет разбивает z на m -битные блоки. Записывается $z = t_1 \| t_2 \| \dots \| t_k, (t_i = 0 \text{ до } M - 1)$. Используется t_i таблица Хаффмана для кодирования одного символа ($i = 1$ до k). Если $i = k + 1$, возвращаемся к выбору криптографически безопасного ПБГ, и повторяем до завершения кодирования.

Законным владелец знает ключ (случайное число s). Таким образом, он в состоянии воспроизвести ключ, сгенерированный ПБГ и используемый в шифровании, что в свою очередь, позволит корректно декодировать битовый поток [1].

2. Перемешивание сегментированной кодированной битовой последовательности на основе вращения. Сжатый зашифрованный битовый поток сначала разбивается на блоки заданных (ключом разбиения) размеров, а затем осуществляется круговое случайное вращение в рамках каждого блока.

Многие операции могут быть использованы для изменения порядка бит в блоке. Перестановка всех бит перемешивает порядок бит наиболее полно, но требует много вычислений. Чтобы уменьшить сложность и облегчить битовый поток обработки, мы ограничиваем манипуляции с битами до простого левого вращения.

Для блока n бит $A = (a_1 a_2 \dots a_n)$, r -битное левое вращение преобразует A в $(a_{r+1} a_{r+2} \dots a_n a_1 a_2 \dots a_r)$, вращая (перемещая) первые r бит конец A.

Пусть $A = (a_1 a_2 \dots a_N)$, битовый поток длиной N. (p, r) -значения вращения и разделения блоков A, обозначаемые $\text{ВБП}(A, p, r)$ с $p = (p_1 p_2 \dots p_m)$, и $r = (r_1 r_2 \dots r_m)$, получают следующие 2 шага:

- Разделение A на m блоков A_i длинной p_i, $i = 1, 2, \dots, m, \sum_{i=0}^{m} p_i = N$;
- Выполнение r_i -битных левых вращений на каждый блок $i = 1, 2, \dots, m$.

Схема алгоритма вращения в разбитом битовом потоке (ВБП) представлена на рисунке 1.

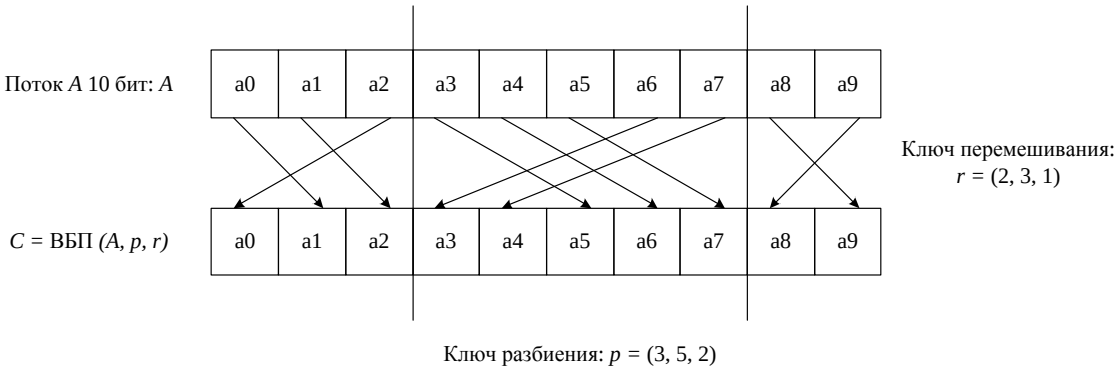
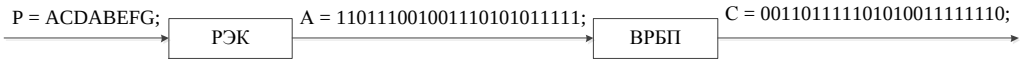


Рис. 1 – Схема алгоритма вращения в разбитом битовом потоке (ВБП)

3. Окончание алгоритма. Конечным результатом работы алгоритма будет являться бинарная последовательность C , первоначально прошедшая через блок РЭК где было осуществлено ее сжатие и кодирование а затем через ВБП для обеспечения более надежного уровня защиты [2].



$P = ACDABEFG$ – входная последовательность символов, составленная из символов I источника входного сигнала; $A = 11011100100111010101111 1$ – сжатая и закодированная бинарная последовательность на выходе блока РЭК; $C = 00110111110101001111111 10$ – конечная перемешанная бинарная последовательность, полученная на выходе блока ВБП;

Рис. 2 – Схема иллюстрирующая процесс работы алгоритма

РЭК / ВРБП парадигма шифрования имеет несколько преимуществ. Во-первых, конструкция использует структуру энтропии кодера, таким образом, требует незначительной стоимости для реализации в аппаратном или программном обеспечении. Во-вторых, шифрование не ухудшает степень сжатия в том смысле, что размер зашифрованного потока точно такой же, как и при стандартном сжатии. С точки зрения безопасности, предлагаемая нами схема может выдержать различные типы атак. [3]

Список использованных источников:

1. Wuand C.P., Kuo C.C.J. // Efficient multimedia encryption via entropy codec design in Security and Watermarking of Multimedia Contents, vol. 4314 of Proceedings of SPIE, San Jose, Calif, USA, 2001, pp. 128–138.
2. Xie D., Kuo C.-C.J. // EURASIP Journal on Information Security, 2007, Los Angeles, CA 90089-2564, USA, 2007.
3. Bose R., Pathak S., // IEEE Transactions on Circuits and Systems I, vol. 53, no. 4, 2006, pp. 848–857.

ЗАЩИТА ИНФОРМАЦИИ В IP-СЕТЯХ

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

Сергеев Н.Н., Белятко А.Л.

Астровский И.И. – к.т.н.,доцент

Организация системы защиты информации сейчас, во время стремительного развития информационных технологий и вхождение их практически во все сферы жизни, стала неотъемлемой частью этого развития. Для создания системы защиты информации необходимо произвести анализ всевозможных информационных угроз. Самыми опасными для инфраструктуры предприятия являются атаки без физического доступа к сети предприятия. Данные атаки направлены на анализ и перехват сетевого трафика, поэтому защита каналов связи является самой приоритетной задачей.

Шифрование трафика – один из наиболее эффективных методов защиты каналов связи.

IP Security (IPSec) – это комплект протоколов, касающихся вопросов шифрования, аутентификации и обеспечения защиты при транспортировке IP-пакетов. В его состав входят около 20 предложений по стандартам. IPsec включает в себя 3 алгоритмонезависимые базовые спецификации:

5) архитектура безопасности IP[1];
6) аутентифицирующий заголовок (AH);
7) инкапсуляция зашифрованных данных (ESP) [2].

Архитектура IPSec представлена на рисунке 1:

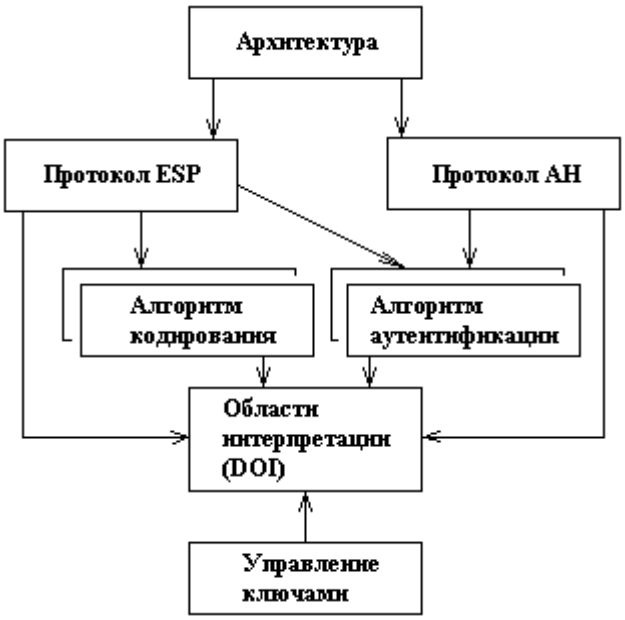


Рис. 1 – Архитектура IPSec

Аутентифицирующий заголовок (AH) является обычным опциональным заголовком. Он располагается между основным заголовком пакета IP и полем данных. Наличие AH никак не влияет на процесс передачи информации транспортного и более высокого уровней. Основное и единственное назначение AH — обеспечение защиты от атак, связанных с несанкционированным изменением содержимого пакета, и в том числе от подмены исходного адреса сетевого уровня.

Основная цель заголовка ESP — обеспечение конфиденциальности данных. Формат ESP может претерпевать значительные изменения в зависимости от используемых криптографических алгоритмов.

Гарантия целостности и конфиденциальности данных в спецификации IPSec обеспечивается за счет использования механизмов аутентификации и шифрования. Спецификация IPSec предусматривает возможность поддержки сторонами информационного обмена различных протоколов и параметров аутентификации и шифрования пакетов данных, а также различных схем распределения ключей. При этом результатом согласования контекста безопасности является установление индекса параметров безопасности, представляющего собой указатель на определенный элемент внутренней структуры стороны информационного обмена, описывающей возможные наборы параметров безопасности.

IPSec работает на сетевом уровне модели OSI. В результате передаваемые IP-пакеты защищены прозрачным для сетевых приложений и инфраструктуры образом.

Основные преимущества IPSec:

– обеспечивает гибкость при выборе алгоритмов шифрования и длины ключей;

– обеспечивает соединение пакетов по безопасному туннелю, что гарантирует качественную работу приложений с малым временем отклика;

– хорошо подходит для связывания узлов по надежным (безопасным) сетям;

– не IP-протоколы не поддерживаются по умолчанию.

Основные недостатки IPSec — требуется постоянный IP-адрес и не всё клиентское ПО одинаково качественное. Поэтому целесообразно использовать IPSec совместно с AuthIP[3].

Сочетание новых опций проверки подлинности пользователя, возможности использования нескольких учетных данных, более гибкого взаимодействия аутентификации и возможности каждой стороны использовать разные способы аутентификации, позволяет IPSec создать надежные и мощные политики без лишней сложности.

Список использованных источников:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы, 3-е изд.: – СПб., Питер, 2006.

2. Домарев В.В. Защита информации и безопасность компьютерных систем, 2007.

3. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах, 2008.

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ ВИДЕОКОНФЕРЕНЦСВЯЗИ НА ПРИМЕРЕ БГУИР

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

Завьялов А.А.

Лыньков Л.М. – д.т.н., профессор

Белорусский государственный университет информатики и радиоэлектроники является крупным научно-образовательным центром Беларуси. В университете учитываются и применяются мировые тенденции в сфере образования. Важной частью политики безопасности университета является аудит безопасности, в частности систем видеоконференцсвязи, используемых в университете.

Аудит информационной безопасности - системный процесс получения качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определенными критериями и показателями безопасности. Основные направления аудита информационной безопасности детализируются на следующие: аттестацию, контроль защищенности информации, специальные исследования технических средств и проектирование объектов в защищенном исполнении.

Различают внешний и внутренний аудит. Внешний аудит – это, как правило, разовое мероприятие, проводимое по инициативе руководства организации. Внутренний аудит представляет собой непрерывную деятельность, которая осуществляется на основании документа, носящего название «Положение о внутреннем аудите», и в соответствии с планом, подготовка которых осуществляется подразделениями внутреннего аудита и утверждается руководством организации.

Видеоконференция – это высокотехнологичный современный инструмент общения, предназначенный для повышения эффективности ведения бизнеса, оптимизации бизнес-процессов, ускорения принятия решений.

Видеоконференцсвязь – это телекоммуникационная технология интерактивного взаимодействия трех и более удаленных абонентов, при которой между ними возможен обмен аудио- и видеоинформацией в реальном времени, с учетом передачи управляющих данных.

Для внедрения видеоконференцсвязи руководителю организации необходимо определить главную цель применения. При этом необходимо учитывать основные правила видеоконференцсвязи:

- гарантированная высокоскоростная услуга связи или выделенные каналы связи только для сеансов видеоконференций;
- стабильное и надежное электропитание телекоммуникационного оборудования и видеоконференцсвязи;
- оптимальные шумо- и эхопоглощающие особенности помещения;
- компетентный обслуживающий персонал.

В белорусском государственном университете информатики и радиоэлектроники уже имеются аудитории, оборудованные системами видеоконференцсвязи. Данное оборудование играет большую роль в работе университета:

- возможность проведения видеоконференций с представителями других университетов, не только находящихся на территории Республики Беларусь;
- проведение видеоконференций для студентов с представителями других университетов, расположенных в других странах и представителями различных организаций;
- возможность проведения видеоконференций и тренингов для преподавательского состава ВУЗа для повышения квалификации и обмена опытом;
- проведение совещаний между представителями других учреждений образования.

Видеоконференцсвязь позволяет решать ряд задач и вопросов в кратчайшие сроки и путем сокращения расходов для достижения желаемого результата. Но для качественной работы видеоконференцсвязи в университете, необходимо производить аудит безопасности системы видеоконференцсвязи, что позволит анализировать риски, связанные с возможностью осуществления угроз безопасности в отношении ресурсов безопасности информационных систем; локализации узких мест в системе защиты информационный систем; оценки соответствия информационных систем существующим стандартам в области информационной безопасности.

Список использованных источников:

Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с

Семененко В. А. Информационная безопасность: Учебное пособие. — М.: МГИУ, 2004—215 с.

3. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях. – М.: ОАО «ДМК Пресс», 2002. – 156 с.

МИКРОСЕРВИСНАЯ АРХИТЕКТУРА ВЕБ-ПРИЛОЖЕНИЙ

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

Щитляк А.Н.

Мухуров Н.И. – д.т.н.,профессор

Возрастающие требования к современным веб-приложениям, такие как возможность предоставление программного интерфейса, интеграция с другими веб-приложениями, обработка большого количества запросов, масштабируемость, обеспечение необходимой скорости доступа к информации, приводят к тому, что корпоративные веб-приложения с монолитной архитектурой становятся неудобными в разработке, сложно тестируются и вводятся в эксплуатацию с большими временными задержками.

Микросервисная архитектура – это метод создания распределенных приложений в виде набора независимо разрабатываемых и развертываемых небольших сервисов, запускаемых как один или несколько изолированных процессов. Основная цель такого разделения – возможность изменения отдельно взятого микросервиса, не меняя при этом связанных с ним компонентов. Бизнес-логика приложения разбивается на отдельные части, каждая из которых представляет собой небольшое приложение, выполняющее одну бизнес-задачу. Число таких приложений ничем не ограничено и между собой они общаются, используя API, построенное, например, на основе HTTP протокола.

Структурная схема микросервисной архитектуры веб-приложения представлена на рисунке 1:

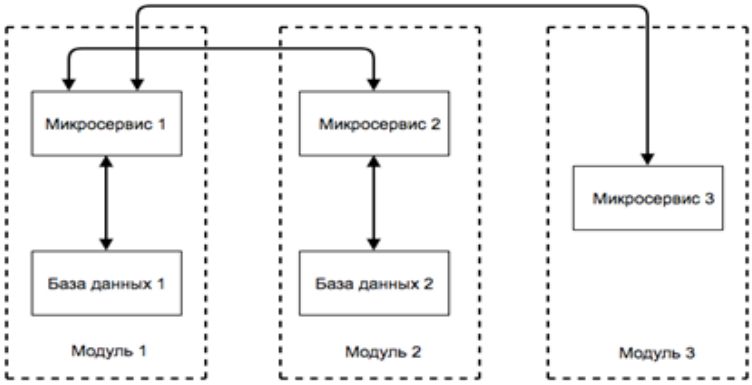


Рис. 1 - Структурная схема микросервисной архитектуры веб-приложения

Основные преимущества микросервисной архитектуры:

– использование различных языков программирования и программных средств, оптимальных для реализации каждого микросервиса;

– взаимозаменяемость микросервисов;

– независимость микросервисов друг от друга, каждый микросервис может быть развернут независимо от других служб;

– упрощение процесса масштабирования разрабатываемого веб-приложения;

– организация микросервисов как модулей вокруг отдельных функций.

Основные недостатки микросервисной архитектуры:

– сложность реализации общего поведения для всех микросервисов (авторизация запросов, агрегация данных из разных микросервисов);

– дополнительные издержки при обработке пользовательских запросов;

– необходимость учитывать, что любой из микросервисов в любой момент времени может быть недоступен.

Важно учитывать, что система на базе микросервисной архитектуры больше подвержена ошибкам из-за использования сети передачи данных для взаимодействия между микросервисами, что приводит к дополнительным издержкам при обработке пользовательских запросов и сложности реализации общего поведения для всех микросервисов (авторизация запросов, агрегация данных).

Подводя итоги, нельзя однозначно утверждать, что микросервисная архитектура – это будущее проектирования программного обеспечения, однако уже сегодня ясно, что микросервисная архитектура обладает большим потенциалом и серьезными преимуществами для разработки и реализации веб-приложений.

Список использованных источников:

1. Микросервисы, SOA и API: друзья или враги? – [Электронный ресурс]. – Режим доступа. – URL: https://www.ibm.com/developerworks/ru/library/1601_clark-trs/index.html
2. Применение микросервисной архитектуры при разработке веб-приложений – [Электронный ресурс]. – Режим доступа. – URL: https://sibac.info/journal/student/18/87616
3. Микросервисы – [Электронный ресурс]. – Режим доступа. – URL: https://dev.by/lenta/anadea/mikroservisy

ЗОНТИЧНАЯ СИСТЕМА МОНИТОРИНГА IT-ИНФРАСТРУКТУРЫ И ПРИЛОЖЕНИЙ БАНКА

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

Сошенко М.С.

Никульшин Б.В. – к.т.н.,доцент

В настоящее время ни одна сфера деятельности не обходится без контроля и мониторинга - работоспособность IT-систем оказывает большое влияние на состояние IT-сервисов. Предлагаются специализированные программы для мониторинга инфраструктуры и приложений, однако с ростом количества используемых решений возникает проблема определения источника проблемы, т.к. все системы взаимосвязаны между собой. Создание единой платформы для мониторинга позволяет усовершенствовать методы контроля работоспособности бизнес-услуг и IT-систем в частности.

Сегодня все критичные процессы и сервисы в организациях основываются или зависят от ИТ-технологий и сервисов. В организациях обычно используются разрозненные средства мониторинга – одни системы для контроля сети, другие – для мониторинга состояния серверов, третьи для баз данных, четвертые для приложений. Основной проблемой при таком подходе является отсутствие единого представления об IT-инфраструктуре, а следовательно, и о влиянии различных событий на качество предоставления IT-услуг. Для контроля их работоспособности требуется комплексный подход – сбор данных со всех источников IT-инфраструктуры.

Есть различные подходы к построению системы мониторинга – подход от инфраструктуры и подход от IT-сервисов. Применение второго подхода заключается в формировании каталога услуг и разработки сервисно-ресурсных моделей, которые будут отражать взаимодействие между сервисом и другими компонентами инфраструктуры, нужными для его работы.

Любую IT-услугу можно представить в виде нескольких основных составялющих – IT-инфраструктура (серверы, системы хранения данных, сетевое оборудования, устройства фильтрации, балансировки трафика и др.), базы данных, а также сервисы, программы и приложения. Принцип реализации такой системы представлен на рисунке 1:

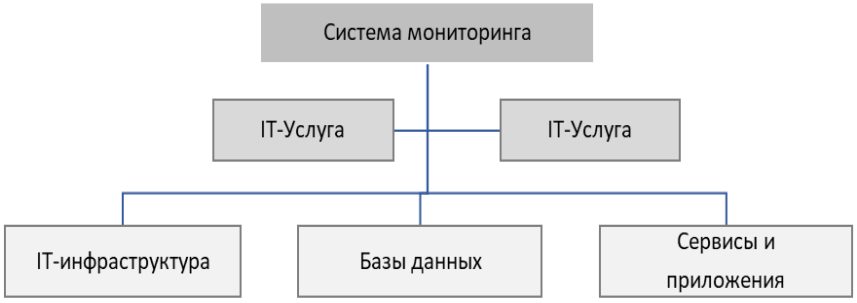


Рис. 1 - Структура построения системы мониторинга

С использованием сервисно-ресурсной модели проводится процедура настройки программы мониторинга с целью контроля функционирования IT-сервиса и всех связанных с ним компонентов инфраструктуры. Для каждой услуги рассчитывается уровень доступности, а также создаётся удобное представление о том, где именно возникла проблема. Система позволяет формировать отчеты, накапливать статистику и понимать, какие компоненты бизнес-приложения недостаточно производительны.

В результате зонтичная (централизованная) система мониторинга позволяет собрать в одной консоли информацию о доступности и работоспособности всей IT-инфраструктурцы, предотвращать возможные инциденты и сократить время на выявление возможных проблем в работе информационных систем. Зонтичный мониторинг позволяет бизнесу оценить реальную эффективность ИТ их влияние на работоспособность компании в целом.

Список использованных источников:
1. Зоря Н. Е., Кузовкова Т. А. Формирование системы мониторинга в сфере инфокоммуникаций // Век качества. 2012. №5-6. URL: https://cyberleninka.ru/article/n/formirovanie-sistemy-monitoringa-v-sfere-infokommunikatsiy (дата обращения: 07.04.2018).
2. Мехтиев Э.М., Комагоров В.П., Фофанов О.Б., Марчуков А.В. К вопросу о проектировании системы мониторинга корпоративной вычислительной сети // Доклады ТУСУР. 2012. №2-1 (26).
3. Yeh H.L. et al. A monitoring system based on Nagios for data grid environments // International Conference on Grid Computing and Applications.
4. C.Toland, C.Meenan, M.Warnock, P.Nagy. Proactively Monitoring Departmental Clinical IT Systems with an Open Source Availability System – J Digit Imaging. 2007 Nov; 20(Suppl 1): 119-124.

ВЫБОР ПРОТОКОЛА БЕЗОПАСНОСТИ ДЛЯ ОРГАНИЗАЦИИ VPN

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

Киселёв Д.В.

Астровский И.И. – к.т.н.,доцент

В настоящее время зачастую перед руководителями IT подразделений стоит вопрос: какой из протоколов безопасности выбрать для построения корпоративной сети VPN. Встаёт выбор между использованием протокола безопасности сетевого уровня IPSec и использованием одного из протоколов прикладного уровня SSL/TLS. Ответ не очевиден так как каждый из подходов имеет как плюсы, так и минусы. Проведём анализ и выявим когда необходимо применять IPSec, а когда SSL/TLS.

IPSec (IP Security) – набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов, а также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

SSL (Secure Sockets Layer) / TLS (Transport Layer Security) – криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет. Используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

Выбор протокола для построения корпоративной сети VPN можно осуществлять по следующим критериям.

1. Тип доступа необходимый для пользователей сети VPN.

1.1. Полнофункциональное постоянное подключение к корпоративной сети. Рекомендуемый выбор – протокол IPSec.

1.2. Временное подключение, например, мобильного пользователя или пользователя использующего публичный компьютер, с целью получения доступа к определенным услугам, например, электронной почте или базе данных. Рекомендуемый выбор – протокол SSL/TLS, который позволяет организовать VPN для каждой отдельной услуги.

2. Является ли пользователь сотрудником компании.

2.1. Если пользователь является сотрудником компании, устройство которым он пользуется для доступа к корпоративной сети через IPSec, может быть сконфигурировано определенным способом.

2.2. Если пользователь не является сотрудником компании к корпоративной сети которой осуществляется доступ, рекомендуется использовать SSL/TLS. Это позволит ограничить гостевой доступ только определенными услугами.

3. Уровень безопасности корпоративной сети.

3.1. Высокий. Рекомендуемый выбор – протокол IPSec. Действительно, уровень безопасности предлагаемый IPSec гораздо выше уровня безопасности предлагаемого протоколом SSL/TLS в силу использования конфигурируемого ПО на стороне пользователя и шлюза безопасности на стороне корпоративной сети.

3.2. Средний. Рекомендуемый выбор – протокол SSL/TLS, позволяющий осуществлять доступ с любых терминалов.

4. Уровень безопасности данных, передаваемых пользователем.

4.1. Высокий, например, менеджмент компании. Рекомендуемый выбор – протокол IPSec.

4.2. Средний, например, партнер. Рекомендуемый выбор – протокол SSL/TLS.

5. Что важнее, быстрое развертывание VPN или масштабируемость решения в будущем.

5.1. Быстрое развертывание сети VPN с минимальными затратами. Рекомендуемый выбор – протокол SSL/TLS. В этом случае нет необходимости реализации специального ПО на стороне пользователя как в случае IPSec.

5.2. Масштабируемость сети VPN – добавление доступа к различным услугам. Рекомендуется протокол IPSec, позволяющий осуществление доступа ко всем услугам и ресурсам корпоративной сети.

5.3. Быстрое развертывание и масштабируемость. Рекомендуемый выбор – комбинация IPSec и SSL/TLS: использование SSL/TLS на первом этапе для осуществления доступа к необходимым услугам с последующим внедрением IPSec.

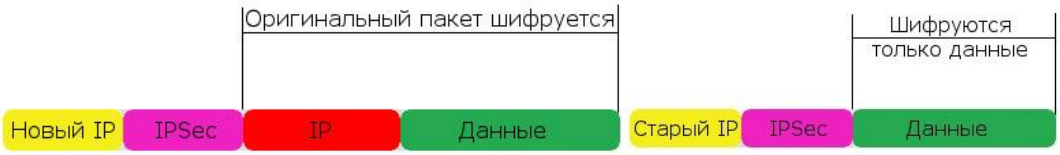


Рис. 1 – Примеры шифрования IP-пакета протоколом IPSec

Как видно из анализа характеристик этих протоколов они не являются взаимозаменяемыми и могут функционировать как отдельно, так и параллельно, определяя функциональные особенности каждой из реализованных VPN.

Список использованных источников:

1. Олифер В. Г.,Олифер Н. П. Глава 24. Сетевая безопасность // Компьютерные сети. Принципы, технологии, протоколы. – 4-е. – СПб: Питер, 2010. – С. 887-902. – 944 с.

2. Stephen Thomas. SSL & TLS Essentials: Securing the Web. – 1-st. – Wiley, February 11, 2000.

АЛГОРИТМ СИСТЕМЫ КОНТРОЛЯ ДОРОЖНОГО ДВИЖЕНИЯ НА ОСНОВЕ НЕЙРОННОЙ СЕТИ

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

Голубович И.В.

Борискевич И.А. – к.т.н.,ассистент

Известно, что стратегия адаптивного регулирования светофора в реальном времени является самым продуктивным средством для устранения проблем связанных с заторами на дорогах. При образовании затора значительно (до 20 раз и более) снижается пропускная способность участка дороги. Если прибывающий поток транспорта превышает пропускную способность участка дороги, затор растёт лавинообразно. Затор обладает рядом очевидных негативных последствий. Однако, достижение масштабируемой оптимизации систем управления дорожным движением по всей сети остается сложной проблемой. Для того чтобы достичь глобальной оптимизации во всей сети, изначально, следуя принципу «разделяй и властвуй», нужно достичь адаптируемого механизма управления светофором на уровне одного перекрестка.

Основная проблема в традиционной системе управления светофорами заключается в том, что они работают в качестве закрытой системы по отношению к внешней среде. Другими словами, они не являются адаптивными к изменению состояния дороги. Такое управление можно назвать «слепым», так как оно работает вне зависимости от настоящих внешних факторов, что приводит к неоптимальному использованию ресурса, т. е. в данном случае перекрестка.

Адаптивные методы превращают статический светофор в живую систему, реагирующую на внешнюю среду. Адаптивный алгоритм должен получать информацию от детекторов о присутствии участников дорожного движения, чтобы настроить синхронизацию сигналов и фаз. Обработав информацию, он сможет дать дополнительное время направлению, с высокой нагрузкой, любо уменьшить время или даже отменить фазу, в случае отсутствия трафика. Детекторы транспорта могут быть сгруппированы в три класса: детекторы под проезжей частью, детекторы над проезжей частью, а также детекторы для обнаружения безмоторного движения.

С точки зрения программирования, подход к данной задаче можно назвать агентно-ориентированным. Такой подход схож с реальной ситуацией, когда инспектор дорожного движения стоит в средине перекрестка и управляет движением транспортных средств из разных направлений. Под системой контроля светофора подразумевается «агент». Задача агента заключается в оптимальном распределении права проезда транспортных потоков по перекрестку без конфликта. В данной задаче можно заметить два важных фактора: оптимальное распределение и отсутствие конфликта. Понятие оптимальности является абстрактным в данном случае, так как оно может определиться в зависимости от требований и ситуаций. С этой точки зрения появляются разные методы для реализации адаптивного алгоритма.

Для реализации данной задачи наиболее подходящими являются алгоритмы на основе искусственных нейронных сетей. Искусственные нейронные сети - это математические модели организации реальных биологических нейронных сетей.

На данный момент существует 3 поколения искусственных нейронных сетей (бинарные, частотно-скоростные, спайковые), и для каждого существуют различные виды нейронных сетей, однако для того, чтобы любая нейронная сеть была способна выполнить поставленную задачу, ее необходимо обучить. Для целей обучения собираются данные и формируются выборки обучающих примеров, а также контрольная выборка. Аналогично существует и множество различных подходов к обучению. В заключение обучения проверяется адекватность обучения нейронной сети, после чего алгоритм готов к работе.

В качестве данных отображающих состояние на перекрестке были выбраны количество машин на полосе и время простоя. Для расчета коэффициентов данных параметров была использована нейронная сеть типа персептрон. Данная нейронная сеть между слоями входных и выходных нейронов имеет связи, проходя по которым параметры умножаются на некоторый коэффициент. При обучении нейронной сети данный коэффициент принимает такое значение, что при прогоне тестовых выборок, на выходе получается значение, наиболее приближенное к правильному значения. По представленным выше параметрам из статистических данных были выбраны необходимые и произведено обучение с последующей оценкой эффективности.

Таким образом был разработан алгоритм системы контроля дорожного движения на основе нейронной сети, подходящий для масштабирования и реагирующий на обстановку на перекрестке в режиме реального времени.

Список использованных источников:

1. S.Ishak, P. Kotha, C.Alecsandru, “Optimization of Dynamic Neural Network Performance for Short-Term Traffic Prediction”. In Transportation Research Record, 1836, pp. 45-56. 2003.
2. B.G. Çetiner, M.Sari, Q.Borat, ”A neural network based traffic flow prediction model”, Mathematical and Computational Applications, Vol. 15, No. 2, 2010, pp. 269-278.
3. S. Pizzuti, F. Moretti, M. Annunziato Advanced Street Lighting Control through Neural Network Ensembling, The Second International Conference on Smart Systems, Devices and Technologies, 2013, pp 76-81.

ОБЕСПЕЧЕНИЕ КАЧЕСТВА КОРПОРАТИВНОЙ ВИДЕОКОНФЕРЕНЦ-СВЯЗИ

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

Алисеенко М.А., Кочеткова А.А.
Никульшин Б.В. – к.т.н, доцент

Возможности современного сетевого оборудования позволяют организовать видеоконференцсвязь с участием десятков оконечных устройств, генерирующих и получающих мультимедийные данные. Исходя из этого, остро стоит проблема выбора оптимальной системы видеоконференцсвязи, которая обеспечит хорошее качество, надежность и безопасность связи.

Одной из базовых составляющих технологии видеоконференцсвязи (ВКС) является обработка и передача видеоданных. В современных условиях применения ВКС на первое место выходят требования пользователей к качеству видеоинформации.

Программная система видеоконференцсвязи представляет собой программное обеспечение для любых стационарных или мобильных устройств, оснащенных устройствами захвата и воспроизведения видео и звука. В качестве сервера ВКС выбирается персональный компьютер с соответствующим ПО. Передача видеоданных может осуществляться как в локальной, так и глобальной сети.

Для оценки качества ВКС следует учитывать передаваемый трафик и выбранные видеокодеки.

На QoS оказывают влияние:

– сквозная задержка (end-to-end delay) – это сумма задержек на разных сетевых устройствах, через которые проходит мультимедийный трафик, оказывает значительное влияние на восприятие пользователем,

– вариация задержки или джиттер (delay variation, jitter) – это изменение времени прибытия между пакетами, введенное переменной задержкой передачи по сети;

– потеря пакетов (packet loss) – это отбрасывание пакетов в периоды перегруженности сети [ITU-T].

Каждый класс сетевого QoS, в частности 0 и 1, который определяет приложения реального времени, создает определенную комбинацию ограничений для значений рабочих характеристик. В определениях классов QoS в таблице 1 представлены границы сетевых показателей качества между интерфейсами пользователь-сеть [МСЭ].

Таблица 1. Нормы для характеристик сетей IP с распределением по классам QoS

Сетевые характеристики	Классы QoS	
	0	1
Задержка доставки IP-пакета, IPTD	100 мс	100 мс
Вариации задержки IP-пакета, IPDV	50 мс	50 мс
Коэффициент потери IP-пакета, IPLR	1×10^{-3}	1×10^{-3}
Коэффициент ошибочных IP-пакетов, IPER	1×10^{-4}	1×10^{-4}

Распространенными видеокодекам в системах ВКС являются H.264 и VP8. Первый стал индустриальным стандартом для видеоконференцсвязи и обеспечил совместимость на любых устройствах. H.264 имеет расширения для базового профиля (HP, SVC), которые позволяют повысить качество видео и снизить временные задержки сигнала, однако могут увеличить количество выделенных ресурсов обработки и требуют наличия шлюзов транскодирования. снижающих общее качество связи [4].

В свою очередь VP8 является свободно распространяемым решением, использующим современные алгоритмы сжатия данных. Кодек устойчив к потере кадров, имеет высокую скорость декодирования видеопотока, легко внедряем и универсален. Однако кодек медленный при кодировании, отсутствует поддержка B-кадров, что может уменьшить степень сжатия, но упрощает декодер.

Таким образом, чтобы обеспечить качество видеоконференцсвязи, следует проводить сетевой анализ трафика, создаваемого сервером и клиентами видеоконференции и учитывать выбор видеокодеков, которые определяют основную видеоархитектуру для поддержки приложений ВКС. Необходимо учесть баланс между качеством видео и скоростью передачи данных, защиту от потери данных и возможность коррекции ошибок, временные задержки сигнала.

Список использованных источников:

1. ITU-T Recommendation H.360 – An architecture for end-to-end QoS control and signalling, 2004.

2. Рекомендация МСЭ-Т Y.1541 – Требования к сетевым показателям качества для служб, основанных на протоколе IP, 2006.

3. Кодеки видеоконференцсвязи [Электронный ресурс]. Режим доступа: http://www.ipvs.ru.

ИНТЕЛЛЕКТУАЛЬНЫЕ АЛГОРИТМЫ КЛИМАТ-КОНТРОЛЯ

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

Борискевич А.А. – д.т.н., профессор

Внутренний климат помещений важен для здоровья и производительности человека, равно как и для некоторых производств. Системы обогрева и кондиционирования широко используются, как в жилых и офисных, так и в промышленных зданиях.

Системы обогрева и кондиционирования воздуха являются одним из основных потребителей энергии и оказывают значительное влияние на общее использование энергии домами и зданиями. В некоторых странах потребление энергии такими системами может достигать 40% от всей энергии, используемой зданием[1]. Таким образом, эффективное управление потреблением энергии системами климат-контроля может привести к значительной экономии энергии для всей энергосистемы.

В результате разработки в области оптимизации систем климат-контроля приобретают важное значение в управлении энергопотреблением.

Цель работы состоит в том, чтобы реализовать алгоритм поддержания температуры в помещении на комфортном уровне, минимизируя при этом потребление электроэнергии. Температура в помещении описывается уравнением теплового баланса:

$$\Delta Q = C_b T_b,$$

где ΔQ – количество полученной теплоты, C_b – теплоемкость помещения, T_b – температура помещения.

Теоретически, эффективный алгоритм можно вывести из уравнения теплового баланса, подставив в него все возможные факторы, влияющие на перенос тепла, например, солнечное излучение, вентиляцию, погодные условия снаружи помещения, теплопроводность стен и т.д. На практике это потребует значительного объема исследований каждого конкретного помещения.

Алгоритмы машинного обучения не требуют явного учета всех возможных факторов на этапе программирования. Такие алгоритмы улучшают свою эффективность в процессе обучения, учитывая всю совокупность факторов, влияющих на систему, хотя и в отсутствие информации о влиянии каждого фактора в отдельности. Обобщенный механизм машинного обучения представлен на рисунке 1.

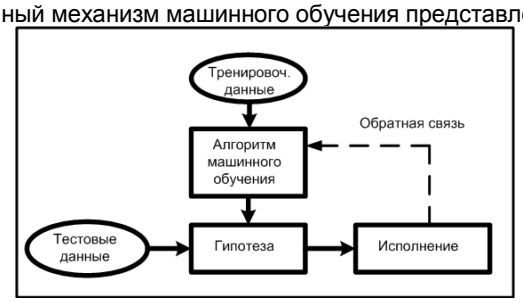


Рис. 1 – механизм машинного обучения

Поэтому представляется целесообразным использовать алгоритмы машинного обучения такие, как системы с нечеткой логикой, нейронные сети, управление с прогнозирующими моделями и генетические алгоритмы.

Преимущество нечеткой логики заключается в том, что контроллер, построенный с ее использованием, не нуждается в тепловой модели помещения, поэтому его легко применять в системе климат-контроля. Система нечеткой логики оптимизируется с помощью алгоритма обучения нейронной сети.

Перспективным методом является метод управления с прогнозирующими моделями. Этот метод улучшением классического управления с отрицательной обратной связью, в котором учитывается предсказание поведения объекта управления на различные типы входных воздействий. Обратная связь в таких системах управления используется для корректировки неточностей, связанных с внешними помехами и неточностью математической модели объекта управления. Для него требуется построить модель теплового баланса в помещении и в информации о погодных условиях из метеопрогноза. Данная модель оптимизируется при помощи генетического алгоритма.

Реализация и исследование вышеназванных алгоритмов проведены в системе MATLAB. Результаты исследования позволяют сделать вывод о применимости машинного обучения в системах климат-контроля для поддержания температуры в помещении на комфортном уровне и минимизации потребления электроэнергии.

Список использованных источников:

1. Sai Ram Gubba, Wen-Tai Li, Wayes Tushar, Chau Yuen, Naveed Ul Hassan, Kristin Wood, Chao-Kai Wen, and H. Vincent Poor, Energy Management by Controlling Air Conditioning Systems in Residential Settings - Indian Institute of Technology, Singapore University of Technology and Design, Lahore University of Management Sciences, National Sun Yat-sen University, School of Engineering and Applied Science, Princeton University

2. Sowjanya Param, Electricity Demand Prediction Using Artificial Neural Network Framework - North Dakota State University of Agriculture and Applied Science

3. Feng Zhang, Building Temperature Control with Intelligent Methods - University of Denver

ЗАЩИТА ИНФОРМАЦИИ В IP-СЕТЯХ

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

Щерба Д.С.
Астровский И.И. – к.т.н.,доцент

В наши дни информация становится одним из основных средств решения проблем и задач государства, различных коммерческих структур и отдельных людей.

С точки зрения защиты информация обладает рядом свойств:

Информация доступна человеку, если она содержится на материальном носителе. Различают носители - источники информации, носители - переносчики информации и носители - получатели информации.

Ценность информации оценивается степенью полезности ее для пользователя (собственника, владельца, получателя). Информация может обеспечивать ее пользователю определенные преимущества: приносить прибыль, уменьшить риск в его деятельности в результате принятия более обоснованных решений и т.д.

Информацию можно рассматривать как товар. Цена информации, как любого товара, складывается из себестоимости и прибыли.

Себестоимость определяется расходами владельца информации на ее получение путем:

- проведения исследований в научных лабораториях, аналитических центрах и т.д.;
- покупки информации;
- добывания информации противоправными действиями.

Прибыль от информации ввиду ее особенностей может принимать различные формы, причем денежное ее выражение является не самой распространенной формой. В общем случае прибыль от информации может быть получена в результате следующих действий:

- продажи информации на рынке;
- материализации информации в продукцию с новыми свойствами или технологии, приносящими прибыль;
- использования информации для принятия более эффективных решений.

Ценность информации изменяется во времени. Распространение информации и ее использование приводят к изменению ее ценности и цены. Характер изменения ценности во времени зависит от вида информации. Ценность большинства видов информации, циркулирующей в обществе, со временем уменьшается – информация стареет.

Невозможно объективно (без учета полезности ее для потребителя, владельца, собственника) оценить количество информации.

При копировании, не изменяющем информационные параметры носителя, количество информации не меняется, а цена снижается. Так как при каждом копировании увеличивается число ее законных и незаконных пользователей, то в соответствии с законами рынка цена уменьшается [1].

Ввиду развития информационных технологий, на предприятиях и в государственных учреждениях большая часть информации обрабатывается с использованием средств вычислительной техники. Чтобы обеспечить оперативный обмен и обработку информации, а также повысить эффективность работы сотрудников, строятся компьютерные сети, что, в свою очередь, вызывает проблему защиты, обрабатываемой на средствах вычислительной техники и передаваемой по сети информации.

Для защиты информации следует регламентировать доступ к информационным ресурсам между сотрудниками предприятия и предотвратить несанкционированный доступ к данным как изнутри корпоративной сети, так и извне.

Защита информации — деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. К защищаемой относится информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, устанавливаемыми собственником информации [2].

Существует две категории угроз информационной безопасности интеллектуальной собственности организации – внешние и внутренние угрозы. Данная классификация предусматривает разделение угроз по локализации злоумышленника (или преступной группы), который может действовать как удалённо, пытаясь получить доступ к конфиденциальной информации предприятия при помощи сети интернет, либо же действовать посредством доступа к внутренним ресурсам IT-инфраструктуры объекта.

В случае внешних атак, преступник ищет уязвимости в информационной структуре, которые могут дать ему доступ к хранилищам данных, ключевым узлам внутренней сети, локальным компьютерам сотрудников. В этом случае злоумышленник пользуется широким арсеналом инструментов и вредоносного программного обеспечения (вирусы, трояны, компьютерные черви) для отключения систем защиты, шпионажа, копирования, фальсификации или уничтожения данных, нанесения вреда физическим объектам собственности и т.д.

Внутренние угрозы подразумевают наличие одного или нескольких сотрудников предприятия, которые по злому умыслу или по неосторожности могут стать причиной утечки конфиденциальных данных или ценной информации. Рассмотрим эти категории рисков информационной безопасности подробнее.

Для решения проблем, связанных с защитой информации необходимо постоянно отслеживать, анализировать и синтезировать оперативные данные, касающиеся атак на информацию, стремиться выделять новые угрозы и оценивать риски, связанные с ними. Важно подбирать наиболее подходящие способы защиты информации, с целью минимизации риска потери конфиденциальной информации.

Для успешной защиты информации требуются специалисты с глубокими знаниями в этой области и опытом работы. Обучение в этой сфере требует больших затрат и вложений и т.д. Наиболее приемлемым дополнением к лекционным занятиям и изучению литературы является применение обучающих и тестирующих программ. Они позволяют моделировать различные ситуации (угрозы, потенциальные проникновения) и разрабатывать новые способы защиты.

В работе намечается сделать обучающую программу, которая облегчит обучение специалистов в сфере защиты информации.

Список использованных источников:

1. Электронный ресурс. – Режим доступа: https://studfiles.net/preview/4515436/
2. Шаньгин В.Ф.. Информационная безопасность и защита информации. М: ДМК Пресс, 2014, 702с.

ТЕХНОЛОГИЯ MPLS L3VPN

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

Скрипелёва А.А.

Саломатин С.Б. – к.т.н.,доцент

На сегодняшний день большинство организаций и предприятий имеют территориально распределенную структуру, вследствие чего возникает необходимость объединения локальных вычислительных сетей территориально распределенных филиалов в одну корпоративную сеть. Кроме того, существуют проблемы защиты информации, аутентификации и авторизации пользователей, предоставления доступа к ресурсам, обеспечение независимости адресных пространств. Эти задачи в настоящее время помогает решить технология виртуальных частных сетей VPN (Virtual Privat Network).

