РАЗРАБОТКА СИСТЕМЫ ДОПУСКОВОГО КОНТРОЛЯ С СЕНСОРНОЙ КЛАВИАТУРОЙ

Арюшкин М.Б. – студент, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В настоящее время весьма часто выходит на первый план проблема обеспечения санкционированного доступа в помещения, имеющие ограничения на круг посещаемых их лиц. Контроль и управление доступом в эти помещения позволяют предотвратить хищение размещенных в них важной информации или оборудования, а также предотвратить или разоблачить промышленный шпионаж и другие незаконные действия персонала.

С данной проблемой прекрасно справляются современные системы допускового контроля (СДК). В общем случае под системой допускового контроля обычно понимают совокупность программно-технических и организационно-методических средств, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также оперативный контроль перемещения персонала и времени его нахождения на территории объекта. Вообще, СДК – это не только аппаратура и программное обеспечение, это продуманная система управления движением персонала.

Несмотря на широкий ассортимент СДК, представленный в настоящий момент на рынке, нельзя не отметить, что эти решения не всегда позволяют достигнуть требуемого уровня безопасности помещения и обеспечить необходимую функциональность, либо их стоимость слишком высока, и поэтому их приобретение и установка не всегда рентабельны. В частности, на сегодня на рынке готовых решений отсутствуют простые, надежные и экономичные предложения, позволяющие без применения аппаратных идентификационных ключей обеспечить временный доступ определенного круга лиц в контролируемые помещения.

После анализа существующих систем было принято решение разработать систему контроля и управления доступом (СКУД), удовлетворяющую перечисленным требованиям, и обеспечивающим:

1. использование сенсорной клавиатуры для идентификации временных посетителей;
2. использование сенсорной клавиатуры и ключей «Touch-Memory» для идентификации постоянных посетителей;
3. хранение информации о существующих ключах и паролях и сроках их действия и редактирования этой информации;
4. сохранение полной функциональности системы в случае отключения электричества (установка бесперебойного блока питания);
5. использование электромеханического замка в качестве запорного устройства для обеспечения защиты контролируемых объектов на время долговременного отсутствия электроэнергии и увеличения времени автономной работы;
6. использование звуковой и световой индикации для уведомления о вводимой информации.

Использование сенсорной клавиатуры связано с тем, что она более надёжна по сравнению с кнопочной. Отсутствие механических элементов и полное отсутствие механического контакта пользователя с клавишами позволяет заметно снизить её износ. Кроме того, ёмкостные элементы защищены пластиковым корпусом толщиной 5 мм. Это позволяет обеспечить дополнительную защиту от климатических факторов и заметно увеличить вандалоустойчивость системы. Клавиатура выполнена на основе автономного цифрового контроллера QT1101.

Система управляется с помощью микроконтроллера AtMega8A-PU. Через последовательный однопроводный интерфейс осуществляется передача данных с клавиатуры на процессор в виде служебных ASCII-символов и двоичной информации. После обработки полученной информации происходит вывод введенных цифр на панель индикатора. После этого выдается звуковой сигнал, оповещающий о результате верификации

введенных данных и, в случае введения верной информации, подается кратковременный сигнал на открытие засова замка.

Выбор в пользу электромеханического замка обусловлен меньшим (по сравнению с электромагнитным замком – в несколько раз) средним значением энергопотребления, что позволяет увеличить продолжительность нормального функционирования СКУД от бесперебойного блока питания в случаях нарушения энергоснабжения. Кроме того, в случае отключения электропитания система прекращает функционировать и при использовании электромагнитного замка дверь окажется открытой. В данной разработке в качестве такого замка был выбран электромеханический замок FASS LOCK 2369-SS как наиболее оптимальный по критерию цена/качество. Контроллер системы управления сенсорной клавиатуры в данной разработке интегрирован с контролером считывателя «Touch-Memory» Z-5R, способным хранить информацию о 1364 ключах. Наличие мастер ключа позволяет легко добавить либо убрать из его памяти информацию о существующих ключах постоянных пользователей.

Разработанная СКУД позволяет обеспечить необходимую защиту от несанкционированного доступа. Кроме того, отсутствие избыточной функциональности позволяет существенно снизить затраты на производство и конечную стоимость продукта, что может обеспечить ему хорошую конкурентоспособность. Данная разработка предназначалась для установки в служебных помещениях кафедры ВСИБ АлтГТУ и ее компьютерных аудиторий, но может быть успешно применена для решения других аналогичных задач при числе временных пользователей, не превышающем 20 человек.

Список использованных источников:

1. Фрайден, Дж. Современные датчики. Справочник [текст] / под редакцией Е.Л. Свинцова. –М.:ТЕХНОСФЕРА, 2005. -592 с.: ил.

2. Дюбери, Дж. QT1101-ISG: Datasheet [Электронный ресурс] / John Dubery, Alan Bowens, Matthew Trend. Режим доступа: http://datasheet.octopart.com/QT1101-ISG-Quantum-Research-Group-datasheet-133458.pdf

3. Ворона В.А. Системы контроля и управления доступом [Текст] / Ворона В.А., Тихонов В.А. – М.: Горячая линия-Телеком, 2010. -272 с.: ил.

РАЗРАБОТКА ДИДАКТИЧЕСКИХ МАТЕРИАЛОВ ПО ВЫПОЛНЕНИЮ РАСЧЕТНОГО ЗАДАНИЯ ПО ДИСЦИПЛИНЕ «СЕТИ И СИСТЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ» ДЛЯ НАПРАВЛЕНИЯ ПОДГОТОВКИ БАКАЛАВРОВ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Анохина А.Г. – студент, Борисов А.П. – доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

На сегодняшний день технология беспроводной передачи данных Wi-Fi получила широкое распространение. Свое применение она получила в развертывании сетей крупных предприятий, для домашнего использования в ситуациях, когда прокладка кабеля невозможна или нецелесообразна. Простота настройки и безопасность информационного взаимодействия способствуют расширению внедрения данной технологии во все сферы быта, бизнеса и образования. Изучение современных средств и технологий беспроводной передачи данных является одной из задач дисциплины «Сети и системы передачи информации».

В настоящий момент актуальной является задача разработки методических указаний для выполнения расчетного задания по дисциплине «Сети и системы передачи информации» для направления подготовки бакалавров «Информационная безопасность». Необходимость разработки расчетного задания обусловлена отсутствием аналогичных материалов по дисциплине и несоответствием существующих расчетных заданий из аналогичных

дисциплин стандартам дисциплины и специальности. Разработка данного дидактического модуля позволит студентам изучить вопрос пространственного размещения точек доступа Wi-Fi применительно к антеннам с различными диаграммами направленности, сравнить различные характеристики точек доступа и их влияние на качество передачи данных, параметры безопасности и схему расположения точек для оптимального взаимодействия. Так же в расчетное задание будет включен расчет зон Френеля, дальности прямой видимости антенн и вероятности ошибки в цифровых каналах связи и настройка сетевого взаимодействия между двумя сетями.

Для решения поставленной задачи в качестве аппаратной платформы выбраны компьютеры с Wi-Fi адаптером и точки доступа Wi-Fi модели D-Link DIR-620. В качестве программного обеспечения выбраны программные продукты TamoGraph Site Survey и VisSim.

Расчетное задание включает в себя три задания:

1) Расчет зон Френеля, дальности прямой видимости антенны и вероятности ошибки в цифровых каналах связи.

Распространение любого сигнала неизбежно сопровождается его затуханием. Учитывая, что необходимым условием для работы радиоканала является прямая видимость между антеннами, важно понимать как зависит высота, на которой установлены антенны и предельная дальность прямой видимости между ними. Но для нормального функционирования радиолинка недостаточно наличия только прямой видимости в связи с тем, что основная электромагнитная энергия сосредоточена в некотором эллипсоиде вращения около линии визирования, называемом зоной Френеля [1]. Перечисленные факты обуславливают необходимость проведения данных расчетов.

2) Создание виртуальной модели двух сетей на базе двух компьютеров и двух точек доступа в программе TamoGraph.

TamoGraph Site Survey — программа для сбора, визуализации и анализа данных в сетях Wi-Fi стандарта 802.11 a/b/g/n. TamoGraph предназначен для построения карт покрытия, анализа интерференции и уровня сигнала, распределения Wi-Fi-каналов, и т.д. TamoGraph может быть использован для проектирования еще не развернутых сетей Wi-Fi, что особенно важно для выполнения расчетного задания. Для создания виртуальной модели окружения студент должен внести в приложение данные о местоположении, размере и типе физических объектов, влияющих на распространение радиоволн [2].

3) Настройка адресации и параметров безопасности средствами Windows.

В данном разделе студентам будет предложено, используя статическую адресацию, настроить соединение между двумя подсетями, прописать настройки в таблицу маршрутизации и продемонстрировать работу сети командой ping. Настроить параметры шифрования средствами операционной системы и продемонстрировать передачу данных с помощью программы CommView.

4) Моделирование канала передачи в VisSim.

С помощью программного продукта VisSim необходимо смоделировать тракт передачи данных с OFDM – мультиплексированием с ортогональным частотным разделением каналов. Это способствует углубленному пониманию процессов модуляции и демодуляции, передачи данных, появления помех и иных процессов, происходящих при информационном взаимодействии [3].

Выполнение заданий способствует достижению целей расчетного задания:

- систематизирует, закрепляет и расширяет знания по дисциплине в процессе решения конкретных профессиональных задач;
- способствует овладению методами исследования при выполнении заданий научно-исследовательского характера;
- формирует у студентов универсальных и предметных компетенций при решении ситуативных вопросов [4].

Список используемых источников:

1) Беспроводные сети. Полезные формулы [Электронный ресурс]. Режим доступа: http://www.comptek.ru/wireless/info/formula.html - Загл. с экрана.

2) Планирование и обслуживание Wi-Fi сетей [Электронный ресурс]. Режим доступа: http://www.tamos.ru/products/wifi-site-survey/ – Загл. с экрана.

3) VisSim [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/VisSim - Загл. с экрана

4) Образовательный стандарт учебной дисциплины Б.3.Б.7 «Сети и системы передачи информации» 090900 Информационная безопасность

РАЗРАБОТКА СИНХРОННОГО ДЕТЕКТОРА СЛАБЫХ ОПТИЧЕСКИХ СИГНАЛОВ НА БАЗЕ МИКРОКОНТРОЛЛЕРА

Аверин И.Н. – студент, Агапов М.Н. –к.ф-м.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Детектирование света - нелинейное преобразование оптического излучения видимого и ИК- диапазонов частот в электрический сигнал в виде последовательности импульсов или колебаний тока, несущее информацию о параметрах оптического излучения (интенсивности, частоте, фазе). Детектирование света осуществляется с помощью фотоприёмников (фоторезисторов, фотодиодов, фотоумножителей) [1]. Детектирование света применяется в системах оптической связи, оптической локации, оптической обработки информации, а также в спектроскопии, интерферометрии, голографии и т. п. [2]. В устройствах детектирования на фотоприёмник поступают полезный оптической сигнал и фоновое излучение. Для повышения уровня сигнала относительно уровня фона возможно использование синхронного детектора. Разработка синхронного детектора на базе микроконтроллера удобная, современная реализация для детектирования сигналов и имеет ряд преимуществ. В первую очередь следует выделить гибкость конструирования и настройки. Правильный выбор микроконтроллера обеспечивает необходимое количество входных и выходных линий, исключив проблемы с их недостатком и необходимостью установки и настройки дополнительных модулей. Применение микроконтроллеров позволяет отказаться от платных сред разработки программного обеспечения, заменив их на бесплатно-распространяемые среды, предлагаемые фирмами-разработчиками. Также преимуществом таких систем является большая экономичность.

При разработке решались следующие задачи:

- Детектирование сигнала с фотопередатчика при высокой фоновой засветке.
- Возможность использования нескольких оптических каналов
- Световая и звуковая индикация для определения силы сигнала
- Возможность управления исполнительными устройствами

На рисунке 1 изображена структурная схема устройства.

Рисунок 1 – Структурная схема устройства

Микроконтроллер отправляет сигнал с ШИМ на фотопередатчик, и на ключ синхронного детектора как опорный сигнал. Данные приходят на фотоприемник, далее сигнал усиливается на этапе предварительного усиления. Усиленный сигнал поступает на вход синхронного детектора, там он перемножается с опорным сигнал и на выход детектора поступает выделенная полезная составляющая сигнала, в интеграторе ведется накопление сигнала, когда сигнал достигает максимального значения (5В) в контролере сигнал сбрасывается и накопление начинается с начала, по изменению скорости накопления сигнала, можно судить о силе оптического сигнала.

Разработанное устройство спроектировано на базе микроконтроллера ATmega8 фирмы Atmel, оснащенного таймерами, ШИМ, АЦП и ЦАП, которые существенно упрощают разработку устройства и расширяют возможности применения.

Устройство может применяться в качестве оптического датчика в охранных системах, а также в качестве датчика дыма

Список используемых источников:

1. Хоровиц П., Хилл У. Искусство схемотехники. М.: Мир, 1993.

2.Ж. Макс. Методы и техника обработки сигналов при физических измерениях. М.: Мир, 1983.

РАЗРАБОТКА ЛАБОРАТОРНОГО ПРАКТИКУМА «ИЗМЕРИТЕЛЬНАЯ АППАРАТУРА АНАЛИЗА ЗАЩИЩЕННОСТИ ОБЪЕКТОВ И ЭЛЕКТРОРАДИОИЗМЕРЕНИЯ»

Ахнина В.И. - студент, Борисов А.П. - к.т.н., доцент

Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Устройства наблюдения не всегда используются во благо. Сегодня именно подслушивание, скрытое наблюдение и запись телефонных разговоров становится главным оружием не только людей, но и целых стран. Постепенно разрабатываются новые, максимально незаметные модели всевозможных жучков, портативных камер. Изначально подобные устройства применялись только агентами спецслужб и военными, но сегодня их покупателями становятся олигархи, бизнесмены и даже преступники. Возможности таких устройств позволяют добыть ценную информацию.

В настоящий момент рынок средств негласного получения информации настолько широк, что не составляет проблемы приобрести закладное устройство, за сравнительно небольшие деньги. В связи с этим и сфера их применения резко расширилась.

Простейшие закладные устройства включают три основных узла, которые определяют их тактико-технические возможности. Это: микрофон, определяющий зону акустической чувствительности жучка, радиопередатчик, определяющий дальность его действия и скрытность работы, источник электропитания, определяющий время непрерывной работы. Закладные устройства работают как обычный передатчик.

Проверку помещений актуально проводить там, где есть вероятность утечки конфиденциальной информации (переговорные, кабинеты руководства и менеджмента, частные дома, квартиры, автомобили). Обнаружение жучков требует проведения специальных мероприятий.

Поиск жучков осуществляется при помощи следующих методов:

1.Визуальный осмотр помещений. Проверка на жучки и проверка помещений проводятся в местах, представляющих наибольший интерес для «похитителей конфиденциальной информации».

2.Проверка помещений на жучки с использованием поисковых металлодетекторов, нелинейных локаторов, осветительных приборов, оптико-волоконных эндоскопов, специальных досмотровых зеркал и т.д.

3.Проверка помещений и обнаружение закладных устройств, применяя сканирующий приемник, сводятся к тому, что в узкополосном спектре принимаемых сигналов, в заданном частотном диапазоне, производится последовательное передвижение по шкале частот [1].

Большое внимание специалисту в области информационной безопасности стоит уделить практическому изучению современных приборов и аппаратных комплексов по защите информации. Для получения базовых и углубленных знаний в области электрорадиоизмерения и измерительной аппаратуры, студентам специальности 090900 «Информационная безопасность» предлагается изучение дисциплины «Измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения». Данная дисциплина входит в вариативную (профильную) часть учебного цикла [2]. Суть практических занятий сводится к тому, чтобы закрепить знания, полученные на лекционных занятиях.

Например, изучив в теории особенности закладного устройства и индикатора поля, проверяют защищенность помещения, условно предназначенного для конфиденциальных переговоров.

Изучение дисциплины «Измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения» дает возможность расширения и углубления знаний, умений, навыков в области электротехники, радиоэлектроники и обеспечения информационной безопасности с использованием индикаторов поля, что позволит студенту получить углубленные знания, умения, навыки для успешной профессиональной деятельности и(или) для продолжения профессионального образования в магистратуре [3].

Особенностью разработанного лабораторного практикума по дисциплине «Измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения» является то, что в ее задачи входит привитие обучаемому большого числа практических навыков, имеющих самое непосредственное отношение к его будущей профессии. Это навыки и методы поиска каналов утечки информации.

В ходе учебного курса специальности 090900 «Информационная безопасность» студентам необходимо выполнить ряд лабораторных работ. Предполагается выполнение лабораторных работ на следующие темы:

- Лабораторная работа №1. «Ииндикатор поля»;
- Лабораторная работа №2. «Средство съёма акустической информации»;
- Лабораторная работа №3. «Активные закладные устройства
- Лабораторная работа №4. «Пассивные закладные устройства»;

Студенты ознакомятся с индикатором (детектором) электромагнитного поля. На практике попробуют выявить закладные устройства (ЗУ), внедрённые в выделенные помещения и на объекты информатизации и использующие для передачи информации радиоканал, а также диктофоны и устройства скрытой видеозаписи.

Таким образом, разработанные курс заданий и полученные навыки работы с приборами, будет иметь практическое применение, как в рамках лабораторного практикума по дисциплине «Измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения», так и в дальнейшей работе по обеспечению информационной безопасности.

Список используемых источников:

1. Цит. по ст. «Поиск жучков и скрытого видео наблюдения» [Электронный ресурс] : Официальный сайт. – Режим доступа: http://intellektium.ru/
2. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 090900 «Информационная безопасность» (квалификация (степень) «бакалавр»).
3. Образовательный стандарт учебной дисциплины Б3.ДВ30.1 «измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения» 090900 Информационная безопасность.

ХОЛТЕР-МОНИТОР НА БАЗЕ МИКРОСХЕМЫ ADS1298

Байраммырадов К.А. – студент, Кайгородов А.В. – аспирант,
Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет (г. Барнаул)

Современная медицинская функциональная диагностика располагает самыми различными инструментальными методами исследования. Некоторые из них доступны только узкому кругу специалистов. Одним из распространенных и доступных методов исследования является холтер-мониторирование, используемое в основном в кардиологии [1-2]. Однако он с успехом применяется и при исследовании больных с заболеваниями легких, почек, печени, эндокринных желез, системы крови, а также в педиатрии, гериатрии, онкологии, спортивной медицине и еще когда есть проблемы с сердцем. Бывает такая ситуация: у пациента есть жалобы, но они, допустим, возникают вечером (или в связи с какими-то событиями). Он записывается на прием к кардиологу, ему снимают электрокардиограмму (ЭКГ), и ничего не обнаруживают, потому что запись ЭКГ была проведена утром или днем, или в тот момент, когда особых жалоб у пациента не было. Дело в том, что стандартная запись ЭКГ - это как бы "моментальный снимок" деятельности сердца. На обычной ЭКГ может быть зафиксировано только несколько сокращений сердечной мышцы: от 3 до 10-20 (в зависимости от кардиографа). Но сердце человека делает около 100 тысяч сокращений в сутки. Людям, попавшим в такую ситуацию, может вам понадобится холтеровский монитор (Холтер). Ежегодно производят десятки тысяч исследований с помощью холтеровского монитора. Этот метод в настоящее время стал достоянием широкого круга врачей – не только специалистов, занимающихся функциональной диагностикой, но и кардиологов, терапевтов, педиатров, спортивных врачей, физиологов и т. д.