Под термином VPN понимают круг технологий, обеспечивающих безопасную и качественную связь в пределах контролируемой группы пользователей по открытой глобальной сети. Цель создания VPN сводится к максимальной степени обособления потоков данных одного предприятия от потоков данных всех других пользователей сети.

MPLS (Multiprotocol Label Switching) — механизм передачи данных, который эмулирует различные свойства сетей с коммутацией каналов поверх сетей с коммутацией пакетов. MPLS работает на уровне, который можно было бы расположить между вторым (канальным) и третьим (сетевым) уровнями модели OSI. Основным преимуществом MPLS считается ускорение скорости продвижения пакетов в ядре сети. MPLS позволяет создавать Layer 3 VPN, не прибегая к туннелированию и шифрованию.

Построение MPLS L3VPN преследует следующие задачи: обеспечение защиты соединения, требуемого качества обслуживания и расширяемость инфраструктуры.

Для решения поставленных задач представлено три компонента MPLS L3VPN:

1. Компонент для разделения маршрутизируемых данных пользователей: VRF (Virtual Routing and Forwarding).
2. Компонент для обмена маршрутизируемыми данными пользователей: MP-BGP (Multiprotocol BGP).
3. Компонент для гибкого управления маршрутизируемыми данными: TE.

Traffic Engineering (TE) — это возможность управления направлением прохождения трафика с целью выполнения определенных условий (резервирование каналов, распределение загрузки сети, балансировка и предотвращение перегрузок).

Основной механизм TE в MPLS — использование однонаправленных туннелей (MPLS TE tunnel) для задания пути прохождения определенного трафика.

На рисунке 1 показан путь передачи пакетов MPLS L3VPN, создаваемой провайдером.

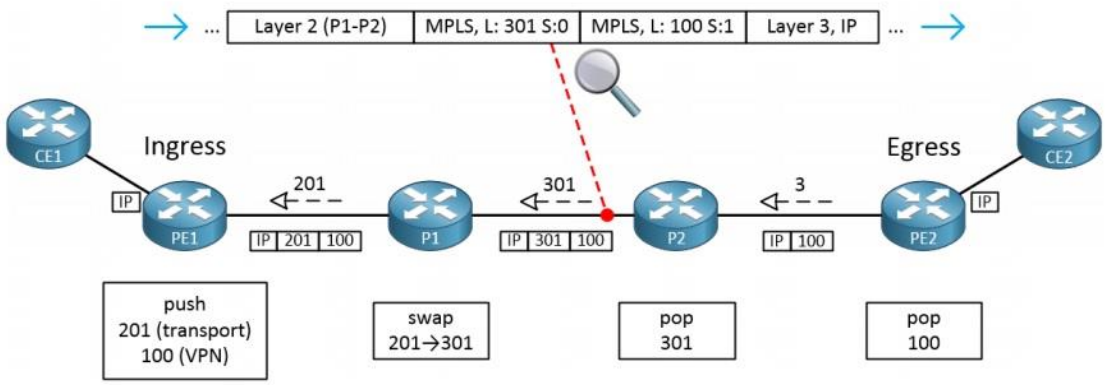


Рис. 1 - Путь передачи пакетов MPLS L3VPN

В состав опорной части сети (core network) входят P-маршрутизаторы (латинская буква «P» обозначает провайдера). В терминологии MPLS эти P-маршрутизаторы называются коммутирующими по меткам маршрутизаторами (Label Switch Routers — LSR). Передача осуществляется с помощью свопинга меток, а управление — с помощью протокола распределения меток (Label Distribution Protocol). Эти маршрутизаторы не осведомлены о существовании виртуальных частных сетей (VPN) и не участвуют в BGP-обмене, который происходит на PE-маршрутизаторах.

PE-маршрутизаторы (периферийную часть сети провайдера) должны присваивать пакету начальную метку при его поступлении в опорную сеть MPLS (MPLS core) и удалять эту метку в момент, когда пакет покидает сеть.

CE-маршрутизаторы (периферия сети заказчика) подключаются к PE-маршрутизаторам и не требуют специальной модификации для поддержки MPLS-VPN.

PE-маршрутизаторы связываются друг с другом по многопротокольному BGP для обмена информацией о подключенных VPN.

Каждое устройство MPLS PE поддерживает по одной таблице VRF (таблица маршрутизации и передачи VPN). MPLS-устройство идентифицирует маршруты, относящиеся к определенной сети VPN с помощью «различителя маршрутов» (Route Distinguisher — RD), который присваивается всем маршрутам соответствующего CE. Эти «различители» (RD) имеют значение только для PE-устройств, так как P-маршрутизаторы коммутируют ячейки или пакеты на основании информации, заключенной в метках.

Магистральная адресация, которая используется для подключения P-маршрутизаторов, полностью отделена от адресации, используемой для подключения CE-маршрутизаторов. Эти две схемы маршрутизации никак не взаимодействуют между собой. PE-маршрутизаторы сохраняют адреса опорной сети в глобальной таблице маршрутизации, которая хранится отдельно от таблиц VRF, где находятся данные обо всех маршрутах каждой VPN, к которой подключены сайты CE. Каждая таблица VRF имеет так называемую «политику импорта» (import policy), которая определяет, какие обновления PE следует принять, и «политику экспорта» (export policy), определяющую, какие маршруты следует объявлять.

Когда PE-устройство присваивает метку на границе сети MPLS, эта метка точно определяет весь маршрут, по которому будет передаваться данный пакет в этой сети. Это происходит потому, что LDP уже определил, какая входящая метка будет заменяться на соответствующую исходящую метку на каждом P-маршрутизаторе с тем, чтобы пакет был доставлен в конечный пункт назначения. Поэтому MPLS представляет собой форму маршрутизации от источника, так как только на периферии принимается решение о маршруте.

Каждый пограничный маршрутизатор заказчика должен инжектировать свои маршруты в соответствующие таблицы VRF, определенные в MPLS-сети для данной VPN. Эта задача выполняется пограничными маршрутизаторами заказчика, настроенными на передачу информации о маршрутах, необходимых другим сайтам своей же VPN. Для этой передачи может использоваться статическая маршрутизация, а также маршрутизация BGP.

Применение технологии MPLS дает возможность маршрутизируемым магистралям провайдера поддерживать VPN-сети и обеспечивает прозрачность механизмов 3-го уровня даже через инфраструктуры 2-го уровня. Такой подход позволяет создавать закрытые пользовательские группы и связанные с ними службы.

Список использованных источников:

1. Cisco Systems, Построение виртуальных частных сетей (VPN) на базе технологии MPLS
2. Бехингер М. Безопасность MPLS VPN. – Индианаполис: Cisco Press, 2005. – 312с.
3. Гейн Л. Основы MPLS. – Индианаполис: Cisco Press, 2007. – 651 с.

МЕТОДИКА ИЗМЕРЕНИЯ ИНДИКАТРИСЫ РАССЕЯНИЯ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

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

Урядов В.Н., Подлужный А.И.

Урядов В.Н. – к.т.н.,доцент

Основными источниками ИК-излучения БЛА являются его силовая установка и составные элементы (блок(-и) цилиндров, головка(-и) блока цилиндров (Г БЦ), система выпуска отработанных газов (ОП), а также струя выхлопных газов. Мероприятия, направленные на снижение ИК-излучения могут привести к нежелательным изменениям летно-эксплуатационных характеристик БЛА, а также повлиять на боевую эффективность. Мероприятия по снижению инфракрасной заметности БЛА являются эффективными, в случае если они не изменяют тактико-технические характеристики ЛА при достижении заданных уровней ИК-излучения.

При проведении экспериментальных исследований БЛА устанавливается на поворотном устройстве (подвешивается на подъемном кране). Размеры площадки при этом должны позволять разместить измерительный прибор таким образом, чтобы исследуемый объект полностью попадал в поле его зрения. Для того чтобы исключить влияние фоновой засветки, измерения необходимо проводить либо в ясную погоду после захода солнца либо в пасмурную погоду, но при условии отсутствия осадков или тумана. Измерения индикатрисы следует проводить в нескольких режимах работы силовой установки: форсажном. крейсерском и полетном малом газе. Для построения индикатрисы необходимо выбирать достаточное количество углов визирования и шаг их регулирования, так как большинство головок самонаведения управляемых ракет работают в диапазонах 1,8-3,2 мкм, 3,5-5,5 мкм, 6-4 мкм. То и измерения следует проводить в данных спектральных диапазонах. Измерения в ИК-диапазоне следует проводить в определенной последовательности:

1. установка и фиксация БЛА в пространстве для достижения требуемых углов визирования;
2. наведение измерительного прибора (тепловизора, радиометра) на объект измерения при помощи визирного устройства либо с учетом максимального принимаемого сигнала;
3. измерение фонового ИК-излучения при неработающем двигателе. В случае применения радиометра (без возможности визуального наведения);
4. вывод двигателя на необходимый режим и стабилизация его в течение заданного времени;
5. измерение ИК-излучения прибором.

В ходе измерений необходимо также регистрировать температуру, относительную влажность, атмосферное давление воздуха, расстояние от измерительного прибора до объекта угол визирования и азимут.

Диаграмма эффективной поверхности рассеяния летательного аппарата на рисунке 1:

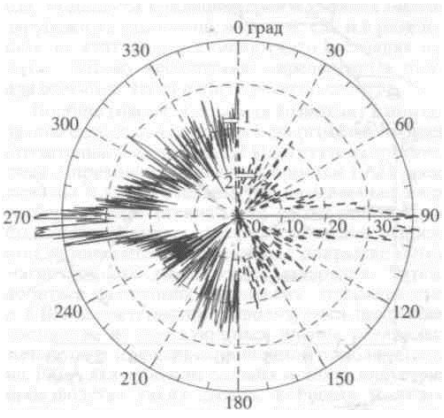


Рис. 1 – Диаграмма эффективной поверхности рассеяния летательного аппарата

При проведении измерений тепловизорами необходимо преобразовать результат измерений полученных матриц температур (термограмм) в энергетические характеристики. На первом этапе преобразований необходимо вырезать из термограмм ячейки которые не относятся к образу объекта исследования, с целью исключения влияний излучающих объектов. попавших в поле зрения измерительного прибора. После этого над матицей температур можно производить преобразования [1].

Список использованных источников:

1. Лукашевич С.А., Урядов В.Н., Подлужный А.И. Измерение индикатрисы излучения беспилотных летательных аппаратов в статическом режиме // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных : материалы международного научно-технического семинара (Минск, апрель – декабрь 2017 г.) = Telecommunications: Networks and Technologies, Algebraic Coding and Data Security. – Минск: БГУИР, 2017. – 96с.

БЕСПРОВОДНЫЕ СЕНСОРНЫЕ СЕТИЯ ДЛЯ МЕДИЦИНСКИХ СИСТЕМ

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

Крупица А.С.

Борискевич И.А. – к.т.н.,доцент

В современной медицине остро стоит проблема организации процесса наблюдения за показателями физического состояния организма (электрокардиограмма, давление крови, пульс, дыхание, температура) пациентов, находящихся на стационарном лечении в больницах и клиниках при минимальном участии медицинского персонала.

Проблема может быть решена при помощи беспроводных сенсорных сетей (БСС), осуществляющих мониторинг основных показателей организма с необходимой частотой снятия данных [1]. В связи с этим в ряде стран интенсивно ведутся работы по созданию БСС медицинского назначения и изучению различных аспектов их применения. Обнаружен ряд проблем, которые необходимо решить для успешного широкого внедрения новой технологии в медицинскую практику. Одной из таких проблем медицинских БСС на основе стандартных узкополосных средств беспроводной связи оказывается пропускная способность коммуникационной сети. Другие проблемы касаются электромагнитной совместимости с электронной медицинской аппаратурой, надежности передачи данных, экологической безопасности, конфиденциальности собираемых и передаваемых данных и др.

Решить эти проблемы призваны СШП БСС, создаваемые на основе принятого в 2012 г. стандарта IEEE 802.15.6 для БСС медицинского и бытового назначения, в котором в качестве носителя информации предполагается в том числе использование хаотических радиоимпульсов [2].

В БСС медицинского назначения можно условно выделить две зоны: крупномасштабную (магистральную), обеспечивающую доставку информации по всему медицинскому учреждению, и локальную – зону беспроводных нательных сетей (БНС) (называемых также беспроводными нательными сенсорными сетями – БНСС), которые располагаются на теле и/или в окрестности тела человека и предназначены для непосредственного наблюдения за его физиологическими параметрами.

В общем случае беспроводные нательные сенсорные сети представляют собой систему разнородных устройств, расположенных в непосредственной окрестности или внутри тела пользователя и взаимодействующих между собой и с центральным координирующим узлом посредством беспроводной связи для получения полезного эффекта для потребителя.

Устройства в нательной сети можно разделить на сенсорные узлы, актуаторные узлы и персональные устройства.

Беспроводный сенсорный узел – устройство, которое реагирует на определенный физический (химический) процесс, собирает данные, при необходимости обрабатывает их и передает беспроводным образом. Сенсорный узел состоит из нескольких компонентов: датчика, блока питания, процессора, памяти, передатчика или приемопередатчика.

Беспроводный актуаторный узел – устройство, которое активно воздействует на тело в соответствии с данными, получаемыми от сенсоров или через взаимодействие с пользователем. Компоненты актуаторного узла сходны с компонентами сенсорного узла. Он содержит собственно актуатор (т. е. прибор для медицинского применения, включающий емкость для хранения медицинского препарата), блок питания, процессор, память, передатчик или приемопередатчик.

Беспроводное персональное устройство – устройство, которое собирает всю информацию, полученную от датчиков и исполнительных механизмов (актуаторов), и информирует пользователя (т. е. пациента, медсестру, врача и т. д.) при помощи внешнего шлюза, привода или дисплея светодиодов на приборе. Компоненты ПУ: блок питания, (большой) процессор, память и приемопередатчик. Это устройство называют также блоком контроля тела (Body Control Unit – BCU) [3], шлюзом тела или стоком. В некоторых реализациях в качестве ПУ используется смартфон.

Сети внутри тела применяют для мониторинга и имплантируемых сердечных дефибрилляторов, контроля функций мочевого пузыря и реабилитации движения конечностей [4]. На теле человека используют мониторинг ЭКГ, давления крови, температуры и дыхания. При использовании БНС пациенты обладают значительной физической мобильностью и в меньшей степени привязаны к больнице.

Список использованных источников:

1. Yang G.-Z. Body Sensor Networks. London : Springer, 2006.
2. IEEE Standard for Local and metropolitan area networks – Part 15.6: Wireless Body Area Networks. N.Y. : IEEE, 2012.
3. System architecture of a wireless body area sensor network for ubiquitous health monitoring / C. Otto [et al.] // J. Mobile Multimedia. 2006. Vol. 1, № 4. P. 307–326.

МЕТОДЫ ЗАЩИТЫ Wi-Fi СЕТЕЙ

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

Королев А.И – к.т.н.,доцент

С момента ратификации стандарта IEEE 802.11 беспроводные сети получили широкое распространение в производственных, общественных местах, а также жилых помещениях. Удобство и легкость реализации данной технологии также дает возможность и злоумышленникам с такой же легкостью осуществить сетевую атаку. Сети стандарта IEEE 802.11 подвержены угрозам нарушения конфиденциальности, целостности, доступности, а также ряду специфических угроз, причиной которых может быть нефиксированная природа связи и открытость среды передачи данных, а также уязвимости системы аутентификации, криптографических протоколов, программного обеспечения и уязвимости, обусловленные человеческим фактором.

Рассмотрим беспроводные сети стандарта IEEE 802.11 как объект угроз информационной безопасности и проведем их классификацию по конфигурации используемых средств защиты.

На сегодняшний день существуют следующие классы беспроводных сетей:

1) Открытые беспроводные сети.

2) Беспроводные сети, использующие базовую аутентификацию.

3) Беспроводные сети с WEP-шифрованием.

4) Беспроводные сети, применяющие протокол TKIP (WPA) и аутентификацию с использованием общих PSK-ключей.

5) Беспроводные сети, применяющие протокол TKIP (WPA) и аутентификацию по протоколам IEEE 802.1x и EAP.

6) Беспроводные сети, применяющие улучшенный алгоритм шифрования AES и аутентификацию с использованием общих PSK-ключей.

7) Беспроводные сети, применяющие улучшенный алгоритм шифрования AES и аутентификацию по протоколам IEEE 802.1x и EAP.

8) Беспроводные сети, использующие виртуальные частные сети как механизм защиты.

Для беспроводных сетей стандарта 802.11 все средства и методы защиты можно условно разделить на следующие три типа:

– средства и методы аутентификации;

– средства криптографической защиты передаваемых данных;

– дополнительные средства защиты.

Если рассматривать технологии защиты беспроводных сетей стандарта IEEE 802.11 в целом, то можно выделить следующие методы защиты:

– методы ограничения доступа (смена настроек, отключения широковещания ESSID, белые и черные списки ACL на основе MAC-адресов, использование политик безопасности и др.);

– методы шифрования (WEP-шифрование, WPA-шифрование, WPA2-шифрование);

– методы аутентификации (открытая аутентификация, аутентификация с общим ключом, аутентификация по MAC-адресу, аутентификация с общим ключом, аутентификация 802.1x);

– организационные методы защиты (мероприятия по предотвращению нарушений путем информирования сотрудников, мероприятия по обнаружению, мероприятия по восстановлению, объектовые мероприятия защиты при функционировании информационной системы, мероприятия по предотвращению, мероприятия по обнаружению).

К основным средствам и методам аутентификации относятся:

– базовая аутентификация (открытая аутентификация, аутентификация с совместно используемым ключом, аутентификация по MAC-адресу);

– аутентификация с использованием общих PSK-ключей;

– аутентификация по IEEE 802.11 и протоколу EAP (Extensible Authentication Protocol) с использованием RADIUS-сервера.

К основным средствам и методам криптографической защиты относятся:

– шифрование с использованием статических WEP-ключей;

– шифрование с использованием протокола TKIP;

– применение улучшенного алгоритма шифрования (AES).

К дополнительным средствам защиты, не предусмотренным производителями оборудования, можно отнести:

– создание виртуальных частных сетей (VPN);

– применение системы обнаружения атак (IDS).

Данные методы звщиты актуальны на сегодняшний день и используются как в промышленных так и в домашних сетях.

Список использованных источников:

1. Иванов П. Беспроводные сети: час настал.// Журнал сетевых решений LAN, 2002, №4, сс.103–108.
2. Хофф С. Безопасность сетей WLAN не дается даром.// Журнал сетевых решений LAN, 2003, №3, сс.44–49.

RESEACH METHODS OF IMPROVING EFFICIENCY OF A MULTISERVICE NETWORK

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

A. Sattar, A. Al Djabi .
Khatskevich O. A .Ph.D, Assoc. Prof.

More and more objects of economy, both public and private ownership in the territory of the Republic of Iraq are starting to develop their own corporate networks. There are several reasons: expansion of businesses associated with the need to ensure reliable and high quality link remote offices and branch offices, as well as increasing bandwidth requirements and reliability of data transfer.

Underfunding the main issue when creating or expanding an existing corporate network is the question of the total price, for the equipment and hire the required communication channels and network administration. The paper considers ways to optimize build corporate networks. For studies taken a large company with head office in Baghdad, a network of branches in provincial cities.

The aim of the study was to improve the quality and performance of corporate networks, reducing the cost of designing, improving protection of the network from external threats.

To address this goal in the following tasks:

1. The choice of technology to build networks of data transmission.
2. Development of applied mathematical model of network communications.
3. Calculation and analysis of the evaluation of quality characteristics of a corporate communication network.
4. Efficiency Optimization of applications and protocols of the POA a corporate communication network, allowing to increase its qualitative characteristics.
5. Information protection issues.

The results of the study allow you to move away from the most common approach in designing information systems-method of expert evaluations. This method though and minimizes the cost at the design stage and quickly estimate the cost of implementing the decision, however, is subjective. The advantage of simulation models is the possibility of substituting the process of change in the system events in real time on an accelerated process of change events in Tempe.

For the decision of tasks in view, it was necessary to give the notion of a corporate network and define its role and peculiarities in the hierarchy of data transmission networks. Based on these features, discussed in the first chapter of the thesis will be made the selection of specific technologies and solutions that meet the requirements of enterprise networks. Will the analysis of literary sources, considered world-wide trends in methods and technology of building modern converged enterprise networks.

On the basis of the received results will suggest the best methods and technologies to build the network. For communication inside and branch offices selected technology Ethernet allowing in the shortest possible time to launch and commissioning of the Network Technology. Ethernet allows you to easily implement scaling network without impact on existing personnel. It should be noted that Ethernet is the global standard for the Organization LAN networks.

For secure connection of geographically dispersed offices appropriate to use technology VPN MPLS. From other technologies building virtual private networks, such as VPNs, ATM or Frame Relay, VPN MPLS technology distinguishes good scalability, the ability to automatically configure and natural integration with other IP services, including Internet access, Web and e-mail services.

MPLS VPN functionality can be summarized as follows:

-MPLS allows a single converged network to support both new and existing facilities, creating an efficient migration path to IP infrastructure.

-MPLS operates over existing systems and transmission networks (ATM, Frame Relay, X. 25, IEEE 802.3, etc).

-MPLS allows you to generate traffic. Routing data packets are carried out through the application of technology of processing labels.

-MPLS supports the provision of services with a guaranteed quality of service (QoS). Packages that need to be delivered with high quality, can be marked, allowing service providers to provide certain small latency for voice and video signals in end-to-end connection.

-MPLS provides appropriate security level to make IP network the same safe as frame relay network in WAN, reducing the need for encryption in IP networks.

When sending confidential information, it is important to ensure a high level of reliability of encryption. The most famous representative of the Organization's encryption technology of protective channel in VPNs is the technology of Internet Protocol Security (IPSec-protected IP).

The main purpose of the IPSec service is to ensure safe PD over IP networks using any link-layer technology (PPP, Ethernet, ATM, etc.). Use Internet Protocol security (IPSec) ensures integrity, authenticity and confidentiality of the data; its membership now includes almost 20 proposals for standards and RFC 18.

IPSec in the following techniques:

-encryption of the original IP packet that provides secrecy of data contained in the package, such as a field in the IP header and the data field;

digital signature IP packets that provides authentication package and source-the sender of the package;

-encapsulate the IP packet in a new secure IP packet with a new header that contains the IP address of the device that disguises the internal network topology.

Thus, the use of VPN MPLS based Ethernet networks with data encryption protocol , IPSEC allows you to design a modern corporate network and create Foundation for further modeling network, whose goal is to further optimization.

Based on the results of this study clearly visible steps of designing a modern corporate network connection. Applying the information, you can create and optimize the performance of existing networks, disabling network efficiency and reliability to a whole new level.

РАЗРАБОТКА МОДЕЛИ БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ СЕТИ М ДИНАМИЧЕСКИ ИЗМЕНЯЮЩЕЙСЯ ТОПОЛОГИЕЙ

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

Белан В.А.

Хоменок М.Ю. – к.т.н.,доцент

Исходя из текущей динамики развития сетевой инфраструктуры, самоорганизующиеся сети с динамически изменяющейся топологией призваны решать большой круг задач как специального так общетехнического назначения в концепции сетей пятого поколения.

Поэтому разработка моделей таких сетей в зависимости от назначения, средств оценки системных параметров и характеристик таких сетей представляет актуальную задачу инженерных и научных исследований.

Беспроводные локальные сети WLAN (Wireless Local Area Network) семейства стандартов IEEE 802.11x (коммерческое название Wi-Fi — Wire-less Fidelity) могут функционировать в нескольких режимах, при этом в одном из них (неинфраструктурном) без наличия точки доступа (AP — Access Point). В этом режиме появляется возможность совместного функционирования терминалов между собой без наличия какой-либо устойчивой инфраструктуры сети, что позволяет реализовать принципы Ad Hoc-сети. Беспроводные децентрализованные самоорганизующиеся сети, состоящие из мобильных устройств называется MANET (Mobile Ad hoc Network) [1]. На рисунке 1 изображена сеть, иллюстрирующая подход к построению Mobile Ad Hoc-сети.

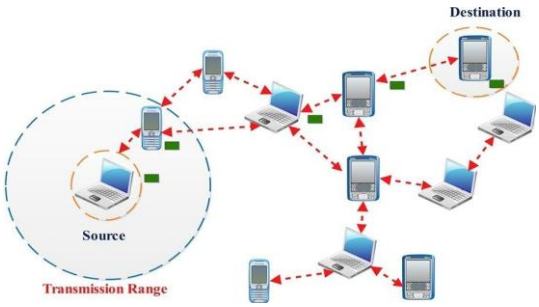


Рис. 1 - Структура сети MANET

Беспроводные сети, построенные на базе мобильных устройств, обладают рядом особенностей:

а) каждое устройство в такой сети может независимо передвигаться в любых направлениях, и, как следствие, часто разрывать и устанавливать соединения с соседями из-за помех или включения/выключения узла;

б) каждый узел сети участвует в процедурах ретрансляции сообщений других абонентов и служебной информации. При этом определение того, какому узлу пересылать данные, производится динамически, на основании связности сети;

в) запас источников питания мобильных узлов может быть ограничен, в связи с чем при проектировании аппаратных средств и протоколов необходимо учитывать еще и энергопотребление.

Основные преимущества MANET:

– возможность передачи данных на большие расстояния без увеличения мощности передатчика;

– устойчивость к изменениям в инфраструктуре сети;

– возможность быстрой реконфигурации в условиях неблагоприятной помеховой обстановки;

– простота и высокая скорость развертывания.

Для моделирования беспроводной сети важна модель передвижения узлов сети, которая должна подражать движению реального мобильного устройства в определенной ситуации. Модели мобильности основаны на определении разных параметров. Основными параметрами являются начальное местоположение мобильных узлов, их направление движения, диапазон скоростей, скорость изменяется со временем [2]. Существует множество моделей мобильности сети, основные из них:

1. Группа мобильности с контрольной точкой (Reference Point Group Mobility).
2. Модель со случайной путевой точки (Random Waypoint).
3. Гаусовско-Марковская модель (Gauss-Markov).
4. Модель Manhattan Grid и др.

Для использования в самоорганизующихся сетях классические протоколы маршрутизации приходится существенно модифицировать. Выделяют 3 класса протоколов: проактивные, реактивные и комбинированные.

В проактивных протоколах при изменении топологии сети инициируется широковещательная рассылка сообщений об этих изменениях. При этом все маршруты хранятся в памяти каждого узла, и он может воспользоваться ими в любой момент. К ним относятся DSDV, TBRPF, FSR и OLSR.

В реактивных протоколах маршрутизации маршруты существуют только тогда, когда они необходимы. К протоколам с реактивной маршрутизацией относятся AODV, DSR, LMR и TORA.

Гибридные протоколы сочетают в себе подходы проактивных и реактивных протоколов на разных уровнях иерархии [2].

Использование различных моделей мобильности и протоколов маршрутизации с одинаковыми параметрами симуляции может привезти к различным результатам.

В сетевом симуляторе NS-3 произведена симуляция MANET сети с 20 и 100 мобильными узлами при различных мобильных моделях и протоколах маршрутизации. Скорость узлов варьировались в диапазоне 5-10 м/с, размер пакета 512 байт, продолжительность симуляции 200 с.

Анализ производился для доли доставки пакета, pdf, который определяется как отношение доставленных и отправленных пакетов. Результаты моделирования представленной на рисунке 2.

В сети с 20 узлами модель RPGM превосходит другие модели. Это происходит потому, что все сообщение делятся между несколькими группами (по четыре группы, каждая с пятью узлами). Кроме того, в сети с 20 узлами реактивные протоколы работают лучше, чем DSDV. Модель RW лучше работает для более высокой плотности, из-за большей вероятности создание правильных маршрутов и их поддержание, поскольку нет ограничений по пространству, как в RPGM модель. Во всех случаях наихудшие результаты получены для модели MG. Это происходит из-за серьезных ограничение движения узла, независимо от их плотности. Кроме того, когда два узла расходятся, вероятность разрыва сигнала трафика увеличивается [3].

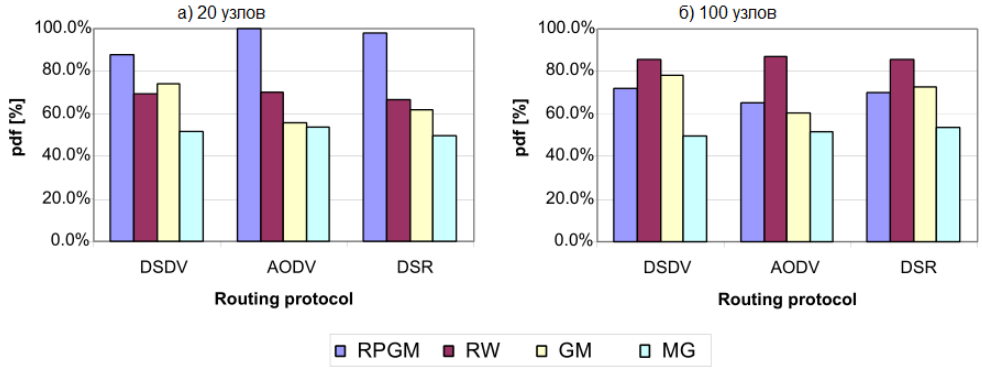


Рис. 2 – Результаты анализа сети MANET

Результаты моделирования показали, что относительное ранжирование протоколов маршрутизации может варьироваться в зависимости от модели мобильности. Относительный рейтинг также зависит от скорости узла и их количества, так как наличие мобильности подразумевает частые сбои связи, и каждый протокол маршрутизации реагирует по-разному во время отказов.

Список использованных источников:

1. А.Е. Кучерявый, Самоорганизующиеся сети и новые услуги // Электросвязь. – Россия. – Москва. – 2009. – 21с.
2. А.П. Метелёв, А.В. Чистяков, А.Н. Жолобов, Протоколы маршрутизации в беспроводных самоорганизующихся сетях // Вестник Нижегородского университета им. Н.И. Лобачевского. – Россия. – Киров : Вятский госуниверситет, 2013. – 75с.
3. V.Timcenko, M.Stojanovic, MANET Routing Protocols vs. Mobility Models: Performance Analysis and Comparison // Proceedings of the 9th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS : Serbia. – Belgrade : Institute Mihailo Pupin, 2009. – 271c.

РАЗРАБОТКА АДАПТИВНОГО МЕТОДА И ПРОГРАММЫ МОНИТОРИНГА КОРПОРАТИВНОЙ СЕТИ

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

Давыдова Н.С. – к.т.н.

Для современного уровня формирования информационного общества характерно интенсивное развитие технологий сетей post-NGN и концепции Интернета Вещей (ИВ). Происходит интенсивное развитие самоорганизующихся сетей связи, в которых абонентами являются не только люди, но и разнообразные автоматические устройства, которые осуществляют информационное взаимодействие друг с другом без прямого участия человека в рамках межмашинной коммуникации (M2M).

В работе рассматриваются крупные сети операторов связи, состоящие из оборудования различных производителей, которые обслуживаются целым штатом инженеров и географически разнесены по разным городам и странам (MAN, WAN). Такие сети требуют комплексных методов управления инфраструктурой с целью понимания происходящих в них процессах. Для решения этих задач существуют различные системы сетевого управления, которые позволяют администратору сети выполнять такие важные функции как: 1) сбор информации о работе сети; 2) контроль текущего состояния сети; 3) конфигурирование отдельных сетевых узлов с целью обеспечения повышения надежности работы сети и оптимизации сетевого трафика; 4) сегментирование загруженных участков телекоммуникационной сети; 5) составление статистических отчетов.

Системы мониторинга и управления компьютерными сетями включают как бесплатные решения, так и предложения от крупных производителей ПО и оборудования, конечную стоимость которых определить не представляется возможным. Из самых популярных можно выделить Nagios, Zabix, Cisco MARS, IBM Tivoli Monitoring. Наиболее привлекательными решениями из распространяемых по лицензии свободного ПО являются системы Nagios и Zabbix. В них реализованы основные необходимые модули, отвечающие требованиям модели FCAPS, такие как мониторинг состояния хостов, отправка оповещений в случае возникновения проблем со службой или хостом, возможность определять иерархии хостов. Однако в данных системах нет возможности отображения на карте местности расположения оборудования. Кроме того, уже существующие встроенные модули, рисующие топологию сети, достаточно громоздки и трудны в восприятии и не делают этого с привязкой к реальной карте местности.

Эффективным решением в дополнение к существующим системам мониторинга сетей может быть разработка адаптивного метода мониторинга сети с интерактивной картой отображения на карте местности с использованием сервиса «Яндекс.Карты» (рис. 1) и протокола SNMP, а также с привязкой к gps-координатам устройств. Отображение интерактивных связей между коммутаторами поможет в определении вышедшего из строя участка сети, поможет установить истинную причину аварии и явно укажет, где надо искать причину, повысит скорость реагирования на аварийную ситуацию.

Рис.1 Смоделированная ситуация потери связи по протоколу snmp с узлом дома по ул. Космонавтов 2. Основная причина – сбой в работе электропитания коммутатора, необходимы дополнительные диагностические мероприятия

Так же предложен алгоритм автоматической балансировки внешнего канала провайдера в зависимости от загрузки подключений к вышестоящим провайдерам. Предложенный подход может быть использован в любых сетях, построенных на стандартах протокола Ethernet группы IEEE 802.3, с любой уже внедрённой системой мониторинга.

Список использованных источников:

1 – Документы, разрабатываемые инженжерным советом Интернета (англ. Internet Engineering Task Force, IETF) www.ietf.org

2 - www.zabbix.com/ru/

4 - Turnbull, James, Pro Nagios 2.0, 2006

5 – Vasfi Gucer, Ana Godoy. Руководство по внедрению IBMTivoliMonitoring, книга IBMTivoliDirectoryServer, 2005

6 - Gary Halleen, Greg Kellogg. Security Monitoring with Cisco Security MARS, Издатель Pearson Education, 2007

ОЦЕНКА КАЧЕСТВА РАБОТЫ МУЛЬТИСЕРВИСНОЙ СЕТИ

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

Лоскот С. Ю., Мурашко А. В.

Хацкевич О. А. – к.т.н., доцент

В настоящее время построение мультисервисных сетей с интеграцией различных услуг является одним из наиболее перспективных направлений развития сетей связи. Переход к новым мультисервисным технологиям изменяет саму концепцию предоставления услуг. Учитывая сложную структуру мультисервисных сетей и повышенные требования к ним по обеспечению заданного уровня качества обслуживания, необходимо разрабатывать подходы, которые позволяют оценить эффективность будущей сети по различным критериям.

Существует единый набор сетевых характеристик, влияющих на качество услуг. Этот набор сетевых характеристик рассматривается в рекомендации МСЭ Y.1540 и включает в себя следующие характеристики: производительность сети, надежность сети/сетевых элементов, параметры доставки пакетов IP (задержка, вариация задержки (джиттер), потери пакетов, ошибки пакетов) [1].

Производительность сети (или скорость передачи данных) пользователя определяется как эффективная скорость передачи, измеряемая в битах в секунду. Следует отметить, что значение этого параметра не совпадает с максимальной пропускной способностью сети, ошибочно называемой полосой пропускания.

Надежность сети/сетевых элементов. Надежность сети может быть определена через ряд параметров, из которых наиболее часто используется коэффициент готовности, вычисляемый как отношение времени простоя объекта к суммарному времени наблюдения объекта, включающему время простоя и время между отказами [2].

Задержка передачи пакетов данных (т) на стыке UNI-UNI может быть вычислена по формуле [1]:

$$\tau = \sum_{i=1}^{n} t_{TP\ .3} \cdot \alpha + \sum_{j=1}^{m} t_{ГРС\ .3} \cdot \beta + \sum_{k=1}^{l} t_{ГРП\ .3} \cdot \gamma,$$

где $t_{TP.3}$ – среднее значение задержки на транзитных узлах сети;

$t_{ГРС.3}$ – задержка на граничных узлах коммутации в направлении NNI;

$t_{ГРП.3}$ – среднее время прохождения через граничные узлы сети UNI;

n – количество промежуточных транзитных узлов коммутации;

m – количество промежуточных граничных узлов NNI;

l – количество граничных узлов коммутации UNI;

α, β, γ – весовые коэффициенты.

Средние значения задержки для отдельных участков суммируются. В первом приближении время задержки через линию связи стремится к нулю.

Пакетный джиттер (Jitter – вариация задержки) – изменение величины временного интервала прохождения по линии доступа IP пакетов, принадлежащих к определенной последовательности (сессии), измеряемого как неравномерность задержки приема кадров. В отличие от естественной задержки при передачи в сети, джиттер появляется не из-за самого факта задержки, а по причине флуктуации времени задержки (d_i) от пакета к пакету.

Оценка пакетного джиттера может быть осуществлена по следующей формуле [1]:

$$JTpac = \sqrt{\frac{\sum_{i=1}^{N} (d_i - \langle \tau \rangle)^2}{N - 1}},$$

где $JTpac$ – величина временного отклонения, джиттер;

d_i – задержка текущего i-го пакета;

τ – средняя задержка передачи пакетов данных;

N – число исследований по получению пакетов данных.

Для MPLS-сетей норма джиттера на стыке UNI-UNI может составлять не более 15 мс.

Процент потерянных пакетов IP (IPLR) может быть оценен путем инверсии вероятности успешной передачи пакетов через количество n сетевых сегментов и рассчитан по следующей формуле [1]:

$$IPLR_{UNI-UNI} = 1 - \left[(1 - IPLR_{NS1}) \times (1 - IPLR_{NS2}) \times \ldots \times (1 - IPLR_{NS\ n})\right],$$

где $IPLR_{UNI-UNI}$ – итоговый показатель сквозных потерь;

$IPLR_{NS1}$, $IPLR_{NS2}$,… $IPLR_{NSn}$ – вероятности потерь для n-го участка сети.

Процент ошибочных пакетов может быть оценен путем инверсии вероятности передачи пакетов, не содержащих ошибки через количество n сетевых сегментов.

Методика оценки качества работы мультисервисной сети рассматривалась на конкретном примере мультимедийной сети с простейшей топологией, состоящей из серверной части и абонетской части сети, а именно : сервера для мультимедийных данных, сервера для пакетных данных (ftp) и сервера обработки речи для ip-телефонии; двух маршрутизаторов обеспечивающих соединение между серверами и

клиентами. Расчеты характеристик будут произведены с учетом различных типов трафика и типов очередей такие как: FIFO – first in, first out (первым пришел, первым ушел); PQ – priority queening (очередь с приоритетом) и WFQ – weighted fair queuing взвешенная справедливая очередь.

Моделирование мультисервисной сети производилось в программе Riverbed Modeler 17.5. Программный продукт Riverbed Modeler 17.5 – это объектно-ориентированный инструмент моделирования сетей связи. Данная программа имеет обширный пакет различных моделей сетевых элементов, библиотеки различных протоколов сетей связи и позволяет производить расчёт основных характеристик с учётом параметров QoS для различных типов трафика [3].

Для пакетных данных рассчитывалось значение потерянных пакетов, для мультимедийных данных – значение сквозной задержки, для речевых данных – значение пакетного джиттера. Результаты моделирования представлены на рисунке 2.

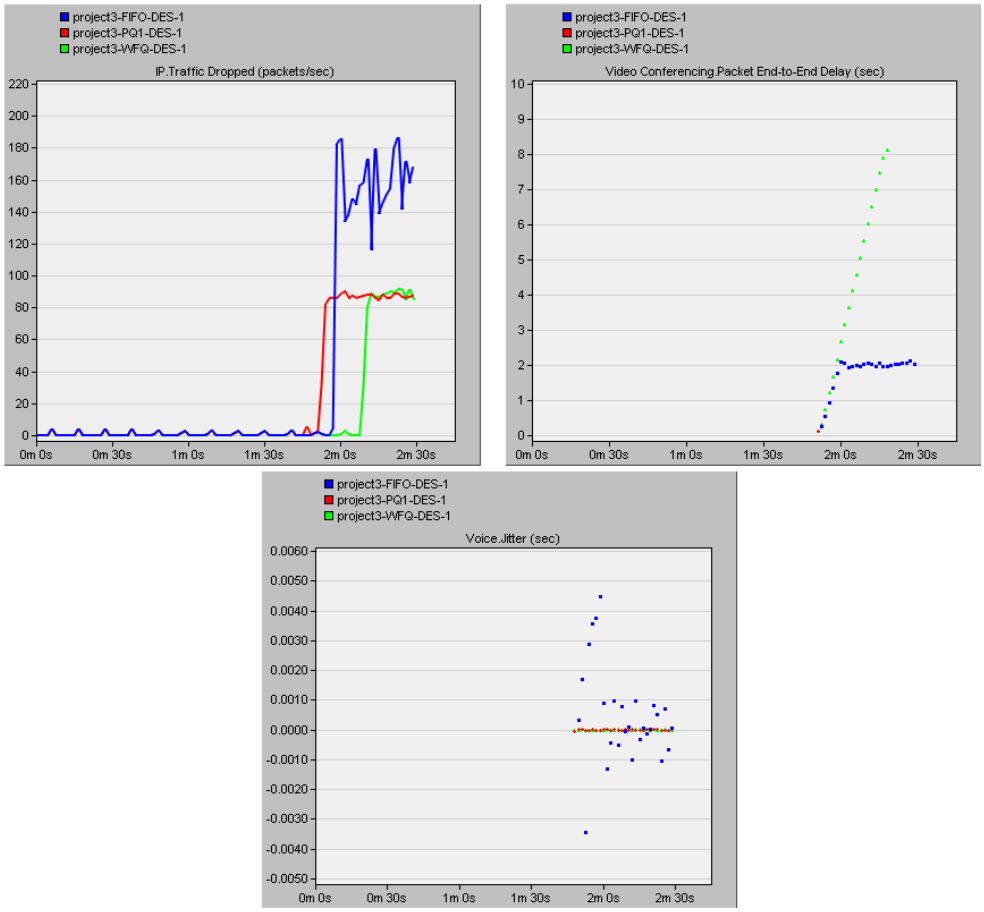


Рисунок 2 – Результаты моделирования

По результатам моделирования можно сделать следующие выводы: при передаче пакетного трафика и мультимедийного трафика целесообразней использовать тип очередей PQ. Такая конфигурации очереди позволяет минимизировать потерю пакетов а также значительно уменьшить сквозную задержку и джиттер при передаче трафика.

Решение задачи обеспечения требуемого качества обслуживания в сетях IP может быть достигнуто прямым путем – на основе предоставления гарантированной полосы пропускания, повышения производительности сетевых устройств – маршрутизаторов и шлюзов, использовании магистралей с высокими пропускными способностями. Однако, наиболее целесообразным представляется применение гибких методов, которые обеспечивают требуемые показатели качества обслуживания при эффективном использовании ресурсов сети для большого набора различных приложений, включая и наиболее критичные аудио- и видеоприложения реального времени.

Список использованных источников:

1. Рекомендация ITU-T Y.1541, Требования к сетевым показателям качества для служб, основанных на протоколе IP, 2006. – 50 с.

2. Ваняшин С.В. Контроль качества предоставления услуг (SLA) в сетях IP/MPLS//Учебное пособие – Самара : ФГОБУ ВПО ПГУТИ, 2013. – 99 с.

3. Тарасов В.Н., Бахарева Н.Ф., Малахов С.В., Ушаков Ю.А. Проектирование и моделирование сетей связи в системе Riverbed Modeler// Учебное пособие – Самара, 2016. – 260 с.

КОНТРОЛЬ И ОПТИМИЗАЦИЯ ЭКСПЛУТАЦИОННЫХ ХАРАКТЕРИСТИК СЕТИ UMTS

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

Лагутик В.В.

Саломатин С.Б. – к.т.н.,доцент

Современные технологии уже давно стали неотъемлемой составляющей нашей жизни. Сегодня трудно представить современного человека без смартфона. Использование ноутбуков, планшетов, мобильных телефонов с возможностью выхода в Интернет для общения, работы, развлечений стало незаменимым и даже обыденным. Число интернет-пользователей возрастает в геометрической прогрессии на протяжении последних лет и эта тенденция, вероятно, продолжится в ближайшие годы. Появляется необходимость постоянного контроля и оптимизации эксплуатационных характеристик сети UMTS.

UMTS (Universal Mobile Telecommunication System) – технология сотовой связи, разработанная Европейским институтом стандар-тов телекоммуникаций (ETSI). Сотовые сети, использующие данную технологию, относят к сетям третьего поколения (сетям 3G). К основным отличиям сетей UMTS от сетей GSM относят использование широкополосных сигналов, и внедрение широкополосной технологии множественного доступа с кодовым разделением каналов (W-CDMA). [1]

В 3G существует несколько типов логических каналов: HS (High Speed), FACH (Forward Access Chanel), URA, IDLE. Интерактивные сервисы (web browsing, online игры), требовательные к скорости и задержкам передаются на канале HS. Background сервис – пакеты малого объема (проверка на смартфоне почты, погоды, ping 32 byte и пр.) в целях экономии ресурсов сети и энергопотребления мобильного терминала передаются на низкоскоростном канале FACH. Оптимальная настройка сети заключается в эффективном использовании абонентом каждого типа канала, в зависимости от типа трафика, его активности и емкости сети. [2] Типы логических каналов представлены на рисунке 1:

Рисунок 1 – Типы логических каналов в 3G

В основе настройки таймерной модели смены состояний лежит баланс между эффективным использованием емкости и минимизации задержек. Пример работы таймеров переходов представлен на рисунке 2. Помимо таймеров сети, каждый смартфон имеет свой собственный таймер (Fast Dormancy), который снижает эффект от увеличения таймера неактивности сети. Изменить таймер FD оператор не может. По истечению этого таймера абонент переходит в режим IDLE. При этом, таймеры сети не учитываются. Производители активируют FD чтобы продлить время работы батареи смартфона. В модемах эта функция не активирована (у модема нет батареи). Для компенсации данного эффекта на сети МТС была активирована одноименная функция “Fast Dormancy”, которая переводит смартфон не в IDLE, а в URA (для терминалов Rel. 8), что позволило уменьшить время задержки при загрузке 1-ой страницы (за счет снижения времени активации HSDPA), значительно снизить сигнальную загрузку и энергопотребление абонентских терминалов. Особенности настроек таймеров перехода представлены на рисунке 3.

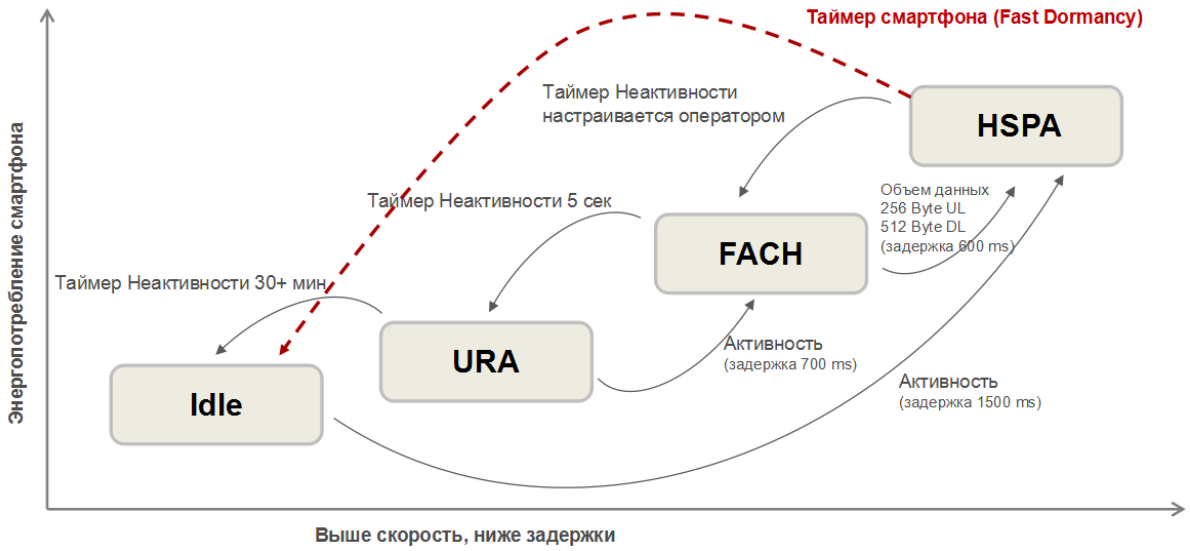


Рисунок 2 – Работа таймеров переходов

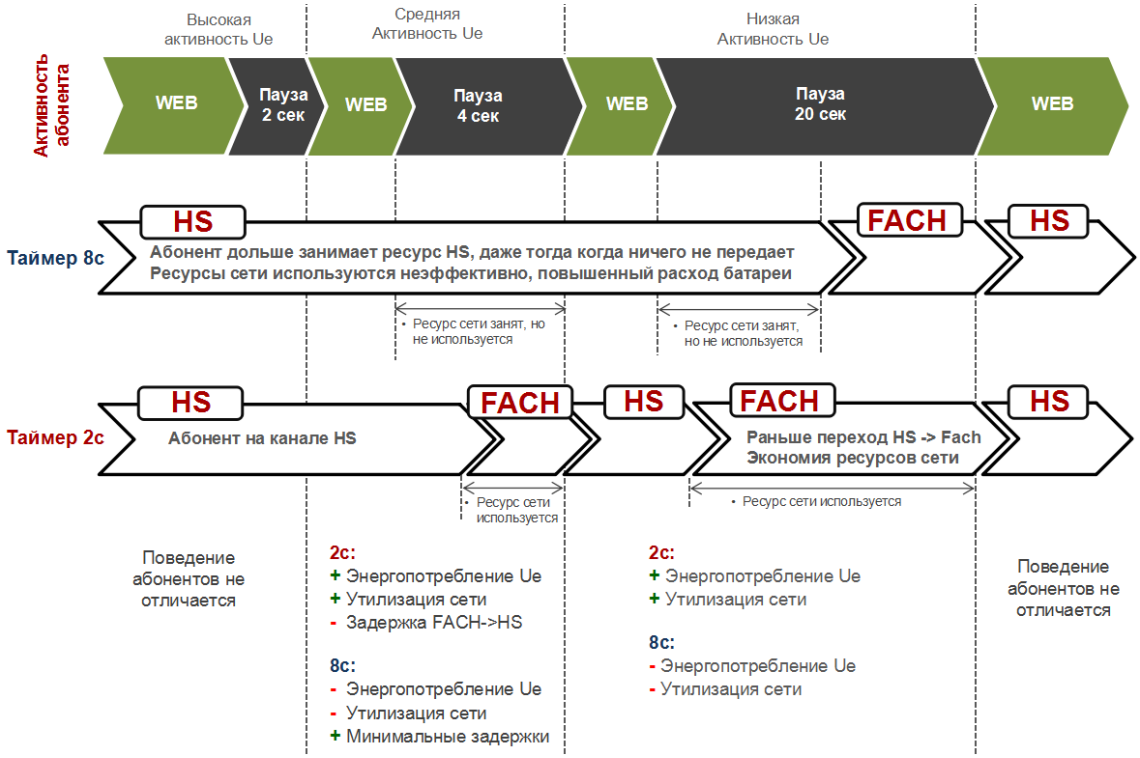


Рисунок 3 – Особенности настроек таймеров перехода

Результаты тестирования настройки таймера перехода из HS в FACH показали:

1 Установки настроек HS Inactivity timers определяют баланс между емкостью и качеством.

2 Увеличение таймера приводит к деградации ключевых показателей эффективности, доступности и непрерывности сети 3G за счет повышения утилизации ее ресурсов.

3 Увеличение Inactivity timer до 4 сек не оказывает положительного влияния на ping.

4 Улучшение ping начинается с Inactivitytimer = 8 сек.

По данным статистики при увеличении Inactivity timer зафиксировано снижение скорости передачи данных (ПД) для трафика большого объема и увеличение скорости фонового трафика. По данным драйв-теста зафиксировано снижение скорости ПД и увеличение “Web Page Open Time”.

Список использованных источников:

1. Попов, Е. А. Сотовые сети мобильной связи стандарта UMTS : учеб. пособие / Е. А. Попов, А. Л. Гельгор – СПб.: Политехн. ун-т, 2011. – 10 с.

2. Каналы в стандарте UMTS [Электронный ресурс]. – Режим доступа : http://pro3gsm.com/kanalyi-v-standarte-umts/

ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ ПРОТОКОЛОВ НА УРОВНЕ ВЗАИМОДЕЙСТВИЯ КЛИЕНТА И СЕРВЕРА

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

Данильчук В.С.

Астровский И.И. – к.т.н., доцент

Веб-приложения - это особый тип программ, построенных по архитектуре "клиент-сервер". Особенность веб-приложения заключается в том, что само приложение находится и выполняется на сервере, в то время как клиентская часть реализует пользовательский интерфейс, формирует запросы к серверу и обрабатывает ответы от него. В работе рассматриваются особенности реализации протоколов функционирующих на уровне взаимодействия клиента и сервера.

Взаимодействие клиента и сервера основано на сетевом протоколе HTTP – протоколе прикладного уровня передачи данных. Протокол HTTP работает с 80 портом протокола TCP. Хотя средства, обеспечивающие поддержку HTTP, можно настроить на работу с любым другим портом, практически все браузеры по умолчанию пытаются сначала установить соединение через порт TCP с номером 80. Именно поэтому подавляющее большинство веб – серверов практически всегда вынуждены опрашивать порт 80. Однако одним из самых очевидных исключений является применение туннелирования протокола HTTP через протокол SSL (Secure Sockets Layer - уровень защищённых сокетов)[1].

Протокол SSL позволяет применить на транспортном уровне шифрование, благодаря которому злоумышленник, вклинившийся в сеанс связи клиента и сервера, уже не сможет увидеть передаваемые команды протокола HTTP в открытом тексте. Однако SSL лишь предоставляет протоколу HTTP “защитную оболочку” - не больше и не меньше. Он не расширяет и не вносит каких-либо существенных изменений в базовый механизм запроса и ответа HTTP. Конечно, в некотором смысле использование протокола SSL повышает безопасность, если и сервер, и клиент задействуют дополнительную возможность протокола, заключающуюся в применении сертификатов клиентов. В настоящее время на основании протокола SSL используется его модифицированная версия, названная TLS (Transport Layer Security - безопасность транспортного уровня). Протоколы SSL/TLS, как правило, используют порт TCP с номером 443 .

Основным объектом манипуляции в HTTP является ресурс, на который указывает URI (Uniform Resource Identifier) — унифицированный идентификатор ресурса в запросе клиента. Обычно такими ресурсами являются хранящиеся на сервере файлы, но ими могут быть и логические объекты. Особенностью протокола HTTP является возможность указать в запросе и ответе способ представления одного и того же ресурса по различным параметрам: формату, кодировке, языку и т.д. Именно благодаря возможности указания способа кодирования сообщения, клиент и сервер могут обмениваться двоичными данными, хотя данный протокол является текстовым.

В отличие от многих других протоколов, HTTP не сохраняет своего состояния. Это означает отсутствие сохранения промежуточного состояния между парами «запрос-ответ». Компоненты, использующие HTTP, могут самостоятельно осуществлять сохранение информации о состоянии, связанной с последними запросами и ответами. Браузер, посылающий запросы, может отслеживать задержки ответов. Сервер может хранить IP-адреса и заголовки запросов последних клиентов. Однако сам протокол не осведомлён о предыдущих запросах и ответах, в нём не предусмотрена внутренняя поддержка состояния, к нему не предъявляются такие требования.

Ключевой частью протокола HTTP являются HTTP cookie . HTTP cookie - это небольшой фрагмент данных, отправляемый сервером на браузер пользователя, который тот может сохранить и отсылать обратно с новым запросом к данному серверу. Это позволяет узнать с одного ли сервера пришли оба запроса, например для аутентификации пользователя [2].

Существует несколько типов протоколов аутентификации, которые можно встраивать в протокол HTTP:

- Базовая: имя пользователя и пароль перекодируются по алгоритму Base64.
- Дайджест: подобна базовой, но вместо паролей передаются дайджесты, что исключает возможность обратной расшифровки пароля.
- NTLM: протокол аутентификации, который реализуется в заголовках запросов и откликов протокола HTTP.

Все эти протоколы аутентификации функционируют поверх протокола HTTP (или SSL/TLS), а данные встраиваются непосредственно в поток данных, передаваемых в ходе обмена запросами и откликами [3].

Список использованных источников:
1. HTTP [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/HTTP
2. Скамбрэй, Д. Hacking exposed: Web Applications // Д. Скамбрэй – 2011.
3. Хол, П. Web Security Testing Cookbook // П. Хол, Б. Вальтер – 2008.

БЕЗОПАСНОСТЬ СЕТИ БЕСПРОВОДНОГО ДОСТУПА

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

Высоцкая В.В.

Лыньков Л.М. – д.т.н., профессор

Большинство современных портативных устройтсв (ноутбуки, КПК, смартфоны) уже имеют встроенные средства для работы в беспроводных сетях. Если беспроводная сеть останется незащищенной, она будет уязвима для доступа из других компьютеров. Защитить домашнюю сеть и сеть малого бизнеса от почти любых форм несанкционированного доступа можно, используя для этого методы защиты.

Угрозы информационной безопасности, возникающие при использовании Wi-Fi сетей, можно условно разделить на два класса:

– прямые – угрозы информационной безопасности, возникающие при передаче информации по беспроводному интерфейсу IEEE 802.11;

– косвенные – угрозы, связанные с наличием на объекте и рядом с объектом большого количества Wi-Fi-сетей.

Есть следующие виды персональной защиты:

1 Открытая и общая сетевая аутентификация. Спецификация 802.11 поддерживает два метода сетевой аутентификации: открытую систему и с использованием общего ключа.

С использованием открытой аутентификации любая станция беспроводной сети может запросить аутентификацию. Аутентификация – это процесс установления подлинности и подтверждения запроса клиента (обычно это ноутбук) для доступа к сети или сетевой точке доступа. После выполнения аутентификации и предоставления доступа клиент получает доступ к сети. Станция, для которой необходима аутентификация для связи с другой станцией беспроводной сети, отправляет управляющий аутентификационный запрос, содержащий ее идентификационную информацию. Приемная станция или точка доступа принимает любой запрос на аутентификацию.

С использованием общего ключа аутентификации каждая станция обязана получить секретный общий ключ через защищенный канал, который независим от коммуникационного канала беспроводной сети 802.11.

2 WEP-шифрование. WEP-шифрование (Wired Equivalent Privacy) использует специальное преобразование данных для предотвращения несанкционированного доступа к данным беспроводной сети. WEP-шифрование использует ключ шифрования для кодирования данных перед их отправкой. Если используется шифрование, все устройства в беспроводной сети должны использовать одинаковые ключи шифрования.

3 WPA-, WPA2-персональная. Режим персональной защиты WPA используется в домашних условиях или сетях малого бизнеса. Для персональной защиты WPA необходимо вручную сконфигурировать предварительно опубликованный общий ключ (PSK) в точке доступа или клиентах. Аутентификация в сервере не используется. Этот пароль, введенный в точке доступа, должен использоваться в этом компьютере и на всех беспроводных устройствах сети для подключения к этой точке доступа. Защита зависит от надежности и секретности пароля. Чем больше длина используемого пароля, тем надежнее защита беспроводной сети.

4 WPA-, WPA2-Enterprise (WPA-предприятие). Корпоративный режим аутентификации предназначен для использования в масштабах предприятий или сетях государственных учреждений. WPA-предприятие проверяет пользователей сети, используя сервер RADIUS или другой сервер аутентификации [1].

Аутентификация 802.1X (корпоративная защита). Аутентификация по стандарту 802.1x – это процесс, независимый от аутентификации по стандарту 802.11. Стандарт 802.11 обеспечивает основы для различных видов аутентификации и протоколов манипулирования ключами. В стандарте 802.1X присутствуют различные типы аутентификации, каждый из которых обеспечивает свой подход к установлению подлинности, но все они используют один протокол 802.11 и структуру для взаимодействия между клиентом и точкой доступа. В большинстве протоколов после выполнения процесса аутентификации стандарта 802.1X приемная сторона (клиент) получает ключ, который она использует для шифрования данных. При аутентификации по стандарту 802.1X используется метод установления подлинности между клиентом и сервером (например, удаленная аутентификация RADIUS – Remote Authentication Dial-In User Service), к которому подключена точка доступа. Процесс аутентификации использует идентификационную информацию, например, пароль пользователя, который не передается через беспроводную сеть. Большинство видов аутентификации 802.1X поддерживают динамические ключи для пользователя, сеанса и для усиления защиты ключа. Аутентификация 802.1X имеет преимущества перед использованием существующего протокола аутентификации EAP (Extensible Authentication Protocol).

Аутентификация стандарта 802.1x для беспроводных сетей имеет три главных компонента:

– аутентификатор (точка доступа);

– запросчик (программное обеспечение клиента);

– сервер аутентификации.

Защита аутентификации стандарта 802.1X инициирует запрос на аутентификацию от клиента беспроводной сети в точку доступа, которая устанавливает его подлинность через протокол EAP в соответствующем сервере RADIUS. Этот сервер RADIUS может выполнить аутентификацию пользователя (с помощью пароля или сертификата) или компьютера (с помощью адреса MAC). Теоретически, клиент беспроводной сети не может войти в сеть до завершения транзакции. (Не все методы аутентификации используют сервер RADIUS. WPA-персональная и WPA2-персональная используют общий пароль, который вводится в точке доступа и в устройствах, запрашивающих доступ к сети). Существует несколько аутентификационных алгоритмов, используемых со спецификацией 802.1X. Эти методы используются при идентификации клиента беспроводной локальной сети в сервере RADIUS. Во время аутентификации в сервере RADIUS пользователи проходят проверку в специализированных базах данных. Аутентификация RADIUS основана на наборе стандартов, предназначенных для аутентификации, авторизации и ведения учетных записей (Authentication, Authorization и Accounting – AAA). Сервер RADIUS содержит прокси-процесс для проверки клиентов в многосерверной среде. Стандарт IEEE 802.1X предоставляет механизм для управления и аутентифицированного доступа к беспроводным сетям на основе портов 802.11 и проводных сетей Ethernet. Управление сетевым доступом, основанным на использовании портов, подобно инфраструктуре локальной сети, управляемой с помощью коммутаторов, которая идентифицирует устройство, подключенное к порту ЛС, и запрещает доступ к этому порту, если процесс аутентификации был неудачен [2].

Протокол аутентификации RADIUS. RADIUS (Remote Authentication Dial-In User Service) – это сервис протокола клиент-сервер для авторизации, аутентификации и ведения учетных записей (Authorization, Authentication и Accounting – AAA), который используется для регистрации клиентов в сервере сетевого доступа по коммутируемой линии. Обычно сервер RADIUS используется поставщиками услуг доступа в Интернет (Internet Service Providers – ISP) для выполнения задач AAA. Далее описаны фазы AAA:

1 Фаза аутентификации (Authentication): Проверяется имя пользователя и пароль в базе данных. После проверки идентификационной информации начинается процесс авторизации.

2 Фаза авторизации (Authorization): Определяется, было ли дано разрешение на запрос доступа к ресурсам. Назначается IP-адрес для клиента, выполняющего доступ по коммутируемой линии (Dial-Up).

3 Фаза ведения учетной записи (Accounting): Выполняется сбор информации об используемых ресурсах для оценки, аудита, учета времени сеанса или учета стоимости затрат.

В сетях Wi-Fi используются следующие виды шифрования данных:

1 AES – CCMP. Advanced Encryption Standard – Counter CBC-MAC Protocol (улучшенный стандарт шифрования – протокол Counter CBC-MAC). Это новый метод защиты при беспроводной передаче данных, определенный в стандарте IEEE 802.11i. Протокол AES-CCMP обеспечивает более надежный метод шифрования в сравнении с TKIP. AES-CCMP используется в качестве метода шифрования, когда необходима повышенная безопасность данных. Протокол AES-CCMP доступен для сетевой аутентификации
WPA/WPA2-персональная/предприятие.

2 TKIP. Протокол TKIP (Temporal Key Integrity Protocol) использует функцию смешения содержимого ключа для каждого пакета, проверку целостности сообщений и механизм манипуляций с ключом. Протокол TKIP доступен для сетевой аутентификации WPA/WPA2-персональная/предприятие.

3 CKIP. Cisco Key Integrity Protocol (CKIP) – это собственный протокол защиты Cisco для шифрования в среде 802.11. Протокол CKIP использует следующие особенности для усовершенствования защиты 802.11 в режиме «infrastructure»:

- Key Permutation (KP) – манипуляции с ключом;
- Message Sequence Number – номер последовательности сообщения.

4 WEP. WEP-шифрование (Wired Equivalent Privacy) использует специальное преобразование данных для предотвращения несанкционированного доступа к данным беспроводной сети. WEP-шифрование использует ключ шифрования для кодирования данных перед их отправкой. Только компьютеры, использующие этот же ключ, могут получить доступ к сети и расшифровать переданные другими компьютерами данные. Корпоративная WEP-защита отличается от персональной WEP-защиты тем, что для нее может быть выбрана открытая сетевая аутентификация, а затем можно выбрать 802.1X и указать нужный тип аутентификации клиентов [3]. Выбор типов аутентификации недоступен для персональной защиты WEP.

Список использованных источников:

1. Шифрование wi-fi сети, какой метод выбрать? [Электронный ресурс]. – https://wifiget.ru.
2. Configuring IEEE 802.1X Port-Based Authentication.
3. Обзор возможностей защиты [Электронный ресурс]. – Режим доступа: http://support.elmark.com.pl.

АУДИТ IT-ИНФРАСТРУКТУРЫ

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

Фурса Д.А..

Лыньков Л.М. – д.т.н., профессор

Аудит IT-инфраструктуры – это комплекс мероприятий, включающих в себя исследование составных частей информационной системы предприятия, проводимого независимыми специалистами по согласованному с заказчиком плану, в соответствии с выбранной методикой и критериями. Услуга предназначена для организаций, которым требуется оценить эффективность существующей информационной системы, максимально полно задействовать и оптимизировать имеющиеся ресурсы, а также профессионально определить основные проблемы и получить рекомендации по их устранению [1].

Составные части ИТ аудита:

1 Аудит оборудования:

а) обследование состояния рабочих мест и оргтехники;

б) обследование состояния серверов;

в) анализ состояния активного и пассивного сетевого оборудования, кабельной системы;

г) анализ функционирования серверного оборудования и соответствия требованиям;

д) анализ источников бесперебойного питания, их достаточности;

2 Аудит программного обеспечения:

а) обследование установленного программного обеспечения на рабочих машинах и серверах компании;

б) проверка программного обеспечения на наличие лицензий, прав на его использование, соответствие количества лицензий и установленных программ;

3 Аудит каналов связи и коммуникации:

а) обследование каналов передачи данных;

б) анализ работы телефонии;

в) анализ работы и настроек корпоративной электронной почты;

4 Аудит систем безопасности:

а) обследование использующихся систем информационной безопасности;

б) проверка работы антивирусной защиты и антиспам защиты электронной почты;

в) обследование систем защиты от взлома инфраструктуры;

г) анализ возможных путей доступа к информации компании;

д) обследование межсетевых настроек безопасности;

е) анализ настроек сетевых политик;

ж) анализ системы хранения и бэкапирования данных.

Существует несколько видов аудита - экспресс, комплексный и направленный.

Экспресс-аудит проводится с целью оценки сложности ИТ-инфраструктуры, найти проблемные места, оценить оптимальность использования оборудования, правильность его функционирования. Срок проведения экспресс ИТ-аудита обычно от одного до трех рабочих дней, в зависимости от сложности инфраструктуры.

Комплексный ИТ аудит – это полная проверка состояния ИТ-инфраструктуры компании и создание глобального проекта по модернизации для достижения важных показателей эффективности – качества, экономичности и вариативности системы.

Этапы комплексного ИТ аудита:

- сбор всей необходимой информации об инфраструктуре;
- создание проекта по модернизации и оптимизации всей информационной системы.

Направленный ИТ-аудит – это получение информации об отдельных элементах ИТ-инфраструктуры: аудит СКС: обследование кабельной сети, активного сетевого оборудование, коммутация, измерение скорости передачи данных; аудит серверной инфраструктуры: обследование настроек, производительности, систем защиты и архивирование; аудит различных сетевых служб: электронная почта, телефонии, облачные сервисы и т.д [2].

Список использованных источников:

1. Аудит IT-инфраструктуры [Электронный ресурс]. – Режим доступа: http://www.its.by.
2. Аудит IT инфраструктуры [Электронный ресурс]. – Режим доступа: http://it-partner.ru/.

ПРОГНОЗИРОВАНИЕ РАСПОЛОЖЕНИЯ ТРАНСПОРТНЫХ СРЕДСТВ В ГОРОДЕ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ ГЛУБОКОГО ОБУЧЕНИЯ

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

Настин А. А.

Королев А.И. – к.т.н., доцент

Искусственная нейронная сеть (ИНС), часто называемая «нейронная сеть», математическая модель или вычислительная модель, основывающейся на биологических нейронных сетях, другими словами, есть эмуляция биологической нейронной системы. Она содержит взаимосвязанные группы искусственных нейронов и информацию процесса с использованием подхода соединительных вычислений. В большинстве случаев ИНС адаптивная система которая имеет изменяющуюся структуру, которая основывается на внешних и внутренних информационных потоках через сеть в течении обучающей фазы.

Виды искусственных нейронных сетей.

Прямая нейронная сеть. Прямая нейронная сеть была первой изобретенной сетью простейшего типа искусственной нейронной сети. В этой сети информация двигалась только в одно направление вперед, из входных узлов, через скрытые узлы к выходным узлам. В сети нет циклов или петлей. Обработка данных могла перемножаться единицами, но связи с обратной связью отсутствуют, что значит, соединения растягиваются из выходных единиц к входным единицам в том же слое или предыдущих слоях.

Рекуррентная сеть. Рекуррентная нейронная сеть содержит соединения обратной связи. В отличии от прямой сети, рекуррентная нейронная сеть (РНС) является моделью с двунаправленным потоком данных. Пока прямая нейронная сеть передает данный линейно из входного слоя в выходной слой, РНС также передаёт данные из поздних этапов обработки к ранним этапам.

Обучение искусственной нейронной сети.

Нейронная сеть должна быть сконфигурирована, так что бы применение данных на вход давала желаемый набор данных на выход. Различные методы устанавливают сильные стороны существующих соединений. Один из способов заключается в том, чтобы весы явно использовали априорное знание. Другой способ тренировать нейронную сеть кормить ее шаблонами и позволяя ей изменять свои веса в соответствии с некоторыми учебными правилами. Обучающие правила категорируются следующим образом:

Контролируемое обучение или ассоциативное обучение, в котором обученная сеть предоставляет входные и согласованные выходные шаблоны. Эти входные, выходные пары могут быть представлены внешним учителем или системой, которая содержит нейронную сеть.

Бесконтрольное обучение или самоорганизация, которая пока не будет обучено реагировать на кластеры шаблона внутри входа. В этой парадигме система предполагает обнаружить статистически характерные черты входной совокупности. В отличие от парадигмы контролируемого обучения нет приоритетного набора категорий, в которые должны классифицироваться шаблоны скорее система должна разработать собственное представление входных стимулов.

Усиленное обучение. Этот тип обучения может быть рассмотренный как промежуточный формой из выше перечисленных двух типов обучения. Вот машинное обучение делает какое-то действие в окружающей среде и получает обратную связь из окружающей среды. Система обучения оценивает свои действие хорошо или плохое на основе ответа и соответственно корректирует его параметры.

Список использованных источников:

1. Rakesh Agrawal, Sakti Ghosh, Tomasz Imielinski, Bala Iyer, and Arun Swami, An Interval Classier for Database Mining Applications, VLDB 92 , Vancouver, British Columbia, Canada.

2. Силен Д., Мейсман А., Али М., Основы Data Science и Big Data. Python и наука о данных, Питер, 2012 – 336с.

ДИСКРЕТНОЕ МОДЕЛИРОВАНИЕ ТРАНСПОРТНОЙ СИСТЕМЫ ГОРОДА

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

Степанов Н.В.

Дворников В.Д. – к.т.н.,доцент

В работе рассматривается применение имитационного моделирования для оценки городского траффика. Рассмотрены методы моделирования транспортных систем для определения основных показателей с целью обеспечения качества пассажирских перевозок. Анализ результатов программы дает возможность определить показатели моделируемой системы.

Быстрые темпы роста городского населения и увеличение его подвижности порождают целый ряд проблем, связанных с развитием транспорта в городах. Управление транспортной системой является одной из основных составных частей инфраструктуры города, которая обеспечивает жизненно важные потребности населения.

Одной из первостепенных задач управления транспортным хозяйством является создание оптимальных маршрутов и интервалов движения рейсовых автобусов. Сложность ее решения состоит в необходимости точного определения потока пассажиров и распределение его во времени в течение дня[3]. Решение этой задачи позволяет сократить простой автобусов, исключить отмену рейсов, повысить эффективность использования подвижного состава. Вместе с тем оптимальное планирование перевозок позволяет повысить производительность автобусов при одновременном снижении количества подвижного состава, поступающего на маршрут при том же пассажиропотоке и высвободить из сфер обращения значительные материальные ресурсы автопарка[2].

В связи этим, целью исследований являлось построение математической модели для решения задачи маршрутизации при распределении пассажирских и транспортных потоков, учитывающей специфику перемещений пассажиров в городе. Особенностью транспортного потока городской сети является его сложный структурный состав. Он включает множество потоков: внутренние потоки индивидуального транспорта, потоки общественного транспорта (городского и маршрутного) и другие. Для обеспечения ритмичного функционирования всей транспортной системы города необходимо учитывать результат воздействия одного потока на другой и их взаимодействие с внешней средой. Особенностью пассажирского потока является его изменяющийся объем на каждой точке городской сети. При этом транспортные сети являются объектами графовой структуры и поэтому для их исследования применимы методы теории графов. Но алгоритмы и модели, построенные на основе этих методов, не позволяют учесть динамически изменяющиеся характеристики и случайный фактор при функционировании транспортных систем [1].

Соответственно для формирования обоснованной маршрутной сети городского общественного пассажирского транспорта в первую очередь необходимо определить величины и характеристики пассажиропотоков, движущихся по территории города.

При исследовании пассажиропотоков основными параметрами (факторами), непосредственно влияющим на их изменение являются:

1. час суток;
2. день недели;
3. месяц сезона года.

Диапазоны изменений факторов весьма значительны, что приводит к появлению большого количества вариантов различных сочетаний параметров. Таким образом, возникает сложная очень трудоемкая задача получения статистического материала по изменению пассажиропотоков по всей территории города. Решение этой задачи сплошным обследованием практически невозможно из-за значительной трудоемкости, а значит дороговизне исследований. Таким образом, необходима математическая модель, адекватно описывающая происходящие процессы и позволяющая с минимальной трудоемкостью получить необходимый статистический материал[4].

Список использованных источников:

1. Липенко, А.В. О разработке имитационной модели городских пассажирских перевозок./А.В. Липенко, Н.А. Кузьмин, О.А. Маслова // Актуальные вопросы инновационного развития транспортного комплекса: материалы международной научно-практической конференции. – Орел, 2011 г. – т.2. – с.50-54.

2. Михайлов, А.Ю. Адаптация методов расчета остановочных пунктов маршрутного пассажирского транспорта к современным условиям / А.Ю. Михайлов [и др.] // Организация и безопасность дорожного движения в крупных городах. - . С-Петербург, 2006 г. – с.205-211.

3. Пыталев, О.А. Определение оптимального числа транспортных средств городского пассажирского транспорта.//Вестник УрГУПС. – 2009 г. – Выпуск 4. – с.120-123.

4. Волкова, М.Н. Логистика пассажирских перевозок в крупном промышленном районе // Приазовский государственный технический университет. – 2011 г.. – с.2-3.

СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ И КОНТРОЛЯ ДОСТУПА ЖИЛОГО ДОМА

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

Чечко А.С.

Ловчий Н.Н. – ассистент

Система видеонаблюдения — система аппаратно-программных средств, предназначенная для осуществления видеонаблюдения.

Система контроля и управления доступом (СКУД)- это совокупность технических средств и организационных мероприятий, которые позволяют контролировать доступ к объектам и отслеживать перемещение людей по охраняемой территории. На данный момент времени, эти системы признаны одним из наиболее эффективных методов решения задач комплексной безопасности для объектов.

От уровня вероятных угроз и поставленных перед системой задач, зависит необходимость подбора оптимального соотношения между людьми и техническими ресурсами системы. Установка системы видеонаблюдения и контроля доступа, позволит не только поднять уровень общей безопасности, но и сократить издержки затрат на ее обеспечение, поскольку они не требуют большого количества персонала для обслуживания, экономичны в потреблении электроэнергии.

В упрощённом виде принцип работы системы видеонаблюдения следующий: видеокамеры и микрофоны «снимают» видеоинформацию с определённой точки объекта и отправляют её на записывающее устройство, которое переводит информацию в специальный формат для её последующего архивирования. Одновременно с этим камера посылает данные на видеомонитор, контролируемый оператором-наблюдателем. Также в систему могут входить дополнительные устройства считывания информации, устройства беспроводной связи, таймеры, датчики движения, удаленные рабочие станции и т.д. для расширения функциональных возможностей и количества видеоканалов системы.

Основные плюсы системы видеонаблюдения:

- безопасность;
- можно следить за всем что происходит (за своими детьми ,которые играют во дворе);
- если залезут воры, можно увидеть, куда они направляются и придумать, как их прогнать;
- если на улице посторонние звуки, можно просто посмотреть на экран и узнать, что происходит;
- если залезут воры, можно увидеть, куда они направляются и придумать, как их прогнать;
- если в квартиру (или дом) вломились посторонние, с помощью программы на телефоне можно наблюдать за квартирой, и вызвать полицию в любой момент;
- камера позволит доказать виновность того или иного человека в краже ваших вещей.

Недостатки системы видеонаблюдения:

- вторжение в личную жизнь детей или соседей;
- стоимость камер и оплата услуг по их установке мастеру;
- нужно научиться разбираться в программном обеспечении камеры;
- если камера во дворе, её могут разбить;
- иногда следует ремонтировать камеры.

Эффективность использования любых технических средств систем видеонаблюдения и контроля доступа зависит от применяемой технологии контроля доступа и квалификации оперативно-технического персонала.

Список использованных источников:

1. Крахмалев А.К. Средства и системы контроля и управления доступом. Учебное пособие. М.: НИЦ "Охрана" ГУВО МВД России. 2003.
2. Горлицин И. Контроль и управление доступом - просто и надежно КТЦ "Охранные системы", 2002.

СИСТЕМЫ ХРАНЕНИЯ ВИДЕОКОНТЕНТА ДЛЯ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ И КОНТРОЛЯ

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

Чечко А.С.

Ловчий Н.Н. – ассистент

Система видеонаблюдения – это важный элемент в охране нашего имущества и жизни, который позволяет не только предоставить доказательную базу правонарушений, но и в некоторых случаях предотвратить их. Самой главной частью любой системы видеонаблюдения является архив записей с камер. Его можно хранить видеорегистраторе, на карте памяти, персональном компьютере или видеосервере. Решение выбирается в зависимости от масштабности системы. В случаях, когда потеря даже одного кадра критична, следует достаточно серьезно подойти к организации хранения видеоархива. Учитывая то, что информацию нужно хранить в течение определенного времени (в зависимости от специфики объекта), часто требуется несколько винчестеров (жестких дисков).

Прежде чем установить систему видеонаблюдения, стоит спроектировать политику хранения данных. Самый очевидный способ - последовательное заполнение дисков. Но, в то же время, и самый устаревший и ненадежный.

Другой способ – это выделить по диску на каждую группу камер видеонаблюдения. Надежность такой организации невелика, за то возрастает быстродействие. В том случае, если один из дисков вышел из строя, то потеряется весь архив данных с этого участка объекта.

Ещё одно решение - организация RAID-массива. Информация делится на небольшие части и раскидывается в случайном порядке на все диски одновременно. Один из них хранит контрольную сумму, которая необходима для восстановления, если какой-нибудь из винчестеров перестанет работать. Raid-массив - достаточно надежный способ хранения данных. Недостатки этого варианта в настройке, требующей определенных знаний, а любая ошибка системного администратора может привести к неизбежным для архива последствиям.

Также при проектировании архива можно использовать технологию MDR (Multi Disk Record). В этом случае поток распределяется по всем дискам и сохраняется по пять Мегабайт на каждом. То есть, при выходе из строя одного из носителей, теряется только каждый четвертый отрезок записи в 5 Мб (при условии, что установлены четыре диска).

Любые системы видеонаблюдения используют облачную инфраструктуру для получения удаленного доступа к видеоархиву, к онлайн просмотру.

Можно отметить четыре основных сценария использования облачной инфрастуктуры:

1.Доступ к онлайн просмотру и видеоархиву на SD карте камеры

Преимущества: низкая стоимость, высокая скорость развертывания, большой выбор оборудования, минимальная и легкая настройка.

Недостатки: видеоархив может быть утрачен, так как. SD карта легко извлекается из видеокамеры. Небольшой размер видеоархива. Низкий срок службы SD карт.

2.Доступ к онлайн просмотру и видеоархиву на NVR, NAS, сервере

Преимущества: большой выбор оборудования. Большая емкость видеоархива. Доступ к видеоархиву предоставляется в виде профессионального программного интерфейса.

Недостатки: видерегистратор, а значит и видеоархив может быть утрачен. Высокая цена на специализированные жесткие диски для видеонаблюдения.

3.Доступ к онлайн просмотру и видеоархиву в дата-центре (хостинг видео)

Достоинства: безопасность хранения и стабильность доступа к видеоархиву. Доступ к видеоархиву предоставляется в виде профессионального программного интерфейса для работы с видеоархивом.

Недостатки: ограниченная доступность аппаратного обеспечения. Постоянные затраты на абонентскую плату.

4.Доступ к онлайн просмотру и видеоархиву на NVR или NAS и бэкап видеоархива в облако

Преимущества: безопасность хранения видеоархива обеспечивается высшей степенью надежности центра обработки данных.

Недостатки: высокая стоимость хранения видео, низкая пропускная способность каналов связи. Затраты на абонентскую плату.

Список использованных источников:

1. Абрамов А.М., Никулин О.Ю, Петрушин А.И. Системы управления доступом. М.: "Оберег-РБ", 1998.
2. Барсуков, В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. - М., 2001

MOBILITY MODELS in MOBILE Ad Hoc NETWORKS

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

Vladislaw Belan, Nouri Zaid Ihsan Nauri, Mohammed Mozahim
М.Ю. Хоменок – к.т.н., доцент

A Mobile Ad hoc NETwork (MANET) is a collection of wireless mobile nodes forming a self-configuring network without using any existing infrastructure. Since MANETs are not currently deployed on a large scale, research in this area is mostly simulation based, figure1

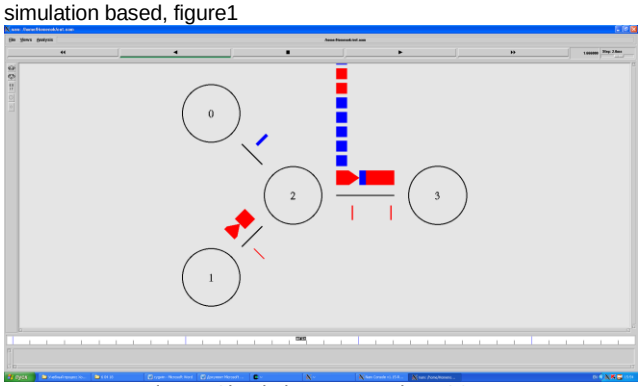


Fig. 1 - Simulation Process by NS2.

Among simulation parameters, the mobility model plays a very important role in determining the protocol performance in MANET. Thus, it is essential to study and analyze various mobility models and their effect on MANET protocols. In the near future, MANETs could potentially be used in various applications such as mobile classrooms, battlefield communication and disaster relief applications.

To thoroughly and systematically study a new Mobile Ad hoc Network protocol, it is important to simulate this protocol and evaluate its protocol performance. Protocol simulation has several key parameters, including mobility model and communicating traffic pattern, among others.

The mobility model is designed to describe the movement pattern of mobile users, and how their location, velocity and acceleration change over time. Since mobility patterns may play a significant role in determining the protocol performance, it is desirable for mobility models to emulate the movement pattern of targeted real life applications in a reasonable way. Otherwise, the observations made and the conclusions drawn from the simulation studies may be misleading.

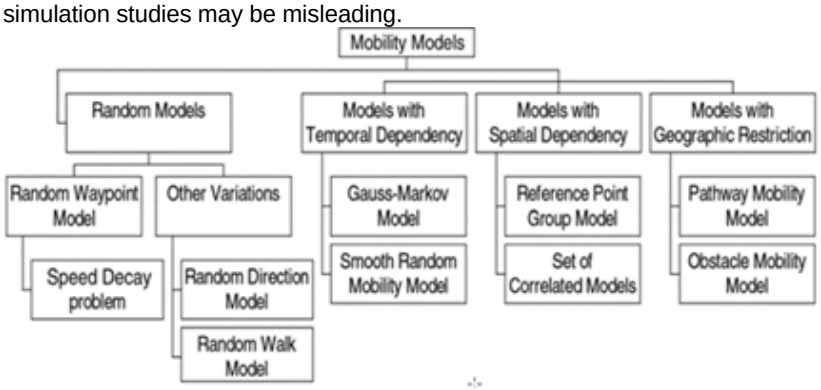


Fig.2 - A Survey of Mobility Models.

Thus, when evaluating MANET protocols, it is necessary to choose the proper underlying mobility model. For example, the nodes in Random Waypoint model behave quite differently as compared to nodes moving in groups. It is not appropriate to evaluate the applications where nodes tend to move together using Random Waypoint model. Therefore, there is a real need for developing a deeper understanding of mobility models and their impact on protocol performance.

One intuitive method to create realistic mobility patterns would be to construct trace-based mobility models, in which accurate information about the mobility traces of users could be provided. However, since MANETs have not been implemented and deployed on a wide scale, obtaining real mobility traces becomes a major challenge. Therefore, various researchers proposed different kinds of mobility models, attempting to capture various characteristics of mobility and represent mobility in a somewhat 'realistic' fashion. Much of the current research has focused on the so-called synthetic mobility models that are not trace-driven.

For mobility patterns in wireless cellular networks, researchers mainly focus on the movement of users relative to a particular area (i.e., a cell) at a macroscopic level, such as cell change rate, handover traffic and blocking probability. However, to model and analyze the mobility models in MANET, we are more interested in the movement of individual nodes at the microscopic-level, including node location and velocity relative to other nodes, because these factors directly determine when the links are formed and broken since communication is peer-to-peer.

One frequently used mobility model in MANET simulations is the Random Waypoint model, in which nodes move independently to a randomly chosen destination with a randomly selected velocity. The simplicity of Random Waypoint model may have been one reason for its widespread use in simulations. However, MANETs may be used in different applications where complex mobility patterns exist. Hence, recent research has started to focus on the alternative mobility models with different mobility characteristics. In these models, the movement of a node is more or less restricted by its history, or other nodes in the neighborhood or the environment. Figure 2 provides a categorization for various mobility models into several classes based on their specific mobility characteristics. For some mobility models, the movement of a mobile node is likely to be affected by its movement history. This type of mobility model is mobility model with temporal dependency. In some mobility

scenarios, the mobile nodes tend to travel in a correlated manner. Such models are mobility models with spatial dependency. Another class is the mobility model with geographic restriction, where the movement of nodes is bounded by streets, freeways or obstacles.