Для разработки холтер-монитора рассмотрим особенности функционирования микросхем для дальнейшей разработки аппаратной части устройства. Для этого будем использовать популярное семейство аналоговых интегрированных интерфейсов ADS1298, а для передачи данных с ADS1298 на ПК используем микросхему MCP2210, которая является конвертером SPI-USB.

Первое устройство в семействе аналоговых интегрированных интерфейсов (AFE) уменьшает число компонентов и потребление энергии до 95%, улучшая мобильность и компактность систем. Фирма Texas Instruments представила первый в семействе полностью интегрированный аналоговый интерфейс (AFE) для портативного профессионального оборудования электрокардиографов (ECG), а также для мониторинга пациентов в бытовых медицинских приборах. Восьмиканальный 24-битный интерфейс ADS1298 уменьшает число компонентов и потребление энергии до 95% по сравнению с решениями на дискретных компонентах. При потреблении 1 мВт на один канал это устройство позволяет достичь высочайшего уровня точности в диагностике.

Отличительные особенности и преимущества приборов серии ADS1298R заключаются в следующем.

- Обеспечение измерения дыхательного импеданса с разрешением 20 мОм, что позволяет вести точный мониторинг и корреляцию дыхания пациента с отклонениями в электрокардиограммах.
- Интеграция средств, состоящих из 44 дискретных компонентов, что позволяет сократить занимаемую решением площадь монтажа на 97%. В дополнение к полностью интегральной реализации функции измерения дыхательного импеданса, с выбираемой пользователем настройкой фазы, приборы ADS1298R оснащены восемью аналого-цифровыми преобразователями (ADC), восемью усилителями с программируемым усилением (PGA), восемью активными фильтрами и интерфейсом детектирования ритма, источником опорного напряжения и рядом других функций.
- Энергопотребление, составляющее всего 750 мкВт/канал, составляет порядка 5% от энергопотребления решения, реализованного на дискретных компонентах. Приборы располагают также множеством конфигурируемых power-down режимов, позволяющих расширить срок службы батарей портативной аппаратуры мониторинга пациентов.
- Типичный соотносимый со входом шум в 4 мкВ (пик-пик) превосходит требования International Electrotechnical Commission IEC60601-2-27/51 стандарта, позволяя получить чрезвычайно высокий уровень точности в портативном и с высокой плотностью каналов ECG оборудовании.

Типовая схема включения ADS1298R приведена на рисунке 1.

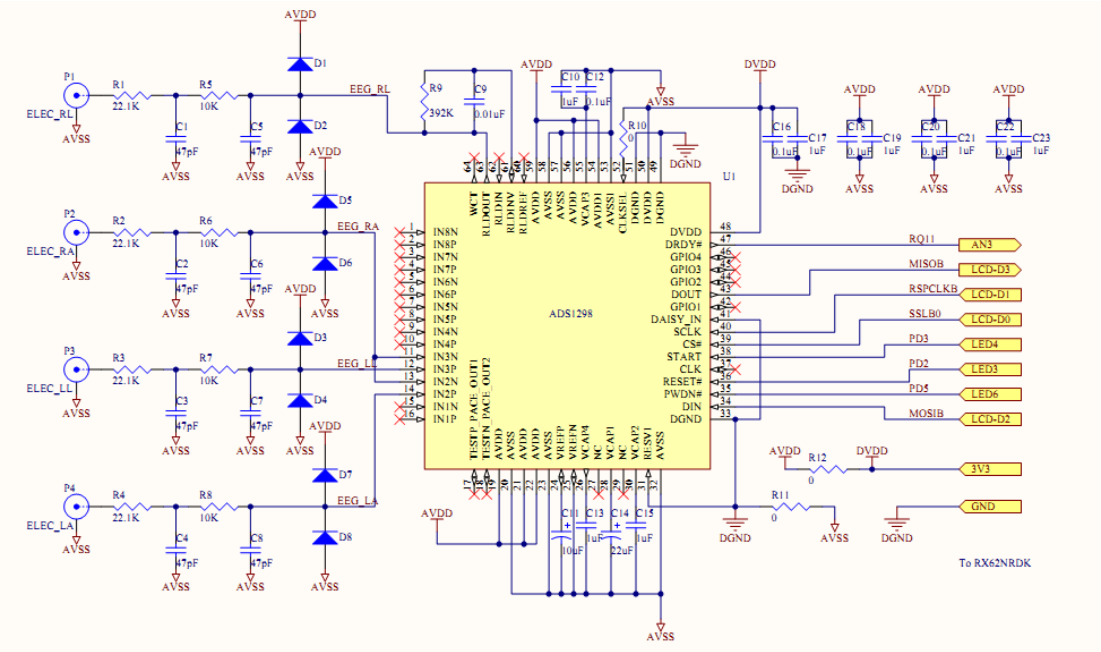


Рисунок 1. Рекомендуемая схема подключения АЦП.

Для передачи данных с АЦП на ПК используется микросхема MCP2210, которая является преобразователем интерфейсов SPI в USB и типовая схема включения которой представлена на рисунке 2.

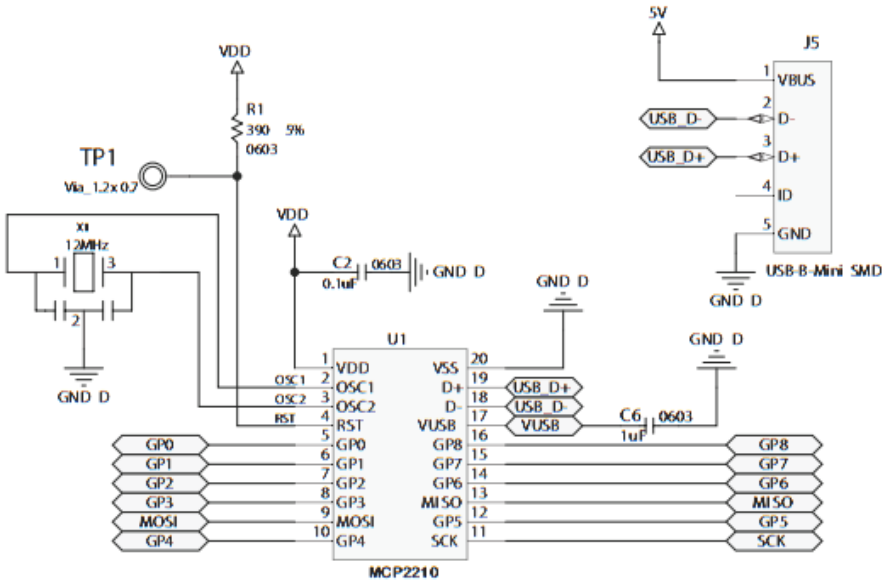


Рисунок. 2. Схема MCP2210.

Микросхема MCP2210 подключается к ADS1298R через SPI и позволяет SPI представить его как устройство USB. Это позволяет подключать ADS1298R без промежуточных управляющих контроллеров практически к любому устройству, имеющему USB порт для подключения внешних устройств и способному выполнять функции USB-хоста. Устройство уменьшает количество внешних компонентов за счет интеграции USB резисторов. MCP2210 также имеет 256 байт интегрированной пользовательской EEPR и девять входов / выходов общего назначения. При этом семь из них имеют дополнительные функции, чтобы задавать состояние связи по USB - интерфейсу.

Таким образом, в результате анализа современного рынка было выбрано решение, позволяющее при минимальных дополнительных затратах создать миниатюрный, простой в обращении и при этом полнофункциональный холтер-монитор с наименьшей возможной ценой и экстремально низким энергопотреблением.

Список используемых источников:

1. Макаров Л.М. Холтеровское мониторирование. 2-е изд. - Москва, Медпрактика-М, 2003.
2. Суточное мониторирование ЭКГ, Дабровски А., Дабровски Б., Пиотрович Р.

ПРИМЕНИЕ НЕЙРОСЕТЕВОГО ПОДХОДА ДЛЯ ОЦЕНКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Бахтин А.М. – студент, Пивкин Е.Н. – к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Одним из этапов решения задачи обеспечения безопасности информации является оценка состояния защищенности объекта информатизации (ОИ). Цель работы – оценка защищенности объекта информатизации комитета по финансам, налоговой и кредитной политике города Барнаула с использованием нейронных сетей.

Для достижения цели был проведен анализ объекта защиты:

– выделена организационная структура комитета;

– определены информационные потоки комитета (по направлениям деятельности построены диаграммы с использованием методологии IDEF0);

– определены объекты защиты;

– составлены модели угроз (по методикам ФСТЭК и ФСБ).

– выделены меры защиты, которые внедрены в настоящий момент в комитете, и выработаны предложения защиты для совершенствования системы защиты информации комитета.

Для оценки защищенности выделают два подхода:

– оценка на соответствие требованиям нормативных документов;

– применение инструментальных средств анализа защищенности.

На основании анализа данных подходов предложено применение математического аппарата нейронных сетей для оценки защищенности ОИ. На основании анализа:

– составлен алгоритм решения задач нейронной сетью;

– проведена классификация нейронных сетей по различным признакам;

– определены общие задачи, решаемые нейронными сетями;

– выделены сферы применения нейронных сетей в областях науки и техники, в том числе и в сфере защиты информации (Рисунок 1) [1];

– проанализированы возможности существующего программного обеспечения для моделирования нейронных сетей.

Рисунок 1 – Сферы применения нейронных сетей в защите информации

Для проверки возможности применения нейросетевого подхода выполнена оценка уровня информационной безопасности в части группового показателя «Обеспечение информационной безопасности средствами антивирусной защиты» Методики Банка России с помощью нейронной сети [2]. А именно:

– выбрана архитектура нейронной сети [3];

– определена оптимальная внутренняя структура нейронной сети (количество скрытых слоев, функция активации нейронов).

Использование нейросетевого подхода для оценки защищенности ОИ позволяет избавиться от некоторых недостатков, характерных для методики Банка России: появляется

возможность добавления новых или удаления неактуальных показателей защищенности и применения непрерывных оценок исходных показателей защищенности.

Для оценки защищенности ОИ комитета определены собственные критерии защищенности:

– управление доступом;
– регистрация и учет;
– контроль целостности;
– управление сетью;
– антивирусная защита;
– криптографическая защита.

Для каждого критерия выбран набор показателей защищенности. Предполагается создание и обучение нейронной сети в соответствии с перечисленными критериями, проведение оценки защищенности ОИ комитета до и после применения предложений защиты.

Список использованных источников:

1. Галушкин А.И. Нейрокомпьютеры в решении задач обеспечения информационной безопасности / А.И. Галушкин // Информационные технологии. – 2011. – №1. – с.58-63
2. Стандарт банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации СТО БР ИББС-1.0-2010.– Москва, 2010. – 74 с.
3. Маслобоев Ю.П. "Введение в Neural Network Toolbox" / Ю.П. Маслобоев.– М.: Диалог-МИФИ, 2010. – 285с.

К ВОПРОСУ О ПРИМЕНЕНИИ НЕЙРОСЕТЕВОГО ПОДХОДА НА ПРИМЕРЕ МЕТОДИКИ БАНКА РОССИИ

Бахтин А.М. – студент, Пивкин Е.Н. – к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В настоящее время любая организация, эксплуатирующая один или несколько объектов информатизации (ОИ), сталкивается с проблемой обеспечения безопасности информации (БИ) на всех этапах жизненного цикла ОИ.

Одним из этапов решения задачи обеспечения БИ является оценка состояния защищенности ОИ.

Оценка выполняется с использованием отечественных и зарубежных методик, различных стандартов. В качестве примера выделяют:

– методику оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББ-1.0-2010;
– систему «Кондор» компании Digital Security, предназначенная для оценки соответствия требованиям стандарта ГОСТ Р ИСО/МЭК 17799 [2];
– систему COBRA (Consultative Objective and Bi-Functional Risk Analysis), является средством анализа рисков и оценки соответствия ИС стандарту ISO17799;
– NIST 800-26 «Руководство по самооценке безопасности для систем информационных технологий» (оценка уровня зрелости).

Согласно этим методикам, решение задачи оценки защищенности сводится к оцениванию определенного количества показателей защищенности. В дальнейшем значения показателей защищенности взвешенно суммируют и определяют итоговую защищенность оцениваемого ОИ (или несколько итоговых показателей по нескольким направлениям защиты).

Существующие методики широко используются, но обладают некоторыми недостатками:

– Неизвестна взаимосвязь между исходными показателями защищенности, поэтому функцию итогового показателя сложно определить формально.

– Сложность адаптации методики при добавлении новых или удаления неактуальных показателей защищенности.

– Возможность применения только фиксированных оценок исходных показателей защищенности.

Для решения этих проблем рассмотрено применение нейронных сетей для оценки защищенности ОИ. В терминах нейронной сети задача оценки защищенности с использованием показателей защищенности сводится к задаче аппроксимации функции.

Для проверки возможности применения нейросетевого подхода выполнена оценка уровня информационной безопасности в части группового показателя «Обеспечение информационной безопасности средствами антивирусной защиты» Методики Банка России с помощью нейронной сети [1].

В выбранный групповой показатель входит 16 частных показателей, следовательно нейронная сеть должна иметь 16 входных нейронов. На выходе нейронной сети – 1 параметр «Оценка группового показателя».

При обучении подаются последовательно векторы-строки (16 входных параметров, 1 выходной в каждом векторе). Область допустимых значений входных параметров: {0; 0.5; 1}, выходные параметры лежат равномерно на интервале [0, 1].

В качестве архитектуры нейронной сети выбрана полносвязная многослойная сеть прямого распространения «Многослойный персептрон».

Было проведено моделирование с помощью нейропакета Matlab [3], которое заключалось в подборе:

– количества скрытых слоев (1, 2, 3);

– количества нейронов в каждом скрытом слое;

– функции активации нейронов (пороговая – hardlim, логистическая – logsig, линейная – purelin, гиперболический тангенс - tansig);

– количества векторов обучения (25, 50, 100, 200).

В зависимости от числа нейронов в каждом слое смоделированы следующие сети:

– однослойная сеть с 8-32 скрытыми нейронами;

– двуслойная сеть с 16-24 нейронами в 1 скрытом слое и с 8-16 нейронами во 2 скрытом слое;

– трехслойная сеть с 24-28 нейронами в 1 скрытом слое и с 18-22 нейронами во 2 скрытом слое, с 12-16 нейронами в 3 скрытом слое.

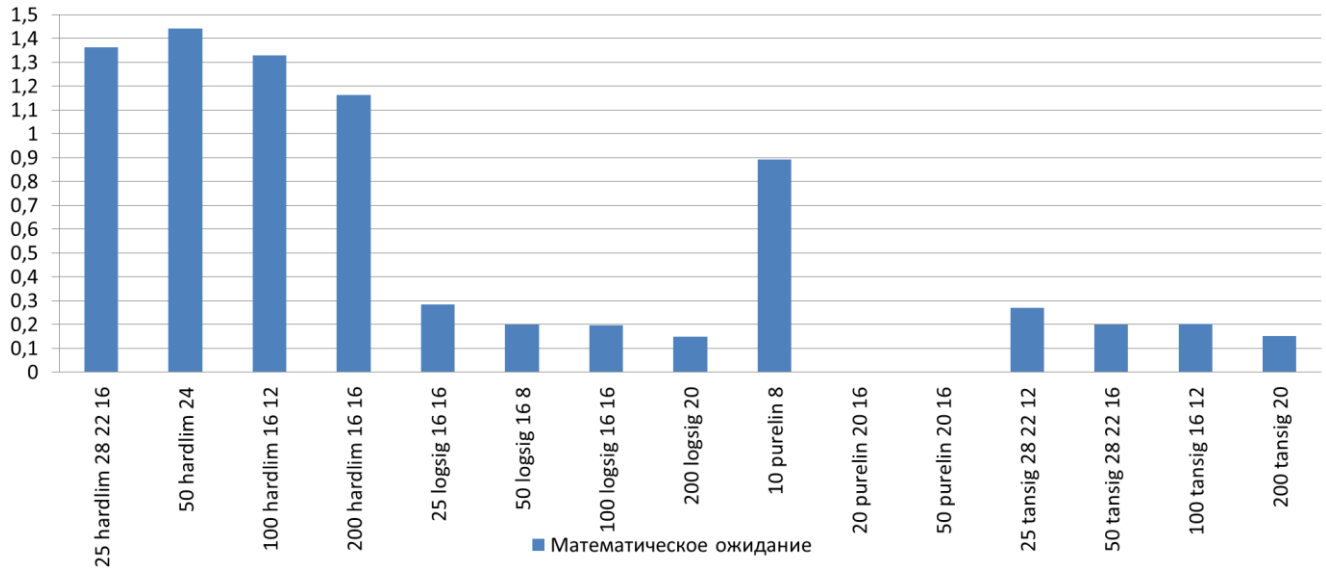
Каждая сеть последовательно обучалась 5 раз, затем результаты обучения усреднялись.

Относительная ошибка на тестовой выборке не должна превышать 10%.

После обучения работа сети проверялась 1000 тестовыми векторами со стандартными для методики значениями входных параметров {0; 0,25; 0,5; 0,75; 1} и 1000 тестовыми векторами с нестандартными для методики значениями входных параметров {0; 0,1; 0,2 … 0,9; 1}.

Для каждого проверочного вектора вычислена относительная ошибка работы сети, создан массив относительных ошибок. Относительная ошибка усреднена на наборе тестовых векторов.