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.

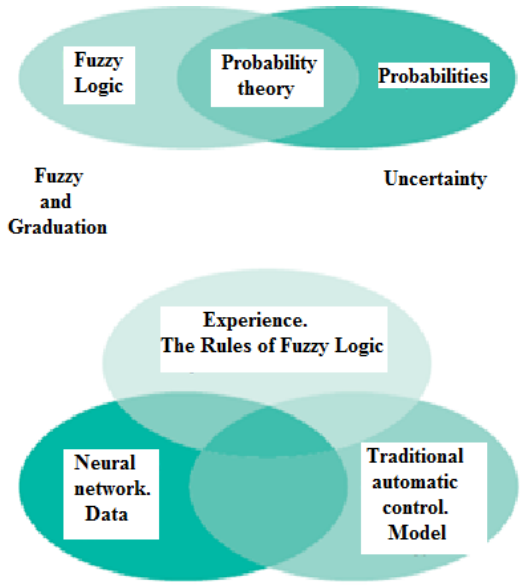
3. Урядов В.Н., Глущенко Д.В. Коллективная пассивная WDM сеть с независимым доступом к оптической среде передачи // Современные средства связи : материалы XIV Междунар. науч.-техн. конф., 29 сент.-1 окт. 2009 года, Минск, Респ. Беларусь. – Минск : ВГКС, 2009. – 23с.

FUZZY LOGIC INTO CONTROL SYSTEM CHALLENGES

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

Nguen Hong Kuan, Al Sabeeh Amjad Karim
М.Ю. Хоменок – к.т.н., доцент

Initially it was just a theory, and at the present time fuzzy logic has turned into a full-fledged management technique. Fuzzy logic does not completely replace the traditional methods of management, but on the contrary it is used in conjunction with traditional methods and makes it easier to create and expand the possibilities of traditional methods.



Comparison of Fuzzy Logic with other control technologies.

Fuzzy logic is based on the following observations:

- knowledge and skills that a person often uses to solve a problem are not perfect, in particular, they can be questionable (people may not be sure of their effectiveness) or not tested;

- a person often solves complex problems on the basis of rough initial data (the accuracy of the initial data is not required), for example, in order to choose an apartment for living, a person can consider different initial data, among which there may be an area, proximity to shops, distance to work and rent price. For that, however, the accuracy of all parameters of the initial information is not required;

- in industry, operators very often solve complex problems with ease, without first studying the possible problem and modeling the system. Just as for driving a car, preliminary modeling of the trip is not required, despite the fact that the car is a very complex system and the trip may not be easy. The more complex the system, the more difficult it is to model and predict its behavior during work.

From all that has been said above, we can draw the following conclusions:

- It is often easier and more useful to model the behavior of a control system operator than to simulate the operation of the system itself;

- instead of using precise mathematical calculations and equations, it is more effective to use qualitative assessments of the situation and apply appropriate processing measures.

Fuzzy logic is well known to engineers as programmers of control systems, as a convenient tool for programming and monitoring process control applications.

By analogy with traditional process controls, fuzzy logic systems can be used to describe the control loops and participate in the calculation of the control action in accordance with one or more reference points for one or more measurements.

Fuzzy logic rules allow to provide:

- application of existing management experience;

- use flexible rules if it is impossible to accurately model the system using traditional means;

- improvement of management quality through self-regulation of the management system and proactive change in the output impact, based on events that cannot be taken into account in the case of traditional management methods.

Fuzzy rules will allow to make control in a case when there is no possibility of control in manual mode or according to known rules. When there is accumulated experience and / or know-how, they can be transformed into rules of fuzzy logic and provide management in the simplest way. Fuzzy logic, besides this, allows you to get the maximum benefit from practical experience and to ensure the absence of losses.

Applications of Artificial Intelligence Techniques (AITs) took place in many areas including medicine such as diagnosis, treatment of illness, patient pursuit, prediction of disease risk and etc. As result AITs allow designing systems that let you build intelligent models for both predicting patients' response in treatment process and determining prediction of illness risk. Since these fields have very high complexity and especially uncertainty, the use of AITs such as fuzzy logic, artificial neural networks, genetic algorithms, artificial immune systems and others have been developed by many researchers.

Fuzzy logic approach, rather than a certain or binary logic, uses a logic and decision mechanism which does not have certain boundaries like human logic. With this concept coined, one of its most common implementation was

in fuzzy logic-based control mechanisms. Fuzzy logic control systems do not require complete model knowledge as in the other known control systems like proportional integral. For this purpose, many design methods have been derived.

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.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ И КАЧЕСТВА ОБСЛУЖИВАНИЯ МУЛЬТИСЕРВИСНОЙ СЕТИ

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

Королев А.И. – к.т.н.,доцент

Для объединения нескольких параллельных каналов передачи данных в сетях Ethernet в один логический используется агрегирование каналов. Использование агрегирования каналов позволяет не только увеличить пропускную способность в сети передачи данных, но и повысить надежность самой сети в случае падения одного или нескольких физических каналов передачи данных[1].

Технология агрегирования каналов в зависимости от поставщика оборудования может иметь различные наименования: Port Trunking, EtherChannel, LAG, Port Channel, Ethernet trunk и т.д. Суть данной технологии заключается в том, что происходит объединение нескольких физических интерфейсов в один логический (Рис.1).

Преимущество агрегации каналов в том, что скорость всех используемых адаптеров суммируется. Также в случае отказа интерфейса, трафик посылается следующему работающему адаптеру, без прерывания сервиса. Большинство технологий по агрегированию позволяют объединять только параллельные каналы, которые начинаются на одном и том же устройстве и заканчиваются на другом.

Схема агрегированного канала представлена на рисунке 1:

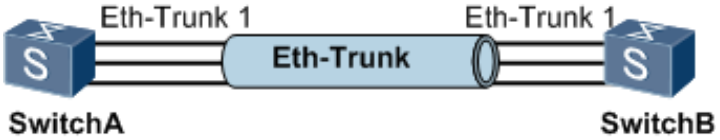


Рис. 1 - Структура агрегированного канала

Если рассматривать избыточные соединения между коммутаторами, то без использования специальных технологий для агрегирования каналов, передаваться данные будут только через один интерфейс, который не заблокирован STP. Такой вариант позволяет обеспечить резервирование каналов, но не дает возможности увеличить пропускную способность (Рис.2) [2].

Принцип резервирования каналов показан на рисунке 2:

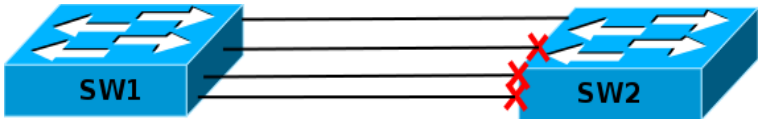


Рис. 2 – Структура резервирования каналов

Без использования STP такое избыточное соединение создаст петлю в сети. Технологии по агрегированию каналов позволяют использовать все интерфейсы одновременно. При этом устройства контролируют распространение широковещательных фреймов (а также multicast и unknown unicast). Для этого коммутатор, при получении широковещательного фрейма через обычный интерфейс, отправляет его в агрегированный канал только через один интерфейс, а при получении широковещательного фрейма из агрегированного канала, не отправляет его назад.

Технологии по балансировке нагрузки в агрегированных каналах, как правило, ориентированы на балансировку по таким критериям: MAC-адресам, IP-адресам, портам отправителя или получателя (по одному критерию или их комбинации). То есть, реальная загруженность конкретного интерфейса никак не учитывается. Поэтому один интерфейс может быть загружен больше, чем другие. Более того, при неправильном выборе метода балансировки (или если недоступны другие методы) или в некоторых топологиях, может сложиться ситуация, когда реально все данные будут передаваться, например, через один интерфейс.

Применение технологии агрегирования каналов связи в сетях передачи данных позволяет увеличить пропускную способность самого канала, а так же повысить безотказность сети, путем резервирования каналов связи[3].

Список использованных источников:

1. Сетевая академия Cisco [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010100001.html – (Дата обращения: 09.04.2018).

2. Официальный сайт компании Huawei [Электронный ресурс]. – Режим доступа: http://support.huawei.com/enterprise/docinforeader!loadDocument1.action?contentId=DOC1000001283&partNo=10052 – (Дата обращения: 09.04.2018).

3. Точка обмена знаниями по UNIX/Linux-системам, системам с открытым исходным кодом, сетям и другим родственным вещам [Электронный ресурс]. – Режим доступа: http://xgu.ru/wiki/Агрегирование_каналов – (Дата обращения: 09.04.2018).

ИЗМЕРИТЕЛЬНЫЙ ПРИЕМНИК ДЛЯ КОНТРОЛЯ КАНАЛОВ СВЯЗИ ПО ЛИНИЯМ ЭЛЕКТРОПЕРЕДАЧИ

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

Цык А.В.

Шатило Н.И. – к.т.н.,доцент

Измерительные приемники контроля каналов связи по линиям электропередачи не выпускаются более 20 лет, за это время изменились требования к такой аппаратуре в соответствии с рекомендациями МЭК, поэтому использовать имеющуюся аппаратуру не представляется возможным.

В настоящее время существует много информации, касающейся измерений параметров и эксплуатации каналов связи сетей общего пользования. Однако, кроме сетей общего пользования, существуют и сети связи специального назначения, например, ведомственные сети. Сети связи специального назначения (СССН) предназначены для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка. Анализ особенностей работы на таких сетях связи, эксплуатационных характеристик каналов связи таких сетей – важная задача при разработке новой специальной техники связи, ее линейных испытаниях и опытной эксплуатации.

Для СССН очень остро стоит проблема «переходного периода» от аналоговых сетей к цифровым. Есть два пути ее решения. Либо полностью менять аналоговую сеть на цифровую, либо создавать каналообразующую и прочую специальную аппаратуру связи для существующих сетей связи с учетом их развития. На полную замену кабельной сети связи, аналоговых каналообразующих средств, существующего парка техники связи уйдут годы. К тому же, развитие цифровых телекоммуникаций в той или иной степени включает в себя оборудование аналого-цифровых и цифро-аналоговых преобразователей для стыка с аналоговыми подсистемами и для сопряжения с аналоговым оборудованием. Поэтому на данный момент разработчикам и заказчикам приходится искать компромисс и создавать технику связи для работы на «смешанных сетях» с учетом современных требований к качеству, скорости, защищенности передаваемой информации. Таким образом, большинство каналов связи одновременно могут рассматриваться, как аналоговые, так и цифровые. Требуется исследование характеристик подобных «смешанных сетей» связи. Напрашивается вывод о необходимости оценки параметров, которые характеризуют аналоговые и цифровые каналы в комплексе. Чтобы понять этот симбиоз, рассмотрим, что мы понимаем под цифровым каналом, что характеризует его качество? А затем рассмотрим аналоговые эксплуатационные параметры каналов СССН, которые требуют оценки и влияют на параметры цифрового канала.

Основным цифровым каналом является цифровой бинарный канал, т.е. канал, в котором циркулирует двоичная информация. К основным показателям качества цифровых систем передачи и коммутации относятся параметры ошибки и готовности канала. В рамках международных стандартов приняты следующие основные параметры качества цифровых систем передачи: BER – количество битовых ошибок, EFS – количество секунд, пораженных ошибками, SES – количество секунд, несколько раз пораженных ошибками, AS – количество секунд готовности канала и UAS – количество секунд неготовности канала. Методология измерений по битам составляет фундамент измерений цифровых каналов связи и используется даже для анализа систем с различными типами модуляции и кодирования. Более подробно параметры, используемые для анализа характеристик бинарного канала, описаны рекомендациями МСЭ-Т G.821, G.826 и M.2100.

Различают два типа измерений бинарного канала – с отключением и без отключения канала. Измерения с отключением канала предусматривают, что канал не используется в процессе измерений для передачи реального цифрового трафика, передается специальная тестовая последовательность. Последовательность заранее известна на приеме, это позволяет анализировать параметры канала с точностью до одной битовой ошибки, правда с учетом точной синхронизации передатчика и приемника. Измерения без отключения канала часто называются мониторингом, поскольку измерения производятся в режиме работающего канала, а анализатор в этом случае подключается параллельно и осуществляет пассивный мониторинг канала. Алгоритм организации измерений основан на применении различных типов цикловых кодов или служебной информации, передаваемой в канале. Точность данного метода хуже, т.е. не позволяет локализовать единичную битовую ошибку, но отсутствие необходимости отключения канала существенный плюс. С учетом анализа функционирования СССН замечено, что первый тип измерений бинарного канала имеет существенное значение при испытаниях новой техники, например, упрощает поиск и разрешение проблемных моментов протокольного обмена. В то время как второй вариант более выигрышный в условиях эксплуатации, когда контроль качества связи необходимо осуществлять без ущерба доступности ресурсов сети, учитывая важность абонентов.

Зависимость параметра ошибки BER от отношения сигнал/шум можно выделить как основную характеристику цифровой системы, поскольку она влияет на стабильность связи. Параметр ошибки оценивается как функция отношения сигнал/шум . А вот уже на уровень шума по отношению к полезному сигналу влияют разные параметры, большинство из которых имеет аналоговый характер.

Первое, что напрашивается из вышеописанного, это необходимость измерения уровня затухания сигнала. Уровень сигнала определяют измерителями уровня. Поскольку уровень сигнала нужно измерять на разных частотах, то нужен еще и измеритель с перестраиваемой частотой. Как правило, эти два вида измерений совмещены в одном приборе. Другими словами, для оценки качества цифровых каналов требуется измерение АЧХ аналоговых каналов. В последнее время распространенными средствами анализа АЧХ, предлагаемыми на рынке измерительного оборудования, являются анализаторы спектра [1].

Абонентские кабельные сети на основе оптоволоконных линий связи в нашей стране еще не сильно развиты, но поскольку они существуют, в том числе и на СССН, то новые измерительные задачи требуют новых измерительных решений. Здесь в отличие от каналов, образованных электрическим кабелем, требуются не измерители уровня электрического сигнала, а измерители оптической мощности [2].

Для проводных сетей характерны так называемые межкабельные переходные влияния [3], т.е. неконтролируемые помехи со стороны соседних кабелей. В общем случае генерируемый сигнал в соседнем кабеле неизвестен, поэтому техническая возможность его компенсации отсутствует. Это накладывает на передачу информации скоростные ограничения, а для абонентов СССН повышение такого критерия как скорость передачи не менее важно, чем для коммерческих сетей. Определение и, соответственно, ограничение влияния этого параметра особенно важно и с

другой стороны, по соображениям информационной безопасности. Межкабельные переходные влияния приводят к нежелательным утечкам информации ограниченного пользования. Еще одной причиной ухудшения качества связи является нарушение электрической симметрии проводов. В общем случае, для количественной оценки симметрии служит так называемый коэффициент затухания асимметрии. Это частотно зависимый параметр, нормируемый в области полосы рабочих частот. Чем больше коэффициент затухания асимметрии, тем менее абонентская линия чувствительна к внешним помехам. Следствием недостаточной симметрии абонентской линии является прослушивание посторонних сигналов — других разговоров, фона переменного тока 50 Гц, канала радиотрансляции и т.д.

Поскольку на СССН используются коммутируемые каналы телефонных сетей общего пользования (ТФОП), то существуют и проблемы присущие этим сетям. Наличие узлов развязки 2-х и 4-х проводных каналов является причиной появления эхо-сигналов в трактах приема. Наличие аппаратуры уплотнения приводит к появлению частотного сдвига. Необходимы измерения параметров эхо-сигналов для оценки их влияния на качество как цифровой, так и аналоговой связи, поскольку эхо-сигналы представляют собой мощную помеху, без устранения мешающего влияния которой практически невозможна организация передачи данных в дуплексном режиме по двухпроводным коммутируемым телефонным каналам. Существуют различные методики и алгоритмы, реализующие подобные измерения[4][5][6]. Другим важным параметром тракта является неравномерность фазово-частотной характеристики. Она влияет на уровень искажений при передаче широкополосных радиочастотных сигналов (сети сотовой связи GSM). Эта неравномерность определяется групповым временем прохождения (ГВП) или еще называют групповым временем задержки (ГВЗ). Для определения ГВП для проводных и беспроводных каналов можно использовать, например, все те же приборы с анализатором спектра в составе, например HP 11758V от Hewlett-Packard.

Список использованных источников:

1. http://www.tempus.kiev.ua
2. http://www.abn.ru/inf/lan/work.shtml
3. Альбрехт М. Олер, Дитер В. Шикетанц. Межкабельная переходная помеха: теория и измерение//LAN.-2006.-№1-С.26-32.
4. П.В. Колготин, Б.В. Султанов. Сравнение эффективности применения цифровых систем синхронизации 1-го и 2-го порядков для оценки сдвига частоты на фоне шума // Материалы 5-ой всероссийской научной конференции: «Проблемы развития системы специальной связи и специального информационного обеспечения государственного управления России». - Орел: Академия ФСО России, 8-9 февраля 2007г.
5. Колготин П. В. Оценка параметров каналов и развитие измерительных технологий в сетях связи специального назначения // Молодой ученый. — 2011. — №10. Т.1. — С. 34-39. — URL https://moluch.ru/archive/33/3789/ (дата обращения: 10.04.2018).
6. Б.В. Султанов. Измерения параметров эхосигналов, возникающих при дуплексной передаче данных по коммутируемым каналам передачи данных / Б.В. Султанов, С.Л. Шутов, В.Е. Захаренков // Электросвязь. – 2002. – № 10. – С. 34 – 37.

ОБЪЕКТНО-ОРИЕНТИРОВАННОЕ КОДИРОВАНИЕ АЭРОИЗОБРАЖЕНИЙ

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

Нгуен А. Т.

Цветков В. Ю. – д.т.н., профессор

The method of compression of images is offered on the basis of low-pass filter, quantization and image region growing to find out egdes of areas. Forming egdes of areas is carried out on the basis of their cultivation. The received coordinates of egdes and information of their intensive then is coded separately. Comparative results of efficiency of compression of test images are resulted on the basis of a considered method and classical formats of coding of the graphic data.

Кодирование изображений имеет своей целью сократить, насколько возможно, число бит, необходимое для представления и достоверного восстановления исходного изображения. Совокупность методов, основанных на этой классической точке зрения на проблему кодирования, относят к методам кодирования изображений первого поколения. Основной идей этих методов является представление набора данных (элементов изображения) в другой набор менее коррелированных данных или коэффициентов [1, 2, 3].

Другая возможность кодирования изображений, открывающаяся в связи с успехами в распознавании зрительных образов и анализе сцен, состоит в описании изображений через внешние границы областей (контуров). Эти методы, назовем их методами второго поколения, сводятся к разделению изображения на области, окруженные внешними границами так, чтобы эти границы по возможности соответствовали границам объектов на изображении. Координаты всех точек границ и их уровней яркости кодируются отдельно. Выделение границ можно производить двумя способами: путём выращивания областей (Region Growing) или с помощью методов выделения границ (egdes-based).

В первом случае получаются внешние замкнутые границы, что позволяют довольно просто характеризовать области и их свойства, а полученное таким образом сегментированное изображение выглядит как мозаика. Во втором случае получаемые границы не обязательно замкнуты и их объединение с яркостью становится более сложным.

Сегментация изображения проводится в четыре этапа: предобработка (фильтрация низких частот, квантование и аффинное преобразование), выращивание областей, выделение и кодирование внешних замкнутых границ.

Алгоритм сжатия изображения на основе предобработки, выращивания и кодирования границ областей, который использовал автор при построении модели обработки изображений, можно представить следующим образом:

1. Предобработка, выращивание областей и выделение внешних замкнутых границ.
2. Кодирование полученных (образованных) замкнутых границ цепным кодом Фримана 8-связности.
3. Восстановление закодированных границ и заполнение изображения.

В настоящее время имеются два эвристических способа уменьшения числа областей, полученных при их выращивании: удаление малых областей или слияние смежных областей с малым контрастом.

Экспериментально показано, что при реализации этого метода, области, содержащие более 2 точек, не должны удаляться. Для достижения максимальных значений коэффициента сжатия число областей, после процедуры сегментации, не должно превышать 100 областей за счет аффинного преобразования, однако качество изображения при этом ухудшается.

Как видно, из рисунка 1 точка пересечения кривых зависимостей $К_{сж}$ от СКО, при кодировании соответствующих изображений методами выращивания областей и JPEG компрессии находится в пределах больше $К_{сж} = 185$, что соответствует удовлетворительной оценки качества восстановленного изображения. Качество изображений, при кодировании методом выращивания областей определяется количеством областей и коэффициентом сжатия аффинного преобразования [4, 5].

Представленный метод кодирования изображений на основе выращивания областей относится к методам кодирования второго поколения: показал, что его качественные и количественные характеристики близки к соответствующим показателям при кодировании изображений методом JPEG компрессии при малых количествах областей сегментации. Предложенный метод кодирование не только даёт хорошее визуальное восприятие закодированных изображений при достаточно высокой СКО, но и сохраняется контурная информация обеъектов. При высоком $К_{сж}$ ($К_{сж} > 1000$) метод еще может выделить

тепловизионные объекты на фоне изображения, что даёт преимущество по сравнением с другими методами сжатия.

Основные результаты обработки представлены на рисунках 1, 2.

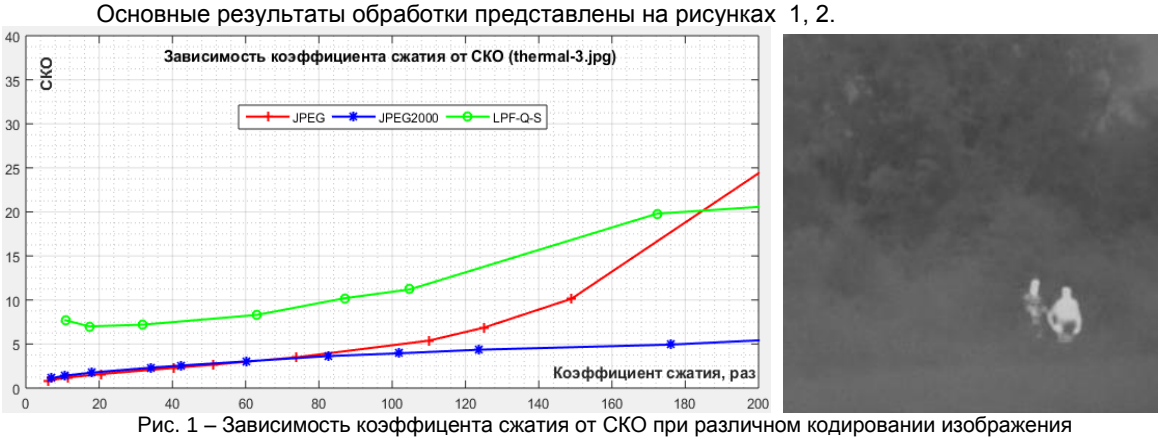


Рис. 1 – Зависимость коэффицента сжатия от СКО при различном кодировании изображения thermal-3.jpg размера 256x256.

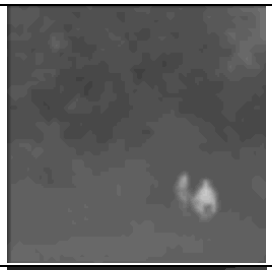
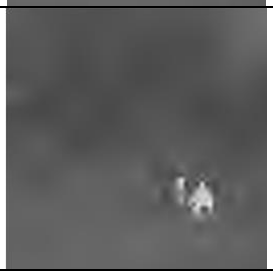
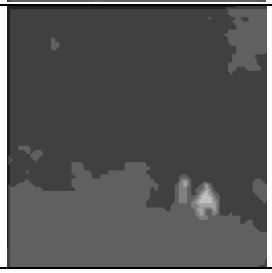
CR	JPEG	JPEG2000	LPF-Q-S
17			
33			
63			
173			

Рис. 2 – Восстановление изображения при различном коэффициенте сжатия

Список использованных источников:
1. Сокращение избыточности. Тематический выпуск // ТИИЭР, 1997, т. 55. № 3. - с. 250.
2. Дж. Миано. Форматы и алгоритмы сжатия изображений в действии . Уч. лособ. - М.: Изд-во Триумф, 2003. - с. 336.
3. Д. Сэломон. Сжатие данных, изображений и звука. Пер. с англ. В. В. Чепыжева. - М.: Техносфера, 2004. - с. 368.
4. Р. Гонсалес, Р. Вудс. Цифровая обработка изображений. – М: Техносфера, 2005. – с. 1072.
5. Р. Гонсалес, Р. Вудс. Цифровая обработка изображений в среде MATLAB. – М: Техносфера, 2006. – с. 618.

МОДЕЛЬ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

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

Михальчук С.Ю.

Астровский И.И. – к.т.н.,доцент

Виды и способы организации электронного документооборота могут быть разными – создание общего файлового хранилища на сервере, использование внутренней почты или иных коммуникационных систем. Но это работает до определенного уровня решаемых задач и масштабов деятельности компании. Если идти дальше, нужно внедрять схему, которая позволит упорядочить работу и с бумажными документами, и с электронными. Это позволяют сделать системы электронного документооборота различных видов.

Сейчас организации, переходящие на электронный документооборот, в первую очередь думают об эффективности. Повышение эффективности возможно двумя способами – через увеличение результата и уменьшение затрат. Современные СЭД используют оба эти способа. Так, снижению затрат способствуют:

Сокращение затрат на бумажные документы (распечатку, копирование, пересылку и пр.).

Сокращение непроизводительных затрат рабочего времени сотрудников. По оценкам западных консалтинговых компаний, доля затрат времени на выполнение рутинных, непроизводительных операций над документами может составлять до 20-30% всего рабочего времени (а на практике – до 60-70%). Снизить такие затраты – одна из важнейших целей внедрения СЭД.

На результативность деятельности организации при внедрении СЭД влияют:

Ускорение информационных потоков (более оперативная информационная поддержка менеджмента – выше скорость принятия решений).

Изменение корпоративной культуры (повышение информационно-технологической подготовленности персонала, способствующее лучшему восприятию инноваций).

Внедряя систему электронного документооборота, организации чаще всего планируют решить следующие задачи:

– повышение эффективности управления путем автоматизации контроля выполнения, большей прозрачности деятельности подразделений и отдельных сотрудников;

– автоматизация бизнес-процессов с их одновременной оптимизацией;

– обеспечение поддержки накопления, управления и организации доступа к корпоративной информации и знаниям;

– протоколирование деятельности организации в целом, ее отдельных подразделений, рабочих групп, сотрудников с использованием этой информации для поддержки принятия решений и т.д.;

– сокращение оборота бумажных документов (с целью снижения издержек);

– упрощение и удешевление хранения документов, использующихся в текущей деятельности, за счет создания оперативного электронного архива.

По функционалу и решаемым задачам выделяют следующие:

1 Системы делопроизводства. Предназначены для организаций с жестко формализованными правилами документооборота и вертикальным управлением.

2 Электронные архивы. Это системы с развитыми средствами хранения и поиска информации. Они не предназначены для поддержки движения документов, главная цель – организация хранения и поиска нужных данных.

3 Workflow-системы. В центре таких систем – бизнес-процессы, которые они и автоматизируют, а документы и документооборот являются средством осуществления потоков работ.

4 ECM-системы. Это комплексные системы управления корпоративным контентом, которые реализуют сразу несколько функций – управление документами; управление образами документов (Document Imaging); управление записями; управление потоками работ (Workflow); управление веб-контентом (WCM); управление мультимедиаконтентом (DAM); управление знаниями (Knowledge Management); управление коллективным взаимодействием (Collaboration) [1].

Список использованных источников:

1. Система электронного документооборота [Электронный ресурс]. –Режим доступа: http://piter-soft.ru/.

УСТРОЙСТВА ФОРМИРОВАНИЯ ТЕСТОВЫХ СИГНАЛОВ ДЛЯ КОНТРОЛЯ ПОМЕХОУСТОЙЧИВОСТИ ИНФОКОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

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

Шатило Н.И. – к.т.н.,доцент

Качество электроэнергии различных электрических сетей далеко от идеальной, особенно в крупных городах. На рисунке 1 показана экспериментальная зависимость числа пиков (выбросов, импульсов) напряжения от времени в течение суток на примере городской сети 220В 50 Гц крупного московского офиса [1].

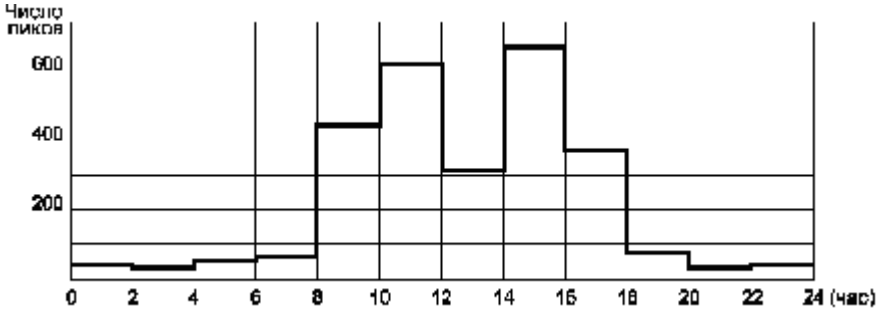


Рис. 1 Зависимость от времени числа пиков напряжения в диапазоне свыше 200 В (с временным интервалом свыше 40 мкс)

Из рисунка 1 легко увидеть, что количество зафиксированных пиков в рабочее время на два порядка выше по сравнению с ночным. Приведенная зависимость как бы реабилитирует МОСЭНЕРГО: источники помех - результат деятельности потребителей электроэнергии. Однако такой вывод можно сделать лишь в отношении группы пиков, вызванных переходными процессами, происходящими при нормальном функционировании аппаратуры.

Пики напряжения в электрических сетях - наиболее «активные убийцы» дорогостоящей производственной и бытовой электронной аппаратуры. Данное утверждение базируется на том факте, что энергия сетевых пиков может достигать единиц килоджоулей, а энергия разрушения современных интегральных микросхем составляет единицы - сотни микроджоулей [2], то есть необходимо ослабление сетевой помехи, доходящей до интегральной микросхемы, на 7 - 9 порядков, что является сложной задачей.

Во всем мире эта проблема известна под названием «электромагнитная совместимость» (ЭМС). Естественные импульсные помехи, наводимые в электрических сетях от молний, и помехи искусственного происхождения, возникающие от воздействия мощных электромагнитных импульсов, например, при коротком замыкании высоковольтной линии электропередачи, крайне велики и соизмеримы друг с другом.

Кроме указанных выше кратковременных помех, в сетях присутствуют и долговременные помехи, обусловленные перепадами сетевого напряжения. Последние также приводят к сбоям в работе аппаратуры.

Для решения проблемы требуется соблюдать национальные и мировые стандарты по ЭМС. Несмотря на значительное количество стандартов, регламентирующих нормы сетевых помех от различной аппаратуры, а также способы их снижения опасные пики в сетях были и будут.

Наиболее опасными для аппаратуры являются импульсные помехи.

Международные и национальные стандарты различают следующие виды импульсных помех: наносекундные [3], микросекундные [4] и колебательные затухающие помехи [5].

Стандарты аккумулируют многолетний инженерный опыт и разработаны таким образом, чтобы при испытании устройств достаточно точно имитировать реальные помехи.

Практически все реальные импульсные помехи могут быть представлены как комбинации этих трех помех. Поэтому, если устройство устойчиво к указанным типам помех, то с высокой степенью вероятности оно будет устойчиво и к реальным помехам, независимо от их происхождения.

Список использованных источников:

1. Колосов В. «Убийцы» аппаратуры – электрические сети. Живая электроника России, 2010, т.1.

2. Черепанов В., Хрул, В А., Блудов И. Электронные приборы для защиты РЭА от электрических перегрузок. Справочник. М.: Радио и связь, 1994.

3. СТБ МЭК 61000-4-4-2014 Электромагнитная совместимость. Часть 4-4. Методы испытаний и измерений. Испытания на устойчивость к наносекундным импульсным помехам.

4. СТБ МЭК 61000-4-5-2014 Электромагнитная совместимость. Часть 4-5. Методы испытаний и измерений. Испытания на устойчивость к микросекундным импульсным помехам большой энергии.

5. СТБ ГОСТ Р 51317.4.12-2012 Совместимость технических средств электромагнитная. Устойчивость к колебательным затухающим помехам. Требования и методы испытаний.

ПЛАНИРОВАНИЕ ЗОН ПОКРЫТИЯ БАЗОВЫХ СТАНЦИЙ СИСТЕМЫ 3GPP LTE

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

Ячменев А.А.

Давыдова Н.С. – к.т.н., доцент

С развитием рынка телекоммуникаций появляется все большее количество пользователей, которым необходимо передавать и принимать высококачественное видеоизображение, поддерживать постоянное высокоскоростное соединение с сетью Интернет, пользоваться разнообразными приложениями, требующими высокие скорости передачи данных и большую пропускную способность. Повсеместное развитие и активное использование современных сетей подвижной радиосвязи четвертого поколения стандарта Long Term Evolution (LTE), пришедшего на смену стандартам третьего поколения, поможет справиться с проблемами, возникшими вследствие постоянно растущей нагрузкой на сети операторов подвижной радиосвязи.

Целью данной статьи является изучение вопросов планирования зон покрытия базовых станций системы LTE. Объектом исследования является система сотовых сетей 3GPPLTE.Предметом исследования является методика, позволяющая оптимизировать процесс планирования зон покрытия базовых станций для обеспечения наилучшего качества передачи информации в сетях LTE, а также для оптимального размещения и функционирования базовых станций. Практическая значимость заключается в выработке методики и стратегии планирования зон покрытия базовых станций сети LTE.

Задача планирования сети сотовой радиосвязи заключается в нахождении такой сети радиосвязи, которая удовлетворяет исходным требованиям (ограничениям) и обладает при этом значением совокупности (вектора) показателей качества, наилучшим в смысле безусловного критерия предпочтения. Если выполняется это условие, то каждый из показателей качества оптимизированной сети не хуже, чем у исходной сети [1].

В данной постановке задача синтеза сети относится к задаче векторной (многокритериальной) оптимизации и заключается в выборе из нескольких вариантов векторно-сравнимых решений такого, при котором сеть обладает наилучшими значениями вектора показателей качества. Из постановки задачи следует, что для решения задачи оптимизации необходимо создать исходную сеть (иначе, построить ее начальное приближение). Успешно решить задачу планирования сотовой сети можно лишь путем сочетания методов математического синтеза, связанного с существенной идеализацией сети, и эвристического синтеза, под которым понимается сложный творческий процесс, заключающийся в отыскании приемлемых решений на основе использования накопленных данных и инженерного опыта. В связи с этим целесообразным общую задачу синтеза сети декомпозировать на ряд частных задач, в решении каждой из которых обязательно активное участие специальных экспертов и применение специального программного обеспечения.

Обобщенный алгоритм планирования сетей мобильной связи представлен на рисунке 1.

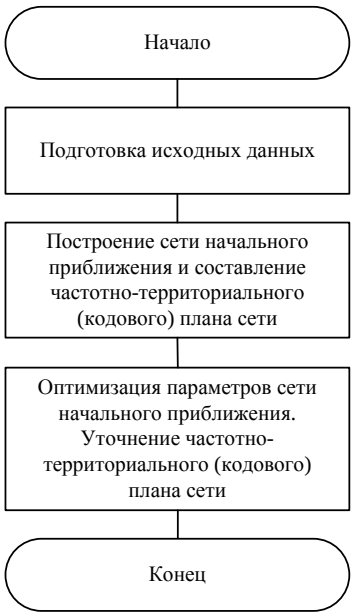


Рисунок 1 – Обобщенный алгоритм планирования сетей мобильной связи

Таким образом, алгоритм планирования сотовой сети включает в себя следующие этапы:

Планирование сети требует довольно обширный набор исходных данных, достоверность которых может существенно повлиять на адекватность принимаемого решения, таким образом, подготовка исходных данных.

Второй этап состоит в построении исходной сети (сети начального приближения). На этом этапе вся сеть декомпозируется на однородные фрагменты на основе значений плотности трафика, применительно к которым находятся распределения базовых станций по зонам обслуживания, параметры базовой сети и распределение частотного ресурса (кодовых сдвигов), таким образом, построение исходной сети.

Третий этап включает привязку участков развертывания базовых станций к карте местности и итеративную оптимизацию параметров базовой сети с использованием геоинформационной базы данных и специального программного обеспечения, позволяющего произвести расчет напряженности поля сигнала в зоне действия сети. Оптимальный набор пространственно-технических параметров сети в наибольшей степени должен соответствовать условиям функционирования сети подвижной связи (СПС) в час наибольшей нагрузки, таким образом, оптимизация исходной сети [2]..

При планировании радиосети LTE целесообразно придерживаться общепринятой временной и логической последовательности действий:

– получение исходных данных.

– калибровка математической модели распространения радиоволн на основе измерений напряженности поля в наиболее характерных точках зоны обслуживания сети.

– построение сети начального приближения.

– привязка участков развертывания базовых станций, определенных планом построения (сети начального приближения) к местности.

– итеративная оптимизация сети при широком использовании средств программного обеспечения, поддерживающих функции синтеза сети и анализа эксплуатационных характеристик.

Исходные данные для расчета параметров зон покрытия базовых станций представлены на рисунке 2.

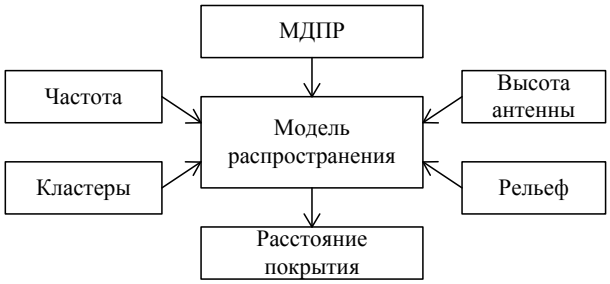


Рисунок 2 – Исходные данные для расчета параметров зон покрытия базовых станций

Решение задачи построения сети мобильной связи стандарта LTE предполагает использование метода приближений в соответствии с алгоритмом частотно-территориального планирования [3]. Алгоритм раскрывает последовательность и содержание этапов построения начального приближения и итеративной оптимизации сети при широком использовании средств программного обеспечения, поддерживающих функции синтеза сети и анализа эксплуатационных характеристик. Следует отметить, что на сегодняшний день вопросы частотно-территориального планирования в сетях мобильной связи стандарта LTE являются наименее разработанными и требуют дальнейшего исследования.

Список использованных источников:

1. 3GPP TS 36.300 – Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2 (Release 12). 2014.

2. Тихвинский В.О., Терентьев С.В., Юрчук А.Б. Сети мобильной связи LTE. Технологии и архитектура. М.: Эко-Трендз, 2010. 284 с.

3. Nohrborg M. LTE Overview [Электронный ресурс] – Режим доступа: http://www.3gpp.org/LTE.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ В БЕСПРОВОДНЫХ СЕТЯХ

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

Ковалев И.А, Радченко А.С., Ставров С.Д.
Бойправ О.В.. – к.т.н.

В современном мире беспроводные сети все более распространены за счет удобств, которые они предоставляют. Рост популярности этих сетей обуславливает увеличение количество выполняемых по отношению к ним атак. выделяют несколько причин реализации атак.

1. Взлом с целью похищения конфиденциальной информации.

2. Стремление воспользоваться чужим Интернет-соединением. В данном случае также происходит воровство, но не осязаемых конфиденциальных документов, а виртуальное - воровство Интернет-трафика. Если злоумышленник пользуется чужим интернет-каналом для сугубо утилитарных целей (электронная почта, веб-серфинг), то ощутимого материального урона он не нанесет, но, если локальная сеть организации используется как плацдарм для рассылки спама или последующей масштабной Интернет-атаки, последствия могут быть крайне неприятными как со стороны интернет-провайдера, так и со стороны контролирующих органов.

Поскольку радиосигналы имеют широковещательную природу, не ограничены стенами зданий и доступны всем приемникам, местоположение которых сложно или вообще невозможно зафиксировать – злоумышленникам особенно легко и удобно атаковать беспроводные сети. Поэтому, формально, даже случайный прохожий может заниматься радиоразведкой вашей сети – сугубо из любопытства. Огромное разнообразие готового инструментария анализа протоколов и уязвимостей, доступного в Интернете, позволяет ему без особых усилий совершить проникновение в корпоративную сеть.

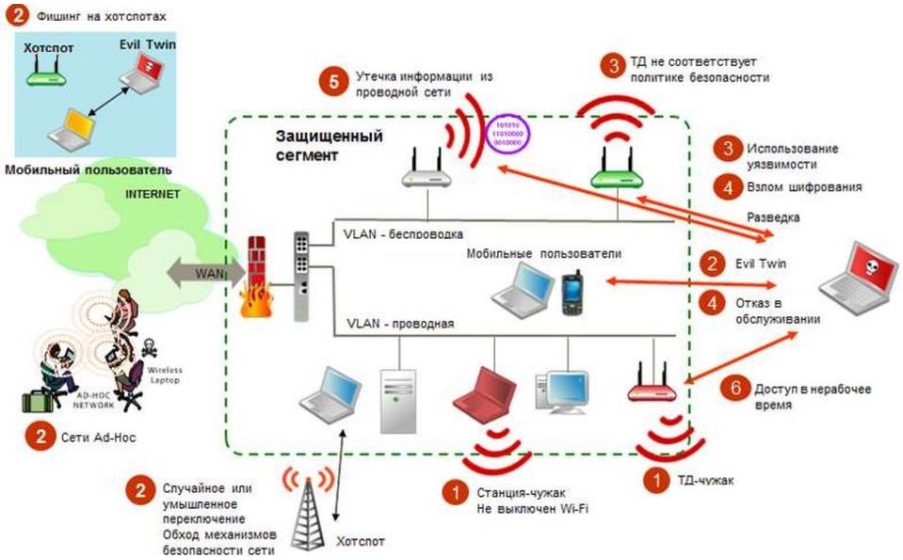


Рисунок 1 – Основные риски беспроводных сетей

Выделяют следующие основные причины реализации угроз информационной безопасности беспроводных информационных сетей.

1. Наличие в составе этой сети устройств, предоставляющих возможность неавторизованного доступа к корпоративной сети, зачастую в обход механизмов защиты, определенных корпоративной политикой безопасности. Чаще всего это те самые самовольно установленные точки доступа. Также в роли чужака могут выступить домашний роутер с Wi-Fi, программная точка доступа Soft AP, ноутбук с одновременно включенными проводным и беспроводным интерфейсом, сканер, проектор и т.д.

2. Нефиксированная природа связи, которая позволяет мобильным устройствам автоматически подключаться к сети. Таким образом, для доступа к информации злоумышленник имеет возможность переключить пользователя на свою точку доступа с последующей атакой или для поиска тонких мест в защите. Примерами являются фишинг на хотспотах, случайное или умышленное переключение, обход механизмов безопасности сети, сети Ad-Hoc, Evil Twin.

3. Уязвимости, связанные с конфигурацией сетей и подключаемых устройств. Некоторые сетевые устройства (точки доступа, беспроводные клиенты) могут быть более уязвимы, чем другие – неправильно сконфигурированы, использовать слабые ключи шифрования или методы аутентификации с известными уязвимостями.

4. Новые угрозы и атаки. Беспроводные технологии породили новые способы реализации старых угроз, а также некоторые новые, доселе невозможные в проводных сетях. Во всех случаях, бороться с атакующим стало гораздо тяжелее, т.к. невозможно ни отследить его физическое местоположение, ни изолировать его от сети. Злоумышленник как правило начинает атаки с предварительной разведки и зачастую совершает атаки типа «Отказ в обслуживании» (Denial of Service, DoS). Серьезной угрозой любой сети, не только беспроводной является имперсонация авторизованного пользователя и Identity Theft. Инструментарий для организации атак на беспроводные сети широко доступен и постоянно пополняется новыми средствами, начиная от всеми известного AirCrack и заканчивая облачными сервисами по расшифровке хешей.

5. Утечки информации из проводной сети. Практически все беспроводные сети в какой-то момент соединяются с проводными. Соответственно, любая беспроводная точка доступа может быть использована как плацдарм для атаки. Но это еще не все: некоторые ошибки в конфигурации точек доступа в сочетании с ошибками конфигурации проводной сети могут открывать пути для утечек информации. Наиболее распространенный пример – точки доступа, работающие в режиме моста (Layer 2 Bridge), подключенные в плоскую сеть (или сеть с нарушениями сегментации VLAN) и передающие в эфир широковещательные пакеты из проводного сегмента. Другой распространенный сценарий основывается на особенностях реализации протоколов 802.11. В случае, когда на одной точке доступа настроены сразу несколько ESSID, широковещательный трафик будет распространятся сразу во все ESSID. В результате, если на одной точке настроена защищенная сеть и публичный хот-спот, злоумышленник, подключенный к хот-споту, может нарушить работу протоколов DHCP или ARP в защищенной сети.

6. Особенности функционирования беспроводных сетей. Некоторые особенности функционирования беспроводных сетей порождают дополнительные проблемы, способные влиять в целом на их доступность, производительность, безопасность и стоимость эксплуатации. Для грамотного решения этих проблем требуется специальный инструментарий поддержки и эксплуатации, специальные механизмы администрирования и мониторинга, не реализованные в традиционном инструментарии управления беспроводными сетями. Такими проблемами являются активность в нерабочее время, точки доступа, разрешающие подключения на низких скоростях, интерференция радиосигналов, способная значительно ухудшить показатели пропускной способности и количества поддерживаемых пользователей, вплоть до полной невозможности использования сети.

Основные этапы, которые необходимо учитывать при построении системы безопасности беспроводных сетей:

– контроль доступа;

– аутентификация пользователей;

– шифрование трафика;

– система предотвращения вторжений в беспроводную сеть;

– система обнаружения чужих устройств и возможности их активного подавления;

– мониторинг радиоинтерференции и DoS-атак;

– мониторинг уязвимостей в беспроводной сети и возможности аудита уязвимостей;

– функции повышения уровня безопасности инфраструктуры беспроводной сетипо способу регистрации и усиления.

Методы повышения общего уровня безопасности беспроводной сети:

– аутентификация и авторизация всех пользователей сети WiFi;

– конфигурирование VLAN-ов для разделения трафика (например, гости/сотрудники, высокий уровень доступа/низкий уровень доступа и т.п.) и введения первичного, грубого сегментирования;

– использование межсетевых экранов на уровне портов для формирования более тонкого уровня безопасности;

– использование шифрования на всей сети для обеспечения секретности;

– определение опасности целостности сети и применение методов решения этих проблем;

– включение обеспечения безопасности конечных устройств в общую политику безопасности;

При использовании беспроводных сетей для передачи данных о держателях карт, следует использовать технологию WPA (WPA2), IPSEC VPN, либо SSL/TLS. Не следует полагаться только технологию WEP для защиты конфиденциальных данных в беспроводных сетях.

ИСПЫТАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ТЕХНИЧЕСКОГО РЕГЛАМЕНТА РЕСПУБЛИКИ БЕЛАРУСЬ ТР 2013/027/BY

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

Грицкевич В.И.

Бойправ О.В. – к.т.н.

Целью испытаний является проверка функций безопасности маршрутизаторов Cisco ASR920 и ASR1001 на предмет соответствия заявленным функциональным (полный перечень представлен в СТБ 34.101.2) и гарантийным требованиям безопасности (полный перечень представлен в СТБ 34.101.3), а также требованиям СТБ 34.101.73. Задачей испытаний является подтверждение того, что все заявленные в заданиях по безопасности требования к объектам оценки (маршрутизаторам) реализованы. Объект оценки считается выдержавшими испытания, если в нём реализованы все заявленные требования. Результаты испытаний объекта оценки отражаются в техническом отчете и протоколе.

Испытания данных маршрутизаторов проводятся на испытательном стенде, состав и структура которого соответствует схеме, приведенной на рисунке 1, где ПЭВМ 1, ПЭВМ 2, ПЭВМ 3, ПЭВМ 4, ПЭВМ Управления, маршрутизатор R1 (маршрутизатор Cisco ASR920 или ASR1001 (зависит от того, какой маршрутизатор испытывается)), маршрутизатор R2 (Cisco ASR 920), маршрутизатор R3 (Cisco ASR 920), а также концентраторы сетевые SW1 (TP-Link TL-SG1008D), SW2 (D-Link DGS-1008D) и SW3 (TP-Link TL-SG1008D) соединяются в соответствии со схемами кабелями UTP категории 5. Конфигурирование маршрутизаторов происходит либо с помощью CLI-интерфейса, либо с помощью протоколов telnet или ssh (определяется методикой испытаний).

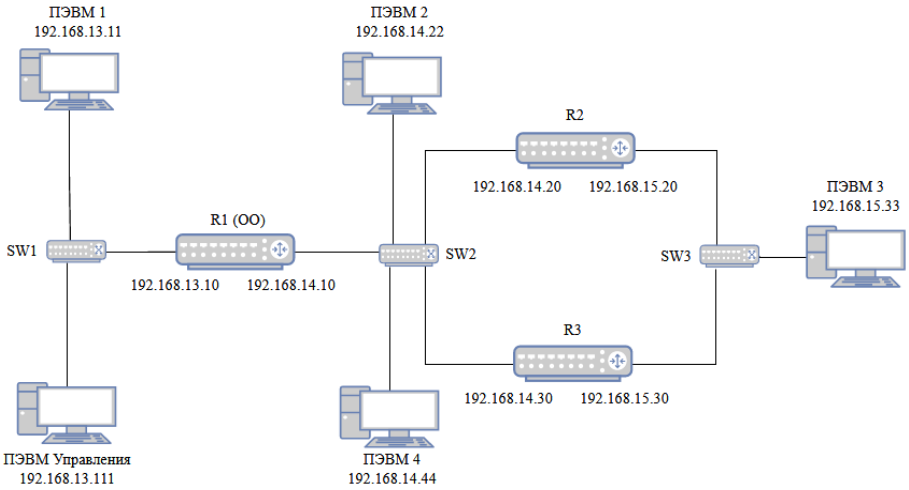


Рис. 1 – Схема испытательного стенда

Полный перечень заявленных функциональных требований безопасности представлен в заданиях безопасности для Cisco ASR920 и Cisco ASR1001. Ниже представлены наиболее важные из них, а также методика проверки требований:

- FIA_ATD.1 «Определение атрибутов пользователя» - на R1 создаются пользователи с различными уровнями привилегий (пример команды: username admin privilege 10 password admin);
- FIA_UAU.2 «Аутентификация до любых действий пользователя» - производятся попытки получить доступ к R1, используя корректный идентификатор и некорректный пароль;
- FIA_AFL.1 «Обработка отказов аутентификации» - на R1 задаётся блокировка на 120с при достижении двух неудачных попыток аутентификации в течении 120с (команда: login block-for 120 attempts 2 within 120);
- FDP_IFF.1 «Простые атрибуты безопасности» - добавляются надёжные стационарные маршруты (пример: ip route 192.168.15.0 255.255.255.0 192.168.14.20), настраивается управление сетевыми потоками (пример: deny ip host 192.168.13.11 any log), просматривается журнал аудита (show logging);
- FPT_FLS.1 «Сбой с сохранением безопасного состояния» - во время работы R1 прерывается подача электропитания с целью подтверждения того, что им невозможно управлять во время сбоя подачи электропитания, а также проверяется утверждение, что после загрузки маршрутизатор требует повторной аутентификации;
- FAU_GEN.1 «Формирование данных аудита» - просматривается журнал аудита (show logging) на наличие следующих записей: запуск средств аудита; использование доверенного канала и идентификатор

инициатора; попытка открытия сеанса связи пользователя; запросы на выполнение операции над объектом, изменения атрибутов безопасности; управление информационными потоками для информации контроля, полученной из недостоверных источников: адрес отправителя, адрес получателя, тип протокола; изменение в установке меток времени;

- FAU_SAR.3 «Выборочный просмотр данных аудита» - выполняется поиск данных аудита на основе значения даты, времени, идентификатора пользователя, IP-адреса отправителя (пример команды: show logging | include “Jun 4”).

Полный перечень заявленных гарантийных требований безопасности представлен в заданиях безопасности для Cisco ASR920 и Cisco ASR1001. Ниже представлены наиболее важные из них, а также методика проверки требований:

- ADV_ARC.1 «Описание архитектуры безопасности» - эксперту необходимо убедиться, что маршрутизатор спроектирован таким образом, что его функциональные возможности безопасности невозможно обойти, а также, что описание архитектуры безопасности составлено на уроне необходимой детализации;

- ADV_TDS.1 «Базовый проект» - эксперту необходимо убедиться, что проект содержит все необходимые компоненты и описания для подсистем, реализующих функциональные требования безопасности;

- ASE_CCL.1 «Утверждение о соответствии» - эксперту необходимо проанализировать задание по безопасности маршрутизатора;

- ASE_OBJ.2 «Задачи безопасности» - проверяется формулировка и обоснование задач безопасности;

- ASE_SPD.1 «Определение проблемы безопасности» - проверяется наличие описания угроз.

Перечень заявленных требований СТБ 34.101.73 представлен в заданиях по безопасности маршрутизаторов. Проверка требований стандарта СТБ 34.101.73 осуществлялась путём анализа результатов проверки функциональных требований безопасности.

По окончании испытаний маршрутизаторов Cisco ASR920 и ASR1001 были составлены следующие документы: технический отчет о результатах оценки и протокол испытаний. В протоколе испытаний указаны точное наименование, состав и конфигурация ОО на момент проведения оценки (испытаний).

В результате проведения испытаний маршрутизаторов Cisco ASR920 и ASR1001 было установлено, что они соответствуют всем заявленным функциональным и гарантийным требованиям безопасности, а также требованиям СТБ 34.101.73.

Список использованных источников:

1. Информационные технологии. Средства защиты информации. Информационная безопасность: ТР 2013/027/BY. Введ. 01.01.2014. – Минск: Госстандарт Республики Беларусь: 2013.

2..Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности: СТБ 34.101.2-2014. – Введ. 28.01.2014. – Минск: Госстандарт Республики Беларусь: 2013.

3. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности: СТБ 34.101.3-2014. – Введ. 28.01.2014. – Минск: Госстандарт Республики Беларусь: 2013.

4. Задание по безопасности ЗБ.Cisco-ASR900-IOS XE 3.16.001–2017 «Программное обеспечение Cisco IOS XE версии 3.16 маршрутизаторов Cisco серии ASR 900».

5. Задание по безопасности ЗБ.Cisco-ASR1000-IOS XE 3.16.002–2017 «Программное обеспечение Cisco IOS XE версии 3.16 маршрутизаторов Cisco серии ASR 1000».

6. Методика испытаний маршрутизаторов серии Cisco ASR 900 с программным обеспечением IOS XE версии 3.16 МИ.СКЛ 04-2018.

7. Методика испытаний маршрутизаторов серии Cisco ASR 1000 с программным обеспечением IOS XE версии 3.16 МИ.СКЛ 05-2018.

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В КОРПОРАТИВНУЮ СЕТЬ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ВИРТУАЛИЗАЦИИ

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

Мурашко Е.А, Прокофьев С.В, Марычев Д.В.

Вишняков В.А., д.т.н., профессор

Системы предотвращения сетевых вторжений и выявления признаков атак на информационные системы уже достаточно длительное время используются как одно из необходимых средств защиты информационных систем. На сегодня системы предотвращения вторжений и атак обычно представляют собой программные или аппаратно-программные комплексы, которые автоматизируют процесс контроля событий, протекающих в компьютерной системе или сети, а также анализируют эти события в поисках уязвимостей. Использование технологий виртуализации для построения системы предотвращения вторжений позволяет обеспечить как более рациональное распределение и использование физических ресурсов, так и упрощает администрирование всех компонентов системы защиты. В качестве средства обнаружения и предотвращения вторжений используется IDS/IPS Snort.

Система предотвращения вторжений (СПВ) (англ. Intrusion Protection System (IPS)) – программное или аппаратное средство, предназначенное для предотвращения попыток получения несанкционированного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть. В дополнение к межсетевым экранам (firewall), работа которых происходит на основе политики безопасности, IPS служат механизмами мониторинга и наблюдения подозрительной активности. Типовая структура IPS включает:

8) Сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы;
9) Подсистему анализа, предназначенную для выявления сетевых атак и подозрительных действий;
10) Хранилище, в котором накапливаются первичные события и результаты анализа;
11) Консоль управления, позволяющая конфигурировать IPS, наблюдать за состоянием защищаемой системы и IDS, просматривать выявленные подсистемой анализа инциденты.

Пример реализации СПВ с использованием технологий виртуализации представлен на рисунке 1:

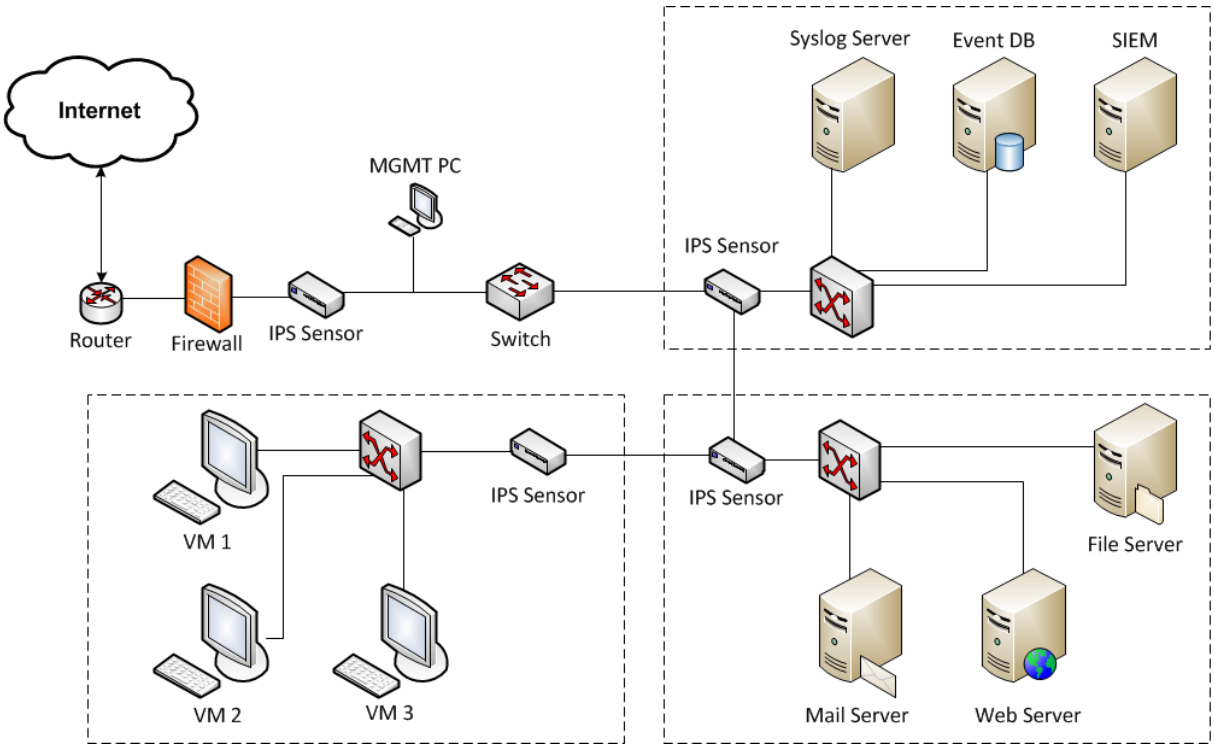


Рисунок 4 - Структура сети с применением различных типов СПВ

Штриховыми областями на схеме обозначены сервера виртуализации, на которых развёрнуты сенсоры сети, виртуальные коммутаторы, различные сервера и виртуальные рабочие станции.

Созданная виртуальная инфраструктура обладает следующими особенностями:

а) события с IPS-сенсоров сети собираются в базу данных на выделенном виртуальном сервере;

б) файлы журналов с сенсоров дублируются на Syslog-сервере;

в) для упрощения работы и анализа событий, принятых от сенсоров сети, развёрнута виртуальная система сбора и обработки данных о событиях информационной безопасности (SIEM).

Основные преимущества использования виртуальной инфраструктуры:

- уменьшение количества используемого физического оборудования;
- возможность быстрой миграции виртуальных машин и создания резервных копий;
- возможность перераспределения используемых виртуальными машинами ресурсов;
- возможность организации защиты как отдельных виртуальных машин, так и гипервизора в целом;
- упрощение администрирования и реконфигурации сети.

Основные недостатки применения виртуализации:

- высокая стоимость качественных серверов и корпоративных лицензий для использования виртуальных гипервизоров;
- риск потери данных и увеличение времени простоя виртуальных серверов или рабочих станций при выходе из строй одного из серверов виртуализации;
- необходимость повышения квалификации сотрудников для работы с виртуальной инфраструктурой;
- необходимость сокрытия факта использования виртуальных средств от обнаружения злоумышленником.

Неизбежный рост количества всевозможных угроз сетевой безопасности ставит всё новые задачи для специалистов по информационной безопасности и сетевых администраторов для предотвращения утечки важной информации и поддержания жизнеспособности критических активов в корпоративной сети. Внедрение технологий виртуализации является залогом успешного развития корпоративных сетей и улучшением их средств защиты.

Список использованных источников:

1. Кёртис, А. Real-time Intrusion Detection Systems. / А. К. Кёртис, Дж. Хамфрис. – Техас : Department Of Computer Science, 2008 – 20 с.

2. Вишняков, В. А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения / В. А. Вишняков. – Минск : Белорусская государственная академия связи, 2016. – 276 с.

3. Национальный открытый университет [Электронный ресурс]. – Режим доступа : http://www.intuit.ru/.

4. Dave Mishchenko. VMware ESXi: Planning, Implementation, and Security.

5. Бэйкер, Э. Р. Snort IDS and IPS Toolkit. / Э. Р. Бэйкер, Дж. Эслер. – Берлингтон : Syngress, 2007. – 766 с.

6. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства. / В.Ф. Шаньгин. – Москва : ДМК Пресс, 2010. – 544 с.

7. BYTE/Россия. Системы обнаружения вторжений [Электронный ресурс]. – Режим доступа : https://www.bytemag.ru/.

МОДЕЛИРОВАНИЕ ВЫСОКОСКОРОСТНОГО ОПТИЧЕСКОГО ЛИНЕЙНОГО ТРАКТА

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

Мойсиевич Ю.С.

Тарченко Н.В. – к.т.н.,доцент

Современный этап развития систем связи характеризуется интенсивными разработками и внедрением волоконно-оптических систем передачи (ВОСП). Это связано с большими возможностями и перспективами, которыми обладают оптические системы. В первую очередь это большая пропускная способность (сотни Тбит/с) и надежность. Способы организации передачи информации по оптическому волокну достаточно многообразны и постоянно совершенствуются, поэтому существенную помощь при их изучении и моделировании оказывает классификация.

В результате проведения библиографического поиска и анализа литературы предложена следующая классификация ВОСП, которая представлена на рисунке 1 [1,2,3,4]:

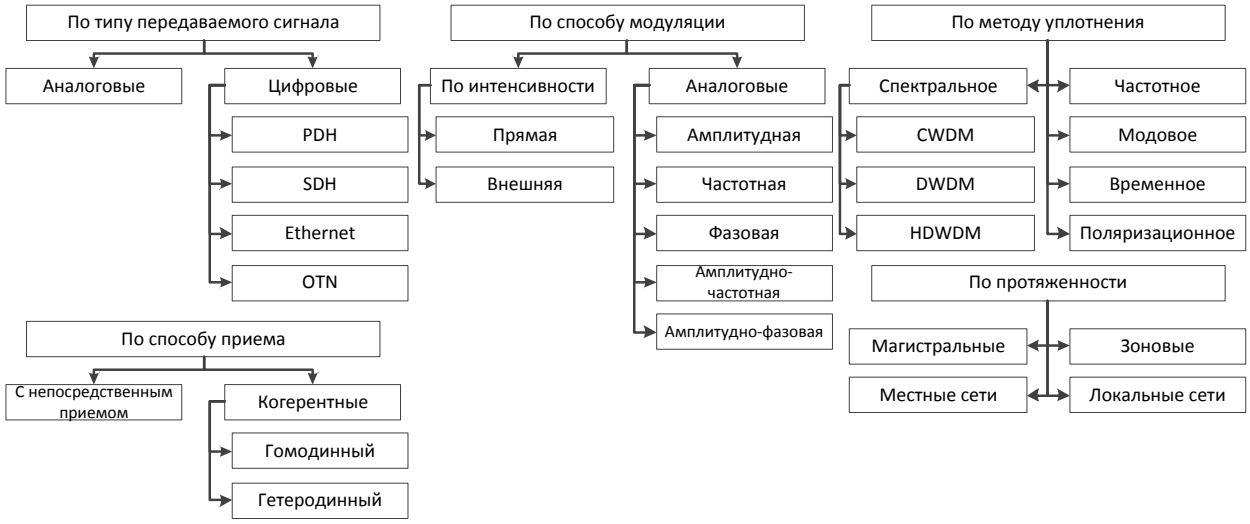


Рис. 1 – Классификация ВОСП

Можно выделить следующие основные классификационные признаки.

1.По типу передаваемого сигнала ВОСП делятся на:

1.1аналоговые, если каналообразующее оборудование строится на основе аналоговых методов модуляции параметров гармонической несущей частоты (амплитудная, частотная, фазовая модуляции и их комбинации) или параметров периодической последовательности импульсов (амплитудно-импульсная, широтно-импульсная, фазоимпульсная модуляции и их комбинации). В настоящее время используются при передаче на небольшие расстояния в системах кабельного телевидения;

1.2цифровые, при которых сигнал, передаваемый по оптическому волокну, является цифровым. В зависимости от применяемой технологии различают PDH, SDH, Ethernet, OTN.

Технология PDH (PlesiochronousDigitalHierarchy – плезиохронная цифровая иерархия) – это принцип построения цифровых систем передачи, которые используют групповой мультиплексированный ИКМ-сигнал, состоящий из 30-канальных потоков (E1 – 2,048 Мбит/с) и требующий синхронизации скоростей цифровых потоков на входе оборудования группообразования. Последующие уровни иерархии образуются мультиплексированием четырех потоков предыдущего уровня. Таким образом, скорость передачи на следующих уровнях составляет 8 Мбит/с (E2), 34 Мбит/с (E3) и 140 Мбит/с (E4).

Технология SDH (SynchronousDigitalHierarchy – синхронная цифровая иерархия) появилась как результат эволюционного скачка, когда PDH перестала удовлетворять требованиям по пропускной способности, гибкости переключения и выделения цифровых потоков, оперативности управления и соответствию структуре услуг связи. Основная скорость передачи составляет 155,250 Мбит/с (STM-1), максимальная скорость – 40 Гбит/с (STM-256).

Ethernet – семейство технологий пакетной передачи данных. В зависимости от скорости передачи данных и передающей среды выделяютогромное количество вариантов технологии. В настоящее время существует стандарт 400GbE, который позволяет передавать данные со скоростью 400 Гбит/с, ведутся разработки 1TbE(1 Тбит/с).

Технология OTN (OpticalTransportNetwork – оптическая транспортная сеть) является на сегодняшний день основной технологией построения магистральных волоконно-оптических сетей связи. Принцип технологии заключается в упаковке сигналов различных форматов в стандартные контейнеры, которые затем передаются по оптическому волокну.В настоящее время достигнута скорость 100 Гбит/с (ODU-4).

2. По способу модуляции оптического излучения ВОСП делятся на:

2.1 системы с модуляцией интенсивности оптического излучения, при которой мощность выходного оптического сигнала изменяются в соответствии с информационным сигналом;

2.2системы передачи с аналоговыми методами модуляции оптического излучения (оптической несущей): амплитудной, фазовой, частотной модуляциями и их комбинациями.

При модуляции интенсивности различают прямую и внешнюю модуляцию. В передатчиках с прямой модуляцией в соответствии с информационной последовательностью модулируется ток накачки, под действием которого модулируется выходная мощность светового излучения лазера.

При внешней модуляции излучение источника, имеющее постоянное значение, подается на модулятор, в котором модулируется под действием информационного сигнала.

3. В зависимости от способа приема оптического сигнала различают ВОСП:

3.1 с непосредственным приемом, при котором происходит непосредственное преобразование интенсивности оптического излучения в электрический сигнал, напряжение или ток которого однозначно отражают изменение интенсивности оптического сигнала;

3.2когерентные, в которых применяется гетеродинноеили гомодинное преобразование частоты независимо от вида модуляции оптического излучения, осуществляемое на промежуточной частоте.

При гетеродинном приеме одновременно с оптическим сигналом частоты f_C на фотодетектор подается достаточно мощное оптическое излучение местного гетеродина с частотой $f_Г$, на выходе фотодетектора выделяется промежуточная частота $f_{ПР} = f_C – f_Г$, на которой и осуществляются дальнейшие преобразования оптического сигнала в электрический.

При гомодинном методе приема частоты колебаний принимаемого оптического излучения и местного гетеродина должны быть одинаковыми, а фазы синхронизированы.

4. По методам уплотнения оптического волокна различают ВОСП:

4.1 со спектральным уплотнением с разделением длин волн (WDM – Wavelenght Division Multiplexing), при котором по одному оптическому волокну одновременно передается несколько спектрально разнесенных оптических несущих, каждая из которых модулируется многоканальный сигналом. В свою очередь современные системы WDM в зависимости от частоты разноса каналов можно подразделить на CWDM (Coarse WDM – грубые WDM) с частотным разносом каналов более 2500 ГГц (не более 18 каналов), DWDM (DenseWDM – плотные WDM) с разносом каналов около 100 ГГц (до 40 каналов), HDWDM (Highdense WDM – высокоплотные WDM) с разносом каналов 50 ГГц и менее (более 64 каналов);

4.2 с частотным уплотнением (FDM – FrequencyDivisionMultiplexing), при котором исходным многоканальным сигналам различных источников в линейных трактах отводятся определенные полосы частот. Поэтому для получения близко расположенных спектральных каналов в ВОСП используются различные несущие не от разных источников, а от одного, но достаточно стабильного, с помощью соответствующего сдвига оптической несущей;

4.3 с временным уплотнением (TDM – Time Division Multiplexing), при котором для передачи каждого компонентного потока по одному оптическому волокну отводится свой временной интервал;

4.4 с модовым уплотнением (MDM – Mode Division Multiplexing), которые находят применение в системах передачи, основанных на использовании многомодового оптического волокна. С помощью модовых селекторов на входе и выходе волокна осуществляется передача независимых информационных потоков (каналов) на соответствующих модах.

4.5 с уплотнением по поляризации (PMD – Polarization Division Multiplexing), т. е. уплотнение потоков информации с помощью оптических несущих, имеющих линейную поляризацию. При этом плоскость поляризации каждой несущей должна быть расположена под своим углом. В отличии от модового уплотнения здесь в качестве среды передачи группового потока может быть использовано одномодовое волокно.

5. По дальности передачи ВОСП подразделяются на:

5.1 магистральные и международные, предназначенных для передачи информации на тысячи километров и соединяющих между собой центры государств или их краев, областей, крупные промышленные и научные центры и др.;

5.2зоновые, предназначенные для организации связи в административных пределах стран и протяженностью до 600 км;

5.3 для местных сетей, предназначенные для организации межстанционных соединительных линий на городских и сельских телефонных сетях;

5.4 для локальных сетей, обеспечивающие связь между вычислительными машинами, организацию локальных компьютерных сетей и сетей кабельного телевидения.

Представленная классификация не является исчерпывающей и полной. Существует большое количество классификационных признаков, но в данной работе были выделены основные.

Список использованных источников:

1. Фокин В. Г. Когерентные оптические сети : Учебное пособие / Сибирский государственный университет телекоммуникаций и информатики; каф.многоканальной электросвязи и оптических систем. – Новосибирск, 2015. – 372 с.

2. Леонов А.В., Наний О.Е., Слепцов М.А., Трещиков В.Н. Тенденции развития оптических систем дальней связи; в журнале Прикладная фотоника, том 3, № 2, 2016 – с. 123-145.

3. Зингеренко Ю. А. Оптические цифровые телекоммуникационные системы и сети синхронной цифровой иерархии. – Учебное пособие. – СПб: НИУ ИТМО, 2013. – 393 с.

4. Соломенчук В.Д., Мищенко В.А., Гура К. Н. Оптические транспортные сети. – Киев: Центр последипломного образования ПАО «Укртелеком», 2014 – стр. 294.

МОДЕЛИРОВАНИЕ КОДЕКОВ РЕЧЕВЫХ СИГНАЛОВ

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

Корытко Д.С.
Тарченко Н.В. – к.т.н.,доцент

Кодек (англ. codec, от coder/decoder – кодер/декодер или compressor/decompressor) – это устройство или программа, способные выполнять преобразование данных или сигнала. Современные кодеки речевых сигналов используют разные математические алгоритмы для цифрового сжатия и кодирования аналоговой аудиоинформации и применяются как в системах фиксированной и подвижной связи, так и в сетях передачи данных. Основные направления в развитии кодеков речевых сигналов:

- обеспечение приемлемого качества речевого сигнала при минимальной скорости передачи;
- минимизация алгоритмической задержки;
- минимизация стоимости.

Целью исследовательской работы является создание программного продукта для моделирования работы кодеков речевых сигналов в реальном времени при различном качестве канала передачи и сравнительный анализ последних.

В основу программы моделирования на сегодняшний день положены алгоритмы обработки речевых сигналов, представленные в рекомендациях МСЭ-Т для кодеков, использующих импульсно-кодовую модуляцию со скоростью 64 кбит/с (Рек. G.711), адаптивную дифференциальную импульсно-кодовую модуляцию со скоростями 40, 32, 24 и 16 кбит/с (Рек. G.726), а также двухскоростной речевой кодек для передачи мультимедийных сообщений со скоростью 5,3 и 6,3 кбит/с. (Рек. G.723.1).

В процессе моделирования имеется возможность записать фрагмент речевого сигнала или выбрать испытательный сигнал (гармонический сигнал заданной частоты), просмотреть осциллограмму и спектр реализации сигнала, произвести предварительную фильтрацию речевого сигнала цифровым фильтром с заданной полосой пропускания.

В дальнейшем необходимо выбрать тип кодека, задать его параметры, параметры канала передачи (ввести вероятность ошибки, вероятность потери пакетов и т.д), и произвести кодирование и декодирование сигнала с учетом параметров канала передачи.

Результатом работы программы является восстановленный аналоговый речевой сигнал. Данная программа предоставляет возможность анализировать сигнал как во временной области (визуально оценить искажения формы сигнала после декодирования), так и в частотной. Имеется возможность оценить отношение сигнал/шум (ОСШ) при использовании кодека для всего записанного фрагмента речевого сигнала, так и для сегмента речевого сигнала (сегментное ОСШ).

Визуально интерфейс разработанной программы представлен на рисунке 1. Предусмотрена возможность звукового воспроизведения восстановленного (декодированного) речевого или испытательного сигнала для оценки качества передачи методом экспертных оценок. Предусмотрена возможность расчета количественной оценки качества воспроизведения и ее сравнение с результатами, полученными в случае использования E-модели [5, 6].

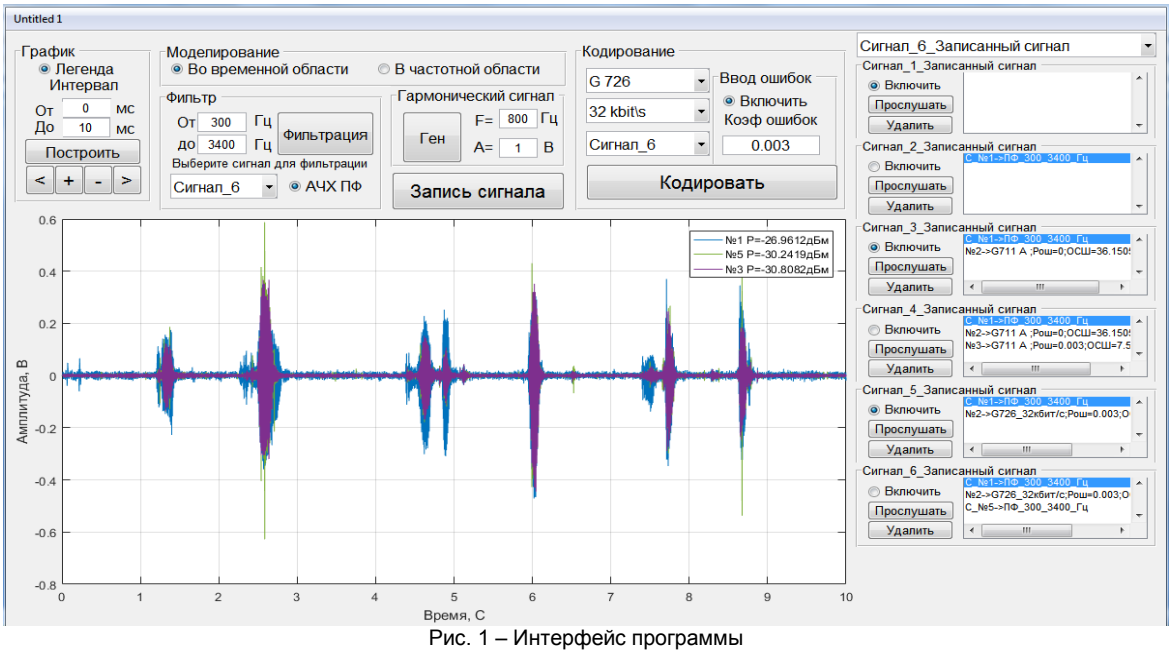


Рис. 1 – Интерфейс программы

Результаты моделирования показали, что использование гибридных кодеков для кодирования речевых сигналов позволяет существенно уменьшить битовую скорость передачи. Однако, низкая скорость передачи не приводит к чувствительному ухудшению качества передачи речевого сигнала. Данный тип кодеков является наиболее устойчивым к битовым ошибкам.

Список использованных источников:

1. Рекомендация МСЭ-Т G.711. Импульсно-кодовая модуляция речевых частот.

2. Рекомендация МСЭ-Т G.726. 40, 32, 24, 16 кбит/с адаптивная дифференциальная импульсно-кодовая модуляция.

3. Рекомендация МСЭ-Т G.723.1. Двухскоростной речевой кодер для передачи мультимедийных сообщений со скоростью 5,3 и 6,3 кбит/с.

4. Рекомендации МСЭ-Т H.323. Мультимедийные системы связи на основе пакетов.

5. Рекомендация МСЭ-Т G.107. E-модель – вычислительная модель, используемая при планировании передачи.

6. Рекомендация МСЭ-Т G.108. Применение E-модели, руководство по планированию.

7. Рекомендация МСЭ-Т G.113. Ухудшение передачи из-за обработки речи.

8. Рихтер, С.Г. Кодирование и передача речи в цифровых системах подвижной радиосвязи/ С.Г. Рихтер – М.: – Телеком, 2010. – 300 с.

ОПРЕДЕЛЕНИЕ НОРМ СИНДРОМА БЧХ-КОДА

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

Пригон А.Н.
Конопельно В.К. – к.т.н.,доцент, профессор

В современных инфокоммуникационных системахиспользуется помехоустойчивое кодирование для уменьшения влияния ошибок на передаваемую информацию. Развитие элементной базы открывает возможность реализовывать сложные, недоступныеранее алгоритмы декодирования, имеющие более качественные параметры. Вычислительный эксперимент показывает, что примерно треть исследуемых кодов обладает корректирующими возможностями, большими конструктивных, и перспективна для применения. Они становятся востребованными в системах передачи информации,требующих высокой надежности передачи информации.

Коды Боуза-Чоудхури-Хоквингема являются результатом обобщения кодов Хэмминга, которые позволяют исправлять множественные ошибки. Они составляют класс циклических кодов, который обеспечивает достаточную свободу выбора длины блока, скорости кода и возможностей коррекции ошибок. Коды БЧХ превосходят своими качествами все другие блоковые коды с той же длиной блока и степенью кодирования. В наиболее часто применяемых кодах БЧХ используется двоичный алфавит и блок кодового слова длиной n = 2m — 1, где m =3, 4, … . Относительно широкий максимум эффективности кодирования, в зависимости от степени кодирования при фиксированном n, для этих кодов находится между скоростью кодирования 1/3 и 3/4.

Норменное декодирование базируется на систематической классификации векторов ошибок в блоковых кодах, анализе спектров синдромов ошибок и норм синдромов примитивных и непримитивных БЧХ-кодов. В основу классификации ошибок положено группа Г циклических сдвигов, принадлежащая группе автоморфизмов многих линейных кодов. Благодаря этому векторы ошибок, переходящие друг друга посредством циклических сдвигов, образуют один класс эквивалентности – Г-орбиту. Понятие нормы синдрома N введено для произвольных БЧХ-кодов, как примитивных, так и непримитивных, являющейся константой для кодов (в узком смысле) с минимальным расстоянием d=5 и вектором при d≥7. Г-орбиты с попарно различными нормами содержат ошибки с непересекающимися спектрами синдромов и можно подобрать набор Г-орбит, исчерпывающий весь спектр синдромов и, следовательно, декодировать любую ошибку из этого набора. Это позволяет при заданном d исправлять существенно большее число ошибок, не корректируемых известными методами, на основе одних и тех же достаточно простых декодеров.

Основное свойство норм синдромов отражает то, что для всякого вектора ошибок $\bar{e}$ и его синдрома $S(\bar{e})$ в БЧХ-коде C справедливо равенство $\overline{N}(S(\sigma(\bar{e}))) = \overline{N}(S(\bar{e}))$. Это же равенство справедливо и для реверсивных кодов C_R^{2r+1}. Все векторы каждой *Г*-орбиты имеют одинаковую норму синдрома, то есть норма синдрома инвариантна относительно группы Γ циклических сдвигов. Нормой $N(J)$ *Г*-орбиты J векторов-ошибок в любом БЧХ-коде, а так же и в реверсивном коде, называется норма синдрома любого вектора-ошибки из этой Г-орбиты.

Норма Г-орбиты является ее однозначной характеристикой, то есть идентификатором этой орбиты и спектры синдромов таких *Г*-орбит не пересекаются. I и J – две Г-орбиты векторов-ошибок с одинаковыми нормами в примитивном двоичном БЧХ-коде C_{2t+1} (в реверсивном коде C_R^{2r+1}). Пусть I – полная Г-орбита с полным спектром синдромов. Тогда для всякого вектора $\bar{f} \in J$ найдется вектор ē ∈ I, такой, что $S(\bar{e}) = S(\bar{f})$.

Множество Г-орбит всех векторов-ошибок весом 1-3 имеет в примитивном двоичном БЧХ-коде C_7 попарно различные нормы. Множество Г-орбит всех векторов-ошибок весом 1-2 имеет в примитивном двоичном БЧХ-коде C_5 попарно различные нормы.

Основные свойства нормы синдрома:

- у всех векторов-ошибок отдельно взятой Г-орбиты норма синдрома одна и та же; норма синдрома является характерным признаком, меткой каждой Г-орбиты;
- если у двух полных Г-орбит совпадают нормы, то и множества синдромов векторов-ошибок этих орбит также совпадают;
- синдромы всех корректируемых векторов-ошибок попарно различны; следовательно, нормы синдромов Г-орбит ошибок любой корректируемой совокупности имеют попарно различные нормы.

Список использованных источников:

1.Липницкий В. А., Олексюк А. О. Теория норм синдромов и плюс-декодирование // БГУИР. 2014. № 8. С. 71–78.

2.Липницкий В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа. 2-е изд. Минск : БГУИР, 2006.

3.Конопелько В. К. Норменное декодирование помехоустойчивых кодов. Минск : БГУ, 2007.

4. Лидл Р., Нидеррайтер Г. Конечные поля : в 2 т.: пер. с англ. М. : Мир, 2004.

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ВОЛОКОННО-ОПТИЧЕСКИХ ТРАКТАХ

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

Кийко В.Н., Лукашевич С.А.

Урядов В.Н. – к.т.н.,доцент

Ранее считалось, что ВОЛС полностью защищены от несанкционированного доступа к информации, передаваемой по линейным трактам. Однако на сегодняшний день, как выяснилось, это можно осуществить, используя различные физические явления при внесении в волоконный световод неоднородностей. Поэтому актуально исследование каналов, способов доступа и методов защиты информации, передаваемой по волоконным световодам.

При изгибе оптического волокна происходит изменение угла падения электромагнитной волны на границе сердцевина-оболочка. Угол падения становится меньше предельного угла, что означает выход части электромагнитного излучения из световода. Изгиб оптического волокна приводит к сильному побочному излучению в месте изгиба, что создаёт возможность несанкционированного съёма информации в локализованной области. Как правило, применяются изгибы меньше некоторого критического $R_{кр}$, при котором все излучение покидает сердцевину ВС и выходит в оболочку.

В прямом световоде с произвольным профилем показателя преломления поле моды в каждой точке поперечного сечения распространяется параллельно оси световода с одинаковой фазовой скоростью, так что плоскость постоянной фазы ортогональна ей. Однако, если световод изогнут в плоскую дугу с постоянным радиусом, как это изображено на рисунке 1, то ясно, что поля и фазовые фронты вращаются вокруг центра кривизны изгиба с постоянной угловой скоростью [1,2]. Таким образом, фазовая скорость, параллельная оси световода, должна линейно возрастать при увеличении расстояния от центра кривизны *C*. Поскольку оболочка световода имеет постоянный показатель преломления, то фазовая скорость может превышать скорости света в данной среде. Поэтому должен существовать некоторый радиус $R_{КР}$ в плоскости изгиба, при превышении которого поле уже не может направляться световодом и должно становиться излучающим, как это изображено схематически на рисунке 1.

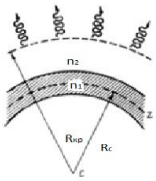


Рисунок 1 – Изогнутый световод с радиусом изгиба R_C, профиль показателя преломления которого в сердцевине - n_1, в оболочке - n_2

В [3] показано, что часть мощности, теряемая на изгибе одномодового волоконного световода равна:

$$P(z) = P(0)\exp(-\gamma z), \tag{1}$$

где $P(0)$ – мощность до изгиба ВС; $P(z)$ – мощность после изгиба ВС; z – длина изгиба радиуса R_c; γ - коэффициент затухания на единицу длины изгиба.

Коэффициент затухания мощности основной моды изогнутого слабонаправляющего световода ($n_1 \approx n_2$) со ступенчатым профилем показателя преломления определяется выражением [3]:

$$\gamma = \frac{\pi^{1/2}}{2a}\left(\frac{a}{R_C}\right)^{1/2}\frac{v^2 w^{1/2}}{u^2}\exp\left(-\frac{4}{3}\frac{R_C}{a}\frac{w^2\Delta}{v^2}\right), \tag{2}$$

где $v = \frac{2\pi}{\lambda}a(n_1^2 - n_2^2)^{1/2}$ – нормированная частота;

$u = a\left[\left(\frac{2\pi}{\lambda}n_1\right)^2 - \beta^2\right]^{1/2}$ – параметр моды в сердцевине;

$w = a\left[\beta^2 - \left(\frac{2\pi}{\lambda} n_2\right)^2\right]^{1/2}$ – параметр моды в оболочке;

β – продольная постоянная распространения $\frac{2\pi}{\lambda} n_2 < \beta < \frac{2\pi}{\lambda} n_1$.