На рисунке 1 представлены результаты относительных ошибок наилучших сетей в зависимости от функции активации и количества обучающих данных:



ww function xx yy zz , где

ww – число обучающих векторов

function – функция активации

xx, yy, zz – количество нейронов в каждом слое

Рисунок 1 – Результаты работы наилучших нейронных сетей в зависимости от функции активации и количества обучающих данных

На рисунке 2 указаны наилучшие относительно ошибок однослойные, двуслойные, трехслойные нейронные сети для каждой функции активации. Нейронные сети с пороговыми функциями активации нейронов (hardlim) не приводятся, так как не решают задачу оценки защищенности при любом наборе обучающих данных

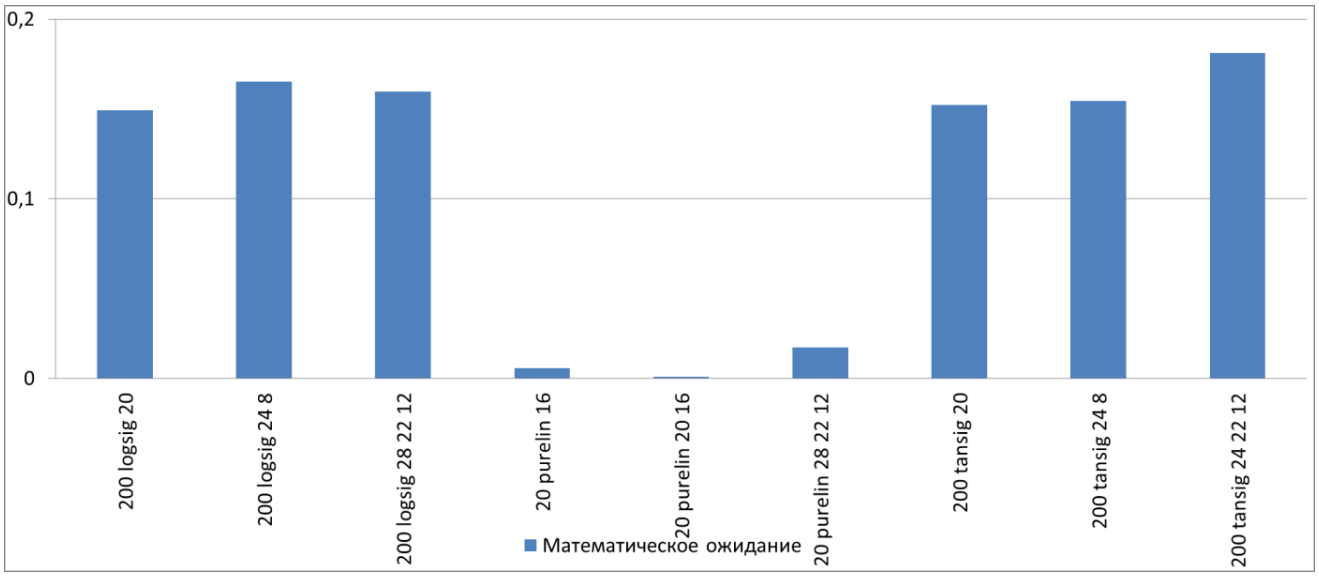


Рисунок 2 – Лучшие нейронные сети в зависимости от количества слоев и функции активации

Анализ проведения испытаний показал позволил сделать следующие выводы: вне зависимости от внутренней структуры сети:

– при применении пороговой функции активации (hardlim) нейронная сеть не выдает желаемые результаты при любом наборе исходных данных;

– при применении логистической (logsig) функции активации и функции активации – гиперболический тангенс (tansig) нейронная сеть выдает желаемые результаты только при большом наборе исходных данных;

– при применении гиперболического тангенса (tansig) в качестве функции активации нейронная сеть часто попадает в локальный минимум;

– лучшая функция активации для решения поставленной задачи – линейная (purelin);

– выбрана наилучшая нейронная сеть – двухслойная нейронная сеть с 20 нейронами в первом скрытом слое, 16 нейронами во втором скрытом слое, обученная 20 примерами. Относительная ошибка обучения при проверке на стандартных для методики значениях – 0,00084, при проверке на нестандартных для методики значениях результаты попали в ожидаемые интервалы.

Таким образом, показано применение нейронных сетей в задачах оценки защищённости объектов информатизации. Этот подход позволяет избавиться от недостатков, характерных для рассмотренных выше методик: появляется возможность добавления новых или удаления неактуальных показателей защищенности и применения непрерывных оценок исходных показателей защищенности.

Список использованных источников:

1. Стандарт банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации СТО БР ИББС-1.0-2010.– Москва, 2010. – 74 с.

2. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.– М: Стандартинформ, 2006. – 54 с.

3. Маслобоев Ю.П. "Введение в Neural Network Toolbox" / Ю.П. Маслобоев.– М.: Диалог-МИФИ, 2010. – 285с.

РАЗРАБОТКА ИНТЕРАКТИВНОГО ДИДАКТИЧЕСКОГО МОДУЛЯ ПО ДИСЦИПЛИНЕ "ЗАЩИТА ИНФОРМАЦИИ"

Белоусов А.С. – студент, Борисов А.П. - к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г.Барнаул)

Сегодня информационные технологии завоевывают все более важные позиции в жизни человека. В информационном обществе главным ресурсом является информация. Именно на основе владения информацией о самых различных процессах и явлениях можно эффективно и оптимально строить любую деятельность, поэтому информация на данный момент имеет очень большую цену. Информация сегодня стоит дорого и ее необходимо защищать. Для предотвращения потери информации разрабатываются различные механизмы защиты. Поэтому крайне важно чтоб специалисты, связанные с информационными технологиями умели правильно пользоваться минимальным набором механизмов связанных с защитой информации.

Целью преподавания дисциплины «Защита информации» [1] является изучение основных средств защиты информации, нормативно-правовых документов. И для этого необходимо закрепление знаний полученных в ходе изучения теоретического материала.

Для закрепления знаний по дисциплине полученных в ходе изучения теоритического материала необходимо практическое применение и для этого был разработан модуль лабораторных работ по дисциплине “Защита информации”.

Целью лабораторного занятия является освоение содержания изучаемой дисциплины, приобретение навыков практического применения знаний дисциплины с использованием технических средств и (или) оборудования [2].

Целью лабораторных занятий по дисциплине «Защита информации» является освоение содержания изучаемой дисциплины, закрепление теоретических знаний, практических умений и навыков в области защиты информации, овладение компетенциями по квалифицированному применению на практике профессиональной терминологии, по классификации защищаемой информации средств и систем её защиты, проведению целенаправленного поиска в различных источниках информации по защите информации, в том числе в глобальных компьютерных системах.

Выполнение лабораторных заданий осуществляется в программном обеспечении Антивирус Касперского, Dr.Web, Avast! Free Antivirus, OpenVPN и VipNET, а так же с помощью оборудования, маршрутизатора D-link DIR-615. Весь курс состоит из 4 лабораторных работ, который выполняется индивидуально или по группам, а так же распределяются по вариантам.

Первая лабораторная работа посвящена настройке и обеспечению безопасности беспроводной точки доступа WI-FI. Выполнение лабораторной работы осуществляется на оборудовании D-link DIR-615.

На сегодняшний день Wi-Fi оборудование оснащено множеством средств обеспечения безопасности и при правильном выборе и профессиональной настройке позволяет достичь высокого уровня защищенности.

В ходе выполнения лабораторной работы студент получит навыки по настройке оборудования Wi-Fi и обеспечение безопасности.

Вторая лабораторная работа посвящена настройке антивирусных средств [4,5,8] и обеспечению безопасности с помощью данного программного обеспечения.

Антивирусная программа (антивирус) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

В лабораторной работе связанной с антивирусами студенты научаться настраивать антивирусное программное обеспечение и осуществлять защиту информации с помощью данной программы.

Третья лабораторная осуществляется с помощью средств создания частных виртуальных сетей [6,7]. Выполнения данных лабораторных работ осуществляется с помощью предложного программного обеспечения.

VPN (виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений).

В данной лабораторной работе студенты научатся создавать безопасное сетевое соединение с помощью средств создания частных виртуальных сетей [3]. Ознакомятся со средствами создания частных виртуальных сетей, а так же смогут осуществлять настройку данных средств.

Четвертая лабораторная работа связанная со средствами шифрования. Выполнение данной лабораторной осуществляется с помощью предложенных средств шифрования. PGP – компьютерная программа, также библиотека функций, позволяющая выполнять операции шифрования и цифровой подписи сообщений, файлов и другой информации, представленной в электронном виде.

Шифрование PGP осуществляется последовательно хешированием, сжатием данных, шифрованием с симметричным ключом, и, наконец, шифрованием с открытым ключом,

причём каждый этап может осуществляться одним из нескольких поддерживаемых алгоритмов. Симметричное шифрование производится с использованием одного из семи симметричных алгоритмов (AES, CAST5, 3DES, IDEA, Twofish, Blowfish, Camellia) на сеансовом ключе. Сеансовый ключ генерируется с использованием криптографически стойкого генератора псевдослучайных чисел. Сеансовый ключ зашифровывается открытым ключом получателя с использованием алгоритмов RSA или Elgamal (в зависимости от типа ключа получателя). Каждый открытый ключ соответствует имени пользователя или адресу электронной почты. Первая версия системы называлась Сеть Доверия и противопоставлялась системе X.509, использовавшей иерархический подход, основанной на удостоверяющих центрах, добавленный в PGP позже. Современные версии PGP включают оба способа.

В заключительной лабораторной работе студенты научатся обеспечивать информационную безопасность с помощью средств шифрования. Ознакомятся со средствами шифрования, а так же смогут осуществлять настройку данных средств.

Таким образом, разработанный лабораторный практикум будет иметь практическое применение, как в рамках лабораторного практикума по дисциплине «Защита информации», так и в дальнейшей работе по обеспечению информационной безопасности с помощью знаний полученных в ходе выполнения данных лабораторных работ.

Список используемых источников:

1. СТО 13.62.1.1201 – 2012. Система качества АлтГТУ. Образовательный стандарт высшего профессионального образования АлтГТУ. Образовательный стандарт учебной дисциплины «Защита информации». – Введ. 2012-2-10. – Барнаул: АлтГТУ, 2012. – 28 с.
2. СТП 12700 – 2007. Система качества АлтГТУ. Образовательный стандарт высшего профессионального образования АлтГТУ. Занятия лабораторные. Общие требования к организации, проведению и методическому обеспечению. – Введ. 2007-09-01. – Барнаул: АлтГТУ, 2007. – 10 с.
3. Стивен Браун. Виртуальные частные сети. Учебное пособие [Текст] / Стивен Браун. – М.: Издательство «М.Лори», 2001. – 508 с.
4. Антивирус Касперского 2012 [Электронный ресурс] / Антивируса Касперского 2012 - Режим доступа: http://www.kaspersky.ru/anti-virus.
5. Dr.Web [Электронный ресурс] / Dr.Web- Режим доступа: http://www.freedrweb.com/cureit.
6. VipNet CUSTOM [Электронный ресурс] / Сетевое экранирование и VPN - Режим доступа: http://www.infoline-rk.ru/vipnet-custom/.
7. OpenVPN [Электронный ресурс] / OpenVPN - Режим доступа: http://ru.wikipedia.org/wiki/Openvpn
8. Антивирусные программы [Электронный ресурс]. Антивирусные программы - Режим доступа: http://www.comss.ru/list.php?c=antivirus

РАЗРАБОТКА ЛАБОРАТОРНОГО ПРАКТИКУМА «СЕТИ ZIGBEE»

Григорьев А.А. – студент, Борисов А. П. – к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Надежные и безопасные беспроводные сети ZigBee к настоящему времени находят широкое применение в сенсорных сетях, системах автоматизации и управления бытовым и промышленным оборудованием, системах автоматического сбора показаний с приборов учета, системах контроля жизнеобеспечения, удаленного управления распределенными системами. Отличительными особенностями таких сетей является большое число узлов, способность к самоорганизации и восстановлению работоспособности, высокая надежность передачи данных, низкое энергопотребление узлов сети, использование сложной ячеистой топологии с маршрутизацией и ретрансляцией сообщений. Однако, поскольку технология

ZigBee предназначена для встраиваемых систем, имеющих, как правило, ограниченные вычислительные ресурсы и ресурсы памяти, то в качестве одной из основных задач разработки данной технологии являлось максимальное понижение требований к аппаратным ресурсам с одной стороны и получения надежной технологии с развитой сетевой функциональностью узлов сети с другой. Стоит отметить, что технология ZigBee относиться только к организации сетевого и транспортного уровней в терминах семиуровневой модели OSI, в то время как физический и канальный уровни описываются стандартом беспроводных сетей IEEE 802.15.4.

Сети ZigBee могут состоять из трех типов узлов: координатора, маршрутизатора(роутера) и оконечного устройства. Только координатор может запустить или остановить новую сеть, при этом координатор определяет различные параметры сети и совмещает функции маршрутизатора. В сети ZigBee допускается наличие только одного координатора. Маршрутизаторы и оконечные устройства могут подключиться только к уже существующей сети. Маршрутизаторы служат для маршрутизации и ретрансляции пакетов, а также являются родительскими узлами для оконечных устройств и других маршрутизаторов сети. Оконечные устройства представляют какие-либо внешние устройства по отношению к самой сети. Оконечные устройства всегда должны иметь строго одного родительского узла, которым может быть либо координатор, либо один из маршрутизаторов сети ZigBee. Координатор и маршрутизаторы, помимо обязательных сетевых функций, могут, как и оконечные устройства, представлять интересы внешних устройств в сети ZigBee для взаимодействия с другими ее участниками.

Немаловажной задачей, решаемой альянсом ZigBee, является обеспечение совместимости устройств разных производителей, использующих в качестве транспортной системы для передачи различных команд и сообщений технологию ZigBee. Альянс ZigBee вводит понятие профиля приложения, в котором определяется состав входных и выходных кластеров(подобны структурам в языке программирования), а также подвергаются конкретизации некоторые сетевые параметры, например, размер сети. К настоящему времени разработано несколько спецификаций профилей: автоматизация зданий, автоматизация бытового оборудования, автоматизация доступа и др.

В настоящее время актуальной задачей является разработка методического и программно-технического обеспечения для проведения лабораторного практикума по технологии беспроводной технологии ZigBee в учебном плане дисциплины «Сети и системы связи». Разработка данного обеспечения позволит студентам в рамках ограниченного времени сконфигурировать и запустить сеть, оценить ее основные эксплуатационные возможности, сделать выводы об эффективности данной технологии.

Для решения поставленной задачи в качестве аппаратной платформы выбран стартовый оценочный комплект AVR RZ RAVEN. В комплект входят один модуль RZUSBSTICK с возможностью подключения к ПК по интерфейсу USB, а также два модуля AVRRAVEN имеющие в качестве органов управления пяти позиционный джойстик и монохромный ЖК-дисплей. На платах модулей AVR RAVEN также расположены динамик, микрофон, терморезистор, микросхема flash памяти 16 Мбит. Перечисленные периферийные блоки дают возможность создания нескольких сценариев проведения лабораторного практикума. Поскольку один комплект включает три платы, и микроконтроллеры каждой из плат имеют достаточно аппаратных ресурсов для загрузки и исполнения микропрограммы согласно ролям координатора, маршрутизатора, либо оконечного устройства, то, используя один комплект AVRRZRAVEN, возможно построить минимальную сеть, состоящую из узлов всех возможных типов. В качестве программного стека протоколов использован полнофункциональный, соответствующий спецификации ZigBee PRO, стек «BitCloud», разработанный фирмой Atmel специально для аппаратных платформ, разработанных этой же фирмой. Данный стек протоколов предоставляется фирмой Atmel бесплатно, что является значительным фактором при использовании стека в учебных целях.

Для проведения полноценной лабораторной работы с использованием комплекта AVR RZ RAVEN разработано программное обеспечение для ПК «RavensNetTest» , а также микропрограммное обеспечение для микроконтроллеров. Приложение «RavensNetTest» предназначено для конфигурирования и тестирования сети, посредством взаимодействия с модулем RZUSBSTICK через виртуальный COM порт поверх USB соединения. Микропрограмма для контроллера модуля RZUSBSTICK взаимодействует с приложением «RavensNetTest» с одной стороны и программным стеком «BitCloud» с другой. Микропрограммы для контроллеров платы AVRRAVEN позволяют получить доступ к периферийным блокам и программному стеку «Bitcloud».

Основными возможностями разработанного программного комплекса являются:

- Подключение и отключение локального узла либо выполнение запроса на отключение от сети любого другого узла.
- Наглядное представление топологии и связей между узлами сети на основе таблицы соседей маршрутизаторов и координатора сети
- Считывание таблиц маршрутизации любого маршрутизатора, либо координатора сети
- Получение конфигурационных параметров с любого узла сети
- Проверка скорости передачи данных между локальным узлом и любым другим узлом сети, при этом возможно варьировать размер пакета, а также использовать либо нет подтверждение доставки каждого пакета и механизма шифрования.
- Пересылка текстовых сообщений между узлами.
- Использование механизмов аутентификации и шифрования, предоставляемых стеком «BitCloud»
- Мониторинг функционирования сети, запущенной по сценарию: «домофон», «приборы учета», «беспроводной выключатель», «монитор температуры», «охранная система»

Таким образом, разработанное программно-техническое обеспечение будет иметь практическое применение при изучении студентами беспроводной технологии ZigBee в рамках лабораторного практикума по дисциплине «Сети и системы связи».

Список используемых источников:

1. Алый А. Разработка модуля беспроводной передачи телеметрических данных в диапазоне частот 2,4 ГГц// Современная электроника №2. 2007. - 52с.
2. ZigBee [Электронный ресурс]//Режим доступа: http://www.zigbee.org/Home.aspx
3. Doc8117 RZRAVEN Hardware User's Guide

ИСПОЛЬЗОВАНИЕ РАДИОМОДЕМОВ МАЛОГО РАДИУСА ДЕЙСТВИЯ В УЧЕБНОМ ПРОЦЕССЕ ДИСЦИПЛИНЫ «СИСТЕМЫ И СЕТИ СВЯЗИ»

Борисов А.П. – к.т.н., доцент, Думнов А.Н. – студент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Беспроводная передача данных в настоящее время переживает бурное развитие. Ввиду продолжающейся компьютеризации различных сфер деятельности и автоматизации работ повышается и уровень предлагаемых технологических решений. Современные предприятия и организации все чаще нуждаются в системах сбора данных и организации удаленного управления процессами, передачи цифровой информации, а также осуществления мониторинга и охраны. При этом проводные линии передачи не могут обеспечить мобильность абонентов и оборудования, вдобавок монтаж проводов не всегда приемлем. Поэтому беспроводные технологии связи являются востребованными решениями.

Среди беспроводных технологий применяются многие стандартизированные решения, закрепленные, например, институтом IEEE. Но на рынке wireless-технологий существуют

собственные нестандартизированные разработки, созданные отдельными предприятиями, институтами или конструкторскими бюро и обеспечивающие радиосвязь большого или малого радиуса действия – радиомодемы.

Использование радиосвязи в России имеет правовой аспект, связанный с особенностями лицензирования. На основании решения ГКРЧ [1] выделены особые нелицензируемые радиочастотные диапазоны. Многие технологии и средства беспроводной связи иностранного производства, в том числе стандартизированные, не используют данные диапазоны, из-за чего подлежат регистрации в соответствующих органах РФ.

Узкополосные радиомодемы малого радиуса действия (РМРД) предназначены для работы в нелицензируемых полосах частот, в которых не действуют нормы на частотное разделение каналов и не выделяются частоты для работы отдельных радиосетей. РМРД строятся на недорогой элементной базе на основе однокристальных приёмопередатчиков. [2]

Студенты, обучающиеся по направлению «Информационная безопасность» (ИБ), изучают предмет «Системы и сети связи». Данная дисциплина подразумевает выполнение лабораторного практикума, включающего в себя рассмотрение организации беспроводных сетей. Как правило, рассматриваются сети на основе Wi-Fi (IEEE 802.11) ввиду их распространенности, быстроте развертывания и скорости передачи. [3] Но для широты кругозора, а также для закрепления теоретической базы принципов радиосвязи уместно поместить ознакомление с узкополосными радиомодемами для построения сетей сбора данных, телеметрии, мониторинга и охраны. При этом практическому закреплению полученных знаний будут служить специальные программно-технические средства.

Новизна работы заключается в изучении и практическом применении специализированных радиомодемов в учебном процессе студентов технического вуза. Поскольку, как уже было отмечено, традиционно из беспроводных технологий в практическом обучении используются технологии Wi-Fi и Bluetooth, применение нестандартизированных радиомодемов восполнит этот пробел в учебно-методическом процессе обучения студентов-бакалавров ИБ.

Исходя из указанного выше, целью работы являлась разработка программно-аппаратного комплекса и методических рекомендаций для выполнения студентами лабораторных работ по технологии беспроводной передачи информации на основе радиомодемов. Для достижения поставленной цели были выполнены следующие задачи:

- Разработана схема устройства, организующего связь радиомодема с персональным компьютером (ПК) на основе микроконтроллера AVR и собрана печатная плата.
- Написано программное обеспечение (ПО) для ПК и разработанного устройства.
- Разработано методическое обеспечение для выполнения лабораторной работы.

В качестве радиомодема был выбран модем РМД400-OEM. Данный радиомодем выполнен в конструктиве DIP40, в виде печатной платы размером 53x20.5 мм с применением микросхемы приемопередатчика CC1120 от Texas Instruments. Радиомодем RMD 400 имеет высокую чувствительность приёмника (до -118дБм). Мощность передатчика – 10 мВт. Модуль обеспечивает дальность связи до 10 км. (таблица 1) [4]

Таблица 1 – Основные технические характеристики радиомодема РМД400-OEM [5]

Диапазон частот:	433,05 ~ 434,79 МГц
Диапазон рабочих температур, °С:	-40 до +80
Напряжение питания:	3,4-5 В, 30/80 мА
Потребляемый ток:	32/47(90) мА (прием/передача)
Скорость данных по UART, кбод:	1,2; 2,4; 4,8; 7,2; 9,6; 19,2; 38,4; 57,6; 115,2
Скорость передачи информации по радиоканалу:	1,2-76,8 кбит/с
Кодирование с исправлением ошибок:	каскадное, перемежение
Кодирование с обнаружением ошибок:	CRC16 для блока до 16 байт
Размер сообщения:	не ограничен

Устройство, сопрягающее радиомодем и компьютер, сделано на основе неспециализированного микроконтроллера AVR серии Mega, осуществляющего связь с ПК по интерфейсу USB класса HID, что обеспечивает скорость передачи данных от ПК к устройству до 64 кбит/с. Преимущество использования HID USB – наличие стандартных драйверов HID в распространенных операционных системах, в том числе Windows (XP и выше), упрощающее разработку ПО. Кроме того, устройство сопряжения соединяется с OEM-модулем радиомодема посредством интерфейса универсального асинхронного приемопередатчика UART микроконтроллера с уровнями напряжений TTL. Программирование микроконтроллера устройства осуществляется внутрисхемным ISP программатором по интерфейсу SPI. Схема сопряжения радиомодема с ПК – на рисунке 1.

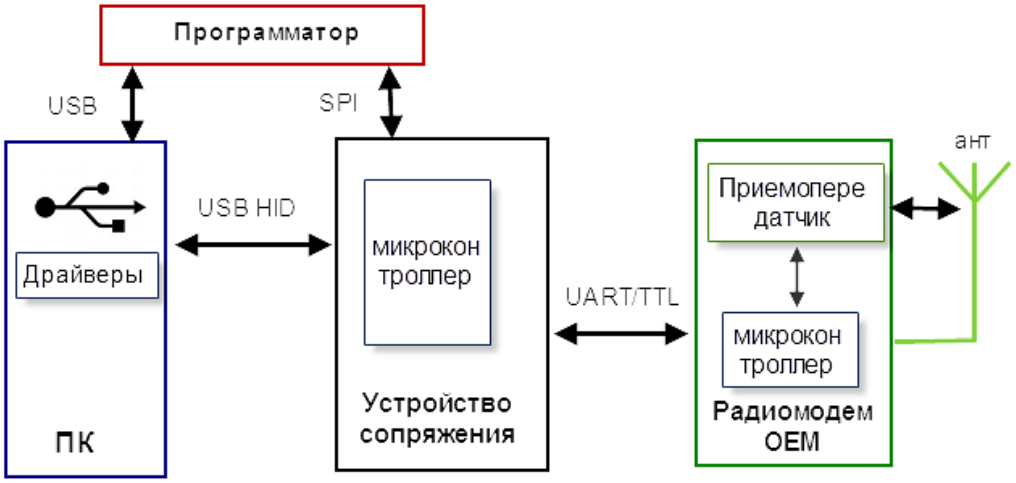


Рисунок 1 – Схема взаимодействия узлов системы

Платы радиомодема и сопрягающего устройства помещены в корпус, в котором сделаны отверстия для разъема USB типа B, SPI (6 pins), внешней антенны и светодиода питания.

Таким образом, разработанный программно-технический комплекс вместе с методическим обеспечением позволяют организовать выполнение лабораторной работы.

Список используемых источников:

1. Решение ГКРЧ от 07.05.2007 № 07-20-03-001 «О выделении полос радиочастот устройствам малого радиуса действия».

2. Немировский М.С. и др. Беспроводные технологии от последней мили до последнего дюйма [текст]: Учебное пособие / Под ред. М.С. Немировского, О.А. Шапорина. – М.: Эко-Трендз, 2010. – 400 с.: ил.

3. Борисов, А.П . Учебно- методическое пособие " Системы и сети связи" / А.П . Борисов; АлтГТУ им. И. И. Ползунова. – Барнаул : Изд-во АлтГТУ, 2013. – 79 с.

4. Сартаков А. Узкополосные радиомодемы малого радиуса действия [электронный ресурс] : статья / Радио-модем. – Режим доступа: http://www.radio-modem.ru/information/artikles/narrow-band_data_radio.htm.

5. Промышленный радиомодем КБ МАРС РМД 400-OEM безлицензионные. OEM вариант модема, последовательные интерфейсы RS-232 и RS-485, разъём DB-9F [электронный ресурс] : статья / Mobil Radio. – Режим доступа: http://www.mobilradio.ru/radiomodem/kb_mars/?rmd400-oem. – загл. с экрана.

ПРОГНОЗИРОВАНИЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МЕТОДОМ ГРУППОВОГО УЧЕТА АРГУМЕНТОВ

Жданов А.С- студент., Плетнев П.В.- ген. директор ООО «ЦИБ»,
Шарлаев Е.В – к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В ранние годы развития корпоративных сетей одной из основных проблем компаний был несанкционированный доступ к коммерческой информации путем внешнего. Сегодня этой проблеме уделяют огромное внимание. На рост рынка IT-услуг в сфере безопасности значительное влияние оказывает и развитие параллельных направлений, таких как внедрение ERP-систем, создание крупных телекоммуникационных сетей и информационных систем, то есть тех направлений, где IT-консалтинг почти всегда входит в список сопутствующих услуг. Предотвращение компьютерных атак со стороны злоумышленников, выявление возможных уязвимостей программного обеспечения – первоочередная задача для специалистов, работающих в сфере информационных технологий.

В современных условиях необходимо разрабатывать эффективные прогнозы как глобальных угроз информационной безопасности, так и возможного появления новых уязвимостей конкретных информационных систем и технологий. В настоящее время существует большое количество методов прогнозирования рисков информационной безопасности предприятия, например, отражено в руководящих и методических документах ФСБ России и ФСТЭК России, ГОСТ 13335-3, COSO, метод когнитивной алгебры логики.

Специфика деятельности предприятия ООО «ЦИБ» вызвала необходимость в расчете рисков информационной безопасности предприятия методом группового учета аргументов (МГУА). Одним из недостатков алгоритмов МГУА является отсутствие возможности работы с входными переменными, имеющими качественный характер, и учета в процессе моделирования экспертных знаний о существующих в системе взаимосвязях между факторами. Использование аппарата теории нечетких множеств и нечеткого логического вывода позволяет учесть экспертную информацию, минимизировав тем самым негативные последствия наличия статистической выборки ограниченного размера.

Большинство математических методов построения идентифицирующих моделей рисков информационной безопасности требует наличия определенного (не менее заданного) объема ретроспективных данных, используемых при построении модели. В случае если данное требование не выполняется, модель либо не может быть полностью определена, либо не обладает характеристиками (точностью, несмещенностью и др.), что приводит к её непригодности для использования в целях прогнозирования информационных рисков. Работать с выборками исходных данных, имеющих ограниченный объем, позволяет метод группового учета аргументов (МГУА), но в процессе построения модели он не учитывает экспертные знания об имеющихся в моделируемой системе взаимосвязях.

Разработанный метод учитывает особенности инфраструктуры ООО «ЦИБ». Рабочие станции ООО «ЦИБ» предоставляют инсайдерам целый ряд каналов утечки информации: принтеры, портативные устройства, беспроводные сети, съемные носители и т.д. Существует целый ряд продуктов, представленных на российском рынке и позволяющих так или иначе решить проблему утечки через рабочие станции. Именно кража конфиденциальной информации волнует ООО «ЦИБ» больше всего. Анализ состояния информационной безопасности на предприятии ООО «ЦИБ» позволяет выявить ряд недостатков: отсутствие регламента доступа к информации, отсутствие политики резервного копирования информации, регламентов работы с информационными ресурсами.

Для устранения недостатков разработан универсальный программный модуль с помощью инструментов пакета расширения FuzzyLogic Toolbox и встроенного командного языка системы Matlab и реализован в виде исполняемого файла данной системы.

С помощью универсального программного модуля проведены имитационные вычислительные эксперименты, в рамках которых осуществлялась проверка работоспособности предложенных алгоритмов реализации нейро-нечеткого МГУА.

Эксперименты показали, что в данные алгоритмы позволяют получить достаточно высокую точность моделирования, даже в случае существенно ограниченных объемов исходных данных и существенном характере нелинейности. Причем результаты экспериментов свидетельствуют, что в условиях недостатка исходных данных в случае наличия нелинейности более высокого порядка предложенный метод обеспечивает более высокий выигрыш в точности по сравнению с другими методами математического моделирования, в частности регрессионными и нейросетевыми. На рисунке 1 представлены результаты прогнозирования МГУА, а в таблице 1 ошибки прогнозов для функций различной степени нелинейности, полученные на обучающей выборке из 40 точек.

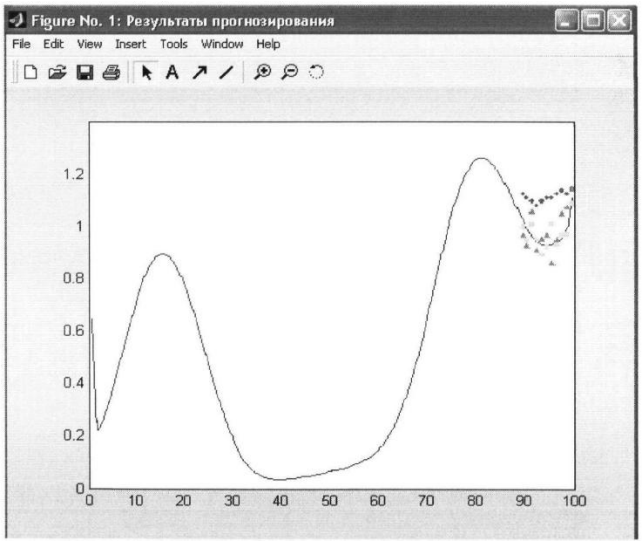


Рисунок 1 -Результаты прогноза для функции 3-го порядка нелинейности

Из приведенной таблицы, при невысокой степени нелинейности нейро-нечеткий МГУА не дает выигрыша в точности, т.к. такая функция может быть успешно аппроксимирована регрессионной зависимостью. По мере увеличения степени нелинейности, погрешность регрессионной модели возрастает, в то время как погрешность нейронной сети и нейро-нечеткой модели МГУА остается приемлемой.

Таблица 1 - Ошибки прогнозов для функций различной степени нелинейности, полученные на обучающей выборке из 40 точек

Степень нелинейности	Регрессия	Нейросеть	МГУА
1	3,7	4,8	2,6
2	12,3	7,6	2,8
3	23	9,2	3,1

Из таблицы видно, что с уменьшением объема обучающей выборки значительно увеличилась погрешность нейросетевой модели, погрешность же МГУА осталась на приемлемом уровне.

Разработанная архитектура предполагает возможность использования разработанного универсального программного модуля в качестве подсистемы аналитической обработки данных, предназначенной для подготовки принятия решений по управлению рисками информационной безопасности.

Список используемых источников:

1. Стиржов В.В. Крымова Е.А. Методы выбора регрессивных моделей. М.: Вычислительный центр РАН, -2010, 60 с.

2. Васильева Т.Н., Львова А.В. Применение оценок рисков в управлении информационной безопасностью// Прикладная информатика. – 2009. – № 5. – С. 68-76.

ПЛАНИРОВАНИЕ И ОПТИМИЗАЦИЯ ТОПОЛОГИИ СИСТЕМ МОБИЛЬНОЙ СВЯЗИ.

Казаков Павел Павлович – магистрант, Дробязко О.Н., д.т.н., профессор
Алтайский государственный технический университет (Барнаул)

Наблюдающееся в настоящее время бурное развитие отрасли мобильной связи, наряду с другими тенденциями, характеризуется быстро расширяющимся спектром новых услуг и технологий. Универсальная Система Мобильной Связи (UMTS) создавалась с целью предоставления абоненту широкого спектра дополнительных услуг, таких как : видеоконференции по мобильному телефону, доступ в Интернет, услуг, связанных с определением местоположения пользователя. Однако, в связи с использованием в UMTS нового типа радиоинтерфейса (WCDMA), возникает ряд технических проблем. Причина этого заключается в необходимости учета множества особенностей, не рассматривавшихся в сетях GSM. К таким особенностям относится смешанный тип трафика с различной скоростью передачи данных, несимметричная загрузка прямого и обратного каналов, требования к качеству для различных услуг.

В данной работе мы будем рассматривать, и изменять параметры только для одной антенны в секторе 1 – диапазона 2100 МГц (UMTS).

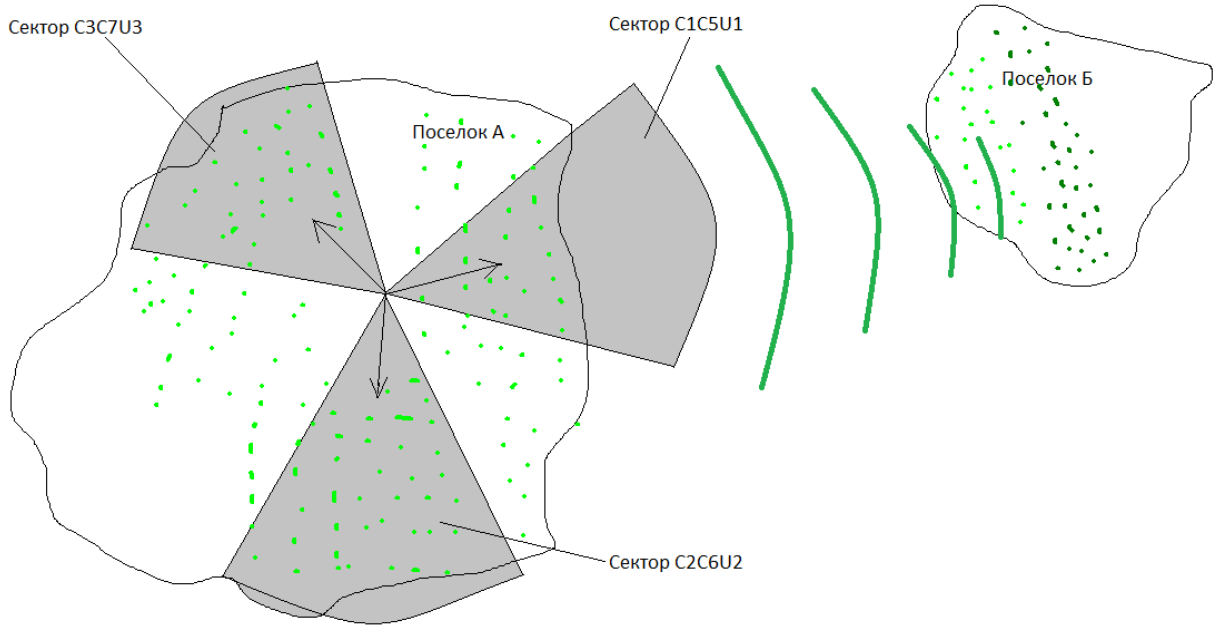


Рис. 1 Схематичное представление обслуживания территории базовой станцией.

На рис. 1. изображена топология, характерная в нашем крае: расположение секторов планируется с учётом покрытия дальних жилых территорий. В отдаленных от БС населенных пунктах при получении качественных услуг связи в стандарте 2G (GSM 900/1800), население активно начинает пользоваться интернет тарифами в 2G(GPRS/EDGE), а также в 3G(WCDMA), последние же по архитектурным особенностям не могут обеспечивать данную территорию стабильно уверенным уровнем сигнала.

После некоторого времени сигнал 3G может вовсе пропасть. Это связано с особенностями построения архитектуры WCDMA: происходит так называемое «схлопывание соты», в следствии чего энергия дальних абонентов, создающих большую интерференцию, перераспределяется на абонентов, находящихся в лучших радиоусловиях(ближней зоне). На соте при этом происходят обрывы(drop), которые

являются одним из ключевых показателей качества. При этом у абонентов возрастает недовольство сетью, увеличивается количество жалоб.

Параметры антенны имеют наибольшее влияние как на интерференционную ситуацию, так и на общее ухудшение параметров в сети сотовой связи. Кроме высоты подвеса антенны и типа диаграммы направленности, может производится настройка таких параметров, как азимут и угол наклона антенн. Следует отменить, что изменение высот подвеса антенн с целью оптимизации сети является нецелесообразным решением, поскольку кроме дополнительных монтажных работ требуется переоформление разрешений на эксплуатацию радиоэлектронных средств. Изменение азимута антенн в свою очередь также требует переоформления разрешений, поэтому является не лучшим решением, однако является менее затратным по времени и финансам.