Излучаемая мощность, которая может быть использована для снятия информации определяется выражением:

$$P_{изл} = P(0) - P(z). \quad (3)$$

Анализируя приведенное выше теоретическое обоснование можно сделать вывод о том, что описанный канал утечки приводит к локальному выходу значительной части оптической мощности за пределы волокна.

Метод снятия информации при изгибе волокна состоит в коллимировании покинувшего волокно излучения с помощью пассивных оптических элементов (линз, призм), фокусирующих свет во вспомогательное волокно эквивалентной конструкции, соединенное с приемным оптическим модулем соответствующего типа.

Для данного метода снятия информации при изгибе волокна существуют промышленно выпускаемые средства, примером которых являются: устройство подключения на изгибе волокна типа «прищепка» EXFO FCD-10B, ответвитель-прищепка FOD-5503.

Были проведены испытания по отводу потока E3 системы Plesiochronous Digital Hierarchy (PDH) из ВОЛС без разрыва линии связи, которые показали возможность полного и безошибочного демультиплексирования цифрового потока.

Эксперимент показал, что работа системы не нарушается, если потери, вносимые прищепкой и линейным трактом системы, не превышают энергетического потенциала системы (разность между уровнем передачи и чувствительностью приемного оптического модуля). Контроль несанкционированного доступа возможен по анализу коэффициента ошибок информационного сигнала.

Данный канал позволяет производить несанкционированное снятие оптического сигнала достаточной мощности для последующего восстановления потока данных в любой точке волоконного световода. При этом изгиб вносит значительное затухание в проходящую мощность, что может ухудшить качество приема в основном канале и может служить индикатором несанкционированного доступа.

Список использованных источников:

1. Волоконно-оптические датчики / Т. Окоси, К. Окамото, М. Оцу, Х. Нисихара, К. Кюма, К. Хататэ; Под ред. Т. Окоси: Пер. с япон.— Л.: Энергоатомиздат. Ленингр. отд-ние, 1990.

2. Затыкин А. А., Моршнев С. К., Францессон А. В. Квантовая электроника, 10, № 11 (1983).

3. Снайдер А., Лав Дж. Теория оптических волноводов: Пер. с англ. – Радио и связь, 1987.

БЕСПРОВОДНЫЕ ИНФОРМАЦИОННЫЕ СЕТИ С АРХИТЕКТУРОЙ MESH

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

Шараев Н.П., Шляхтич А.Н.

Бойправ О.В. – к.т.н.

На современном этапе в структуре информационно-телекоммуникационных систем все большее развитие получают системы беспроводного доступа. Уже сегодня технология беспроводных информационных сетей, в основе которой лежит стандарт IEEE 802.11, является наиболее популярной технологией беспроводных сетей передачи данных, быстро развивается. В сложившихся условиях mesh-технология становится особенно необходимой в отсутствие проводной инфраструктуры для соединения станций [1].

Введение

Преобразования беспроводных информационных сетей в инструмент корпоративной коммуникации и действительно массовую технологию обмена данными поставило перед разработчиками серьезную проблему «бесшовного» межсетевого роуминга (802.11i/r/k/v). Эта проблема решается в рамках mesh-топологии. Информационные сети, организованные по данной топологии, получили за последние полтора-два года большое признание [1]. Масштабы проектов выросли до тысяч точек доступа и десятков тысяч пользователей, так как это вполне осмысленный следующий шаг в развитии беспроводных сетей. В mesh-сети пользователь «сам себе провайдер» и его нельзя: отключить от этой сети, разорвать договор об использовании интернета.

I. Топология и принцип работы беспроводных информационных сетей с архитектурой Mesh

Сети с архитектурой mesh или mesh-сети представляют собой многошаговую сеть, устройства которой обладают функциями маршрутизатора и способны использовать различные пути для пересылки пакета. Топология в таких сетях, как правило, ячеистая, т.е. построенная на принципе ячеек, в которой рабочие станции сети соединяются друг с другом и способны принимать на себя роль коммутатора для остальных участников. Визуализация ячеистой топологии представлена на рисунке 1.

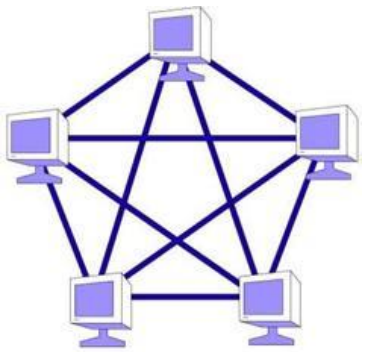


Рис. 1 – Сеть с mesh топологией

Каждый узел в mesh-сети обладает такими же полномочиями, как и все остальные, т.е. все узлы в сети равны. Также сети бывают самоорганизующиеся и настраиваемые, первый тип сетей при включении оборудования, которое его поддерживает, автоматически подключаются к существующим участникам, выбирают оптимальные маршруты и самонастраиваются внутри сети. Настраиваемые же сети, это те сети, которые следует настроить перед использованием.

Полноценная беспроводная mesh-сеть – это такая сеть, для подключения к которой не требуется дополнительного ПО, кроме DHCP-клиента и поддержки IPv6 системой. ПО такой сети позволяет превратить любое устройство в полноценного участника сети. Также у такой сети нет единого центра для получения IP адресов, а маршруты в ней полностью распределенные и динамические.

Объединение таких сетей происходит в автоматическом режиме – когда устройство подключено одновременно к двум сетям, узел который подключен к этим двум сетям становится мостом, который их объединяет [2].

Принцип работы сетей mesh сходен с путями отсылки пакетов для обычных сетей Интернет - данные будут идти от одного устройства к другому, пока они не достигнут заданного адресата. Это позволяет реализовать возможность динамической маршрутизации, поддерживаемой всеми устройствами mesh. Чтобы реализовать возможность динамической маршрутизации, каждый узел должен сообщить свою информацию о маршрутизации всем узлам, соединяющимся с ним практически в режиме

реального времени. После этого каждый узел в сети mesh самостоятельно решает, что сделать с данными, которые это получает - передать их следующему устройству или оставить. Используемый алгоритм маршрутизации позволяет гарантировать, что данные выберут самый быстрый маршрут до адресата.

Данная технология решает следующие проблемы:

– позволяет быть независимым от провайдеров;

– любой пользователь может сам построить свою сеть с использованием маршрутизаторов для беспроводных информационных сетей;

– каждый новый клиент, который подключился к сети, увеличивает емкость сети;

– с помощью беспроводной mesh-сети можно быстро восстановить сеть для связи, если возникла такая необходимость, и соединить ее с глобальной сетью [3].

Также рассмотрим достоинства и недостатки беспроводных сетей.

Достоинства беспроводных mesh-сетей:

– независимость от провайдера;

– некоторые современные протоколы для организации mesh-сетей гарантируют шифрование всего трафика, проходящего через сеть;

– использование динамической автоконфигурируемой маршрутизация;

– возможность объединять mesh-сети посредством Интернета;

– mesh-сети являются самовосстанавливающимися: сеть будет работать, даже когда в сети имеется неисправный узел или потеряно подключение;

– организация таких сетей требует меньших затрат денежных средств.

К числу недостатков сетей с такой архитектурой можно отнести:

– первоначальный запуск такой сети достаточно сложен;

– сеть эффективно работает только в том случае, когда в ней много участников;

– негарантированная ширина канала;

– негарантированное качество связи.

II. Технологии, протоколы и их реализация

В нынешнее время самые популярные протоколы для организации беспроводных информационных сетей с архитектурой mesh это:

– CJDNS;

– B.A.T.M.A.N.;

– DTN;

– Netsukuku;

– OSPF.

Сравнение этих протоколов изображено на рисунке 2.

	CJDNS	B.A.T.M.A.N.	DTN	Netsukuku	OSPF
Авто-назначение адреса	Да	Нет	Нет	Да	Нет
Авто-конф. Маршрутизация	Да	Да	Да	Да	Частично
Распределенная маршрутизация	Да	Да	Да	Да	Частично
Объеденение сетей	Да	Нет	Нет	Нет	Нет
IPv4/v6	IPv6	IPv4/v6	IPv4/v6	IPv4	IPv4
Шифрование трафикка внутри сети	Да	Нет	Нет	Нет	Нет
Авто-настройка	Да	Да	Да	Нет	Да
Разработка	Активная	Закончена	Активная	Нет	Закончена
Поддержка UNIX\LINUX\OpenWRT	Да	Да	Да	Да	Да
Поддержка Windows	В разработке	Нет	Нет	Нет	Нет
Поддержка Mac OS X	Да	Да	Да	Да	Да
Потребление ресурсов	Низкое	Низкое	Низкое	Высокое	Низкое
Оверлейны режим работы	Да	Нет	Нет	Нет	Нет
Интеграция в ядро Linux	Нет	Да	Нет	Нет	Да

Рис.2 – Сравнительные характеристики mesh-протоколов

Из рисунка 2 видно, что самым востребованным является протокол CJDNS. CJDNS – сетевой протокол, с помощью которого можно создать масштабируемую, безопасную и простую в настройке сеть. Сеть может работать как поверх интернет соединения, так и между маршрутизаторами напрямую.

Работа протокола осуществляется через сетевой туннель. Программы могут работать в данной сети, при условии, что они поддерживают протокол IPv6. После установки нужного программного обеспечения трафик автоматически перенаправляется в данную сеть, что позволяет избежать дополнительной настройки программ. В сети для пользователя генерируется IPv6 адрес, который относится к приватной части IPv6 адресов, а значит не будут происходить коллизии между настоящим IPv6. При подключении через обычный интернет нужно найти уже существующий узел сети и узнать его адрес и ключ. При подключении маршрутизатор-маршрутизатор – все происходит самостоятельно. Каталог маршрутов постоянно обновляется из-за того, что конфигурация сети может поменяться, таким образом, сеть поддерживает оптимальную нагрузку через все узлы и выбирает самый короткий путь для трафика [4].

III. Заключение

Так как эта беспроводная инфраструктура сети имеет огромный потенциал и обходится значительно дешевле и доступней, чем построение обычных сетей, то большое число беспроводных провайдеров уже приступили к созданию своих собственных беспроводных mesh-сетей [3]. Единственным препятствием для широкого развития таких сетей является необходимость получения разрешения на использование частоты.

Список использованных источников:

1. Что такое mesh? // InCore.me [Электронный ресурс]. – Режим доступа: http://www.incore.me/internet-texnologii/chto-takoe-mesh-mesh-set-eto/ . – Дата доступа: 07.04.2018.
2. Wi-Fi Mesh сети для самых маленьких // Хабрарабр [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/196562/. – Дата доступа: 08.04.2018.
3. Бекетов, О.В. Беспроводные сети mesh / О.В. Бекетов. – 7 ноября 2006г. – с. 4.
4. CJDNS // Википедия – свободная энциклопедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Cjdns. – Дата доступа: 07.04.2018.

ВИРТУАЛЬНАЯ СИСТЕМА VPN В СОТОВОЙ СЕТИ LTE

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

Ловенецкий Д.А.

Саломатин С.Б.. – к.т.н.,доцент

Несмотря на «сетевую» интерпретацию, технологии VPN на самом деле имеют и более широкую трактовку, поскольку по своим принципам в некотором смысле напоминают функционирование прокси-серверов с установкой защищенного соединения и шифрованием передаваемой и принимаемой информации. Для осуществления подключения через VPN применяется принцип так называемого туннелирования.

Собственно, особой разницы между тем, что собой представляет доступ в Интернет посредством использования VPN на стационарных компьютерах, ноутбуках, смартфонах или планшетах, нет.

Это самое обычное туннелирование, которое по принципам работы несколько похоже на функционирование анонимных прокси-серверов, иначе называемых анонимайзерами. VPN в телефонах это инструмент, позволяющий изменить внешний IP девайса для доступа на заблокированные ресурсы. При смене IP соответственно меняется и местоположение пользователя, который пытается войти на определенную страницу, к которой доступ в его регионе не разрешен. Кроме того, при таком положении дел пользователь остается как бы неузнанным в Сети, а его данные полностью шифруются на основе защиты WPA. Правда, только буквально на днях стало известно, что протокол WPA2, в большинстве случаев используемый для подключений через Wi-Fi, имеет достаточно серьезные уязвимости, которые позволяют злоумышленникам отслеживать исходящий и входящий трафик целиком и полностью.

Защищенные виртуальные сети способны обеспечить надежную шифрованную передачу данных через Интернет. В качестве примера можно привести PPTP, OpenVPN и IPSec. В случае, если передающая среда считается достаточно надежной и вопросы безопасности решены в рамках базовой локальной инфраструктуры, можно настроить и использовать доверительные ВПН-соединения L2TP (обычно используется в тандеме с IPSec) или MPLS.

В качестве алгоритма кодирования наиболее часто применяется Triple DES. Он обеспечивает 168-разрядное шифрование тремя различными ключами. Это дает стопроцентную гарантию того, что прочитать данные сможет лишь пользователь, обладающий соответствующими правами. Эффективных алгоритмов криптографических атак на этот симметричный шифр не существует, а значит вероятность его расшифровки даже профессиональным хакером стремится к нулю.

Основные преимущества VPN:

- 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;
- анонимной работы в сети интернет;
- загрузки приложений, в случае, когда ip адрес расположен в другой региональной зоне страны;
- безопасной работы в корпоративной среде с использованием коммуникаций;
- простоты и удобства настройки подключения;
- обеспечения высокой скорости соединения без обрывов;
- создания защищённого канала без хакерских атак.

Преимуществ в использовании таких технологий хватает. Но есть и свои проблемы. Самая главная из них состоит в том, что используемый туннель не может одновременно следить за разными типами сетей, по которым осуществляется подключение к Интернету. Например, связь может пропадать при смене Wi-Fi на 3G/4G. Проблему начали устранять только недавно. На выделенных VPN-серверах появилась специальная авторизация, которая позволила осуществлять двустороннюю передачу данных, вне зависимости от того, какая именно сеть используется в данный момент. Тут основное преимущество состоит в том, что в криптографическом плане и виртуальный интерфейс пользовательского гаджета, и сеть оператора, и сам протокол доступа стали одинаковыми.

Список использованных источников:

1 Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. / В.Г. Олифер, Н.А. Олифер –СПб. Питер, 2010. – 944 с

2 Олвейн, В.. Структура и реализация современной технологии MPLS.: Пер. с англ. – М. Вильямс, 2004. – 480 с.

3 Virtual Local Area Network [Электронный ресурс]. – Режим доступа : http://www.admindoc.ru/.

КАЛИБРОВКА МНОГОЛУЧЕВЫХ АНТЕННЫХ УСТРОЙСТВ СИСТЕМ ТЕЛЕКОММУНИКАЦИЙ

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

Ксендиков В.С.

Кореневский С.А. – к.т.н.,доцент

В настоящее время в системах телекоммуникаций все более широкое применение находят многолучевые антенные устройства, позволяющие динамически оптимизировать обслуживаемую зону покрытия путем формирования диаграммы направленности адаптивной плотности для территориально распределенных абонентов и формирования нулей диаграммы направленности в направлениях источников помех.

Цифровая антенная решетка – это антенная система, представляющая собой совокупность аналого-цифровых каналов с общим фазовым центром, в которой диаграмма направленности формируется в цифровом виде, без фазовращателей. Теоретические основы такого подхода к построению антенн были заложены еще в 60–70 е годы прошлого века. Но лишь теперь, с развитием микропроцессорной техники, стало возможным практически реализовать накопленный научный задел.

Ключевая особенность ЦАР – цифровое формирование лучей диаграммы направленности антенны. В задачах связи это позволяет динамически оптимизировать обслуживаемую зону покрытия, оперативно перенацеливая цифровые приемопередающие лучи в зависимости от территориального распределения абонентов[1].

Технология ЦДО существенно улучшает качество связи в условиях многолучевого распространения радиоволн, а также резко повышает помехозащищенность системы при интенсивном радиопротиводействии. Это объясняется тем, что характеристики цифровых фильтров в антенных каналах практически идентичны[2].

Один из методов калибровки многолучевых антенных решеток «PN Gating Method», что в переводе означает «Селекция по шумоподобному сигналу». Данный метод подходит для решеток как плоских, так и линейных. Для плоской антенной решетки, у которой M – массивов излучателей и N – излучателей в массиве диаграмма направленности можно записать следующим образом:

$$E(\theta,\varphi) = \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} x_{mn}\cdot G(\theta,\varphi)\cdot e^{-jk\sin\left(\varphi\left[n-\frac{N-1}{2}\right]\right)d_x}\cdot e^{-jk\sin\left(\theta\left[m-\frac{M-1}{2}\right]\right)d_y},$$

где $G(\theta,\varphi)$ – диаграмма направленности элемента решетки(в случае изотропных источников равна единице);

k – волновое число;

d_x, d_y – расстояния между элементами по осям y и x;

$x_{mn} = a_{mn}e^{j\varphi_{mn}}$ – коэффициент, показывающий фазовый набег и коэффициент усиления в элементе.

Процедура калибровки антенны приводит к установлению необходимых фазовых набегов в фазовращателях и необходимых коэффициентов усиления.

Метод приведенный выше помогает избежать очень трудоемких по времени и средствам измерениям диаграммы направленности антенны посредством зондирования пространства вокруг нее. Метод предполагает присваивание каждому излучателю своего индивидуального кода. Все коды между собой ортагональны. В данном методе используется код Уолша, при составлении которого используется матрица Адамара. Код Уолша был выбран потому, что Матрица Адамара, из которой он построен, формируется рукурсивно, на основе матриц более низкого порядка, что удобно, также такая матрица симметрична относительно основной диагонали. Каждой строке матрицы будет соответствовать один элемент антенной решетки. При умножении кодового слова на несущую, последняя получит сдвиг фазы на $\pm 90°$ в зависимости от знака. Число разрядов кода должно быть больше либо равно числу излучателей в решетке, будь то линейная или плоская решетка. В результате модуляции несущей кодом и суммировании канальных сигналов от всех элементов в итоге будет сформирован композитный сигнал решетки.

Список использованных источников:

1. Слюсар В.SMART-АНТЕННЫ. – ЭЛЕКТРОНИКА: НТБ, 2004, №2,с. 62–65.
2. Слюсар В. Цифровое формирование луча в системах связи:будущее рождается сегодня. – ЭЛЕКТРОНИКА: НТБ, 2001, № 1,с. 6–12.

ВИБРАЦИОННЫЕ ПРЕОБРАЗОВАТЕЛИ: ВИДЫ, ПРИНЦИП ДЕЙСТВИЯ, УСТАНОВКА

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

Какоренко П. С., Шашков А. Г.

Давыдов Г. В. – канд. техн. наук, доцент

Введение

При выборе помещения, за пределы которого не должна выходить речевая информация, важно помнить о виброакустическом канале утечки информации. Акустические сигналы, возникающие при ведении разговоров в выделенном помещении, при воздействии на инженерно-технические коммуникации (трубы водоснабжения, отопления, воздуховоды) и строительные конструкции (окна, стены, двери, потолки), вызывают в них упругие колебания, которые могут регистрироваться датчиками средствами разведки. Использование звукоизоляции (т.е. ослабления уровня речевого сигнала) – вариант не всегда надежный.

Рис. 5 - Схема виброакустического канала утечки информации

Активные методы защиты речевой информации, основанные на использовании виброакустической маскировки информационных речевых сигналов, более эффективны. К ним относятся системы виброакустического зашумления. Оконечными устройствами в таких системах могут выступать вибрационные преобразователи.

I. Виды вибрационных преобразователей и принцип действия

В настоящее время в активных системах защиты информации широко используются следующие виды вибрационных преобразователей: электромагнитные, пьезоэлектрические, электродинамические. Все они отличаются между собой конструкцией и рабочими характеристиками.

Электромагнитный преобразователь представляет собой устройство, состоящее из корпуса, в котором установлен постоянный магнит для создания магнитного поля, в отверстие магнита вставляется катушка индуктивности, прикрепленная к крышке, для возбуждения переменного магнитного поля между магнитом и мембранной со штоком. Наличие резиновой прокладки обеспечивает зазор между магнитом и крышкой. Электромагнитные преобразователи весьма эффективны в области низких частот (до 400 Гц) и обеспечивают динамические значения выталкивающей силы 0,1 Н во всем речевом диапазоне частот. Данный вид преобразователей используется, к примеру, в совокупности с устройством защиты речевой информации «Прибой», созданным в научно-исследовательской лаборатории БГУИР.

Рис.2 – Электромагнитный преобразователь

Пьезоэлектрические преобразователи состоят из цилиндрического металлического корпуса с закрепленным внутри пьезокристаллом. При подаче напряжения на кристалл происходит его сжатие. Таким образом, при подаче на кристалл электрического шумового сигнала он передает колебания корпусу преобразователя, а тот, в свою очередь, через крепление – в конструкцию, к которой он крепится. Пьезоэлектрические преобразователи не

обеспечивают высокой эффективности в области низких частот, т.к. обладают низкой выталкивающей силой на частотах до 400 Гц. Но в отличие от электромагнитных преобразователей пьезоэлектрические более компактны и наиболее эффективны в области высоких частот.

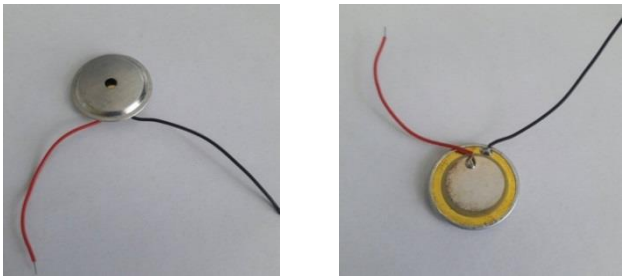


Рис.3 – Пьезоэлектрический преобразователь

Электродинамические преобразователи отличаются сложностью конструкторской реализации, заключающейся в наличии мембраны, малым магнитным зазором для обеспечения большой индукции. Предназначены для зашумления труб отопления, стен и перекрытий. Преимущество электродинамического преобразователя перед электромагнитными заключается в более широком диапазоне рабочих частот. С конструктивной точки зрения электромагнитные и пьезоэлектрические преобразователи просты в изготовлении и надежны в эксплуатации по сравнению с электродинамическими преобразователями.

Все эти устройства преобразуют электрические шумовые колебания в вибрационные, тем самым увеличивая энергию помех в виброакустическом канале утечки информации. Это, в свою очередь, ведет к снижению разборчивости речи. При этом технические средства разведки злоумышленника будут продолжать работать, но отделить полезный сигнал от помех перестанет представляться возможным.

II.Установка

Эффективность системы виброакустической маскировки во многом определяется правильным выбором мест установки, а также способом крепления преобразователей.

Рис.4 – Внешний вид части помещения, оснащенного вибрационными преобразователями

Необходимое количество вибрационных преобразователей определяется, исходя из мест их расположения, конструкции и материалов ограждающих поверхностей, оконных проемов и инженерных коммуникаций, а также эффективного радиуса подавления преобразователей на данных поверхностях (т.е. максимальное расстояние по поверхности от преобразователя до приемника средств разведки, при котором полезный речевой сигнал все еще маскируется).

Монтаж преобразователей на поверхности строительных конструкций проводится, как правило, с использованием специального штока, закрепляемого в перекрытии с помощью эпоксидной шпатлевки. Виброизлучатель навинчивается на шток после полимеризации шпатлевки, обычно через 2–3 часа после ее нанесения. Монтаж выполняется по следующему принципу: 1 преобразователь на 6–8 кв. м, причем должен соблюдаться отступ в 1–2 толщины стены от углов стены.

Преобразователи устанавливаются по одному на каждом элементе остекления в углу на расстоянии 100 мм от рамы. Для крепления на поверхность стекол используют специальный клей для склеивания металла со стеклом.

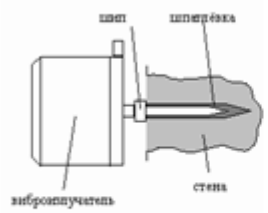


Рис.5 – Схема соединения преобразователя со

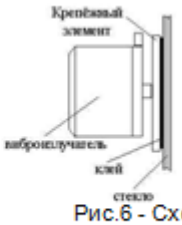


Рис.6 - Схема соединения преобразователя со стеклом

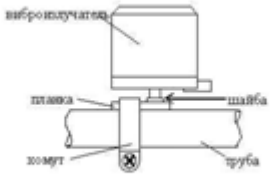


Рис.7 - Схема соединения преобразователя с трубой

При зашумлении инженерных коммуникаций вибрационные преобразователи устанавливаются на каждую входящую/выходящую трубу на расстоянии 100–300 мм от стены. Монтаж осуществляется с помощью хомута.

III. Заключение

Преобразователи, работающие в системах защиты речевой информации, должны иметь достаточно широкую частотную полосу, соответствующую полосе речевого сигнала. Кроме того, их параметры не должны существенно изменятся в рабочем или заданном диапазоне температур и во времени. На данный момент поставлена цель совершенствования конструкции преобразователей. Необходимо, чтобы устройство сочетало в себе характеристики электромагнитного и пьезоэлектрического преобразователей, а именно, эффективно маскировала речевой сигнал, как на высоких, так и на низких частотах.

ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ СМК В ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

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

Борбашова Е.И.

Белошицкий А.П. – к.т.н.,доцент

В настоящее время проблематика эффективного менеджмента является актуальной за счет предъявления высоких требований к качеству продукции и услуг. Энергетическая отрасль – одно из важнейших направлений, обеспечивающих нормальную жизнедеятельность населения Республики Беларусь. Качество электрической энергии, ее передача и распределение являются значительными вопросами, требующими детализации. В данной статье рассматриваются особенности внедрения и функционирования системы менеджмента качества в рамках энергетической отрасли, аспекты, на которых необходимо сконцентрировать внимание при осуществлении контроля.

Рассмотрим применение каждого принципа менеджмента качества относительно энергетической отрасли.

Принцип ориентации на потребителя в рамках функционирования организаций вне энергетической отрасли, значительно влияет на эффективность работы предприятия в целом. Результаты деятельности энергетического предприятия не зависят от уровня удовлетворенности потребителя вследствие монополистичности организаций отрасли. Реализация данного принципа позволяет повысить авторитет организации, снизить временные потери на рассмотрение жалоб и рекламаций, организовать устойчивую обратную связь, снижая риск несвоевременной идентификации несоответствий при подключении потребителя, в том числе юридических лиц. Данный принцип может быть реализован как в форме производственной инструкции, так и стандарта организации на любом уровне энергетической отрасли.

Принцип лидерства на предприятии энергетической отрасли может быть реализован установлением целей и политики в области качества, назначением ответственного из числа руководителей за результативность СМК, разработкой стратегии развития на определенный период (год, 5 лет, 10 лет). Концепция всеобщего лидерства в энергетической отрасли рассматривается не только с точки зрения одной организации (филиала), но и учитывает внутреннюю структуру всей отрасли, принимая стратегические решения в ГПО «Белэнерго» и адаптируя требования к филиалам РУП «Облэнерго». Основной особенностью тут является установление в стратегических задачах конкретной величины снижения уровня реализации рисков как при эксплуатации сети, так и при осуществлении своей трудовой деятельности сотрудниками.

Принцип вовлеченности персонала позволяет повысить результативность функционирования СМК в целом, и снизить общее число несоответствий для каждого отдела (службы), что отражается в карте оценки рисков ежегодно. Понимание ответственности за осуществление конкретных видов деятельности позволяет достигать целей организации либо идентифицировать причины невозможности их реализации. Вовлеченность персонала также способствует повышению компетентности и стимула сотрудников к получению качественного результата их деятельности, что влияет на эффективность работы всей организации. Данный принцип в филиале может быть реализован проведением Дня качества, обучением в рамках филиала, в сторонних организациях, премированием персонала за результаты деятельности и др.

Процессный подход – один из принципов, оказывающих наиболее существенное влияние на результаты деятельности. На каждом предприятии энергетической отрасли определяются процессы (по основной деятельности организации) и подпроцессы (разбиение в рамках каждого процесса для определения ответственности конкретных служб за участок жизненного цикла предприятия). Взаимодействие между процессами и подпроцессами представляет собой организованную систему, методы управления которой зависят от конкретной деятельности, осуществляемой предприятием. На примере филиалов электрических сетей процесс «Передача и распределение электрической энергии» включает функционирование всех служб и отделов, в задачи которых включены обслуживание, эксплуатация и ремонт сетей и (или) оборудования. Здесь процессный подход применяется не только при осуществлении непосредственной деятельности, но и при организации планирования затрат. Особенностью является рассмотрение при идентификации каждого подпроцесса всех рисков, прямо или косвенно влияющих на результативность подпроцесса. Все риски обязательно включаются в сводную карту оценки рисков по филиалу.

Реализация принципа улучшения в энергетической отрасли влияет не только на снижение затрат, но и уровня риска возникновения несчастных случаев. Надежность сети определяется системой показателей, улучшение каждого из которых влияет на стоимостную оценку электрической энергии для потребителей, безопасность эксплуатации. Направлениями для улучшения в филиалах могут являться:

- тайм-менеджмент работников;
- снижение числа отказов оборудования за счет повышения компетентности персонала, осуществляющего его обслуживание;
- повышение уровня информированности населения о работе электрической сети;
- снижение затрат за счет автоматизации оборудования и т.д.

Основной особенностью принципа улучшения на энергетическом предприятии является учет всех показателей качества при строительстве и реконструкции подстанций, эксплуатации сети, генерации электрической энергии и т.д.

Принцип принятия решений, основанных на свидетельствах обязателен к применению в энергетической организации вследствие сложности организационной структуры и структуры деятельности с точки зрения функционирования процессов. С этой целью в филиалах реализованы следующие виды контроля: мониторинг и измерения процессов внутри организации; анализ со стороны руководства; аудит (как внешний, так и внутренний); оценка удовлетворенности потребителей; производственный контроль и др.

Результаты контроля позволяют принимать обоснованные решения, а также осуществлять точечные воздействия при идентификации несоответствий на конкретном этапе каждого процесса.

Принцип менеджмента взаимоотношений со всеми заинтересованными сторонами является значимым при организации следующих видов деятельности в отрасли энергетики: заключение договоров на обслуживание, предоставление услуг, поставки; проведение плановых и внеплановых ремонтов; поставка электрической энергии потребителю и так далее. Особенностью принципа является учет большого количества организаций, задействованных в реализации данного принципа, следовательно, в ведении базы, учитывающей вклад в результат каждой.

С учетом специфики энергетической отрасли, высокого уровня травматизма и несчастных случаев как со стороны сотрудников организаций, так и населения страны, на предприятии в обязательном порядке организована система управления охраной труда (далее – СУОТ). С учетом ориентации Республики Беларусь на снижение техногенного влияния на окружающую среду, необходимости ее защиты от воздействия производственных факторов, на предприятии энергетической отрасли в обязательном порядке организована система управления окружающей средой (далее – СУОС). Интеграция СМК, СУОС и СУОТ является важной задачей, решение которой представлено в виде разработки согласованных между собой внутренних нормативных документов, совместного осуществления контроля, своевременной актуализации требований каждой системы при изменении хотя бы одной и так далее.

Таким образом, функционирование энергетического предприятия – сложный и многоуровневый процесс, требующий своевременного воздействия на внутренние процедуры. Проблематика отрасли энергетики требует интеграции СМК, СУОС и СУОТ, адаптации принципов для конкретных филиалов, а применение стандартов ISO серии 9000 – детального предварительного рассмотрения. СМК филиалов является неотъемлемой частью основной деятельности предприятия, выполняющей функции контроля каждого этапа жизненного цикла организации и осуществляя совершенствование подходов к функционированию структурных подразделений.

Список использованных источников:

1. Минскэнерго [Электронный ресурс]. – Электронные данные. – Режим доступа : http://www.minskenergo.by/.
2. СТБ ISO 9001-2015 «Системы менеджмента качества. Требования».

РАЗРАБОТКА ЛОКАЛЬНЫХ ДОКУМЕНТОВ СМК НА ПРЕДПРИЯТИИ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

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

Борбашова Е.И., Сапожникова В.А.
Белошицкий А.П. – к.т.н.,доцент

Требования, предъявляемые к СМК, регламентированы стандартами ISO серии 9000. Учитывая, что эти ТНПА являются обобщенными и не детализируют требования для конкретной отрасли, являясь руководством по разработке собственных критериев, возникает необходимость создания внутренних стандартов и других локальных документов СМК конкретной организации. В данной статье рассматриваются особенности функционирования системы менеджмента качества в рамках энергетической отрасли, а именно локальные документы, которые обязательно разрабатываются на энергетическом предприятии.

Учитывая сложную организационную структуру любой энергетической организации, следует разделить стандарты предприятий, где СМК, СУОС и СУОТ интегрированы, и где СМК, СУОС и СУОТ представляют собой самостоятельные системы, взаимодействующие между собой посредством контроля, а также по вопросам перекрестной деятельности.

В филиале «Минские кабельные сети» РУП «Минскэнерго» (далее – МКС), на примере которого представлена специфика разработки локальных документов, СМК и СУОС являются интегрированными системами, внедренными на предприятии в 2009 году, а СУОТ – самостоятельной системой, внедренной в РУП «Минскэнерго» в 2007 году.

1.1 С целью установления единообразия всех внутренних документов необходимо разработать стандарты по управлению документацией. Учитывая, что деятельность энергетических организаций всегда имеет отношение к функционированию не только организаций отрасли, необходимо предусмотреть два локальных документа: управление документацией внутреннего происхождения и управление документацией внешнего происхождения.

Стандарт предприятия «Управление документацией внутреннего происхождения» устанавливает единый порядок управления документацией внутреннего происхождения МКС. Требования стандарта применяют при разработке, проверке, согласовании, утверждении, введении в действие, внесении изменений, пересмотре, учете, хранении, рассылке, отмене, изъятии, архивировании, идентификации и уничтожении документов систем менеджмента качества.

Стандарт предприятия «Управление документацией внешнего происхождения» устанавливает единый порядок по управлению документацией внешнего происхождения, порядок идентификации, получения доступа к действующим законодательным и другим требованиям, обеспечения техническими нормативными правовыми актами, их учета, хранения, выдачи, актуализации и архивирования. Требования стандарта применяют при управлении внешними нормативными правовыми и техническими нормативными правовыми актами. Стандарт применяют при формировании реестров НПА и ТНПА, перечней НПА и ТНПА структурных подразделений, общего фонда ТНПА МКС и фондов ТНПА структурных подразделений, а также в случаях возникновения необходимости переписки со сторонними организациями, не входящими в структуру энергетической отрасли.

1.2 Основной деятельностью МКС является передача и распределение электрической энергии. Данный процесс должен быть прописан в стандарте организации.

Стандарт предприятия «Передача и распределение электрической энергии» устанавливает требования к порядку передачи и распределения электрической энергии МКС. Требования стандарта распространяются на описание процесса, включая цели, ресурсы, входные и выходные данные, а также мониторинг и оценку результативности процесса. Стандарт предназначен для применения высшим руководством, владельцами процессов, руководителями и работниками подразделений, осуществляющими эксплуатацию, обслуживание и ремонт электрических сетей.

В случае, если энергетическая организация не относится к электрическим сетям, стандарт описывает основной вид деятельности любого предприятия.

1.3 С целью осуществления контроля, поддержания функционирования, а также обслуживания электрических сетей МКС применяет оборудование, производственные здания и сооружения, а также другие ресурсы, необходимые для бесперебойного электроснабжения потребителей города Минска. В таком случае необходим локальный документ, описывающий порядок управления инфраструктурой.

Стандарт предприятия «Управление инфраструктурой» устанавливает порядок определения, обеспечения и поддержания в рабочем состоянии инфраструктуры, необходимой для достижения соответствия установленного качества работ МКС. Требования стандарта применяют к управлению такими ресурсами, как производственные здания и сооружения, рабочее пространство, оборудование и средства труда, вспомогательные службы, информационные и коммуникационные технологии, а также транспортные средства.

1.4 С учетом роста населения города Минска, активного строительства зданий и сооружений, возникает необходимость расширения электрической сети, что требует разработки проектной документации на передачу и распределение электрической энергии. С этой целью необходимо разработать стандарт предприятия «Разработка проектной документации на передачу и распределение электрической энергии», который устанавливает требования к разработке и согласованию проектной

документации в соответствии с лицензией на проектные работы МКС. Требования стандарта распространяются на порядок разработки проектной документации, включая подготовку и выдачу технических условий на проектирование, а также разработку и выдачу технических условий на электроснабжение.

1.5 Учитывая специфику деятельности для филиалов электрических сетей обязателен к разработке стандарт «Оценка удовлетворенности потребителей», который устанавливает порядок организации и методику проведения оценки удовлетворенности потребителей. Требования стандарта распространяются на мониторинг информации о восприятии внешних и внутренних потребителей выполнения предприятием их требований, методы получения и использования этой информации.

1.6 С целью осуществления внутреннего аудита, порядка его проведения, установления требований и критериев оценки необходима разработка соответствующего стандарта. Стандарт предприятия «Внутренний аудит» устанавливает требования к проведению внутренних аудитов и к аудиторам систем менеджмента качества МКС. Требования стандарта распространяются на планирование, подготовку, организацию и проведение внутренних аудитов, документальное оформление и анализ результатов аудитов, а также проведение корректирующих действий и подготовку данных руководству для анализа по результатам внутреннего аудита.

1.7 С целью установления порядка действий по устранению несоответствующей продукции (услуги), либо по результатам установления несоответствия в процессе проведения контроля необходимо разработать стандарты «Управление несоответствующей продукцией (услугой)», «Несоответствия, корректирующие действия».

Стандарт «Управление несоответствующей продукцией (услугой)» устанавливает требования к управлению несоответствующей услугой по передаче и распределению электрической энергии, разработке проектной документации по передаче и распределению электрической энергии в МКС. Требования стандарта распространяются на выявление несоответствий в процессе оказания услуги, идентификацию, регистрацию данных о несоответствиях, уведомление о выявленных несоответствиях, оценку и анализ несоответствий, а также устранение несоответствий, повторную верификацию, обобщение результатов анализа несоответствий, разработку корректирующих действий и подготовку ответа на замечания о несоответствиях.

Стандарт «Несоответствия, корректирующие действия» устанавливает порядок определения фактического и потенциального несоответствий, разработки и выполнения корректирующих действий в МКС. Требования стандарта применяют при установлении и анализе несоответствий системы менеджмента качества, законодательным и другим требованиям в области качества, а также при установлении причин несоответствий, разработке корректирующих действий, анализе результативности и эффективности предпринятых действий.

2. Положения СМК

2.1 Управляющий совет (далее – УС) является высшим коллегиальным и совещательным органом в СМК и создается для рассмотрения и решения вопросов, возникающих при разработке, внедрении, функционировании и улучшении СМК в соответствии с требованиями СТБ ISO 9001. УС обеспечивает эффективное взаимодействие подразделений и служб предприятия при разработке и функционировании СМК.

С целью установления порядка работы УС необходимо разработать Положение об Управляющей совете, которое устанавливает общие положения, основные задачи и функции, состав, организацию и порядок работы УС МКС, обязанности, полномочия и ответственность его членов.

2.2 С целью реализации процессного подхода в энергетической организации необходима разработка Положения о владельце процесса, которое устанавливает обязанности, полномочия и ответственность владельца (руководителя) процесса системы менеджмента качества МКС, отвечающего за перспективное планирование и управление процессом, действующего в рамках СМК. Положение распространяется на организацию работ по разработке, внедрению, поддержанию в рабочем состоянии и совершенствованию процессов, необходимых для СМК МКС.

2.3 С целью поддержания функционирования СМК, а также информирования о результатах деятельности СМК персонала организации, необходимо разработать Положение о проведении Дня качества. Положение устанавливает основные цели, задачи, порядок проведения «Дня качества» в МКС и организацию, порядок работы постоянно действующей комиссии МКС для проведения «Дня качества». Положение определяет сроки и порядок обмена информацией по повышению качества работ, выполняемых на оборудовании и в электрических сетях, обеспечивающих надежную и бесперебойную передачу электрической энергии потребителям, внедрению, поддержанию в рабочем состоянии и совершенствованию СМК предприятия.

В заключение следует отметить, что разработка локальных документов в области СМК требует детализации требований, предъявляемых к системам менеджмента в целом, адаптации требований ISO 9000 к конкретной деятельности, а также установлению целей организации.

Не смотря на разноплановость организаций энергетической отрасли, перечень локальных документов, установленных в настоящем докладе, обязателен к разработке при внедрении СМК любого энергетического предприятия. Конкретное содержание стандартов и положений зависит от специфики деятельности.

Список использованных источников:

1. Минскэнерго [Электронный ресурс]. – Электронные данные. – Режим доступа : http://www.minskenergo.by/.
2. СТБ ISO 9001-2015 «Системы менеджмента качества. Требования».

УПРАВЛЕНИЕ ЗНАНИЯМИ В ISO 9001-2015

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

Сапожникова В.А., Борбашова Е.И
Белошицкий А.П. – к.т.н.,доцент

В данной статье рассматриваются требования, предъявляемые к СМК, в области управления знаниями при внедрение новой версии стандарта ISO 9001-2015.. Рассматриваются особенности термина “знание”, его классификация. Дается определение понятиям данные, информация, знания, управление знаниями.

Основным добавленным пунктом является новой версии стандарта ISO 9001-2015 является:

7.1.6 Знания организации

Организация должна определить знания, необходимые для функционирования ее процессов и для достижения соответствия продукции и услуг.

Знания должны поддерживаться и быть доступными в необходимом объеме.

При рассмотрении изменяющихся нужд и тенденций организация должна оценивать текущий уровень знаний и определять, каким образом получить или обеспечить доступ к дополнительным знаниям и их необходимым обновлениям.

Примечания

1 Знания организации - это знания, специфичные для организации; знания, полученные в основном из опыта. Знания - это информация, которая используется и которой обмениваются для достижения целей организации.

2 Основой знаний организации могут быть:

a) внутренние источники (например, интеллектуальная собственность; знания, полученные из опыта; выводы, извлеченные из неудачных или успешных проектов; сбор и обмен недокументированными знаниями и опытом; результаты улучшений процессов, продукции и услуг);

b) внешние источники (например, стандарты, научное сообщество, конференции, семинары, знания, полученные от потребителей и поставщиков).

Отдельно стоит отметить, что требования к управлению информацией описаны в пункте:

7.5. Это свидетельствует о том, что в стандарте имеются четкие различия между управлением знаниями и управлением информацией [1].

Многие специалисты в области менеджмента считают, что включения этого пункта является спусковой кнопкой для мотивирования организаций заняться управлением знаний. Хотя новая версия этого стандарта не содержит в себе конкретных и строгих пунктов по внедрению на предприятиях инструментов управления знаниями. В мировой практике давно существует понятие «Управление знаниями» и «Система управления знаниями» и наработана довольно обширная база методов, инструментов и технологий в этой области.

Для разъяснения такого термина как «управление знаниями», необходимо дать определения самому понятию «знания» и продемонстрировать его связь и отличия от таких понятий как «информация», «данные».

Данные – это набор объективных фактов об объектах, событиях, явлениях, процессах, это все то, что регистрируется, описывается и воспринимается человеком. Данные могут быть цифровыми (факты, результаты измерений), графическими, аудио, видео и т.п. Они могут описываться на различных языках (символьном, математическом, графическом и т.п.). Качественными мерами для данных являются своевременность, соответствие и точность.

Информация - это данные в определенном контексте (необходимые пользователю, полезные для решения). Информация это совокупность данных и метаданных, содержащих их описание (данные о данных).

Используя предыдущие определения можно прейти к такому определению термина знания как совокупность информации и метаинформации, т.е. информации в контекст. Конечно определений такому понятию как знание существуют множество, начиная с гносеологических исследований Древней Греции. Однако предлагаю рассмотреть такой вариант:

«Знание – это сложная сеть понятий и многообразных отношений (оценки, мнения, причинно-следственные и пространственно-временные связи и зависимости) между ними, которая сознательно (логически) или бессознательно используется нейронной сетью головного мозга при необходимости выработки новых суждений или принятия разнообразных решений» [2].