Таким образом, в настоящей работе оптимизация сети основана на изменении типа антенны, угла наклона антенны и логических параметров ячейки.

Для достижения поставленной цели в данной работе используется три правила управления параметрами радиоподсистемы при оптимизации сети UMTS:

1) Увеличение емкости сети достигается путем изменения углов наклона антенн и значений мощности пилот-каналов – «CPICH + TILT»
2) Увеличение емкости сети достигается путем изменения только значений мощности пилот-каналов ячеек сети «CPICH only»;
3) Увеличение емкости сети достигается путем изменения значений мощностей пилот канала в соответствии с углом наклона антенн и с учетом свойств диаграммы направленности антенны в вертикальной плоскости – «CPICH=f(TILT)»

В нашем случае, то что мы имеем сейчас, изменяя параметры мощности и углы наклона антенны, будут влиять на всех абонентов сразу, так как у имеющейся антенны «широкая» диаграмма направленности(ДН) и сигнал «покрывает» большую территорию. Это приводит к тому, что много абонентов ближней зоны могут оказаться под управлением в этой ячейке. В связи с этим зона покрытия в «часы пик» будет уменьшаться, что сведет на нет все исследования и эксперименты по расчёту мощности для дальних зон, так как у них даже при оптимальных параметрах мощности пилот-канала и угла наклона антенн не будет сети 3G.

Чтобы минимизировать фактор влияния абонентов ближней зоны на абонентов дальней зоны, можно провести реконфигурацию, и разделить имеющейся сектор на 2 сектора, и вместо одной антенны с ДН=65 градусов установить 2 антенны с узконаправленными ДН=32. И только после этого необходимо подобрать оптимальные значения мощности и угол наклона антенны.

В данном случае, у нас есть перечень изменяемых параметров. Для того, чтобы получить наилучшие показатели, мы должны просчитать результат для каждого из варьируемых параметров, а также должны спрогнозировать эффективность обеспечения связи, как на определенной территории, так и на заданном множестве абонентов, анализируя и используя существующие методы такие как: генетический метод, метод отжига, многофакторный эксперимент, а также метод экспертной оценки. Для верификации полученных данных мы можем использовать несколько вариантов:

Моделирование.

Моделирование производится на геоинформационной системе Asset Aircom, таким путем мы можем задать параметры антенны(тип антенны, высоту, азимут, угол наклона, мощность пилот-канала, данный способ получения спрогнозированных параметров мы можем применять в любом случае.

Физический эксперимент.

Физический эксперимент состоит в следующем, - каждую неделю в течении месяца, мы меняем параметры для данного сектора: мощность пилот-канала (CPICH) и угол наклона антенны. После каждого изменения анализируем статистику: количество обрывов, жалоб и т.д. Однако данный метод неприемлем из-за своего растяжения во времени и противоречит регламентам компании «О проведении работ на сети».

Комбинированный метод.

Комбинированный метод состоит в том, чтобы провести ряд экспериментов в геоинформационной системе и смоделировать тем самым все значения высот, мощностей и внутренних углов антенн. После этого выбрать значения, при которых количество абонентов с определенным сервисом будет выше, а предполагаемое количество обрывов на сети будет меньше. В соответствии с результатами моделирования проводить физическое изменение оборудования: менять параметры мощности(CPICH) на контроллере, а также изменять угол наклона антенны при этом параллельно проводить измерения в поселке Б.

Используя вышеперечисленные методы, можно с определенной вероятностью спрогнозировать, уровни напряженности поля на определенной территории, количество, а также качество предоставляемых сервисов по технологии WCDMA.

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ СПОСОБОВ ПРОЕКТИРОВАНИЯ ПРОГРАММНОГО И АППАРАТНОГО ОБЕСПЕЧЕНИЯ КАРДИОЛОГИЧЕСКИХ ДИАГНОСТИЧЕСКИХ КОМПЛЕКСОВ

Кайгородов А.В. – аспирант, Якунин А.Г. – д.т.н., проф.
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Современная электрокардиография располагает большим выбором средств системного (компьютерного) анализа. Применение таких средств в электрокардиографической диагностике позволяет проводить цифровую обработку и картирование биоэлектрических потенциалов сердца [2]. Современные вычислительные системы, являются ли они высокопроизводительными серверами или маломощными мобильными телефонами, все требуют повышения энергоэффективности. А рост интереса к «системам на кристалле» (SOC) придает все большее значение созданию широкого спектра устройств на одной микросхеме, из высокопроизводительных транзисторов с большой энергоэффективностью. Одной из таких микросхем является ADS1298 - фронтэнд для кардиографии, выпущенный в феврале этого года компанией Texas Instruments.

В данной микросхеме реализованы специфические функции, характерные для измерения сигналов биологического происхождения (таких как ЭКГ или ЭЭГ). Эта интегральная схема включает в себя все такие аналоговые компоненты, как инструментальные усилители, аналоговые фильтры, необходимые для построения прибора медицинской направленности, а также встроенный 24-битный аналогово-цифровой преобразователь.

ADS1298 способен преобразовывать одновременно до восьми входных каналов со скоростью 32000 выборок в секунду для каждого из них. Каждый канал имеет разрешение вплоть до 24 бит и индивидуальные настройки усиления в диапазоне от 1 до 12. Самое высокое разрешение предоставляется только до частоты дискретизации в 8 кГц на канал и уменьшается до 19 бит при частоте дискретизации в 16 кГц и до 17 бит при 32 кГц. Данная микросхема, хоть и способна работать с биполярным питанием, всё же рекомендуется использовать однополярное питание, диапазон которого лежит в пределах от 2,8 до 5,25В, а подавление синфазной помехи составляет 115dB. Для связи с внешним миром используется последовательный периферийный интерфейс (SPI), который позволяет управлять устройством с помощью микроконтроллера [6].

ADS1298 имеет низкое токопотребление (около 1 мА в состоянии ожидания команд). Исследованное потребление тока представлено в таблице 1.

Количество каналов	Частота дискретизации		
	4 кГц	8 кГц	16 кГц
0	1 мА	1 мА	1,1 мА
1	1,3 мА	1,3 мА	1,3 мА
2	1,57 мА	1,57 мА	1,57 мА
4	2,15 мА	2,16 мА	2,16 мА
8	3,23 мА	3,31 мА	3,5 мА

Таблица 1. Потребление тока при 3,3В

Отличительной особенностью электрофизиологических сигналов является сложная взаимосвязь процессов различной природы и принципиальная неустранимость помех при исследовании конкретного органа. Это обстоятельство ограничивает разрешающую способность любых методов измерения параметров. По современным представлениям, конечной целью исследования тонкой структуры биоэлектрических сигналов является достижение более глубокого понимания причинных механизмов, вызывающих какие-либо процессы. При съеме биоэлектрических сигналов возникает комплекс помех и искажений, обусловленных различными причинами. Наибольшее влияние во всех без исключения исследованиях оказывают следующие виды помех:

1) эффект поляризации электродов, приводящий к смещению нулевого уровня сигнала;

2) квазигармонический процесс, представленный составляющими наводки напряжения промышленной частоты;

3) артефакты смещения электродов, создающие выбросы случайной амплитуды и длительности;

4) электрофизиологические помехи (тремор).

Электрокардиограммой считается составляющая поверхностных потенциалов, обусловленная электрической активностью сердца. Остальные составляющие потенциалов рассматриваются как помехи. Собственно, электрокардиографический сигнал представляет собой последовательность кардиоциклов, повторяющихся через определенные интервалы времени. Каждый отдельный кардиоцикл представляется квазидетерминированной функцией сложной формы, последовательные компоненты которого имеют стандартные буквенные обозначения. Помехи искажают сигнал электрокардиограммы (рисунок 1).

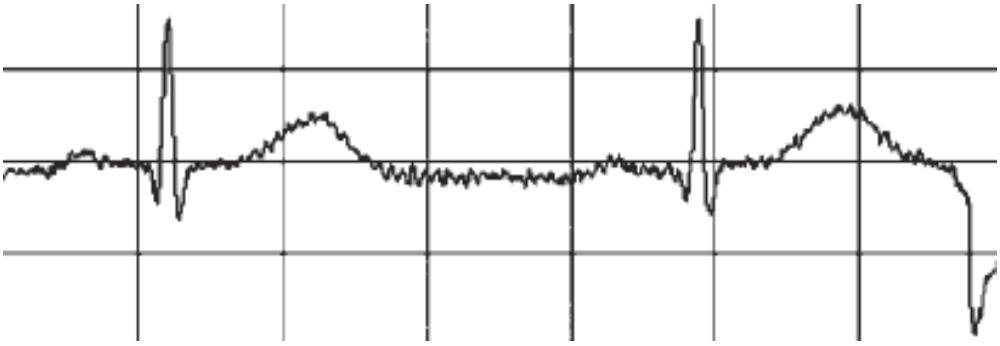


Рисунок 1. Кардиограмма с помехами

Основная мощность QRS-комплекса сосредоточена в области частот 2–20 Гц с наличием максимума на частоте около 15 Гц. Спектр ЭКГ-сигнала может изменяться в зависимости от морфологии сигнала. Спектр шумов от мышц является неоднородно распределенным и характеризуется значительной вариабельностью. Рассмотрение соответствующих зависимостей показывает, что при благоприятных условиях съема компенсация помех поляризации и наводки не представляет особых сложностей, для чего существует ряд эффективных методов, и в основном помеха представлена в виде случайного процесса,

создаваемого электрической активностью мышц, спектр которого имеет значительное перекрытие со спектром ЭКГ.

Использование современных решений типа SOC позволяет уменьшить энергопотребление, и тем самым интегрировать в автономные системы новые модули для выделения дополнительных диагностических признаков. Так, используя данные, полученные с акселерометра, можно адаптировать методы велоэргометрии для исследования сердца в повседневной жизни человека, а также создать новые методы диагностики за счет учета двигательной активности и ее взаимосвязи с сердечным ритмом.

Большинство современных мобильных устройств обладает хорошей поддержкой акселерометра и относительной простотой программного интерфейса (API) при использовании акселерометра. Однако использование API предоставляет доступ только к основным возможностям, но если необходимо на основе данных, полученных с акселерометра анализировать двигательную активность, или, например, жесты пациента, то готовых программных решений для этих целей в мобильных устройствах нет. Однако задача идентификации сигналов с акселерометра упрощается благодаря решениям сторонних разработчиков и их библиотекам. Так, на Windows Phone уже создана библиотека жестов встряски (или шейк-жестов), и акселерометр устройства способен определять движение телефона в трёхмерном пространстве (по трём осям – x, y, z).

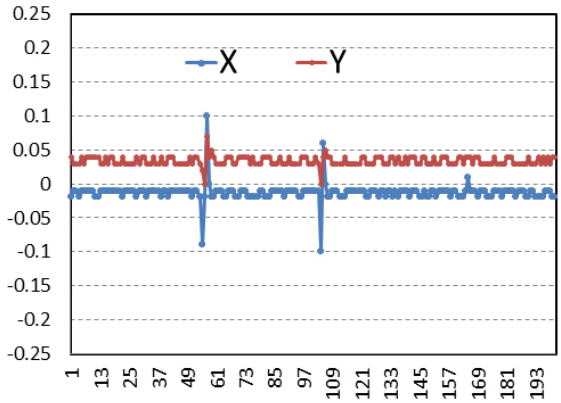


Рисунок 2. Данные акселерометра по осям x и y для двух постукиваний по левому краю устройства с незначительным движением устройства.

На этапе проектирования программного обеспечения кардиологического комплекса возникает необходимость в переносимости алгоритмов обработки данных между различными платформами. Кроссплатформенность может достигаться различными средствами. Одним из простых способов является написание библиотеки на языке C++ с последующей инициализацией данной библиотеки исполняющей средой. В случае с ОС Anrdroid управляющей средой является Java-машина (Dalvik), и инициализация библиотеки производится средствами JNI (Java Native Input), которая, при необходимости, пересылает вызовы C++ кода в Java и наоборот. Для iOS основным языком разработки является Objective-C, который представляет собой надмножеством языка Си, поэтому проблем с интеграцией библиотек, как правило, не возникает.

Следует отметить, что в библиотеке должна быть полная реализация алгоритмов обработки сигналов, т.к. эта часть является общей для всех платформ. Кроме того, в этой библиотеке должен присутствовать ряд абстрактных классов, выполняющих обмен данными с устройством, реализация которых была бы специфична для каждой платформы. Применение платформозависимого кода должно быть сведено к минимуму, и, в случае применения, должно быть определено специальными директивами препроцессора для компиляции одних и тех же исходных файлов под различные платформы.

Широкое применение методов прикладного анализа случайных процессов дает возможность повысить информативность результатов измерений параметров сигналов.

Накопленный клинический и экспериментальный материал позволяет в некоторых случаях по-новому подойти к решению традиционных проблем, а зачастую существенно расширить их возможности. Исследование тонкой структуры регистрируемых сигналов является основой для развития принципиально новых подходов к диагностике патологий и контролю эффективности лечебно-восстановительных процедур.

Список используемых источников:

1. Автоматический анализ ЭКГ: проблемы и перспективы // Здравоохранение и медицинская техника, №1, февраль, 2004.
2. Мурашко В.В., Струтынский А.В. Электрокардиография. М.: Медицина, 1987. 256 с..
3. Компани-Бош Э., Хартманн Э. Электрокардиограф на базе микроконвертора //Компоненты и технологии, №6, 2004.-104-108.
4. Суворов А.В. Клиническая электрокардиография. – Нижний Новгород. Изд-во НМИ,1993
5. Ширяев В.В. Компьютерные измерительные средства (КИС): Учебное пособие
6. Texas Instruments. ADS1298 datasheet.
7. Аналогово-цифровой преобразователь // Компоненты и технологии, №6, 2008.-85-89.

ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ КАК СРЕДСТВО ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ

Кириченко М. Е. – студент, Шарлаев Е. В. – доцент, к.т.н.
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Виртуальные частные сети (VPN) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет).

VPN функционируют на базе существующей общедоступной сетевой инфраструктуры, в роли которой обычно используется Internet. Именование «виртуальная» применяется по той причине, что на основе физических подключений формируется логическая связь. При объединении сетей через Internet, возникает вопрос о безопасности передачи данных, поэтому существует необходимость в механизмах позволяющих обеспечить конфиденциальность и целостность передаваемой информации. Система безопасности VPN защищает всю информацию от несанкционированного доступа: информация передается в зашифрованном виде, прочитать полученные данные может лишь легитимный пользователь обладающий ключом шифрования.

Средства VPN решают следующие основные задачи:

Обеспечение конфиденциальности – это гарантия того, что в процессе передачи данных по каналам VPN эти данные не будут просмотрены посторонними лицами.

Обеспечение целостности – это гарантия сохранности передаваемых данных. Никому не разрешается менять, модифицировать, разрушать или создавать новые данные при передаче по каналам VPN.

Обеспечение доступности – это гарантия того, что средства VPN постоянно доступны легитимным пользователям.

При подключении локальной сети к открытой сети возникают угрозы безопасности двух основных типов:

– несанкционированный доступ к корпоративным данным в процессе их передачи по открытой сети;

– несанкционированный доступ к внутренним ресурсам корпоративной локальной сети, получаемый злоумышленником в результате несанкционированного входа в эту сеть.

Защита информации в процессе передачи по виртуальной частной сети основана на выполнении следующих основных функций:

- аутентификации взаимодействующих сторон;
- криптографическом закрытии (шифровании) передаваемых данных (для обеспечения целостности и конфиденциальности информации);
- авторизации (проверке подлинности и целостности доставленной информации).

Для этих функций характерна взаимосвязь друг с другом. Их реализация основана на использовании криптографических методов защиты информации.

Объектом работы является сегмент сети лечебно-профилактического учреждения (ЛПУ). В целях повышения уровня защищенности объекта и выполнения требований законодательства, возникла необходимость увеличения уровня сетевой безопасности. Данную задачу, представлялось возможным, решить при помощи внедрения на объекте защиты, защищённой виртуальной частной сети на баз технологии VipNet.

Выбранный комплекс, включает в себя программные и программно-аппаратные средства защиты информации. Он предназначен для объединения в единую защищенную виртуальную частную сеть произвольного числа рабочих станций, мобильных пользователей и локальных сетей. Данное объединение обеспечивает между пользователями системы защищённый обмен конфиденциальной информацией, который достигается шифрованием предаваемого между узлами трафика.

Целью работы являлась разработка защищённой виртуальной частной сети ЛПУ на базе технологии VipNet.

В рамках работы необходимо было решить следующие задачи:

- произвести оценку угроз;
- выполнить анализ информационных потоков учреждения;
- проанализировать существующую структуру сети предприятия;
- осуществить анализ существующих продуктов организации VPN;
- обосновать выбор средства защиты;
- подобрать необходимые компоненты для построения защищённой виртуальной частной сети.

В результате выполнения работы, была разработана и построена защищённая виртуальная частная сеть сегмента сети ЛПУ на базе технологии VipNet. Для достижения поставленной цели были приобретены и настроенные следующие проигранные и программно – аппаратные средства защиты:

- ViPNet Administrator (1шт.);
- ViPNet Coordinator HW1000 (1 шт.);
- ViPNet Coordinator (Linux) (1 шт.);
- ViPNet Client (20 шт).

Разработанная виртуальная частная сеть должна успешно противостоять угрозам информационной безопасности, соответствовать требованиям законодательства в области защиты информации и удовлетворять потребностям организации.

Список используемых источников:

1) VPN - виртуальные частные сети [Электронный ресурс].– Электрон. дан. – Режим доступа: http://www.price.od.ua/articles.phtml?id=72.

2) Задачи VPN [Электронный ресурс].– Электрон. дан. – Режим доступа: http://pautina34.ru/?p=311.

3) Виртуальные частные сети (VPN) [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.infotecs.ru/solutions/vpn.

ПРИМЕНИЕ DMZ-ЗОНЫ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ДОМАШНИХ WEB-РЕСУРСОВ

Киселев И.В. – студент, Шарлаев Е.В. – к.т.н, доцент каф. ВСИБ
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Информационные технологии с каждым годом становятся все доступней для простого обывателя, а грамотность в сфере IT - технологий среднестатистического пользователя неуклонно возрастает. Встречаются случаи, когда в Интернете появляются проекты различной сложности и назначения, созданные не только серьезными крупными компаниями с большим бюджетом, но и обычными людьми, вдохновленными только собственным энтузиазмом. Рождаются эти проекты в домашней обстановке и, как правило, впервые становятся доступны для пользователей сети Internet при посещении домашней сети создателя проекта. Становиться уместным вопрос: Как защитить своё детище, а вместе с ним и домашнюю локальную сеть от неизбежных атак из интернета?

Наиболее дешевым и доступным способом защиты представленной и подобных систем является создание демилитаризованной зоны. Демилитаризованная зона (ДМЗ или DMZ) это технология обеспечения защиты информационного периметра, при которой серверы, отвечающие на запросы из внешней сети, находятся в особом сегменте сети и ограничены в доступе к основным сегментам с помощью межсетевого экрана (файрвола), с целью минимизировать ущерб при взломе одного из общедоступных сервисов, находящихся в ДМЗ.

В зависимости от требований к безопасности, ДМЗ может организовываться одним, двумя или тремя файрволами. Конфигурация с одним файрволом представлена на рисунке 1.

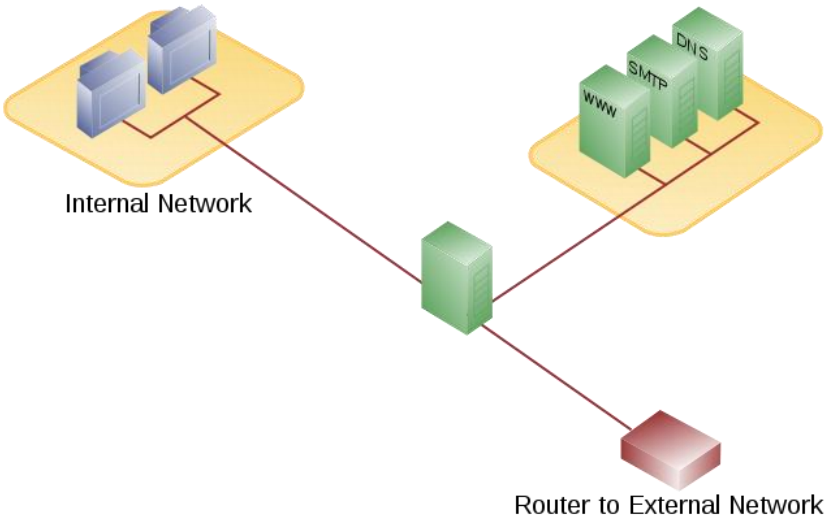


Рисунок 1. Конфигурация с одним файрволом

Простейшей (и наиболее распространённой) схемой является схема, в которой ДМЗ, внутренняя и внешняя сеть подключаются к разным портам маршрутизатора (выступающего в роли файрвола), контролирующего соединения между сетями. Подобная схема проста в реализации, требует всего лишь одного дополнительного порта. Однако в случае взлома (или ошибки конфигурирования) маршрутизатора сеть оказывается уязвима напрямую из внешней сети.

В конфигурации с двумя файрволами (см. рис. 2) ДМЗ подключается к двум маршрутизаторам, один из которых ограничивает соединения из внешней сети в ДМЗ, а второй контролирует соединения из ДМЗ во внутреннюю сеть. Подобная схема позволяет минимизировать последствия взлома любого из файрволов или серверов,

взаимодействующих с внешней сетью — до тех пор, пока не будет взломан внутренний файрвол, злоумышленник не будет иметь произвольного доступа к внутренней сети.

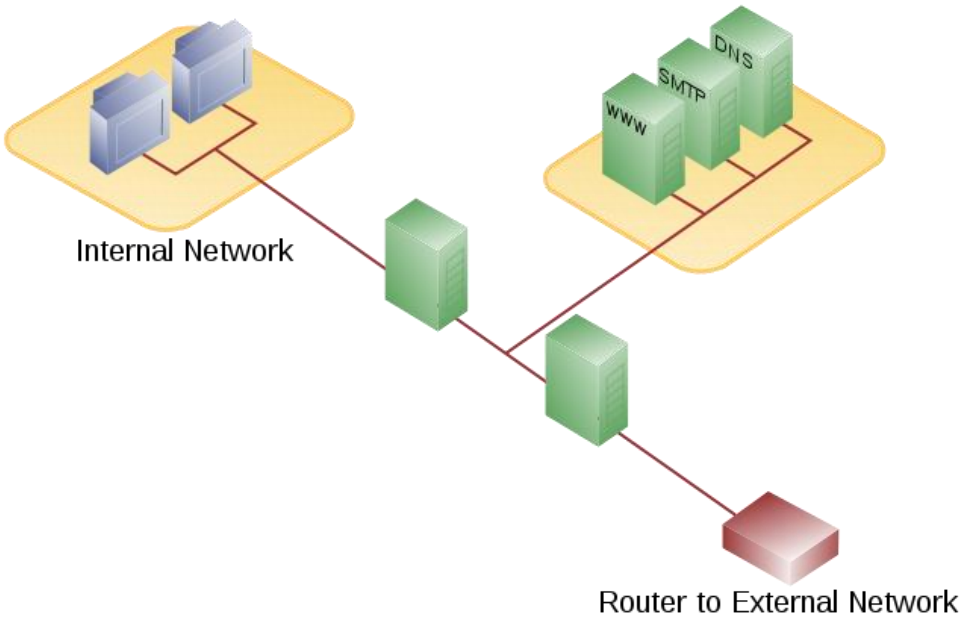


Рисунок 2. Конфигурация с двумя файрволами

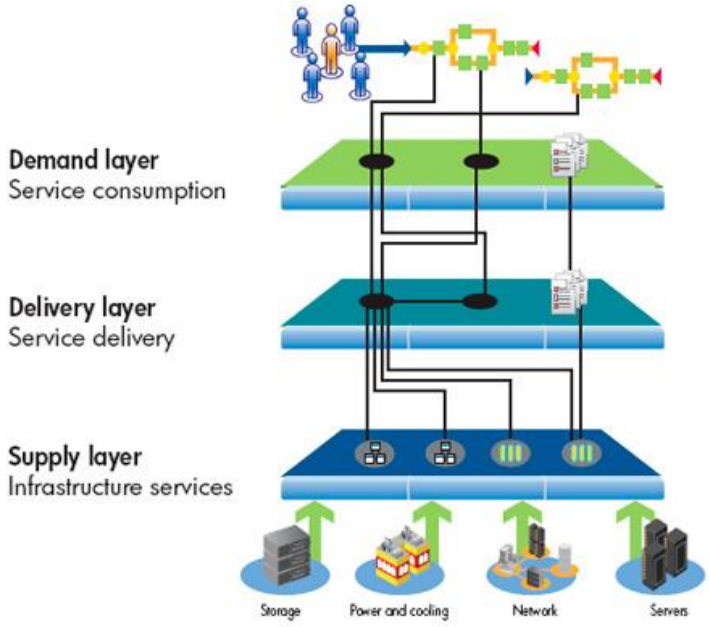
На сегодняшний день на рынке сетевого оборудования существует огромный выбор моделей сетевых устройств, позволяющих организовать подобную топологию сети посредством прошивки самого устройства, что является огромным плюсом: при наличии такой возможности заранее заложенной в устройство – не нужно разбираться в тонкостях устройства вычислительных сетей или иметь специальное образование, достаточно просто активировать необходимую функцию в имеющемся в наличии маршрутизирующем устройстве. Таким образом, любой обладатель «домашнего» интернет-проекта может защитить свою локальную сеть от большинства атак на неё направленных.

РАЗРАБОТКА ПРОЕКТА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ КОНФИГУРИРОВАНИЯ РЕШЕНИЙ НА ОСНОВЕ SaaS ДЛЯ ООО «ЦЕНТР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Кожевников М.А. – студент, Чугунов Г.А. – старший преподаватель
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Облачные технологии – это технологии обработки данных, в которых компьютерные ресурсы предоставляются Интернет-пользователю как онлайн-сервис. Слово «облако» здесь присутствует как метафора, олицетворяющая сложную инфраструктуру, скрывающую за собой все технические детали. Это одна большая концепция, включающая в себя много разных понятий, предоставляющих услуги. Самое важное то, что облачные системы являются сервис-ориентированными: их основная задача — обеспечить потребителя качественной услугой. Соответственно, выделяется несколько моделей предоставления услуг: инфраструктура как услуга (IaaS), платформа как услуга (PaaS), ПО как услуга (SaaS) — предоставление программного обеспечения. Согласно SaaS-концепции вы платите не единовременно, покупая продукт, а как бы берете его в аренду. Причем, используете ровно те функции, которые вам нужны. В облачной модели вычислений ИТ-возможности доставляются потребителям с помощью Интернета или веб-технологий. Наиболее важными

из них являются портал самообслуживания, пул разделяемых ресурсов, автоматическое выделение, изменение и освобождение этих ресурсов и повсеместный доступ. Например, HP CloudSystem обеспечивает эти возможности, используя трехуровневую архитектуру.

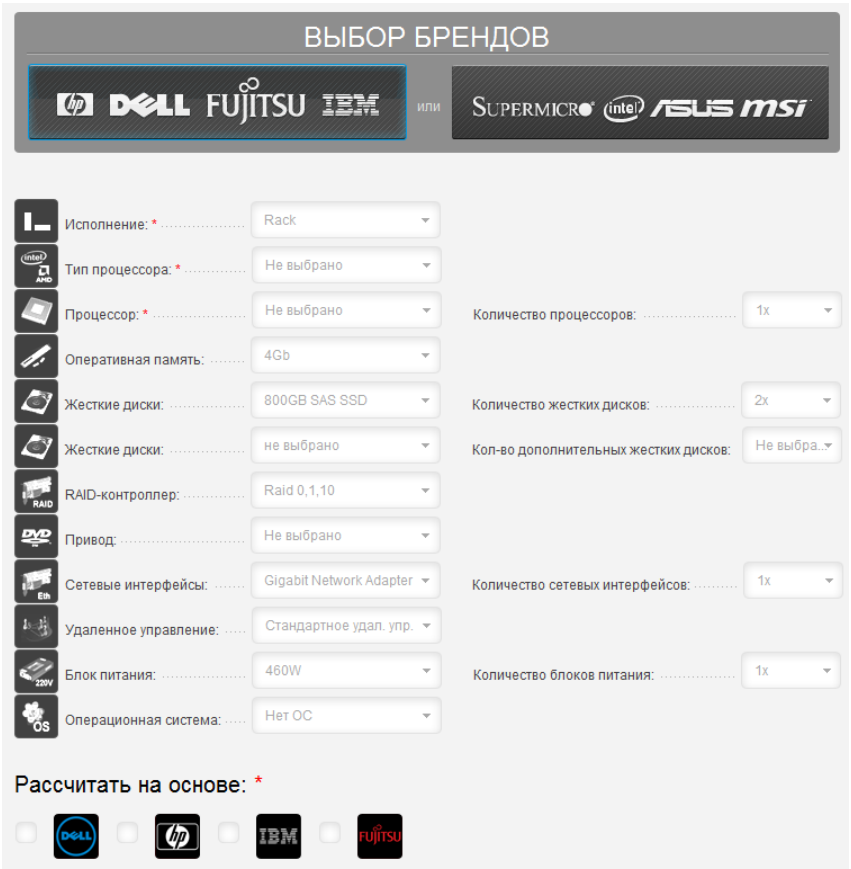


Базовый уровень обеспечения (supply) содержит все инфраструктурные сервисы — это физические и виртуализированные ресурсы. Уровень доставки (delivery) обеспечивает приложения как сервис, а уровень запроса (demand) содержит порталы самообслуживания и является «местом», где сервисы действительно потребляются конечными пользователями или подписчиками.

Вообще, для введения облачного решения в компании клиента необходимо для начала такое решение разработать и сконфигурировать. Лучшим решением для этого становится конфигуратор, так как он за короткое время позволяет разработать решение, которое в дальнейшем может быть внедрено специалистами.

На данный момент существует множество конфигураторов для серверного оборудования, калькуляторов, помогающих рассчитать затраты на покупку программного обеспечения, но их главным недостатком является одно направленность, они подходят только для решения одной типовой задачи. Основной задачей было поставлено разработать конфигуратор, способный решать более широкие задачи, объединяющие в себе задачи нескольких конфигураторов. Данная задача решалась поэтапно. На начальном этапе было решено выбрать среду разработки и сделать конфигуратор выборки серверного оборудования, а далее расширить его до возможности выбора для него программного обеспечения.

На данный момент большинство компаний имеет свои конфигураторы, размещенные на собственных сайтах, так как это очень удобно для клиентов плохо разбирающихся в программных или аппаратных продуктах. Однако такие конфигураторы имеют один значительный минус, они предназначены для решения только одной задачи, и, следовательно, не являются универсальными.



На рисунке предоставлен конфигуратор серверного оборудования, причем конфигуратор этой компании отличается тем, что он выдает решения на основе оборудования разных компаний, таких как HP, Dell, IBM, Asus, Intel и т.д. Данный конфигуратор отлично подходит для клиентов, желающих приобрести сервер, они могут сравнить разные ценовые категории серверов и выбрать подходящий. Входными данными данного конфигуратора являются исполнение (установка в стойку или нет), тип процессора и количество процессоров, оперативная память, марка жестких дисков и их количество, тип RAID-контроллера, сетевые интерфейсы, блок питания, операционная система и т.д. однако данный конфигуратор решает только одну задачу.

Вообще создание конфигуратора преследует определенные цели:

- Создание оптимального типового решения на основе желаний заказчика
- Экономия времени и затрат на разработку проекта решения
- Возможность конфигурирования решений любой сложности
- Огромная целевая аудитория

В качестве хранения данных следует использовать базу данных, так как это наиболее удобный способ оперирования и работы с данными. Для работы с базами данных используются системы управления базами данных (СУБД). На данный момент самыми распространенными СУБД являются клиент-серверные СУБД. Клиент-серверная СУБД располагается на сервере вместе с БД и осуществляет доступ к БД непосредственно, в монопольном режиме. Все клиентские запросы на обработку данных обрабатываются клиент-серверной СУБД централизованно. Недостаток клиент-серверных СУБД состоит в повышенных требованиях к серверу. Достоинства: потенциально более низкая загрузка локальной сети; удобство централизованного управления; удобство обеспечения таких важных характеристик как высокая надёжность, высокая доступность и высокая безопасность. Примерами клиент-серверных СУБД являются Oracle, MS SQL, PostgreSQL и MySQL. Для разработки собственного конфигуратора была выбрана MySQL, так как эта система управления базами данных отвечает требованиям, предъявляемым к ней (решение

для малых и средних приложений). Так же она является одной из самых распространенных на рынке в наши дни, и, наконец, данная система является свободно распространяемой, что тоже играет важную роль.

Для возможности размещения конфигуратора в сети Интернет было решено, что он должен разрабатываться в качестве веб-приложения. В настоящее время самым распространенным языком для разработки веб-приложений является язык PHP. Это скриптовый язык, в настоящее время поддерживается подавляющим большинством хостинг-провайдеров и является одним из лидеров среди языков программирования, применяющихся для создания динамических веб-сайтов. Преимуществом данного языка перед аналогами, например ASP.NET, является распространенность, на данный момент скриптовый язык PHP – один из самых популярных и, как было сказано раньше, поддерживается большинством хостинг-провайдеров. Так же на распространение данного языка влияет его большая доступность, открытость кода и простота.

Из вышесказанного следует, что модель конфигуратора включает в себя более широкие возможности по сравнению с аналогами, а также имеет возможность охватить большую аудиторию клиентов.

Список используемых источников:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПБ.: Питер,2010. – 944с.:ил.

2. Gillam, Lee. Cloud Computing: Principles, Systems and Applications / Nick Antonopoulos, Lee Gillam. — L.: Springer, 2010

3. Облачные решения/технологии. Обзор статей [Электронный ресурс] // Режим доступа: http://ecm-journal.ru/post/Oblachnye-reshenijatekhnologii-Obzor-statejj.aspx

К ВОПРОСУ О ПРИМЕНЕНИИ СТАНДАРТОВ ЭЛЕКТРОННОЙ ПОДПИСИ В РОССИИ И ЗА РУБЕЖОМ.

Красников И.А. – студент, Пивкин Е.Н. – к.т.н., доцент

Одним из ключевых факторов, препятствующих развитию и внедрению информационных технологий, является проблема однозначной идентификации лица, подписавшего электронный документ. Для решения данной задачи на сегодняшний день успешно используется электронная подпись (ЭП).

В качестве объектов исследования были взяты стандарты ЭП России, Германии и США.

В России действует обновлённый ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» [6].

В Германии на 2013 год «Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen» приняло каталог алгоритмов ЭП. Основополагающим является ECGDSA (The Elliptic Curve German Digital Signature Algorithm), принятый в декабре 2005 [10].

В США используется стандарт DSS (Digital Signature Standard) принятый NIST в 2009, который описывает алгоритм ЭП ECDSA (The Elliptic Curve Digital Signature Algorithm) [7].

Сравнительный анализ стандартов ЭП проводился по следующим критериям:

1. типы вычислительных задач, на которых основаны алгоритмы;
2. используемые алгоритмы хеширования;
3. процедуры формирования и проверки подлинности ЭП;
4. международная стандартизация алгоритмов;
5. законодательная база.

1 критерий. Существует два типа вычислительных задач, на которых может быть основана ассиметричная криптография: дискретного логарифмирования и факторизации сложных чисел. Во всех трёх странах используются алгоритмы, основанные на проблеме

дискретного логарифмирования в группе точек эллиптической кривой [1]. Это даёт ряд преимуществ, самым важным из которых является возможность работы алгоритма на значительно меньших полях. Надлежащий выбор типа эллиптической кривой позволяет многократно усложнить задачу взлома схемы ЭП. Это позволит сократить длины открытого ключа в 4 раза (биты), что положительно отразится на скорости криптографических преобразований [8].

2 критерий. В США стандарт DSS включает в себя не только комплекс криптографических алгоритмов для ЭП, но и алгоритм хеширования информации «Secure Hash Algorithm Version 2» (SHA-2). В зависимости от предъявляемых требований по защите, возможно использование SHA-2 в нескольких режимах, когда длина дайджеста сообщения равна 224,256, 384, 512 бит. В 2012 году NIST утвердил новый алгоритм «Keccak» (SHA-3) [11]. Появление ещё одного действующего стандарта (SHA-3) позволит увеличить гибкость выбора. Так как заложенные в SHA-2 и SHA-3 алгоритмы кардинально отличаются по своей сути, в случае выявления уязвимости в одном из них, останется возможность откатиться на другой.

В Германии используется алгоритм SHA-2 с разными длинами дайджеста сообщения. Их использование описано в «Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung» [10].

В России в 2013 году произошла смена стандарта по хешированию. ГОСТ ГОСТ Р 34.11-94 был заменён на ГОСТ Р 34.11-2012 «Стрибог». Новый ГОСТ состоит из двух хэш-функций с длинами результирующего значения в 256 и 512 бит, которые отличаются начальным внутренним состоянием и его частью, принимаемой за результат вычислений [9].

3 критерий. Процедуры формирования и проверки ЭП рассматриваемых стандартов состоят из нескольких этапов. На первом происходит генерация ключа подписи и ключа проверки. Затем к сообщению применяется хеш-функция. Следующим этапом является процедура подписи, которая включающая в себя ряд операций, применяя которые вычисляется значение электронной подписи. Исходными данными этого процесса являются ключ подписи и подписываемое сообщение, а выходным результатом – электронная подпись.