В литературе знания, как правило, подразделяются на явные и неявные (которые находятся в головах сотрудников). Однако эта классификация кажется слишком упрощенной и даже вводит в некоторое заблуждение. Существует более продуманная и адекватная классификация знаний: явные, потенциально явные и неявные знания.

Явные: информация или знания, зафиксированные на материальных носителях.

Потенциально явные: информация или знания, которые еще не зафиксированы в материальной форме, но могут быть преобразованы в явные.

Неявные: информация или знания, которые сложно зафиксировать на материальных носителях.

Неявные знания существуют в умах специалистов, развиваясь во времени, через опыт, почерпнутый из профессиональной деятельности, книг, наставничества, а также обучения. Неявные знания зависят от жизненных ресурсов личности, от ее биофизических свойств и психологического потенциала [3].

Явные знания хранятся на реальных физических носителях (в книгах, бумажных документах, рисунках, схемах, фильмах, аудио и видео записях, магнитных и электронных файлах и базах данных и т.п.). То есть к явным знаниям относятся многочисленные компоненты информационных систем компании, такие, как:

• данные (файлы с данными, базы данных, базы инструкций и правил регламентного характера);

• документы (файлы с текстами в разных форматах); • программы (расчетные, аналитические, управления данными, графические, экспертные), реализующие разнообразные алгоритмы решения задач;

• адреса ресурсов и ссылки, фиксирующие местонахождение различных информационных ресурсов в архивах компании и в сетях Интернет.

Управление знаниями в организации – это систематический процесс идентификации, использования и передачи информации, знаний, которые люди могут создавать, совершенствовать и применять. Это процесс, в ходе которого организация генерирует знания, накапливает их и использует в интересах получения конкурентных преимуществ.

Управление знаниями – это комбинация отдельных аспектов управления персоналом, инновационного и коммуникационного менеджмента, а также использования новых информационных технологий в управлении организациями.

Управление знаниями включает в себя следующие компоненты:

• стимулирование прироста знаний;

• отбор и аккумулирование значимых сведений из внешних по отношению к данной организации источников;

• сохранение, классификацию, трансформацию, обеспечение доступности знаний;

• распространение и обмен знаний, в том числе в рамках организации;

• использование знаний в деловых процессах, в том числе при принятии решений;

• воплощение знаний в продуктах, услугах, документах, базах данных и программном обеспечении;

• оценку знаний, измерение и использование НМА организации;

• защиту знаний.

Цели управления знаниями:

• создать и закрепить свои конкурентные преимущества;

• максимально реализовать профессиональные и личностные возможности сотрудников[4].

Управления знаниями может стать спасательным кругом и опорной точкой для развития и лидерства в отрасли различных организаций. Внедрение нового пункта и демонстрация отличия понятий знания и информация в новой версии стандарта несомненно подталкивает организации к использованию этого относительно молодого, но перспективного инструмента СМК.

Список использованных источников:

1. СТБ ISO 9001-2015 «Системы менеджмента качества. Требования».
2. Тузовский А.Ф., Чириков С.В., Ямпольский В.З. Системы управления знаниями (методы и технологии) / Под общ. ред. В.З. Ямпольского. – Томск: Изд-во НТЛ, 2005. – 260 с
3. Michael E. D. Koenig (2012) What is KM? [Электронный ресурс]. – Электронные данные. – Режим доступа : http://www.kmworld.com/Articles/Editorial/What-Is/What-is-KM-Knowledge-Management-Explained-122649.aspx
4. Управление знаниями : учебное пособие / Л.А. Трофимова, В.В. Трофимов. – СПб. : Изд-во СПбГУЭФ, 2012. – 77

МЕТОДЫ ИСПЫТАНИЙ ЭЛЕКТРОПРИБОРОВ

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

Михайловский Н.В., Рагунович С.С.

Кострикин А.М. – к.т.н.,доцент

Испытание - опытное определение количественных и (или) качественных свойств предмета испытаний как результата воздействий на него, при его функционировании, при моделировании предмета и (или) воздействий. Испытания обычно проводят с целью получения сведений, необходимых для принятия решения о соответствии предмета испытаний заданным требованиям.

В соответствии с Соглашением по техническим барьерам в торговле Всемирной торговой организации (Соглашение по ТБТ ВТО) применение международных стандартов является одним из важных условий, обеспечивающих устранение технических барьеров в торговле.

Применение международных стандартов осуществляется путем их принятия в качестве региональных или национальных стандартов.

С целью обеспечения взаимопонимания национальных органов по стандартизации в части применения международного стандарта Международной электротехнической комиссии (IEC) подготовлен ГОСТ IEC 60335-1.

Данный стандарт относится к группе стандартов, регламентирующих требования безопасности бытовых и аналогичных электрических приборов (ГОСТ IEC 603351-2015) - общие требования безопасности, а также вторых частей, устанавливающих дополнительные требования к конкретным видам приборов.

Стандарт содержит нормы, правила и методы испытаний, являющиеся общими для всех бытовых и аналогичных электроприборов.

При отсутствии стандарта на конкретный тип прибора допускается распространять действие данного стандарта (насколько это приемлемо) на этот конкретный тип.

Данный стандарт действует одновременно с аналогичными стандартами ГОСТ 27570.0-87 (IEC 335-1:76), ГОСТ 30345.0-95 (IEC 335-1:91) и ГОСТ МЭК 60335-1-2008 (IEC 60335-1:2001) и соответствующими им стандартами, устанавливающими дополнительные требования к конкретным типам приборов.

Данный стандарт устанавливает требования безопасности к электрическим приборам бытового и аналогичного применения, номинальное напряжение которых не превышает 250 В для однофазных приборов и 480 В для других приборов.

Данный стандарт распространяется также на приборы, не предназначенные для обычного применения в быту, но которые, тем не менее, могут быть источником опасности для людей, не являющихся специалистами, но пользующихся приборами в магазинах, в легкой промышленности и на фермах.

Насколько это возможно, данный стандарт учитывает основные виды опасностей при использовании приборов, с которыми люди сталкиваются внутри и вне дома. Настоящий стандарт не учитывает опасности, возникающие:

- при использовании приборов людьми (включая детей), у которых есть физические, нервные или психические отклонения или недостаток опыта и знаний, препятствующие безопасной эксплуатации прибора без надзора или обучения;
- при использовании приборов детьми для игр.

Следует учитывать, что для приборов, предназначенных для применения в транспортных средствах, на бортах кораблей или самолетов, могут быть необходимы дополнительные требования, а так же во многих странах дополнительные требования определяются национальными органами здравоохранения, национальными органами, отвечающими за охрану труда, и подобными органами.

Приборы должны быть сконструированы таким образом, чтобы при нормальной эксплуатации они работали безопасно и не причиняли вреда лицам или окружающей среде даже в случае небрежного обращения, возможного при нормальной эксплуатации.

В основном этот принцип достигается выполнением соответствующих требований, содержащихся в настоящем стандарте, а соответствие проверяют проведением соответствующих испытаний.

Список использованных источников:

1. ГОСТ IEC 60335-1-2015 «Бытовые и аналогичные электрические приборы. Безопасность. Часть 1. Общие требования».

2. ДП СМ 7.5.1-07-2015 «Процесс испытаний продукции». Система менеджмента БелГИСС.

Сравнительный анализ доступности системы «Умный дом» для потребителя в Республике Беларусь и станах ЕС

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

Рагунович С.С., Михайловский Н.В.

Кострикин А.М. – к.т.н.,доцент

Автоматизированные устройства (системы) все больше внедряются в современную жизнь человека. Одной из таких систем является система «Умный дом». Данная система обрела популярность не только в нашей стране, но и за рубежом, причем устройства к системе каждый человек может подобрать по своим потребностям и экономическим возможностям. В данной статье проводится сравнительный анализ для потребителя системы «Умный дом» в нашей стране и странах Европейского союза.

Умный дом — это система домашней автоматизации, которая обеспечивает информацией об изменении состояния отдельных объектов в помещениях и выполняет поставленные задачи в автоматическом режиме без участия человека.

Человек, при выборе той или иной системы руководствуется следующими критериями:

1 Функциональность, предполагает реализацию большого числа функций для максимального охвата потребностей пользователя в обеспечении комфорта;

2 Стоимость, предполагает доступность услуг и оборудования для потенциальных пользователей;

3 Масштабируемость, предполагает возможность решения по охвату как можно большей территории;

4 Легкость установки, предполагает легкость установки аппаратного и программного обеспечения (ПО), а также легкую замену и добавление нового оборудования;

5 Удобство использования, предполагает удобство и простату в эксплуатации;

6 Защищенность передаваемой информации, предполагает аутентичность, целостность и конфиденциальность передаваемой информации;

7 Надежность, предполагает устойчивое решения к системным сбоям в работе, а также безопасную обработку системой (например, отключение поврежденных отдельных элементов).

Сегодня на территории Республики Беларусь существует множество компаний, предлагающие нам различные типы систем «Умный дом». Самой известной компанией по предоставлению услуги является компания РУП «Белтелеком». Проведем анализ доступности системы «Умный дом» на базе компании РУП «Белтелеком» в Республике Беларусь и других странах ЕС (таблица 1).

Страна	Оператор	Тип используемых устройств	Перечень датчиков, входящих в состав комплекта	Бизнес-модель	Цена для потребителя
Республика Беларусь [1]	Бел-телеком	Базовый комплект оборудования	абонентское устройство (контроллер), датчик задымленности, датчик движения и датчик открытия дверей/окон.	Ежемесячная абонентская плата, оплата за установку (при необходимости)	2.41 Euro .
		комплект оборудования	Базовый комплект + видеокамера, сирена, умная розетка, датчик температуры и влажности, датчик протечки воды.		5.81 Euro
Германия [2]	Deutsche Telecom	пакет устройств Magenta SmartHome.	датчик открытия дверей/окон, внутренняя камера и адаптерная розетка	Оплата стоимости устройств. Ежемесячная абонентская плата	150 Euro, 4,95 Euro ежемесячно
		комплект оборудования	датчик температуры и влажности, датчик протечки воды, видеокамера, умная клавиатура		От 30 Euro до 200 Euro за единицу
Польша [3]	Orange	Базовый комплект из 2-х оборудований	контроллер и, на выбор, датчик движения, камера, умная розетка или датчик протечки воды	Ежемесячная абонентская плата	2,2 Euro
		Базовый комплект из 3-х оборудований	контроллер, датчик дыма, датчик протечки воды		4,5 Euro
		дополнительные датчики	камера, датчик движения, умная розетка, датчик открытия двери, датчик дыма		22-30 Euro
Латвия [4]	Smart-House	пакет устройств	Умное освещение, климат-контроль, централизованное управление, видеонаблюдение. Панель управления с многочисленными возможностями.	Оплата стоимости устройств.	От 1 500 Euro

Европейский и Белорусский рынок систем «Умный дом» все еще находится на ранней стадии развития. На конец 2016 года, на рынке было 10,9 млн систем «Умный дом» в 28 странах ЕС. Около 1.4 млн таких систем были многофункциональными, тогда как 9.5 млн - "точечные" решениями. Согласно прогнозам внедрения системы «Умный дом», продолжит рости со среднегодовыми темпами в 57% в ближайшие пять лет, что позволяет ожидать рост числа "умных домов" до 80.6 млн к 2021 году [5].

Список использованных источников:

1. «Умный дом» в Республике Беларусь [Электронный ресурс]. – Электронные данные. – Режим доступа : https://www.beltelecom.by/.

2. «Умный дом» в Германии [Электронный ресурс]. – Электронные данные. – Режим доступа : https://www.telekom.de/.

3. «Умный дом» в Польше [Электронный ресурс]. – Электронные данные. – Режим доступа : https://www.orange.pl/.

4. «Умный дом» в Латвии [Электронный ресурс]. – Электронные данные. – Режим доступа : http://www.smarthouse.lv/.

5. Рынок «Умного дома» [Электронный ресурс]. – Электронные данные. – Режим доступа : http://www.mforum.ru/.

ПРИЕМО-ПЕРЕДАЮЩИЙ МОДУЛЬ ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ ОПРЕДЕЛЕНИЯ КООРДИНАТ ОБЪЕКТОВ

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

Лисов Д.А., Булавко Д.Г.

Гусинский А.В. – к.т.н.,доцент

В настоящее время в системах радиолокации всё большее применение находят приемо-передающие модули СВЧ-диапазона. Увеличение рабочей частоты модуля и переход в миллиметровый диапазон длин волн повышает разрешающую способность системы и точность измерения угловых координат объектов и их скоростей. Применение низкотемпературной совместно обжигаемой керамики повышает эффективность работы системы на сверх высоких частотах, позволяет применять в качестве проводников металлы с низким значением удельного сопротивления (платина, золото, серебро) и позволяет получать более высокую плотность компоновки.

Основой перспективных измерительных систем являются многоканальные приемо-передающие модули, позволяющие создавать многолучевые приемные структуры, гибкие в управлении своими режимами работы и хорошо адаптирующиеся в условиях различного рода помех и изменяющейся электромагнитной обстановки. Остались позади попытки разработать монолитные схемы для модулей из-за слишком высокой их стоимости. Развитие электроники привело к созданию унифицированных микросхем широкого применения: фазовращателей, аттенюаторов, переключателей — элементов, отличающихся высокими техническими характеристиками, малыми габаритами, универсальностью.

Разрабатываемый модуль состоит из излучателя и двух трактов − передающего и приемного (рисунок 1). Развязку между трактами обеспечивает циркулятор.

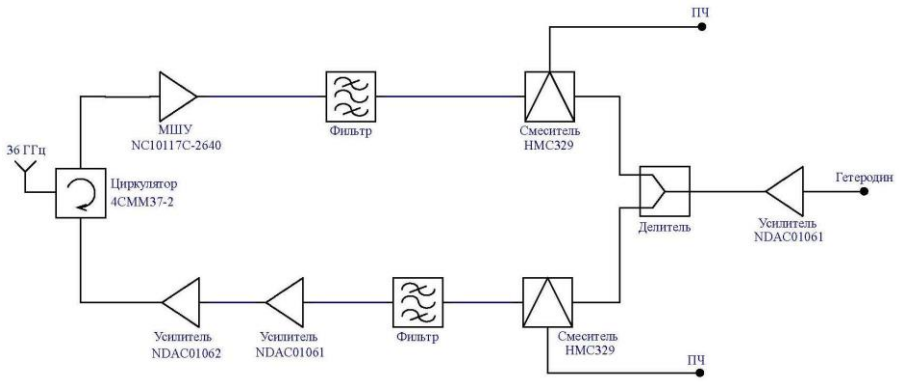


Рис. 1 – Структурная схема приемо-передающего модуля

В передающем тракте расположены смеситель, полосовой фильтр, предусилитель и выходной усилитель мощности. Приёмный тракт состоит из малошумящего усилителя, полосового фильтра и смесителя.

Производство печатной платы было решено произвести с использованием технологии низкотемпературной совместно обжигаемой керамики (LTCC). Для наших целей подходят системы A6-M и A6-S компании Ferro. Эти системы включают в себя полный спектр материалов. Среди них керамический порошок, керамические ленты и листы, пасты для создания внутренних и внешних проводников, пасты для металлизации переходных отверстий, пасты для создания встроенных резисторов. Разварка кристаллов будет производиться золотой проволокой диаметром 18 мкм, поэтому верхний слой металлизации целесообразно делать при помощи золотосодержащих проводящих паст.

Реализация гетеродина в данном конструктиве является проблематичной и экономически нецелесообразной. Поэтому считаем сигнал гетеродина сформированным вне модуля. Поскольку у данного модуля выходной сигнал с частотой 36 ГГц, а промежуточная частота равна 30 МГц, то частота гетеродина будет равна 35,97 ГГц.

Моделирование параметров микросборки производилось в программе SustemVue 2016.08. В результате была показана возможность работы разработанного приёмо-передающего модуля. Было установлено, что сигнал на выходе с частотой 36 ГГц имеет мощность 23,9 дБм, а сигнал промежуточной частоты в приёмном тракте различим на уровне шума и усилен до приемлемого уровня.

Результаты проделанной работы будут использованы при изготовлении макета многоканальной приемной системы в диапазоне частот 36 ГГц.

Список использованных источников:

1. Активные фазированные антенные решётки / под ред. Д. И. Воскре-сенского и А. И. Канащенкова. – М. : Радиотехника, 2004. – 488 с.

2. Кондратюк, Р. LTCC – Низкотемпературная совместно обжигаемая керамика / Р. Кондратюк // Наноиндустрия. – 2011. – №2. – С. 26–30.

МНОГОКАНАЛЬНЫЙ ПРИЕМНИК ИЗМЕРИТЕЛЬНОЙ СИСТЕМЫ МИКРОВОЛНОВОГО ДИАПАЗОНА

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

Булавко Д.Г., Лисов Д.А., Свирид М.С.

Гусинский А.В. – к.т.н.,доцент

В настоящее время интенсивное использование для целей радиолокации миллиметрового диапазона длин волн требует разработки современных устройств обладающих высокими техническими характеристиками. Одним из основных блоков современных радиолокационных измерительных систем и комплексов микроволнового диапазона является многоканальный приемник, во многом определяющий параметры и характеристики измерительной системы.

Многоканальный приемник измерительной системы микроволнового диапазона предназначен для принятия из окружающего пространства сверхвысокочастотного излучения (СВЧ), обработки его, как то перенос его на промежуточную частоту (ПЧ), усиление ПЧ и передачу в вычислительный блок. В данной работе разрабатывается приемник с одним переносом частоты. Структурная схема приемника представлен на рисунке 1.

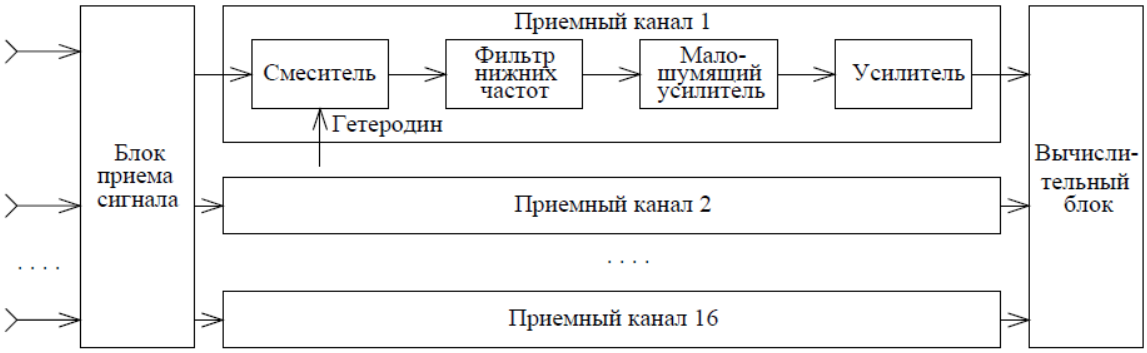


Рис. 1 - Структура схема измерительной системы

Многоканальный приемник состоит из трех блоков:

Антенная система выполнена в виде антенной решетки. Каждый канал антенной решетки состоит из волноводного прямоугольного рупора, отрезка волновода и перехода на щелевую линию передач.

Для выделения требуемой частоты используется смеситель. В смесителе происходит преобразование принимаемых частот и последующее выделение требуемой частоты. Формирование частоты гетеродина для 16 каналов приемника осуществляется блоком деления частоты по мощности. Сигнал гетеродина формируется внешним синтезатором. Усиление ПЧ осуществляется двух-каскадно: первый каскад представлен мало-шумящим усилителем, второй каска усиливает сигнал до нужного уровня вычислительного блока.

Вычислительный блок состоит из нескольких уровней. Первый уровень обрабатывает сигналы приходящие из блока обработки сигналов, усиливает и оцифровывает промежуточную частоту. Второй уровень уже обрабатывает сигналы приходящие с первого уровня.

Была проведено моделирование параметров приемника на системном уровне, разработана топология платы приемного модуля. Общий вид разработанной платы с установленными СВЧ элементами представлен на рисунке 2. Приемный модуль предполагается изготавливать по технологии низкотемпературной керамики. Был выбран материал низкотемпературной керамики A6M-E. Заявленные свойства данного материала:

– температурный коэффициент расширения 7 ppm/°C;
– сжатие ленты по X, Y 15,4±0,3%, по Z 24±0,3%;
– плотность более 2,45 г/см3;
– толщина 93 микрометра;
– диэлектрическая постоянная (от 1 до 100 ГГц) 5,9±0,2;
– напряжение пробоя >5000 В/слой;
– сопротивление подложки более 1012 Ом/см;
– тангенс угла потерь 0,003.

В качестве делителя сигнала гетеродина используется микрополосковые делители по мощности рассчитанные и реализованные в виде элементов топологии платы. Данный полосковый делитель является простейшим шестиполюсником состоящий из двух четвертьволновых отрезков линии передачи, две пары полюсов которого соединены параллельно, а две оставшиеся пары полюсов связаны через активное сопротивление.

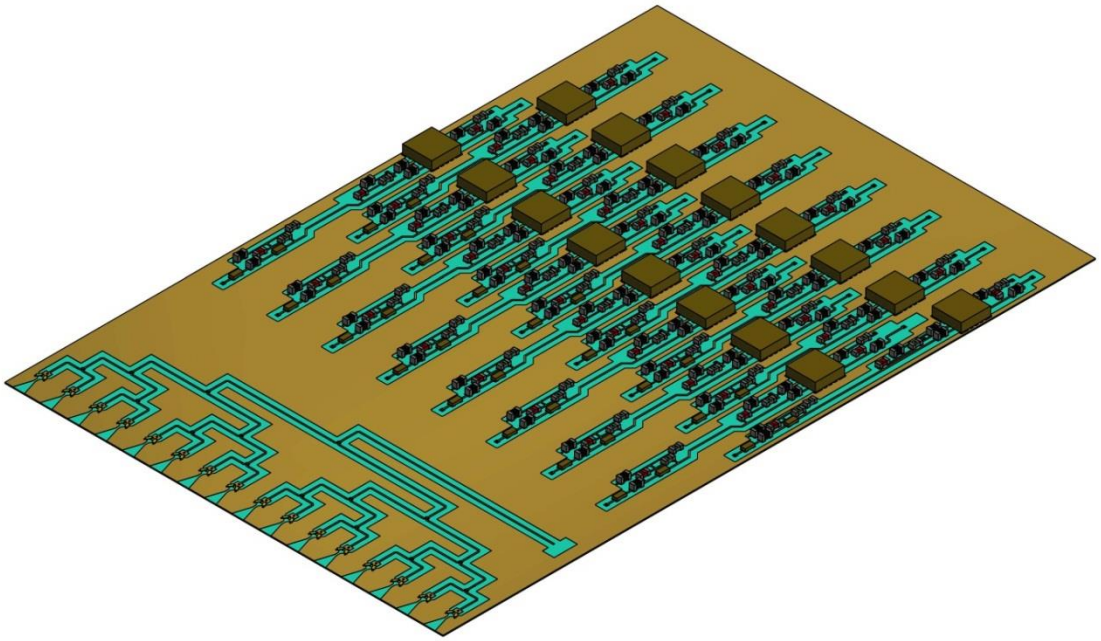


Рис. 2 – внешний вид платы приемного модуля

Проведенное моделирование параметров многоканального приемника и разработанная топология будет использоваться при изготовлении макета многоканальной приемной системы.

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

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

Мурашко Е.А, Марычев Д.В, Петкевич Д.А.

Вишняков В.А., д.т.н., профессор

Системы обнаружения сетевых вторжений и выявления признаков атак на информационные системы уже достаточно длительное время используются как одно из необходимых средств защиты информационных систем. Поскольку количество различных типов и способов организации несанкционированных проникновений в чужие сети за последние годы значительно увеличилось, системы обнаружения атак (СОА) стали необходимым компонентом инфраструктуры большинства организаций. Использование виртуальной инфраструктуры для построения системы обнаружения вторжений позволяет обеспечить как более рациональное распределение и использование физических ресурсов, так и упрощает администрирование всех компонентов системы защиты. В качестве средства обнаружения и предотвращения вторжений используется IDS/IPS Snort.

Система обнаружения вторжений (СОВ) (англ. Intrusion Detection System (IDS)) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть. СОВ всё чаще становятся необходимым дополнением инфраструктуры сетевой безопасности. В дополнение к межсетевым экранам (firewall), работа которых происходит на основе политики безопасности, СОВ служат механизмами мониторинга и наблюдения подозрительной активности. Архитектура СОВ включает:

12) Сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы;

13) Подсистему анализа, предназначенную для выявления сетевых атак и подозрительных действий;

14) Хранилище, в котором накапливаются первичные события и результаты анализа;

15) Консоль управления, позволяющая конфигурировать СОВ, наблюдать за состоянием защищаемой системы и СОВ, просматривать выявленные подсистемой анализа инциденты.

Пример реализации СОВ с использованием виртуальной инфраструктуры представлен на рисунке 1:

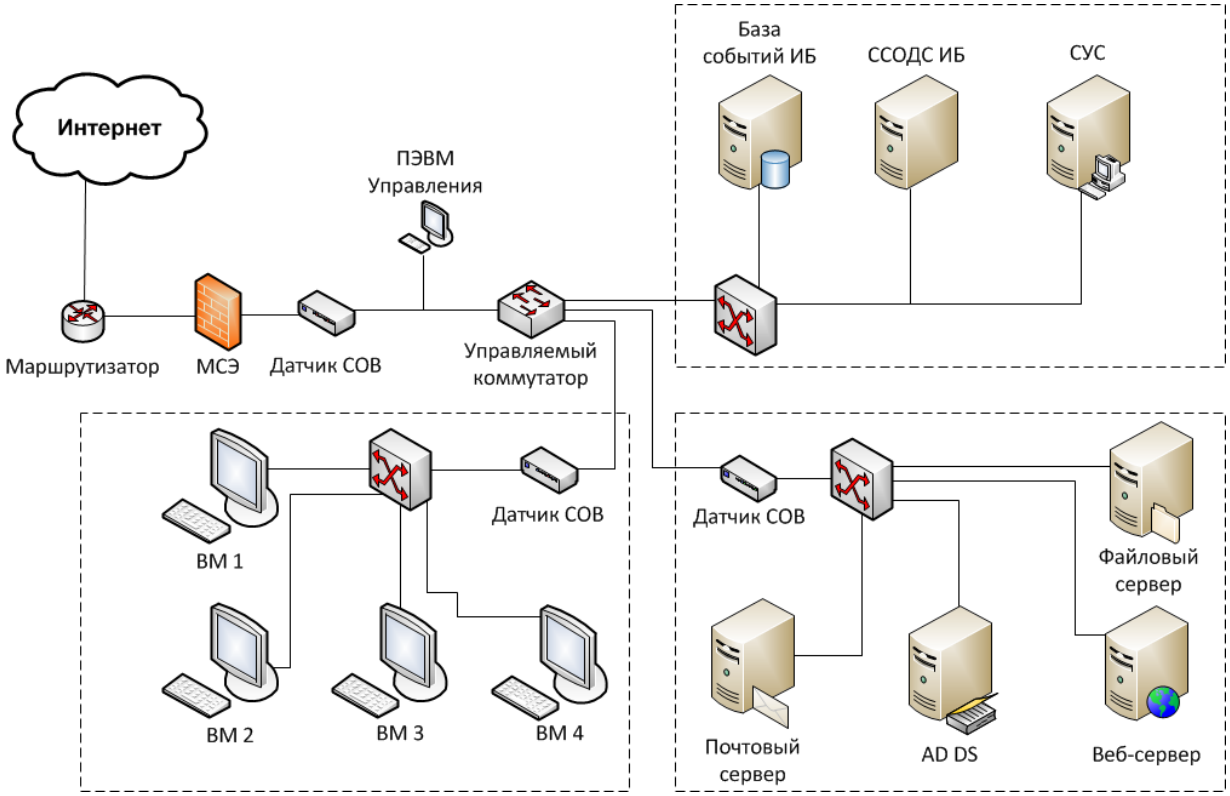


Рисунок 6 – Упрощённая структура сети с виртуальными и физическими СОВ

Штриховыми областями на схеме обозначены сервера виртуализации, на которых развёрнуты

датчики сети, виртуальные коммутаторы, различные сервера и виртуальные рабочие станции.

Созданная виртуальная инфраструктура обладает следующими особенностями:

а) события с датчиков СОВ собираются в базу данных на выделенном виртуальном сервере;

б) для упрощения работы и анализа событий, принятых от датчиков сети, развёрнута виртуальная система сбора и обработки данных о событиях информационной безопасности (ССОДС ИБ).

Основные преимущества использования виртуальной инфраструктуры:

- возможность быстрой миграции виртуальных машин и создания резервных копий;
- возможность перераспределения используемых виртуальными машинами ресурсов;
- уменьшение количества используемого физического оборудования;
- упрощение администрирования и реконфигурации сети;
- упрощение добавления новых рабочих мест и серверов.

Основные недостатки применения виртуализации:

- высокая стоимость серверов и корпоративных лицензий для использования виртуальных гипервизоров;
- необходимость повышения квалификации администраторов и пользователей для работы с виртуальной инфраструктурой;
- риск потери данных и увеличение времени простоя виртуальных серверов или рабочих станций при выходе из строй одного из серверов виртуализации.

Эволюция технологий виртуализации открывает новые возможности для обеспечения оптимальной и максимально удобной организации любых современных локальных сетей. Неизбежный рост сетевой инфраструктуры способствует всё большей популяризации использования средств виртуализации как для простых объектов, как-то рабочие места сотрудников предприятий, так и более сложных и комплексных информационных систем. Переход от исключительно физической инфраструктуры сети к комбинированной с виртуальной является залогом успешного развития локальных и глобальных сетей.

Список использованных источников:

1. Вишняков, В. А. Информационная безопасность в корпоративных системах, электронной коммерции и облачных вычислениях: методы, модели, программно-аппаратные решения / В. А. Вишняков. – Минск : Белорусская государственная академия связи, 2016. – 276 с.

2. Национальный открытый университет [Электронный ресурс]. – Режим доступа : http://www.intuit.ru/.

3. Таненбаум, Э. Компьютерные сети. Пятое издание. / Э. Таненбаум, Д. Уэзеролл – Санкт-Петербург. : Питер, 2012. – 960 с.

4. Dave Mishchenko. VMware ESXi: Planning, Implementation, and Security.

5. David Chisnall, The definitive guide to the Xen hypervisor. ISBN-13: 978-0-13-234971-0.

6. Бэйкер, Э. Р. Snort IDS and IPS Toolkit. / Э. Р. Бэйкер, Дж. Эслер. – Берлингтон : Syngress, 2007. – 766 с.

СЕНСОРНЫЙ МОНИТОРИНГ СОСТОЯНИЯ СЕРДЕЧНО-СОСУДИСТОЙ СИСТЕМЫ ЧЕЛОВЕКА

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

Вышемирский А.О.
Борискевич А.А. – д.т.н., профессор

В настоящее время потребности в удалённом мобильном телемониторинге растут с каждым днём. Более всего, ощущается недостаток мобильного мониторинга состояния сердечно-сосудистой системы пациентов, Огромное количество людей, как во всем мире, так и в нашей республике, испытывают проблемы со здоровьем и не имеют возможности часто посещать врача, либо находиться под стационарным наблюдением в клинике. В подобной ситуации оказываются и люди, которые занимаются активными видами спорта, а также представители некоторых экстремальных профессий. В этом случае эффективным решением является применение устройств мобильного мониторинга сердечно-сосудистого состояния человека, позволяющих отправлять данные наблюдений врачу посредством сети передачи данных.

Под мониторингом сердечно-сосудистой системы понимается исследование и наблюдение функциональных особенности сердца, касающиеся всех его функций: автоматии, возбудимости, проводимости и сократимости. Важным аспектом исследования является сократительная функция миокарда [5, с. 52].

Для количественной оценки кардиодинамики применяется фазовый анализ систолы левого желудочка. Он заключается в измерении продолжительности периодов и фаз систолы.

Данные изменения гемодинамики могут сниматься как непосредственно с сердечной аорты (путём инвазивных датчиков, в строенных в кардиостимуляторы, или неинвазивных, закреплённых на коже в точке в области сердца) так и с других точек тела и других типов датчиков [2, 5].

Существуют следующие инструментальные методы исследования сердечно-сосудистой системы человека:

стационарная электрокардиограмма (ЭКГ);
Холтеровское мониторирование (Холтеровская ЭКГ);
фонокардиография;
сфигмография (фотоплетизмограмма) и др. методы исследования на основе пульсации крови;
рентгенография;
эхокардиография;
доплероэхокардиография;
радиоизотопное исследование сердца;
магниторезонансная томография;
катетеризация сердца и ангиокардиография;
измерение артериального давления;
инвазивное исследования сердца [5, 6].

Разберём более подробно некоторые методы:

Стационарное ЭКГ — регистрация электрической активности сердца с помощью электродов с поверхности тела. Изменения электрической активности связаны с суммацией электрических процессов деполяризации и реполяризации.

Значение ЭКГ: позволяет выявлять нарушения сердечного ритма, расстройство коронарного кровообращения, отражает увеличение отдельных полостей сердца, способствует выявлению склеротических и дистрофических процессов в миокарде.

Типы датчиков: металлический электрод с резиновой присоской.

Количество каналов: (отведений) – 1, 3, 6, либо 12.

Количество датчиков: один и более, но кратно количеству отведений (чаще всего 12)

Тип входного сигнала: аналоговый (полезная полоса частот от 0.5 до 60 Hz).

Холтеровское ЭКГ — тоже регистрация электрической активности сердца, регистрирующая с помощью электродов с поверхности тела. Но, в отличие от стационарного мониторирования, данные при Холтеровском мониторировании снимаются в течении длительного периода времени, от суток до 7-и, посредством специального носимого мобильного прибора.

Значение Холтеровского ЭКГ: позволяет выявить нарушения ритма и проводимости сердца, с неясными обмороками, а также частично для регистрации «немой» (безболевой) ишемии миокарда, для оценки некоторых параметров работы электрокардиостимулятора.

Типы датчиков: миниатюрный электрод на самоклеющийся поверхности.

Количество каналов (отведений): 3 -12.

Количество датчиков: как правило, 7, включая контакт «земля»)

Тип входного сигнала: аналоговый (полезная полоса частот от 0.5 до 60 Hz) [2, 6].

Фонокардиография — метод графической регистрации звуковых колебаний сердца.

Значение фонокардиографии: обладает способностью выявлять и оценивать различные добавочные тоны и шумы сердца, которые не выслушиваются аускультативно (т. е. по средством

физического метода медицинской диагностики, заключающегося в выслушивании звуков, образующихся в процессе функционирования внутренних органов).

Типы датчиков: специализированный динамический либо конденсаторный микрофон воздушной или вибропроводимости сигнала.

Количество каналов (отведений): 4 (аускультативный, низкочастотный, средне- и высокочастотный).

Количество датчиков: 4.

Тип входного сигнала: аналоговый, звуковой, инфразвуковой и ультразвуковой (полезная полоса частот от 0.3 до 1000 Hz) [6].

Эхокардиография (УЗИ) — метод ультразвукового исследования сердца, изучающий структуру и функцию сердца, основанный на отражении звуковых волн, направленных на изучаемые структуры, которые возвращаются к датчику, где и регистрируются. Определяет толщину стенок и размеры камер сердца во время систолы и диастолы.

Значение эхокардиографии: оценка размеров сердца и его отдельных структур (желудочки, предсердия, межжелудочковая перегородка, толщина миокарда желудочков, предсердий и так далее), наличие и объём жидкости в перикарде — «сердечной сорочке», состояние клапанов сердца.

Типы датчиков: ультразвуковой (на основе множества пьезоэлектрических преобразователей и фокусной линзы) секторный, механический, либо микрокосвенный с глубиной воздействия 10-20 мм. Используется совместно с ультразвуковым генераторам (частота генерации 1000 импульсов в секунду).

Количество каналов (отведений): 1.

Количество датчиков: 1.

Тип входного сигнала: аналоговый (3,5 -5 GHz) [5, 6].

Сфигмография (фотоплетизмография) и другие методы исследования на основе пульсации крови — методы регистрации колебания стенок артерий, в частности, сонной (в сфигмографии датчик устанавливается на шее в области сонной артерии, а в фотоплетизмографии в области других артерий и сосудов). Для повышения надежности может применять в сочетании с ЭКГ [6].

Типы датчиков: миниатюрный фотодатчик (источник света, чаще всего LED и фотоприёмник), также существуют лазерные датчики, где в качестве источника излучения применяется лазер [4]. .

Количество каналов (отведений): 1 – 3 (как правило, 1.).

Количество датчиков: 1 и более, (как правило, 1).

Тип входного сигнала: аналоговый (полезная полоса частот от 0.5 до 7 Hz) [1].

Значение Фотоплетизмографии: позволяет осуществлять мониторинг сердечного ритма, пульса, также посредствам ФПГ является эффективным прогнозирование коронарного атеросклероза [6].

Одним из важных направлений для исследования является фотоплетизмографиия (и её мобильная реализация). Использование мобильной фотоплетизмографии для исследования сердечно-сосудистой системы человека обладаем рядом преимуществ:

1. возможность ведения длительного, в т. ч. круглосуточного, наблюдения за пациентом без посещения им учреждений здравоохранения;
2. возможность пациенту самому наблюдать за показателями своего здоровья;
3. ФПГ-датчик может быть установлен практически в любое устройство, такое как часы, либо смарт-браслет [2].

Основной недостаток мобильной фотоплетизмографии, также как и стационарной фотоплетизмографии – это возможность получения лишь основных медицинских показателей. Но этот недостаток решается путём использования совместно с ФПГ-датчиком, других типов датчиков, необходимых для получения более полной биометрической картины [3].

Изучение, развитие и внедрение технологий сенсорного мониторинга состояния сердечно-сосудистой системы человека является неотъемлемым аспектом для формирования здорового генофонда нации и повышения качества жизни.

Список использованных источников:

1. Jindal, V. A Deep Learning Framework to Monitor Heart Rate During Intensive Physical Exercise // MobileSOFT – 2016 - University of Texas, Dallas, TX

2. Lu G, Yang F, Taylor JA, Stein JF. A comparison of photoplethysmography and ECG recording to analyse heart rate variability in healthy subjects // J Med Eng Technol. 2009. -Vol. 33 (8). - P. 634 - 641.

3. Servati A. et al. Novel Flexible Wearable Sensor Materials and Signal Processing for Vital Sign and Human Activity Monitoring //Sensors. – 2017. – Т. 17. – №. 7. – С. 1622.

4. Алексеев, В. А. Фотоплетизмограф с импульсным источником интенсивного лазерного излучения / В. А. Алексеев, С. И. Юран, А. С. Перминов // Приборостроение – 2014 : материалы 7-й Междунар. науч.-техн. конф., Минск, 19–21 нояб. 2014 г. / НАН Беларуси [и др.] ; редколл.: О. К. Гусев (пред.) [и др.]. – Минск, 2014. – С. 22–24

5. Макеева, В.С. Мониторинг физического состояния: учебное пособие / В.С. Макеева. – Орёл: Госуниверситет-УНПК, 2013. – 100 с.

6. Шугуров, О.А. Инструментальные методы исследования сердечно-сосудистой системы: учебное пособие для студентов II - V курсов специальности "Биологическая физика". — Днепропетровск: ДНУ, 2007. — 57 с.

MODELLING OF INFORMATION TRANSMMIISION ON LOCAL NETWORKS

The Belarus state university of computer science and radio electronics
Minsk, Belarus

Ileberi Emmanuel, Al-Rubayie Issa
Astrovsky I. I. - associate professor

Considering the questions on working out a complex of programs in MATLAB programming system, Cisco Packet Tracer and MyTestX that simulates systems of information transfer. Annotated screenshots are used to aid understanding. Important notes or tips are presented in tip boxes. Like any simulation, Packet Tracer relies on a simplified model of networking devices and protocols. Real computer networks, experienced both in-person/hands-on and remotely, remain the benchmark for understanding network behavior and developing networking skills.

Introduction

In Nigeria, communication tools such as telephones and the Internet are increasingly critical to economic success and personal advancement. The advent of the Internet has been variously described as being as important for society as the development of the personal computer, the telephone or even the printing press, the Internet serves many functions as virtual community, electronic marketplace, information source and entertainment center, among others. Through the Internet, we can create new businesses or facilitate the delivery of basic services such as health and education.

Almost all countries are on-line and Internet users grow by an average of 78 million new users annually. The growth of the Internet is creating opportunities for new high speed data networks, new multimedia applications, Voice over Internet Protocol (Internet Phone) and convergence of technologies.

For the maintenance of existing equipment, modernization and expansion of telecommunication networks, the country needs competent specialists. For their training, special software can help significantly to optimize and speed up the learning process.

Modeling of information transmission in local networks.

The Goal of this article is the development of a software product with the help of which it is possible to simulate computer networks and study both the operation of networks as a whole and to study individual nodes, protocols and algorithms for their operation. Development of a program for modeling the information transmission system in local networks for effective training of specialists in the field of communications.

The advantage of this topology is that, in comparison with topologies it has better fault tolerance, since it includes all the best qualities of other topologies.

Thus, this project will be organized by the backbone network on the basis of the ring, which will combine the core network routers (Bayelsa, Rivers, Delta, Imo). Network access and distribution, in turn, will be represented by a hybrid topology of the tree-ring: subscribers will be connected to the switches of the working groups on the tree structure, in turn switches to routers include transportation access rings. This will keep the services of the subscribers in case of emergency.

Core routers are included in the big ring road that connects the routers branches from a central router Bayelsa provides access to the PSTN and the Internet. The network topology in conjunction with a map of Nigeria

To verify the simulation results has been built in the Packet Tracer 5.3 model of the segment, adjust the basic units, the distribution of IP-addresses, and then were evaluated by the operation of its main characteristics. The maximum packet delay for VoIP services without the use of reserve satellite was 145 ms. The obtained value corresponds to the delay requirement for QoS networks for VoIP traffic in the TOR (150 ms).

Conclusion

The presented screenshots show separate stages of the program, including the preliminary task, the task for performance, theoretical data and methodical instructions on work with software product. The program is supplied by its own calculator to calculate the generalized characteristics of signals and noises under the set experimental conditions.

References

1. King, P.R. Modeling and Measurement of the Land Mobile Satellite MIMO Radio Propagation Channel/ P.R. King // University of Surrey. – 2007.

ИНТЕЛЛЕКТУАЛЬНЫЕ АЛГОРИТМЫ РАСПОЗНАВАНИЯ ЭМОЦИОНАЛЬНОГО СОСТОЯНИЯ ЧЕЛОВЕКА

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

Азарко И.В.

Борискевич А.А. – д.т.н.,профессор

Для распознавания эмоционального состояния используют устройство, в котором размещены датчики движения: акселерометр, гироскоп, магнитометр, которые в свою очередь включают в себя психоэмоциональные датчики для определения состояния человека.

Полученные с датчиков данные обрабатывают с помощью средств начальной обработки, размещенных в составе устройства и передают с помощью проводных или беспроводных технологий в устройства дальнейшей обработки и/или воспроизведения информации.

В работе предлагается использовать алгоритмы распознавания эмоционального состояния человека на основе данных сигнала акселерометра.

Данные акселерометра приводят к некоторым неточностям, когда дело доходит до качества предобработки данных:

– При ходьбе с телефоном в кармане он не имеет последовательного позиционирования, поэтому сравнивать показания с отдельными осями затруднительно;

– Расположение кармана оказывает влияние на показания, то есть лежа в кармане, расположенного ниже, на ноге, когда телефон становится более подвижным, чем лежа в кармане дальше;

– Существует много неуверенности относительно того, прошел ли участник в течение всего времени записи.

Алгоритмы обработки сигнала подразумевают:

– Преобразование сигнала акселерометра;

– Сегментацию сигнала акселерометра;

– Выделение сигнала акселерометра.