На этапе проверки подписи исходными данными являются подписанное сообщение, электронная подпись и ключ проверки. Затем следует выполнение ряда операций, в ходе которых устанавливается соответствие подписанного сообщения и цифровой подписи.

4 критерий. В 2006 году ISO/IEC был принят стандарт «14888-3 Information technology — Security techniques — Digital signatures with appendix —Part 3: Discrete logarithm based mechanisms», который включил в себя ряд наиболее надёжных алгоритмов и популярных схем ЭП, в том числе и ECDSA и ECGDSA [2]. В 2010 году в данный международный стандарт был добавлен российский ГОСТ Р 34.10-2001, являющийся предшественником действующего ГОСТа. Это событие повлекло за собой ряд положительных моментов:

- включение российского алгоритма в международный стандарт является признанием его достаточной криптографической стойкости;
- усиление международного интереса к российским алгоритмам, что позволит эффективней развиваться криптографической науке в нашей стране;
- возможность выхода российских компаний с отечественным стандартом на международный рынок.

5 критерий. В США действует общефедеральный закон об ЭП 30 июня 2000 года «Electronic Signatures in Global and National Commerce Act» [4]. Он является первым в мире принятым законом об ЭП.

Германия вторая страна мира , в которой был принят закон об ЭП от 21 мая 2001 года «Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften» [3].

В России закон об ЭП впервые был принят в 2002 году. N 1-ФЗ "Об электронной цифровой подписи". На сегодняшний день действует

усовершенствованный законопроект N 63-ФЗ "Об электронной подписи" от 6 апреля 2011 года [5].

В результате сравнительного анализа стандартов, можно сделать следующие выводы:

1. Международное сообщество активно содействует принятию и использованию стандартов ЭП, с целью развития межгосударственной и зарубежной торговли, путём удаления бюрократических препятствий для электронных сделок и принятия не дискриминационного подхода к использованию ЭП по сравнению с традиционной подписью.
2. Во всех трёх странах создана необходимая законодательная база для использования ЭП.
3. Рассмотренные стандарты ЭП основываются на одинаковых принципах ассиметричной криптографии. Наблюдается практически полное соответствие: стандарты ЭП России, США и Германии базируются на родственных модификациях схемы ЭП Эль-Гамаля с использованием эллиптических кривых. Они различаются лишь некоторыми числовыми параметрами и отдельными деталями выработки ключевой пары, вычисления и проверки подписи.
4. Можно проследить, что во всех 3 странах идёт активная работа над разработкой новых алгоритмов хеширования, и на сегодняшний день самые передовые идеи реализованы в стандартах.
5. Практическая синхронность принятия и обновления стандартов и законов об ЭП в России, Германии и США может говорить в пользу того, что государства находятся на примерно одном и том же уровне в научных исследованиях в области ассиметричной криптографии.
6. Из всей системы стандартов наиболее сильно различаются лишь стандарты хеширования. Но, несмотря на это они соответствуют предъявляемым угрозам.

Список использованных источников

1. ЭЦП [Электронный ресурс].- Электрон. текст. дан.- Режим доступа: http://ru.wikipedia.org/wiki/ЭЦП -Загл. с экрана.

2. ISO/IEC 14888-3: 2006 «Information technology — Securitytechniques — Digital signatures with appendix —Part 3: Discrete logarithm based mechanisms»
3. «Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer orschriften». Vom 16. Mai 2001
4. «Electronic signatures in global and national commerce act». Public law 106–229—june 30, 2000
5. Федеральный закон от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи".
6. ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
7. «Digital Signature Standard (DSS)». Information Technology Laboratory. National Institute of Standards and Technology Gaithersburg, MD 20899-8900. Issued June, 2009
8. ECDSA [Электронный ресурс].- Электрон. текст. дан.- Режим доступа: http://ru.wikipedia.org/wiki/ECDSA -Загл. с экрана.
9. П.А.Лебедев. «Сравнение старого и нового стандартов РФ на криптографическую хэш-функцию на ЦП и графических процессорах nvidia». Московский институт электроники и математики национального исследовательского университета. Высшая школа экономики.
10. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen).
11. Keccak [Электронный ресурс].- Электрон. текст. дан.- Режим доступа: http://ru.wikipedia.org/wiki/Keccak -Загл. с экрана.

РАЗРАБОТКА АВТОНОМНОГО КОНТРОЛЛЕРА С ETHERNET-ИНТЕРФЕЙСОМ ДЛЯ СИСТЕМЫ ТЕРМОМОНИТОРИНГА

Лузай Р.В. – студент, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Необходимость измерения температуры возникает во многих сферах деятельности человека. Температура является важнейшим параметром любого технологического процесса. Необходимость мониторинга температуры воздуха в ответственных помещениях, например в цехах и складах готовой продукции, а также допустимых температур при работе двигателей, генераторов, приводного оборудования, трансформаторов и т.д. обуславливает применение высокотехнологических решений в плане измерения температуры [1].

С развитием электроники, вычислительных систем и, в частности, с появлением технических средств, таких как микроконтроллеры и полупроводниковые датчики температуры, стало возможным создание малогабаритных устройств для решения задачи термомониторинга. Анализ полученных с их помощью данных позволяет организовывать регулирование работы инженерных систем.

Обзор существующих систем термомониторинга показал, что такие системы обладают избыточной функциональностью, которая зачастую остается невостребованной, и, как следствие, имеют высокую цену. После анализа данных недостатков было принято решение реализовать программно–аппаратный комплекс термомониторинга, основными требованиями к которому являются:

1. Наличие Web-интерфейса для возможности просмотра показаний датчиков температуры в режиме реального времени и для изменения пользовательских настроек, в том числе и сетевых настроек (IP);
2. Отправка показаний датчиков температуры в базу данных на удаленный сервер по сети Ethernet;
3. Запись значений температуры в кольцевую память, если сеть временно недоступна.

Разработанная система термомониторинга имеет следующий состав.

Микроконтроллер с управляющей программой - является главным элементом в системе. Микроконтроллер осуществляет опрос всех подключенных датчиков. В нем программно реализуется стек протоколов TCP/IP, необходимый для доступа устройства к сети Ethernet, а так же веб-интерфейс.

Датчики температуры - позволяют контролировать температуру интересуемых объектов – газов, тел, жидкостей. Датчики являются вторым по важности элементом системы термомониторинга на основе микроконтроллера.

Поскольку одной из важнейших характеристик информационно-измерительной системы является гибкость, это накладывает определенные требования на разрабатываемое устройство - система должна поддерживать достаточное количество датчиков с возможностью дальнейшего расширения. В связи с этим в данной разработке применяются цифровые интегральные датчики температуры.

Цифровые датчики объединяют на кристалле кремниевый термодатчик, аналого-цифровой преобразователь, регистры верхнего и нижнего допустимого значения контролируемой температуры, регистры конфигурации и гистерезиса, аналоговые компараторы, логику управления и реализации протоколов последовательной передачи данных (SPI, SMBus, I2C, 1-Wire, 2-Wire) и стабилизатор питания [2]. Цифровые датчики температуры обладают невысокой стоимостью, компактным исполнением и низким током потребления.

Микросхема памяти требуется в случае временного отсутствия соединения с сетью Ethernet, для того, чтобы исключить потерю показаний датчиков на этот период.

Часы реального времени нужны для привязки даты и времени к показаниям датчиков. Их настройка осуществляется через веб-интерфейс устройства.

К исполнительным устройствам относится интерфейсная микросхема, необходимая для сопряжения микроконтроллера с сетью Ethernet.

В процессе проектирования рассматривались два типовых варианта реализации устройства - на основе двух микроконтроллеров и на основе одного микроконтроллера с большей производительностью и большим объемом памяти.

Первый вариант предполагает сопряжение двух размещенных на одной печатной плате микросхем с помощью одного из подходящих промышленных интерфейсов и механизма внешних прерываний. При этом один из микроконтроллеров отвечает за связь устройства с сетью Ethernet, реализует стек протоколов TCP/IP и веб-интерфейс, а так же хранит во встроенной flash-памяти пользовательские настройки. Другой микроконтроллер взаимодействует с датчиками температуры, микросхемой реального времени и микросхемой памяти.

Второй вариант предполагает объединение описанных выше функций в одном микроконтроллере. При выборе микроконтроллера для данного варианта необходимо учесть большую вычислительную нагрузку, особенно программная реализация стека протоколов TCP/IP, и большой объем управляющей программы. При реализации данного варианта система будет иметь более простое схемотехническое устройство, однако в большинстве случаев стоимость системы будет выше.

Разработанная система термомониторинга была реализована на основе двух микроконтроллеров. Датчики температуры подключаются к шине 1-Wire, поскольку данный стандарт обеспечивает большую длину линии (до 300 метров), а для подключения датчиков в режиме паразитного питания достаточно двух проводов – сигнального и заземления [3]. Опытный образец отвечает поставленным требованиям, удобен, прост и гибок в эксплуатации и может использоваться на реальном объекте, где существует потребность термомониторинга.

Список используемых источников:

1. Температура и ее роль в нашей жизни [Электронный ресурс] // Режим доступа: http://www.ecounit.ru/artikle_62.html

2. Цифровые датчики температуры [Электронный ресурс] // Режим доступа: http://www.electronshik.ru/class/tsifrovie-datchiki-temperaturi-01050202

3. Технология 1-Wire-сетей [Электронный ресурс] // Режим доступа: http://www.elin.ru/1-Wire/

РАЗРАБОТКА МИКРОКОНТРОЛЛЕРОНОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОСВЕЩЕНИЕМ В ТЕАТРЕ

Лымарев М.П. – студент, Агапов М.П. – к.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Любой театральный спектакль – это не только сплав драматурга и актеров, но и огромная техническая поддержка, одной из составных частей которой является театральный свет.

Театральное освещение решает задачи от создания на сцене общего освещения до передачи тончайших нюансов действия и материального влияния на публику, находящуюся в зрительном зале.

Свет позволяет передать время суток или года. С его помощью легко передать время рассвета или заката, или например, сымитировать пожар. Театральное освещение может выразить и подчеркнуть характеры основных действующих лиц спектакля. Изменения освещение при появлении на сцене какого-либо героя, можно сконцентрировать на нем внимание зрителей, одновременно выразив характер этого действующего лица.

С помощью света можно передать и духовную атмосферу спектакля (тревогу, мир, войну и т. д.). Театральное освещение дает возможность зрительно увеличить пространство сцены и, если требуется разделить ее на отдельные участки.

Все это делает театральное освещение не только важным элементом современного театра, но и видом самостоятельного искусства.

С развитием технического прогресса развивалось и театральное освещение. В настоящее время – это сложная многоуровневая система, управляемая при помощи компьютеров. В последние годы происходит полномасштабная замена устаревшего театрального оборудования на новое. Однако современные системы управления освещением зачастую очень дороги, и могут быть неподъемными для некоторых театров. В связи с этим появляется необходимость разработки более дешевой системы управления освещением, обеспечивающую базовую функциональность театральному оборудованию

При разработке микроконтроллерной системы управления освещением в театре решались следующие задачи:

- Управление прожекторами из единой точки(включение/выключение, поворот вокруг осей x и y);
- Контроль доступности удаленных прожекторов;
- Возможность подключения нового оборудования без модификации прошивки микроконтроллера и управляющей программы;

Рис. 1. – Структурная схема устройства

Система управления представляет собой платы управления с микроконтроллерами и персональный компьютер, оснащенной программой.

Взаимодействие между компьютером и платой контроля осуществляется в виде обмена транзакциями: компьютер отправляет микроконтроллеру команду либо читает данные, подготовленные блоком контроля и передачи данных. Если микроконтроллер получает команду, он формирует пакет, добавляя к данным старт- и стоп-биты, адрес устройства, которому предназначена команда и отправляет этот пакет блоку управления прожектором. В ответ на пакет, если он успешно распознан, блок управления прожектором отправляет свой пакет с флагом успешного завершения операции. В том случае, если ответа нет, микроконтроллер в блоке контроля и передачи данных трижды дублирует команду, и, в случае неудачи, отправляет сообщение об ошибке программе на компьютере.

Рис. 2. – Структура команды

Устройство спроектировано на базе микроконтроллера ATmega8 фирмы Atmel. Данный контроллер содержит достаточный объем flash-памяти – 8 Кбайт и работает на частоте 16 МГц. Поскольку микроконтроллер может обеспечить необходимую скорость передачи данных, и передаваемый трафик небольшой, производительности микроконтроллера будет хватать для поставленных целей.

Для обмена данными между блоком контроля и передачи данных и ПО на компьютере используется интерфейс USB, что позволяет подключаться напрямую к ПК без использования разнообразных переходников.

Блок контроля и передачи данных спроектирован как HID – устройство, что позволяет использовать его без установки каких – либо драйверов.

Обмен данными между блоком контроля и передачи данных и блоком управления прожектором осуществляется по интерфейсу RS-232 на основе универсального асинхронного приемо-передатчика. Так же в схемы плат заложена возможность реализации протокола DMX, позволяющего создать сеть из последовательно соединенных устройств

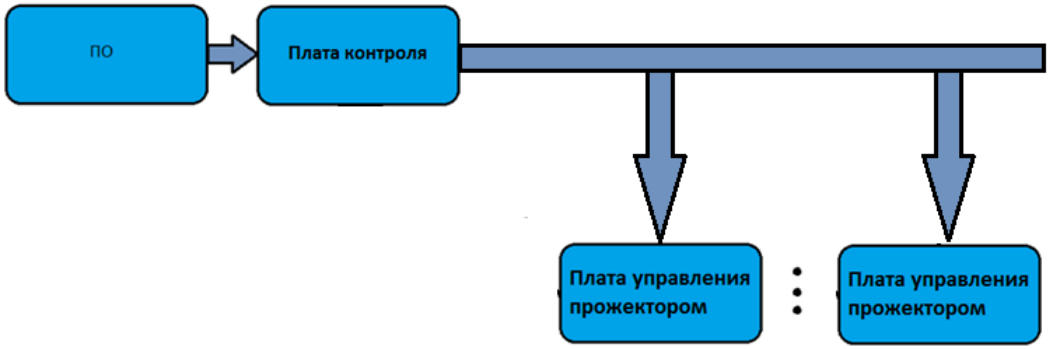


Рис. 3. – Структурная схема устройства с применением протокола DMX

В ходе работы было разработано и реализовано устройство, отвечающее поставленным требованиям.

Список используемых источников

1) Освещение и светильники в современном театре [Электронный ресурс] / Режим доступа: http://www.magazine-svet.ru/analytics/27828/

2) Исмагилов В. Г. Театральное освещение [Текст] / В. Г. Исмагилов – ЗАО « ДОКА Медиа», 2005.- 361 с.

3) Интерфейс rs-485 – наука и искусство [Электронный ресурс] / Режим доступа: http://www.emag.ru/pdf/teldor.pdf

4) USB для AVR. Часть 2. HID Class на V-USB [Электронный ресурс] / Режим доступа: http://we.easyelectronics.ru/electro-and-pc/usb-dlya-avr-chast-2-hid-class-na-v-usb.html

5) Пример работы с V-USB[Электронный ресурс] / Режим доступа: http://avrhobby.ru/index.php?option=com_content&view=article&id=90:vusbex3&catid=40:vusbpages

6) Using V-USB and the HID Class [Электронный ресурс] / Режим доступа: http://lackawanna.hackhut.com/2011/10/06/using-v-usb-and-the-hid-class-part-ii/

ЗАЩИТА АВТОРСКОГО ПРАВА НА ЭТАПЕ ДО ОПУБЛИКОВАНИЯ ПРОИЗВЕДЕНИЯ

Масалова К.В. – студент, Шарлаев Е.В. – к.т.н, доцент каф. ВСИБ
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Защитой авторских прав, в отличие от патентного права, в России начали активно заниматься сравнительно недавно. Стремительное развитие сети Интернет наряду с увеличивающейся компьютерной грамотностью способствует распространению плагиата в различные сферы человеческой деятельности (образование, коммерческая деятельность, наука, искусство и т.д.). Постепенно, с ростом числа копий, становится всё сложнее отыскать истинного автора [1].

Присвоение авторства направлено не только на исключительное право, но и на личные неимущественные права, которые являются неотчуждаемыми. Эти права возможно присвоить только на этапе до опубликования (выхода в свет) произведения. В РФ действует презумпция авторства, поэтому плагиатор будет считаться автором до тех пор, пока не будет

доказано обратное [2]. Также возможно присвоить идею произведения опередить в создании истинного автора и выпустить произведение до него. Поскольку авторское право не распространяется на идеи, то привлечь к ответственности плагиатора будет невозможно [2]. Существует несколько способов предотвращения воровства личного неимущественного права до опубликования произведения:

1. опубликование произведения по частям, по мере процесса создания;
2. пересылка произведения по частям, по мере процесса создания, самому себе заказным письмом и хранение их в запечатанном виде;
3. наличие свидетелей;
4. защита произведения техническими, криптографическими, программно-аппаратными (и организационными – для предприятия или организации) методами.

Первые два способа сводятся к закреплению временного приоритета по обладанию конкретным объектом авторского права зафиксированным в материальной форме в конкретное время истинным автором произведения. Однако в этих способах есть ряд недостатков. Основной недостаток заключается в том, что произведение не всегда можно разделить на части. Первый способ так же может снизить экономическую выгоду от опубликования уже завершенного произведения. Второй способ плох тем, что письма могут быть преднамеренно или непреднамеренно вскрыты самим автором или третьими лицами.

Третий способ подразумевает под собой наличие человеческого фактора, а значит, не может быть полностью надежен.

Последний способ не имеет вышеперечисленных недостатков, однако экономически более затратен.

Если произведение разрабатывается автором на предприятии (в организации), то такой информации может быть присвоен гриф «конфиденциально» или «для служебного пользования», и защита будет производиться в соответствии с установленным на предприятии режимом защиты конфиденциальной информации. Как правило, в режим защиты включена техническая, криптографическая, программно-аппаратная и организационная защита. В случае, если произойдет хищение, тогда будет возможно в сжатые сроки установить плагиатора и привлечь его к ответственности не только за присвоение авторства, но и за нарушение режима защиты информации на предприятии (в организации).

В большинстве случаев автор единолично заинтересован в сохранении авторства, то защита будет реализовываться силами самого автора. Организационная защита становится неактуальной, основные материальные затраты сводятся именно к криптографической, технической, программно-аппаратной защите. Решение задачи по защите авторского права на произведение до его опубликования можно свести к защите компьютера и/или помещения, где создается произведение, причем, предполагаемые затраты на защиту произведения не должны быть больше предполагаемой выручки от его опубликования или продажи имущественных прав на него. Автор может принимать во внимание рекомендации документов ФСТЭК и ГОСТы по информационной безопасности, и применять некоторые способы защиты данных, например: идентификация и аутентификация при входе пользователя в систему, контроль целостности файла, установлению и настройке антивирусных программ и брандмауэров (если компьютер подключен к Интеренту или локальной сети), а так же защите от подглядывания и подслушивания за счет расположения компьютера в помещении. В таком случае автор будет единолично виноват в утечке, если она произойдет и некого будет привлекать к ответственности. Отсюда видно насколько беззащитен, с точки зрения права, автор, разрабатывающий произведение в одиночку.