В результате считывания данных, возникает вопрос с зашумленными данными. Одним из способов борьбы с зашумленными данными при обработке является применение метода средних значений (Moving average, MA) один из самых простых методов фильтрации шума. Задача распознавания эмоций накладывает одно существенное требование к фильтру – требование производительности достаточной для того, чтобы использовать фильтр в режиме реального времени с минимальными задержками. Большим плюсом фильтра является приближенность значений к начальным.

В ходе работы для программной реализации были выбраны Python и MATLAB. Это связано с тем, что Python и MATLAB хорошо подходят для научного и математического программирования. Библиотека Python SciPy, модуль NumPy, используется для различных операций с массивами и матрицами. Методы поддержки векторной машины и определения дерева решений получают через библиотеку scikit-learn, а также библиотеку обучения с открытым исходным кодом для Python. Параметры для разных классификаторов были определены экспериментально. Это было сделано частично, начиная с опций по умолчанию и экспериментируя вручную, а частично через процесс, называемый grid-поиском.

Список использованных источников:

1. Andreas F.O., Detecting Human Emotions Using Smartphone Accelerometer Dat, 2016, pp. 1–103.

THE LTE MOBILE RADIO ACCESS NETWORK

Belarusian State University of Informatics and Radio Electronics
Minsk, Republic of Belarus

Saddawi Rasol Kareem

Mishchenko V.N.- Ph. D., ass. professor

Cellular mobile communication system is a kind of mobile communication for transmission to subscribers of mobile telephone communications and digital data. Cellular network got its name in accordance with the principle of territorial distribution of work areas (cells). In the center of each work area is a base station communicates by radio with the mobile stations, which may be stationary or movable. Due to the property of attenuation of radio waves propagation, it has been able to use the same set of radio channels in different cells. LTE standard was confirmed as the next after UMTS Third Generation Partnership Project (3GPP) standard mobile broadband network international union in January 2008. Standard provides a throughput and a data rate that are necessary for the growing number of subscribers increasingly demanding. In Belarus, the LTE network was put into commercial operation in the city of Minsk in December 2015 by the infrastructure operator beCloud. Minsk became the first Belarusian town, where there was this network. Currently it runs construction of networks for the fourth generation mobile communication in other cities of Belarus, including regional centers and other cities.

The main task in the LTE mobile penetration is the development of a radio access network for a given number of users and selected area coverage in given frequency band. LTE network employs large number of the base stations and uses the frequency band 20 MHz to 1800 MHz (LTE band 3). If necessary it is possible to activate of the second band - 30 MHz in the range of 2600 MHz. However, development of LTE at 1800 MHz are given the cost is less on average 60% than the development of networks in the high-frequency bands. LTE network consists of two major components: a radio access network E-UTRAN and a core network SAE (System Architecture Evolution). The radio access network E-UTRAN examined in a number of technical specifications according to which it consists only of the eNB (evolved Node B) base stations. A simplified diagram of LTE network when it interacts with the packet switched domain (PS-Domain) networks according to other 3GPP technical specification 3GPP TS 23,401 is illustrated in Figure 1 [1].

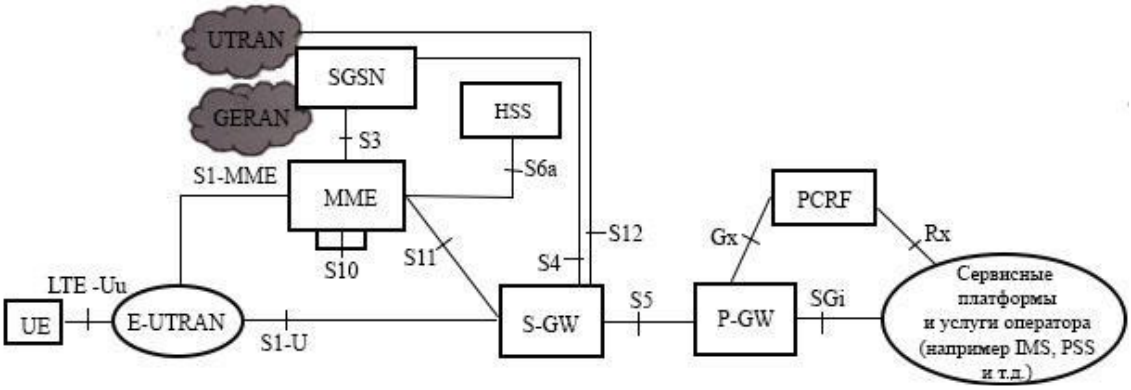


Figure 1. A simplified diagram of LTE network

Radio access networks are used GERAN network, UTRAN and E-UTRAN. Note that in practice the network elements - SGSN service node serving gateway S-GW and P-GW gateway packet can be constructively combined. According to the scheme of Figure 1 the main LTE network interfaces interact with 3GPP networks (GERAN / UMTS) are interfaces S3, S4 and S12. Interfaces S3 and S4 provide interaction logic control MME mobility gateway and S-GW LTE network service node SGSN 3G network using the tunneling protocol GTP (GPRS Tunnelling Protocol). S12 interface for its intended purpose similar to Gn interface between the service and the SGSN GGSN GPRS network gateway.

In simulation number of base stations has been determined to coating service area for town Polotsk with the given number of users and area. We estimated the maximum allowable losses in the propagation of the signal for the uplink (from the cellular phone to base station) and downlink radio link (base station to mobile phones). We used a well-known model COST-231-Hata to determine the propagation loss of radio signals in selected frequency ranges [2]. Software program complex Atoll was used for the calculation of coverage of the base stations for given region of the Polotsk. The software package Atoll is one of the best solutions for radio planning and optimization of different radio technologies for mobile communication systems, including LTE / LTE-Advanced.

List of sources used:

1. Tikhvinsky, V.O., Terentyev, S.V. B. Yurchuk A.B. LTE mobile networks: technologies and architecture / V O. Tikhvinsky, S. V. Terentyev, A. B. Yurchuk. - M .: Eco-Trends, 2010. - 284 p.

2. Mishchenko V.N. Radio access networks of cellular radio systems with code division channels "/ V.N. Mishchenko. - Minsk: BSUIR, 2016. - 65 p.

МЕТОДЫ ПОВЫШЕНИЯ ЭНЕРГЕТИЧЕСКОГО ПОТЕНЦИАЛА ВОЛОКОННО-ОПТИЧЕСКИХ СИСТЕМ ПЕРЕДАЧИ

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

Дамашевич А.С.

Урядов В.Н. – к.т.н.,доцент

В настоящее время системы использующие в магистальных линиях связи должны иметь большие длинны реляционных элементов. Длина реляционного участка зависит от энергетического потенциала, который стараются увеличить различными методами.

Энергетический потенциал – это разность между уровнем оптического сигнала на выходе передающего и чувствительностью приемного оптических модулей, где чувствительность приемного оптического (ПрОМ) – минимальный уровень оптического сигнала на входе ПрОМ, при котором обеспечивается требуемый коэффициент ошибок (БЕР).

Волоконно-оптические системы передачи включают в себя оптический передатчик, волоконно-оптическая система передачи и оптический приёмник.

Рис. 1 – структура ВОСП

Существуют основные способы повышения энергетической эффективности:

– Увеличение мощности передатчика

– Использование новых высокоэффективных методов модуляции;

– Использование предуселителей и усилителей

– Использование высокоэффективных приёмников и методов приёма

Все эти способы должны обладать эффективностью против нелинейных искажений, вынужденного рассеяние Мандельштама-Бриллюэна (ВРМБ), релеевского рассеяния, флуктуации фазы и частоты.

Список использованных источников:

1. Сагиев, Р. К. Исследование энергетической эффективности различных видов модуляции : учеб. пособие / Р. К. Сагиев. – Казань : КНИТУ, 2016. – 8 с.

2. С. А. Булгакова, А. Л. Дмитриев. Нелинейно-оптические устройства обработки информации / Учебное пособие. – СПб: СПбГУИТМО, 2009. – 56с.

3. Ярив, А. Н. Введение в оптическую электронику : учеб. пособие / А. Н. Ярив. – Москва : Выш. Шк., 1983. – 398 с.

4. Урядов, В. Н. Волоконно-оптические системы передачи : электронный учебно-методический комплекс / В. Н. Урядов. – Минск : Выш. Шк., 2006. – 226 с.

5. Иванов, А. Б. Волоконная оптика. Компоненты, системы передачи, измерения : электронный учебно-методический комплекс / А. Б. Иванов. – Москва : SYRUS SYSTEMS, 1999. – 671 с.

6. Бунас, В. Ю. Волоконно-оптические системы передачи : лабораторный практикум / В. Ю. Бунас, Н. В. Тарченко, В. Н. Урядов. – Минск : БГУИР, 2016. – 54 с.

7. Физическая энциклопедия [Электронный ресурс]. –2017. – Режим доступа : http://femto.com.ua/articles/part_1/2319.html.

ПОРОГОВОЕ ДЕКОДИРОВАНИЕ СИСТЕМАТИЧЕСКИХ САМООРТОГОНАЛЬНЫХ СОСТАВНЫХ БЛОКОВЫХ КОДОВ

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

Картошников Д.Н.

Королев А.И. – к.т.н.,доцент

Достоинства порогового алгоритма декодирования, а именно, высокая скорость (В ≥ 100 Мбит/с) декодирования информации, коррекция ошибок более гарантированной исправляющей способности кода, возможность организации непрерывного контроля качества канала связи без внедрения дополнительной избыточности и др. определили широкое применение данного алгоритма в реальных системах связи для обеспечения заданной достоверности передачи информации [1-4].

Теория построения линейных блоковых самоортогональных кодов (ЛБСОК), допускающих реализацию порогового алгоритма декодирования, рассматривается в работах [1-4]. Данные коды строятся либо на основе использовании простых совершенных разностных множеств (СРМ) [1-4], либо на основе укорочения (усечения) сверточных кодов. Принципиальное отличие принципа построения ЛБСОК с пороговым алгоритмом декодирования на основе простого СРМ от самоортогональных сверточных кодов (ССК) с пороговым алгоритмом декодирования состоит в том, что свойства цикличности необходимое для линейных блоковых СОК, требует, чтобы число "ε", определяющее модуль $\varepsilon^2 + \varepsilon + 1$ простого СРМ, было степенью числа 2. В связи с этим длина кодовой последовательности ЛБСОК определяется выражением [1-3]:

$$n = 2^{2s} + 2^{s} + 1, \text{ дв. симв.} \quad (1)$$

где s – целое положительное число.

Для ССК длина кодового ограничения n_a определяется максимальным числом простого СРМ и числом $n_0 = k_0 + 1$, носящего название мини-блока кодовых символов, $k_0 \geq 1$ – мини-блок информационных символов. Однако для скорости передачи кода $R = k_0 / n_0 = 1/2$ ЛБСОК и ССК могут быть построены на основе одного и того же простого СРМ. В соответствии [1-4] количество информационных символов "k" ЛБСОК со скоростью передачи кода R = 1/2 должно удовлетворять следующему неравенству:

$$k \geq m + 1, \text{ дв. симв.} \quad (2)$$

где m (m ≥ 2) – максимальная ступень порождающего полинома.

Длина кодовой последовательности "n" определяется равенством:

$$n = 2 * k, \text{ дв. симв.} \quad (3)$$

Кратность корректируемых ошибок определяется следующим неравенством:

$$t_{\text{корр}} \leq d_0 - 1/2 = (J + 1) - 1/2 \geq J/2, \quad (4)$$

где J – число ортогональных проверок кода, равное числу ненулевых членов порождающего полинома $P(x) = x^m + x^{x-1} +, \ldots, + x^{m-j} +, \ldots, +1, i \neq j$.

Эффективным способом повышения корректирующей способности известных кодов является использование метода перемежения информационных символов, участвующих в формировании J ортогональных проверок. Данный метод позволяет построить составные групповые коды. Важнейшим параметром метода построения линейных блоковых самоортогональных кодов являются коэффициент перемежения α ≥ 2. На практике наибольшее применение получили два способа перемежения информационных символов: простой и обобщенных [1-4].

При простом способе перемежения информационных символов все показатели степеней порождающего полинома P(x) умножаются на коэффициент перемежения α, а порождающей G(x) и проверочной H(x) матрицах между строками и столбцами соответственно вставляются (α – 1) нулевых строк и столбцов. При обобщенном способе перемежения информационных символов не все показатели степеней порождающего полинома умножаются на α, а в порождающей G(x) и проверочной G(x) матрицах нулевые (α – 1) строк и столбцов соответственно вставляются только между строками и столбцами соответствующие показателям степеней, которые умножаются на α.

Принципиальное отличие принципа построения канального кодека на основе составного ЛБСОК с пороговым алгоритмом декодирования от канального кодека на основе ССК с алгоритмом порогового декодирования состоит в принципе построения только формирователя проверочных символов кодера и декодера ($ФПС_{к(д)}$). $ФПС_{к(д)}$ ССК выполняются в виде последовательного регистра сдвига с m (m – максимальная степень порождающего полинома) ячейками памяти с нумарацией ячеек памяти либо

слева направо и с вынесенными сумматорами по модулю два (схема Возенкрафта и Рейффена), либо с нумерацией ячеек памяти справа налево и со встроенными сумматорами по модулю два (схема Месси). $ФПС_{к(д)}$ составного ЛБСОК выполняются в виде последовательного регистра сдвига с обратной связью, содержащего (2m + 1) ячеек памяти с нумерацией их слева направо, с вынесенными сумматорами по модулю два с выходом проверочных символов с первичного сумматора по модулю два, а также наличием соответствующего количества ключей управления [1-4].

Достоинством предложенного метода построения составных ЛБСОК с пороговым алгоритмом декодирования является возможность корреляции зависимых (пакетных) ошибок в α (α ≥ 2) раз больше корректирующей способности исходного (базового) ЛБСОК. Общими недостатками исходных (базовых) и составных ЛБСОК, реализующих пороговый алгоритм декодирования, являются: задержка информации $l_1 = 2m + 1$ тактов при кодировании и $l_2 = 2(2m + 1)$ тактов при декодировании и высокая избыточность (r = 50%) передаваемой информации.

Увеличить скорость передачи составного ЛБСОК возможно на основе использования перфорации (выкалывания) определенных проверочных символов кодовой последовательности. К недостатку перфорированных помехоустойчивых кодов относится снижение энергетического выигрыша за счет кодирования (ЭВК). Снижение ЭВК может достигать до 0,5 дБ при переходе от скорости кода R = 1/2 к $R_{перф.}$ = 7/8 при жестком принятии решения на выходе канала связи.

Список использованных источников:

1. Питерсон, У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлтон. – М.: Мир, 1976. – 594 с.

2. Конопелько, В.К. Теория прикладного кодирования в 2-х Т / В.К. Конопелько [и др.]; под ред. Проф. В.К. Конопелько. – М.: БГУИР, 2004.

3. Королев, А.И. Помехоустойчивое кодирование информации / А.И. Королев, Аль-алем Ахмед Саид, В.К. КОнопелько. – Минск: Бестпринт, 2013. – 277 с.

4. Касами, Т. и др. Теория кодирования – М.: Мир, 1978 – 640 с.

ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ СКАНЕРА УЯЗВИМОСТЕЙ

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

Михейчик А.Д.

Хацкевич О.А. – к.т.н., доцент

В работе рассматриваются сертифицированные сканеры уязвимостей в Республике Беларусь, с помощью которых можно осуществить повышение информационной безопасности в корпоративных сетях . Показываются основные сходства и различия между представленными сканерами, а также практическое применение одного из них.

В мае 2017 года произошла одна из самых серьезных хакерских атак, которая заразила 500 тысяч компьютеров под управлением операционной системой Microsoft Windows в 150 странах мира. Речь идет о программе-вымогателе WannaCry. Данная программа осуществляет сканирование в Интернете для нахождения открытого 445 порта (протокол SMBv1, служащий для удаленного доступа к сетевым ресурсам). После нахождения открытого 445 порта на компьютере, программа эксплуатирует на нем уязвимость EternalBlue, и в случае успеха устанавливает бэкдор DoublePulsar, благодаря которому загружается и запускается код WannaCry [1].

Для того чтобы обезопасить себя от таких программ-вымогателей, специалисты по информационной безопасности рекомендуют использовать лицензионное антивирусное программное обеспечение, автоматическое обновление операционной системы Windows, а также проверенные программные средства для предотвращения атак. В данной работе предложено использовать сканеры уязвимостей в качестве проверенных программных средств.

Сканеры уязвимостей предназначены для мониторинга сети, приложений и отдельных компьютеров на предмет нахождения проблем сетевой безопасности, а также для оценки и устранения найденных неполадок.

В Республике Беларусь существует два сертифицированных Оперативно-Аналитическим Центром сканера уязвимостей – Max Patrol 8 и PCS-1. Представленные сканеры имеют общие черты, такие как генерация отчетов в процессе завершения сканирования, список рекомендаций по их устранению, нахождения открытых портов, идентификация операционной системы, показатель критичности найденных уязвимостей. Также данные сканеры имеют и различия.

Главными особенностями Max Patrol 8 являются: удаленное сканирование, используя встроенные механизмы удаленного администрирования; возможность автоматического мониторинга сети; проверка web-приложений на нахождения уязвимостей; база данных обновляется высококвалифицированными специалистами из Positive Technologies [2].

Другой сканер, PCS-1, имеет следующие преимущества: проверка web-браузеров, установленных на компьютерах; организация защиты данных, передаваемых в пределах сети и от пользователя, от раскрытия и модификации; показывает не возможную уязвимость, а конкретную; обновляется ежедневно. В качестве серьезного недостатка можно выделить то, что при выполнении сканирования в корпоративной сети на нахождения уязвимостей, может замедлить работу фирмы, в которой осуществляется сканирование.

В качестве примера практического применения использовался сканер PCS-1. Сканируемая сеть представлена на рисунке 1.

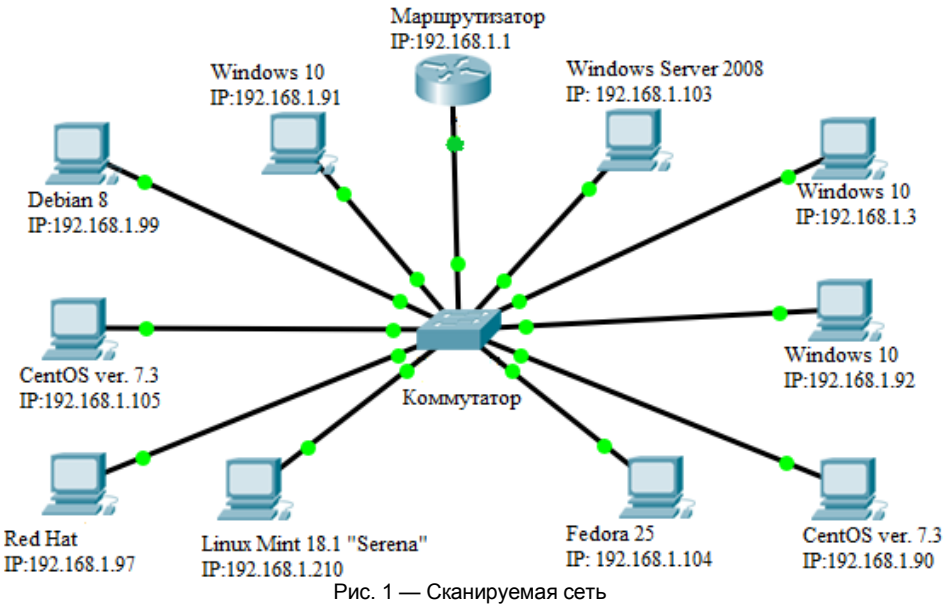


Рис. 1 — Сканируемая сеть

Сканируемая сеть, представленная на рисунке 1, представляет собой десять хостов, которые находятся в одной сети и имеют различную операционную систему. CentOS, Fedora, Linux Mint, Debian, Red Hat относятся к UNIX-подобным операционным системам. Все компьютеры подключены к коммутатору, который подключен к маршрутизатору, с помощью которого осуществляется доступ в Интернет.

При сканировании указывается либо конкретный IP-адрес, либо диапазон адресов. В данном случае указывался диапазон: 192.168.1.1 — 254.

При завершении сканирования генерируются отчеты, где указываются уязвимости, рекомендации по устранению уязвимостей, критичность уязвимости. На рисунке 2 представлена краткая общая информация: количество найденных уязвимостей, критичность уязвимостей (высокая, средняя, низкая).

Host	High	Medium	Low	Log	False Positive
192.168.1.1	2	1	0	16	0
192.168.1.103	2	10	1	31	0
192.168.1.3	0	2	1	8	0
192.168.1.91	0	2	1	8	0
192.168.1.92	0	2	0	20	0
192.168.1.210	0	1	2	18	0
192.168.1.99	0	1	0	24	0
192.168.1.105	0	0	1	6	0
192.168.1.97	0	0	1	11	0
192.168.1.104	0	0	0	4	0
192.168.1.90	0	0	0	4	0
Total: 11	4	19	7	150	0

Рис. 2 — Краткая статистика

Проанализировав рисунок 2, можно убедиться, что в сети существует 4 критических уязвимостей, 19 средних и 7 низких. С помощью сканера можно не только обнаружить, где и какие уязвимости расположены, но и, используя рекомендации, устранить их. Пример рекомендации по устранению найденной уязвимости представлен на рисунке 3.

References

CVE: CVE-2009-2526, CVE-2009-2532, CVE-2009-3103
BID: 36299
CERT: DFN-CERT-2009-1443
Other: http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx

Рис.3 – Пример рекомендации по устранению найденной уязвимости

Таким образом, в данной работе показана эффективность применения сканеров уязвимостей для повышения информационной безопасности в корпоративных сетях на примере сертифицированного в Республике Беларусь сканера PCS-1.

Список использованных источников:
4. WannaCry [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/WannaCry.
5. Max Patrol 8 [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/products/mp8/.

МЕТОДИКА ОПРЕДЕЛЕНИЯ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК ВЕКТОРНЫХ АНАЛИЗАТОРОВ ЦЕПЕЙ МИКРОВОЛНОВОГО ДИАПАЗОНА

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

Теслин П.А., Кузюков А.Н.

Белошицкий А.П. – к.т.н.,доцент

Достижения в области теории и техники микроволнового диапазона открывают принципиально новые возможности создания и развития систем скоростной передачи информации, систем радиолокации и радионавигации, радиоразведки и радиопротиводействия, систем связи и телевидения. Для определения параметров и характеристик этих систем и их компонентов наиболее часто используются векторные анализаторы цепей (ВАЦ) [1,2]. Для практического применения этих анализаторов необходимо определение их метрологических характеристик (МХ) по специально разработанным методикам.

В докладе рассматривается методика калибровки ВАЦ Р4-МВМ-118. Анализатор предназначен для автоматизированного исследования волноводных устройств микроволнового диапазона и автоматизированного измерения комплексных коэффициентов передачи и отражения (|S11(22)| и |S21(12)|) волноводных устройств с цифровым отсчетом измеряемых величин и воспроизведением их частотных характеристик в декартовой системе координат на экране анализатора.

Рабочий диапазон частот анализатора от 78,33 до 118,1 ГГц. Пределы допускаемой относительной погрешности установки частоты не более ± 0,2 % от установленной частоты. Диапазон измерения модулей коэффициентов отражения от 0 до минус 26 дБ. Диапазон индикации КСВН от 1,1 до 5. Пределы допускаемой погрешности при измерении модуля коэффициента отражения не более |S11(22)| ± (0,50 + 0,07|S11(22)|) дБ. Диапазон измерения модуля коэффициента передачи от 0 до минус 50 дБ. Пределы допускаемой погрешности при измерении модуля коэффициента передачи |S21(12)| не более ± (0,30 + 0,05|S21(12)|) дБ. Диапазон измерения фазы коэффициента отражения и фазы коэффициента передачи от минус 180 до плюс 180 градусов. Пределы допускаемой погрешности при измерении фазы коэффициента отражения не более ± 8 градусов. Пределы допускаемой погрешности при измерении фазы коэффициента передачи не более ± 7 градусов.

При калибровке анализатора определяются следующие метрологические характеристики:

– действительное значение и неопределенность измерения модуля и аргумента коэффициентов отражения (КО);

– действительное значение и неопределенность измерения модуля и аргумента коэффициентов передачи (КП);

– действительное значение и неопределенность установки и отсчета частоты, на которых определяются КО и КП.

Для калибровки ВАЦ выбраны следующие эталонные средства: частотомер электронно-счетный РЧ3-72; набор мер КСВН 1,4 и 2,0; аттенюатор поляризационный АП-20; комплект мер фазового сдвига КМФС-3.

Для оценки неопределенностей измерений калибруемых параметров были использованы следующие модели измерения.

Модель измерения при оценке неопределенности установки и отсчета частоты сигнала на выходе генератора анализатора

$$\Delta_f = f_г - f_э - \Delta_э + \Delta_д, \text{ Гц}, \quad (1)$$

где $f_г$ – показание калибруемого анализатора, Гц;
$f_э$ – показание эталонного частотомера, Гц;
$\Delta_э$ – поправка на неточность эталонного частотомера, Гц;
$\Delta_д$ – поправка на дискретность установки частоты калибруемого анализатора, Гц.

– Модель измерения отклонения результатов измерений КСВН

$$\Delta_{K_{CTU}} = K_{CTU_и} - K_{CTU_{эт}} + \Delta_{кв} + \Delta_{рас}, \quad (2)$$

где $\Delta_{K_{CTU}}$ – оцениваемое отклонение измерения КСВН;
$K_{CTU_и}$ – показание калибруемого анализатора;
$K_{CTU_{эт}}$ – значение КСВН эталонной нагрузки;
$\Delta_{кв}$ – поправка из-за конечного разрешения калибруемого анализатора;
$\Delta_{рас}$ – поправка, обусловленная рассогласованием в измерительном тракте.

– Модель измерения отклонения результатов измерений ослабления

$$\Delta_A = A_и - A_{эт} + \Delta_{кв} + \Delta_{рас}, \text{ дБ}, \quad (3)$$

где Δ_A – оцениваемое отклонение измерения ослабления, дБ;
$A_и$ – показание калибруемого анализатора, дБ;
$A_{эт}$ – значение ослабления эталонного аттенюатора, дБ;
$\Delta_{кв}$ – поправка из-за конечного разрешения калибруемого анализатора, дБ;
$\Delta_{рас}$ – поправка, обусловленная рассогласованием в измерительном тракте, дБ.

– Модель измерения отклонения результатов измерений фазы коэффициентов передачи

$$\Delta_{\varphi_{КП}} = \varphi_{КПи} - \varphi_{КПэт} + \Delta_{кв} + \Delta_{рас}, \text{ град.}, \quad (4)$$

где $\Delta_{\varphi_{кп}}$ – оцениваемое отклонение измерения фазы КП, град.;
$\varphi_{КПи}$ – показание калибруемого анализатора, град.;
$\varphi_{КПэт}$ – значение фазы аттенюатора, град.;
$\Delta_{кв}$ – поправка из-за конечного разрешения калибруемого анализатора, град.;
$\Delta_{рас}$ – поправка, обусловленная рассогласованием в измерительном тракте, град.

– Модель измерения отклонения результатов измерений фазы коэффициентов отражения

$$\Delta_{\varphi_{КО}} = \varphi_{КОи} - \varphi_{КОэт} + \Delta_{кв} + \Delta_{рас}, \text{ град.}, \quad (5)$$

где $\Delta_{\varphi_{КО}}$ – оцениваемая погрешность измерения фазы КО, град.;
$\varphi_{КОи}$ – показание калибруемого анализатора, град.;
$\varphi_{КОэт}$ – значение фазы эталонной нагрузки, град.;
$\Delta_{кв}$ – поправка из-за конечного разрешения калибруемого анализатора, град.;
$\Delta_{рас}$ – поправка, обусловленная рассогласованием в измерительном тракте, град.

Полный результат измерения состоит из оценки измеряемой величины y, и соответствующей ей расширенной неопределенности U и представляется в виде: y±U (в единицах измерения), где число, следующее за знаком ±, является численным значением расширенной неопределенности.

Рассмотренная методика определения МХ может быть использована при разработке методики калибровки ВАЦ предназначенных для работы в других участках микроволнового диапазона, а представленные математические модели для оценки неопределенности измерения калибруемых параметров.

Список использованных источников:

1. Белошицкий, А. П. Измерения в оптическом и микроволновом диапазонах длин волн. В 2 ч. Ч.1. Учебно-методическое пособие. / А. П. Белошицкий, А. В. Гусинский, А. М. Кострикин. – Минск : БГУИР, 2016.
2. Гусинский, А. В. Векторные анализаторы цепей миллиметровых волн: монография В 3 ч. Ч. 3 (кн. 1) : Принципы построения и анализ схем векторных анализаторов цепей / А. В. Гусинский, Г. А. Шаров, А. М. Кострикин. – Минск : БГУИР, 2008.

МЕТОДИКА ОПРЕДЕЛЕНИЯ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК СКАЛЯРНЫХ АНАЛИЗАТОРОВ ЦЕПЕЙ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ДЛИН ВОЛН

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

Кузюков А.Н, Теслин П.А.

Белошицкий А.П. – к.т.н.,доцент

К числу наиболее эффективных измерительных средств, предназначенных для анализа параметров СВЧ и КВЧ устройств (цепей), относятся скалярные анализаторы цепей [1,2]. Современные САЦ являются высокопроизводительными информационно-измерительными системами, позволяющие провести необходимые измерения параметров устройств с гарантированной точностью в широких диапазонах с представлением и хранением измеренной информации о параметрах и характеристиках испытуемых устройств.

Поддержание высоких метрологических характеристик скалярных анализаторов цепей КВЧ диапазона невозможно без их метрологического обеспечения, а также выполнения таких видов метрологических работ, как метрологическая аттестация, периодическая поверка и калибровка.

Для их проведения требуются специально разработанные методики, учитывающие специфику проведения КВЧ измерений, конструктивные и эксплуатационные характеристики анализаторов и требования нормативных документов в этой области.

В докладе рассматривается методика метрологической аттестации скалярного анализатора цепей Р2-МВМ-53. Анализатор предназначен для автоматизированного исследования волноводных КВЧ устройств, работающих в частотном диапазоне от 37,50 до 53,57 ГГц и измерения их параметров – модулей коэффициентов передачи $|S_{21}|$ и отражения $|S_{11}|$, 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. Упрощенная структурная схема анализатора представлена на рисунке 1.

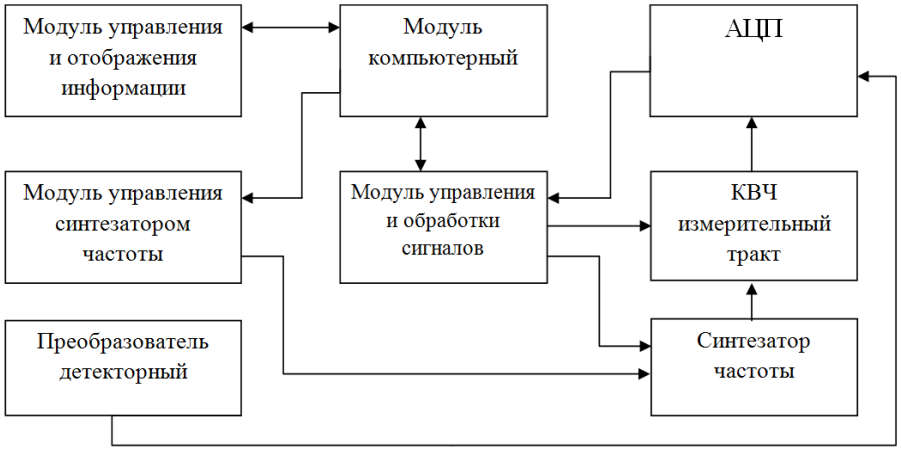


Рисунок 1 – Структурная схема скалярного анализатора цепей

Скалярный анализатор цепей имеет следующие метрологические и технические характеристики: рабочий диапазон частот: 37,50 – 53,57 ГГц; пределы допускаемой относительной погрешности установки и отсчета частоты $\pm 5 \cdot 10^{-5}$ % от f_{max}; нестабильность частоты выходного сигнала генератора за 15 минут не более $1 \cdot 10^{-6}$ от f_{max}; диапазон измерения модулей коэффициентов отражения от 0 до минус 26 дБ; диапазон измерения КСВН от 1,1 до 5; пределы допускаемой основной погрешности измерения модуля коэффициента отражения $|S_{11}|$ не более $\pm(0{,}3 + 0{,}06\ |S_{11}|)$ дБ; диапазон измерения модуля коэффициента передачи от 0 до минус 40 дБ; пределы допускаемой основной погрешности измерения модуля коэффициента передачи $|S_{21}|$ не более $\pm(0{,}2 + 0{,}04\ |S_{21}|)$ дБ.

Для проведения метрологической аттестации были выбраны следующие эталонные средства: частотомер электронно-счетный РЧ3-72, аттенюатор поляризационный волноводный Д3-37.

Определение диапазона рабочих частот, погрешности установки и нестабильности частоты выходного сигнала анализатора производится на частотах: 37,50; 41,00; 45,50; 50,00; 53,57 ГГц.

Определение диапазона измерения и основной погрешности измерения модуля коэффициента отражения $|S_{11}|$ производится для значений: 0,0 дБ ($K_{СТИ} > 100$); минус 9,55 дБ ($K_{СТИ} = 2{,}0$); минус 15,56 дБ ($K_{СТИ} = 1{,}4$);

Определение диапазона измерения и основной погрешности измерения модуля коэффициента передачи $|S_{21}|$ производится для значений: 0,0 дБ; минус 10,0 дБ; минус 20,0 дБ; минус 30,0 дБ; минус 40,0 дБ

Обработка результатов измерений проводится в следующей последовательности.

При определении относительной погрешности установки и отсчета частоты анализатора вычисляют:

- оценку среднеквадратического отклонения относительной случайной составляющей погрешности измерения частоты в *j*-й точке частотного диапазона и среднее значение измеренной частоты:

$$\bar{f}_j = \frac{\sum_{i=1}^{10} f_{ij}}{10}; \qquad \tilde{\sigma}(\delta_{fj}) = \frac{1}{\bar{f}_j}\sqrt{\frac{\sum_{i=1}^{10}(f_{ij} - \bar{f}_j)^2}{9}} \cdot 100$$

- оценку относительной систематической составляющей погрешности установки и отсчета частоты в *j*-й точке частотного диапазона:

$$\tilde{\delta}_{Sfj} = \frac{\sum_{i=1}^{10}(f_j - f_{ij})}{10 \cdot f_j} \cdot 100\,\%$$

При определении относительного значения нестабильности частоты в *j*-й точке вычисляют:

- нестабильность частоты за 15 минут:

$$\Delta_{нfj} = f_{\max\ j} - f_{\min\ j}$$

- относительное значение нестабильности частоты:

$$\tilde{\delta}_{нfj} = \frac{\Delta_{нfj}}{f_j}$$

При определении погрешности измерения $|S_{11}|$ вычисляют:

- оценку среднеквадратического отклонения случайной составляющей погрешности измерения модуля коэффициента отражения для *j*-й точки частотного диапазона:

$$\left|\bar{S}_{11}\right|_j = \frac{\sum_{i=1}^{10}\left|\bar{S}_{11}\right|_{ij}}{10}, \qquad \tilde{\sigma}(|S_{11}|_j) = \sqrt{\frac{\sum_{i=1}^{10}(|S_{11}|_{ij} - \left|\bar{S}_{11}\right|_j)^2}{9}}$$

- оценку систематической составляющей погрешности измерения модуля коэффициента отражения:

$$\tilde{\Delta}_{11j} = \left|\bar{S}_{11}\right|_j - |S_{11}|_{Эj}$$

При определении погрешности измерения $|S_{21}|$ вычисляют:

- оценку среднеквадратического отклонения случайной составляющей погрешности измерения модуля коэффициента передачи:

$$\left|\bar{S}_{21}\right|_j = \frac{\sum_{i=1}^{10}\left|\bar{S}_{21}\right|_{ij}}{10}, \qquad \tilde{\sigma}(|S_{21}|_j) = \sqrt{\frac{\sum_{i=1}^{10}(|S_{21}|_{ij} - \left|\bar{S}_{21}\right|_j)^2}{9}}$$

- оценку систематической составляющей погрешности измерения модуля коэффициента передачи определяют:

$$\tilde{\Delta}_{21j} = \left|\bar{S}_{21}\right|_j - |S_{21}|_{Эj},$$

Рассмотренная методика метрологической аттестации может быть использована при метрологической аттестации САЦ различных диапазонов частот.

Список использованных источников:

1. Белошицкий, А. П. Измерения в оптическом и микроволновом диапазонах длин волн. В 2 ч. Ч.1. Учебно-методическое пособие. / А. П. Белошицкий, А. В. Гусинский, А. М. Кострикин. – Минск : БГУИР, 2016.

2. Гусинский, А. В. Векторные анализаторы цепей миллиметровых волн: монография В 3 ч. Ч. 3 (кн. 1) : Принципы построения и анализ схем векторных анализаторов цепей / А. В. Гусинский, Г. А. Шаров, А. М. Кострикин. – Минск : БГУИР, 2008.

МЕТОДИКА ОПРЕДЕЛЕНИЯ МЕТРОЛОГИЧЕСКИХ ХАРАКТЕРИСТИК ИЗМЕРИТЕЛЯ ПОГЛОЩАЕМОЙ МОЩНОСТИ МИКРОВОЛНОВОГО ДИАПАЗОНА

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

Кейзеров Е.И.

БелошицкийА.П. – к.т.н.,доцент

Среди большого разнообразия видов радиоизмерений микроволнового диапазона одно из ведущих мест занимает измерение мощности. Измерители мощности микроволнового диапазона входят в число основных приборов, используемых на всех этапах разработки, регулировки и выпуска в сферу обращения генераторов и усилителей, для определения потерь в четырехполюсниках, коэффициента отражения, частотных характеристик различных радиоустройств [1, 2].

В докладе рассматривается методика калибровки измерителя поглощаемой мощности *Agilent E*4418*B*.

Измеритель поглощаемой мощности предназначен для измерения мощности синусоидальных сигналов микроволнового диапазона в коаксиальном тракте.

Принцип действия измерителя поглощаемой мощности основан на преобразовании КВЧ энергии в постоянный ток на амплитудном детекторе. Структурная схема измерителя поглощаемой мощности представлена на рисунке 1.

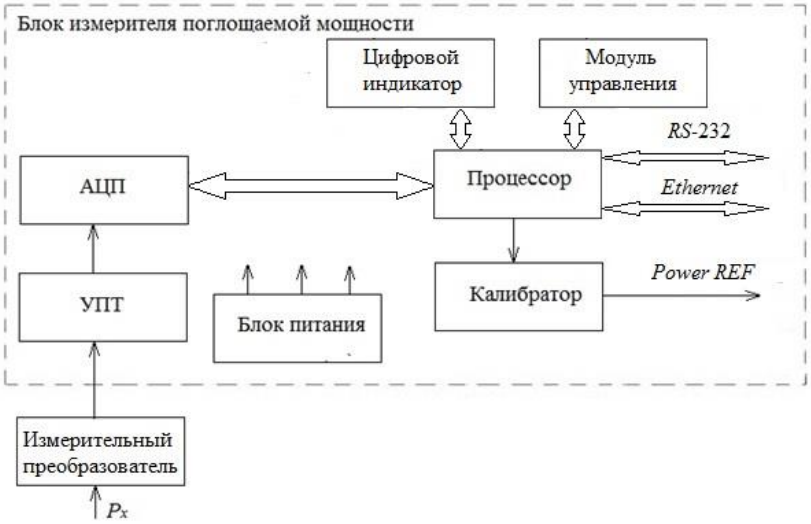


Рисунок 1 – Структурная схема измерителя поглощаемой мощности

Рабочий диапазон частот измерителя поглощаемой мощности от 37,5 ГГц до 53,6 ГГц. Пределы измерения мощности от 1 мкВт до 25 Вт (от минус 30 дБм до 44 дБм). Предел допускаемой погрешности измерения мощности ±4 %. Коэффициент эффективности не менее 0,9. КСВН входа преобразователя не более 1,2. Пределы допускаемой погрешности установки нуля ±0,05 мкВт. Выходная мощность встроенного калибратора 1,00 мВт. Частота встроенного калибратора 50МГц. Пределы допускаемой погрешности выходной мощности встроенного калибратора ±1,9 %.Волновое сопротивление 50 Ом. Нестабильность показаний измерителя мощности в установившемся режиме, включая «дрейф нуля», при неизменной температуре окружающего воздуха (в пределах ± 1°С) в нормальных условиях не превышает 0,2 мВт/мин.

Разрешающая способность:

– в логарифмическом режиме 1,0дБ; 0,1дБ; 0,01дБ; 0,001дБ;

– в линейном режиме, число разрядов от 1 до 4.

При калибровке измерителя определяются следующие метрологические характеристики:

– коэффициент отражения входа преобразователя;

– коэффициент калибровки измерителя поглощаемой мощности.

Для калибровки измерителя поглощаемой мощности выбраны следующие эталонные средства: векторный анализатор цепей *Keysight N*5234*A*; генератор ВЧ-сигналов *Agilent E*8257*D*; преобразователь проходящей мощности *Tegam F*1109*H*; мост измерительный двухканальный *Tegam* 1806*A*; мультиметр *Agilent* 3458*A*.

Для оценки неопределенностей измерений калибруемых параметров были использованы следующие модели измерения.

Модель измерения при оценке неопределенности коэффициента отражения входа преобразователя

$$\Gamma_{преоб.} = \Gamma_{ВАЦ} + \Delta_{и} + \Delta_{кв}, \quad (1)$$

где $\Gamma_{ВАЦ}$ – показание векторного анализатора цепей;
$\Delta_{и}$ – поправка из-за неточного измерения $\Gamma_{ВАЦ}$;
$\Delta_{кв}$ – поправка из-за конечного разрешения ВАЦ.

Модель измерения при оценке неопределенности коэффициента калибровки измерителя мощности

$$K_K = \frac{P_{E4418B} \cdot M_p \cdot R_m}{K_{кэ} \cdot (U_1^2 - U_2^2)}, \quad (2)$$

где $K_{кэ}$ – коэффициент калибровки эталонного преобразователя проходящей мощности *Tegam F*1109*H*;
M_p – коэффициент рассогласования;
P_{E4418B} – показание калибруемого измерителя мощности *Agilent E*4418*B*, мВт;
$R_т$ – сопротивление термистора эталонного преобразователя проходящей мощности *Tegam F1109H*;
U_1 – постоянное напряжение, измеряемое мультиметром *Agilent* 3458*A*, при отсутствии мощности, В;
U_2 – постоянное напряжение, измеряемое мультиметром *Agilent* 3458*A*, при поданной мощности, В;

Полный результат измерения состоит из оценки измеряемой величины y, и соответствующей ей расширенной неопределенности U и представляется в виде: y±U (в единицах измерения), где число, следующее за знаком ±, является численным значением расширенной неопределенности.

Рассмотренная методика определения метрологических характеристик может быть использована при разработке методики калибровки измерителей поглощаемой мощности предназначенных для работы в других участках микроволнового диапазона, а представленные математические модели для оценки неопределенности измерения калибруемых параметров.

Список использованных источников:

3. Белошицкий, А. П. Измерения в оптическом и микроволновом диапазонах длин волн. В 2 ч. Ч.1. Учебно-методическое пособие. / А. П. Белошицкий, А. В. Гусинский, А. М. Кострикин. – Минск : БГУИР, 2016.
4. Доницков, О.В. Ваттметр поглощаемой мощности СВЧ диапазона. / О.В.Доницков, А.В. Гусинский, А.Н. Луферов, А.В. Ворошень, В. К. Демидович // Материалы Международной НТК, приуроч. К 50-летию МРТИ - БГУИР в 2-х ч. Ч. 1 - Минск, 2014.– 163 с.