В судебном порядке без подтверждения временного приоритета оспорить авторство практически невозможно, поэтому следует заботиться о сохранности прав на произведение до его опубликования и использовать вышеперечисленные меры в комплексе.

Список используемых источников:

1. Архитектура сервиса определения плагиата, исключающая возможность нарушения авторских прав, В. В. Дягилев, А. А. Цхай, С. В. Бутаков, Вестник НГУ, Серия: Информационные технологии, 2011, том 9, выпуск 3, стр. 23-29.

Гражданский кодекс Российской Федерации от 30.11.1994 N 51-ФЗ.

ПРОГРАММНЫЙ КОМПЛЕКС ДЛЯ СИСТЕМЫ КОНТРОЛЯ И УПРАЛЕНИЯ ДОСТУПОМ НА ПРЕДПРИЯТИИ

Москаленко А.В. – студент, Якунин А.Г. – д.т.н., проф.
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В последнее время широкое распространение получили системы контроля и управления доступом (СКУД). Система контроля и управления доступом (СКУД) — совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение / регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через двери, ворота, проходные (т. н. «точки прохода») [1]. Примеры объектов, на которые ставятся СКУД:

- Офисы компаний, бизнес - центры;
- Учреждения образования (школы, техникумы, вузы);
- Банки;
- Промышленные предприятия;
- Автостоянки, парковки;
- Частные дома, жилые комплексы, коттеджи;
- Гостиницы;
- Общественные учреждения (спорткомплексы, музеи, метрополитен и др.)

Целью НИР является создание программного комплекса для контроля доступа. Данный комплекс может быть использован в учебных заведениях, офисах компаний, бизнес – центрах и т.д.. Основным отличием данного комплекса от известных прогриаммно-технических решения является то, что оно позволяет обеспечить возможность предоставления сотрудникам предприятия разрешать доступ приходящим к ним временным посетителям без использования специальных технических средств аутентификации, например таких как карточки RFID (карточки радиочастотной идентификации) и без привлечения к этому сотрудников соответствующих служб безопасности.

В предлагаемом комплексе персонал, которому предоставлено соответствующее право, может добавлять себе гостей через Web – интерфейс путем внесения в базу данных записи, включающей такую информацию как время начало и конца посещения, причина посещения, фамилия и инициалы посетителя – гостя, а также значения числового кода. По этому коду посетитель может зайти на охраняемое предприятие, введя его на цифровой клавиатуре.

По истечению указанного в базе времени гость становится неактивным и не отображается в списке посетителей сотрудника предприятия. Общее управление предоставлением сотрудникам возможности доступа к базе осуществляет администратор базы данных, который может добавлять как гостей, так и персонал, а также просматривать лог событий (кто и когда добавил, удалил или изменил гостей). У персонала и у администратора есть логин и пароль, с помощью которого они могут зайти в систему. Персонал может только добавлять, изменять и удалять своих гостей, а администратор может редактировать всех гостей. Структура базы данных приведена на рис. 1.

Приложение для работы написано на языке PHP, в качестве базы данных реализована в среде СУБД MySQL. При разработке программного обеспечения был использован объектно-ориентированный подход, реализованный с использованием пакета Propel ORM, позволяющего генерировать PHP классы. В качестве WEB сервера был использован сервер Apache. Эти четыре компонента: PHP, Apache, MYSQL и Propel ORM являются свободно распространяемыми программными продуктами. Сервер может быть установлен на

операционной среде Linux Ubuntu, которая также является свободной распространяемым продуктом. Данное приложение позволит отказаться от бюро пропусков на предприятии, сделав процесс добавления, изменения и удаления гостей более удобным, так как теперь каждый наделенный соответствующим правом сотрудник сможет сам управлять процессом допуска к себе гостей. Данная разработка изначально была реализована для применения в университете, но можно сделать универсальный конструктор, который позволит добавлять группы пользователей предприятия при установке программы и генерировать PHP файлы и код. Также можно будет назначать, какие группы пользователей имеют логин и пароль, то есть могут добавлять гостей, а какие нет. Данное приложение будет универсальным и сможет применяться на любом предприятии.

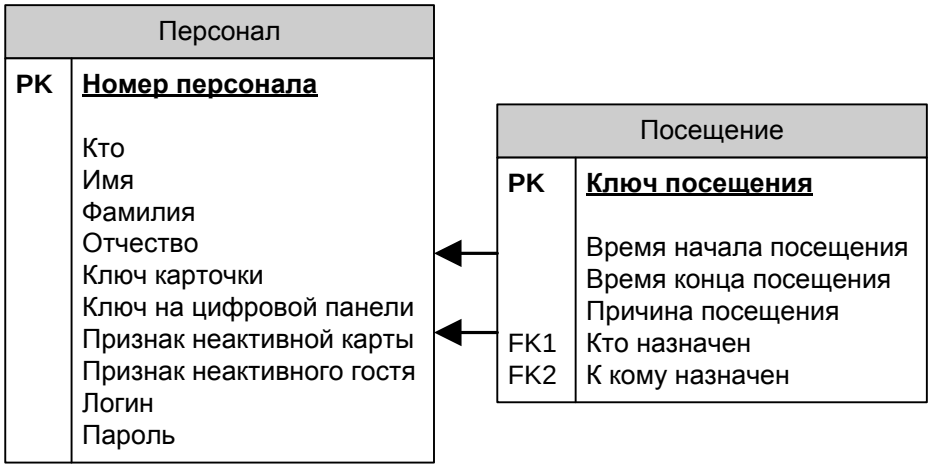


Рис. 1 – структура базы данных.

Список используемых источников:

1. Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. М.: Горячая линия-Телеком, 2010. - 272 е.: ил.

СИСТЕМА РЕГИСТРАЦИИ ДВИЖЕНИЙ НА БАЗЕ МИКРОСХЕМЫ LSM330DL

Овечкин Т.Л. – студент, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В последнее время широкое распространение получили микроэлектромеханические (МЭМС) акселерометры и гироскопы. Акселерометры – устройства, измеряющие проекцию кажущегося ускорения, гироскопы – угловое ускорение. Они применяются в различных мобильных устройствах для автоматической ориентации экрана, в разнообразных системах защиты для обнаружения свободного падения и ударов, в системах инерционной навигации, в робототехнике для определения положения в пространстве и балансировки, при диагностике движения человека и других устройствах. К основным преимуществам МЭМС акселерометров и гироскопов можно отнести малый размер, отсутствие вращающихся элементов и низкое энергопотребление.

Целью данной работы является создание устройства для диагностики двигательной активности человека путем идентификации его движений. Устройства подобного типа могут быть использованы в медицине, различных манипуляторах и др. Стоит отметить, что на рынке представлено крайне мало отдельных устройств для мониторинга движения (исключением являются шагомеры). Обычно подобные задачи решаются встроенными модулями других приборов (например, Холтер-мониторов). Среди имеющихся в продаже таких отдельных устройств можно выделить систему MoutionPod компании Movea. Датчик системы MotionPod включает в себя трехкоординатный твердокристаллический гироскоп,

акселерометр с тремя осями, микропроцессор со специализированным программным обеспечением и передатчик системы беспроводной связи на частоте 2.4 ГГц, действующий на расстоянии до 30 метров от приемника, подключаемого к компьютеру через порт USB. Данное устройство имеет малые габариты, благодаря чему возможно расположение нескольких датчиков на теле, что позволяет выполнить захват движений с высокой точностью. Помимо простого захвата движений, система MotionPod может выполнять функцию распознавания поз и движений, сравнивая реальные получаемые данные с библиотекой поз и движений [1]. Цена данного устройства составляет около 5 000 рублей.

Поскольку MotionPod является законченным устройством, поставляемым со специальным программным обеспечением, отсутствует возможность внесения каких-либо модификаций в его состав и использование в качестве системы для отладки и создания модулей для регистрации движения. В связи с этим была поставлена задача разработки системы, позволяющей получать информацию о движении исследуемого объекта в виде необработанных данных (угловые скорости, ускорения), которые в дальнейшем позволят создавать модули для различных контролирующих движение устройств.

В разрабатываемом устройстве используется микроконтроллер компании Atmel, который принимает данные с датчика LSM330DL фирмы ST Microelectronics. Данный датчик является акселерометром и гироскопом, выполненными в одном корпусе, имеет широкий диапазон измерений ($\pm 2g/\pm 4g/\pm 8g/\pm 16g$ для акселерометра и $\pm 250/\pm 500/\pm 2000$ °/с для гироскопа), низкое энергопотребление, а также оснащен цифровыми интерфейсами, что упрощает с ним работу. Кроме того, можно использовать программируемые прерывания от датчика для обнаружения свободного падения или движения. Данный датчик имеет ряд преимуществ по сравнению с другими. Например, датчик LIS3LV02DQ имеет схожие характеристики акселерометра, но в нем отсутствует гироскоп. Одновременное использование акселерометра и гироскопа обусловлено тем, что акселерометр регистрирует на все ускорения, а значит, может передать одинаковые результаты как при повороте, так и при ускоренном движении в одной плоскости. Использование раздельного акселерометра и гироскопа может увеличить как сложность изготовления изделия, так и его стоимость. Еще одним преимуществом является наличие цифровых интерфейсов. Некоторые датчики, например, LSM320HAY30, оснащены только аналоговым выходом, что требует использования дополнительных ресурсов микроконтроллера при получении и обработке данных. Также стоит отметить невысокую стоимость компонентов разрабатываемого устройства, составляющую около 500р.

Список используемых источников:

1. Система MotionPod на основе MEMS-датчиков обеспечивает точный захват движений человеческого тела [Электронный ресурс] // Режим доступа: http://www.dailytechinfo.org/infotech/2603-sistema-motionpod-na-osnove-mems-datchikov-obespechivaet-tochnyj-zaxvat-dvizhenij-chelovecheskogo-tela.html.

ИСТОЧНИКИ ПОГРЕШНОСТИ ИЗМЕРЕНИЯ ВРЕМЕНИ РАСПРОСТРАНЕНИЯ УЛЬТРАЗВУКОВЫХ ИМПУЛЬСОВ В АКУСТИЧЕСКИХ АНЕМОМЕТРАХ

Плотников А.Д. – аспирант, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Современные акустические анемометры определяют скорость воздушного потока на основе измерения времени распространения ультразвуковых импульсов через движущуюся воздушную массу [1]. По разности между временами распространения импульсов в прямом и обратном направлениях относительно движения воздушного потока определяется его скорость. Акустический анемометр состоит из решетки пар пьезоэлектрических преобразователей (далее ПЭП), обычно расположенных друг относительно друга на

расстоянии от 10 до 20 см, и электронного устройства измерения времени прохождения акустической волны. ПЭП в паре работают попеременно в режиме приемник/излучатель и обеспечивают излучение в воздух и прием из него ультразвуковых импульсов. Трехмерная решетка позволяет определить горизонтальную и вертикальную составляющие скорости ветра. Скорость воздушного потока определяется по формуле:

$$v = \frac{x(t_2 - t_1)}{2t_1 t_2},$$

где x – расстояние между парой ПЭП;

v – скорость потока;

t_1 – время распространения ультразвуковой волны по потоку;

t_2 – время распространения ультразвуковой волны против потока.

Основными источниками погрешности измерения времени распространения ультразвуковых импульсов являются время задержки системы и шум, возникающий в компонентах электрической схемы анемометров.

Понятие времени задержки системы определяется как разница между детектируемым электронным устройством полным временем прохождения сигнала и реальным временем прохождения [1]. Время между электронной генерацией передаваемого сигнала и электронным детектированием полученного сигнала больше, чем время прохождения, из-за времени передачи сигнала через пьезоэлектрические преобразователи и электронную цепь. С учетом введения понятия времени задержки системы выражение для скорости воздушного потока примет следующий вид:

$$v' = \frac{x(t_2' - t_1')}{2(t_1' - t_d) \cdot (t_2' - t_d)},$$

где t_d – время задержки системы;

t_1' – время распространения ультразвуковой волны по потоку, зафиксированное электронной схемой;

t_2' – время распространения ультразвуковой волны против потока, зафиксированное электронной схемой;

v' - скорость воздушного потока, вычисленная с учетом времени задержки системы.

Была проведена оценка величины ошибки вычисления скорости воздушного потока v_e без учета времени задержки системы. Для этого использовалась следующая формула:

$v_e = v' - v.$

Рассмотрим акустический анемометр, разработанный в Алтайском государственном техническом университете им. И.И. Ползунова [2], в котором измерение скорости ветра ведется без учета времени задержки системы. Расстояние между парами ПЭП x=20 см. Температура окружающей среды принята равной T=293К (≈20°С), тогда скорость звука в воздухе равна c=343 м/с [3]. Был проведен расчет времен распространения ультразвуковых импульсов и скорости воздушного потока с учетом времени задержки системы, за величину которого были приняты значения 1×10^{-8}, 1×10^{-7}, 1×10^{-6}, 1×10^{-5}, 1×10^{-4}, 2×10^{-4} с.

По полученным данным можно сделать вывод, что при значении времени задержки системы t_d<1×10^{-6}с величина ошибки v_e практически не влияет на измеряемую величину скорости потока v_e<0.1м/с. При этом время задержки системы t_d>1×10^{-6}с вносит ошибку, соизмеримую со скоростью воздушного потока. Следовательно, такие задержки недопустимы в работе акустического анемометра, и их необходимо минимизировать, либо исключать расчетным путем.

Была установлена зависимость ошибки определения скорости воздушного потока без учета времени задержки системы v_e от скорости звука в воздухе c, которая в свою очередь зависит от температуры воздуха c^2=403×(t+273) [3]. По полученным результатам можно сделать вывод, что на интервале температур воздуха от -60..+60 °С время задержки системы t_d ~1мкс вносит ошибку вычисления скорости порядка Δv=0,1м/с.

Для оценки влияния шума электронных компонентов были проведены эксперименты по определению углового коэффициента переднего фронта огибающей принимаемого сигнала с

последующим моделированием этого сигнала и шумовой составляющей. На рис. 1 представлена осциллограммы излучаемого и детектированного принимаемого сигналов.

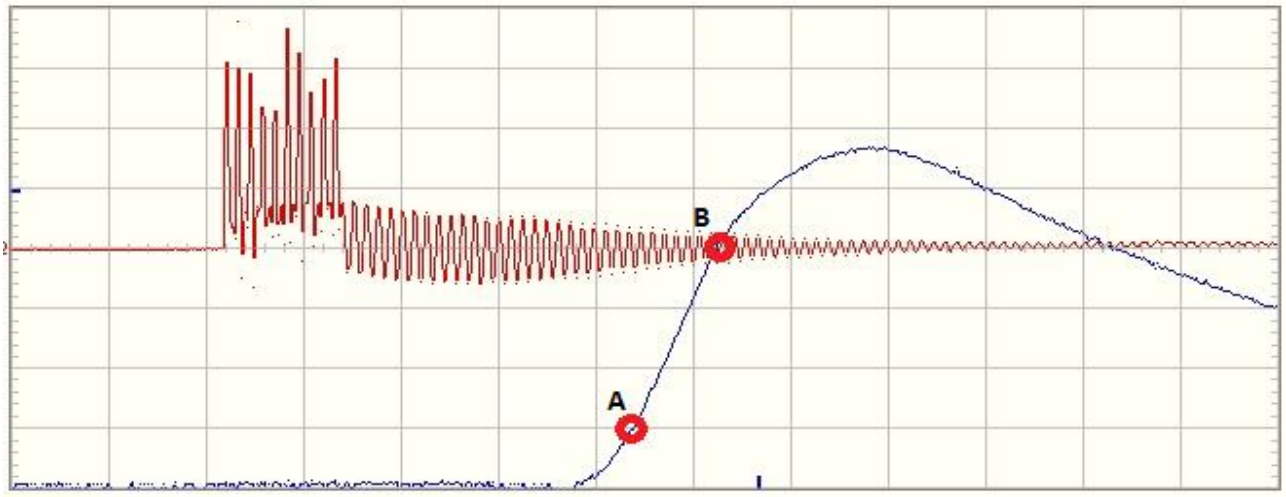


Рис. 1. Осциллограммы излучаемого и детектированного принимаемого сигналов

Участок детектированного принимаемого сигнала АВ будем считать прямолинейным. Точка А соответствует уровню напряжения U_A=1В, точка В на рис.1 соответствует уровню напряжения U_B=4В. Период времени между этими точками составляет t_{AB}=0,2мс. Угловой коэффициент линейного участка АВ k_{AB}=15 В/мс. При уровне напряжения шума U_n=0,01В абсолютная погрешность измерения времени распространения ультразвуковых импульсов составляет Δt=0,6мкс. Эта величина вносит погрешность в измерение скорости воздушного потока Δv=0,32 м/с.

Для уменьшения погрешности измерения скорости ветра акустическими анемометрами необходимо учитывать время задержки системы и минимизировать шумы электронной схемы анемометра. Возможными путями снижения погрешности являются применение для определения временной задержки системы фазовой автоподстройки и усреднение результатов измерения за несколько циклов.

Список используемых источников:

1. ГОСТ Р ИСО 16622-2009. Метеорология. Акустические анемометры-термометры. Методы приемочных испытаний при измерениях средней скорости ветра. – М. Стандартинформ, 2010. – 25с.

2. Плотников, А.Д. Разработка микроконтроллерного устройства для регистрации параметров воздушных потоков [Текст] / А.Д. Плотников, Л.И. Сучкова, А.Г. Якунин // Измерение. Контроль. Информатизация : материалы тринадцатой Международной научно-технической конференции. – Барнаул, АлтГТУ, 2012. – с. 134-138.

3. Kaimal, J.C. Another look at sonic thermometry [Текст] / Kaimal, J.C., J.E. Gaynor // Boundary Layer Meteorology, 1991. - с.410-410

СПОСОБ ОПРЕДЕЛЕНИЯ ЭНЕРГИИ РАЗРУШЕНИЯ ЗЕРНОВОГО МАТЕРИАЛА

Солопов В.С. – аспирант, Борисов А.П.– к.т.н., доцент,
Злочевский В.Л.– д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Введение.

Маятниковый деформатор разработан на кафедре МАПП АлтГТУ Злочевским В. Л., и представляет собой установку для деформирования зерновых материалов в колебательном процессе рабочих поверхностей. Рабочими поверхностями маятникового деформатора являются две цилиндрические поверхности (опорная и маятниковая). Энергозатраты на

разрушение зерна являются косвенным показателем такой важной характеристики как стекловидность (при известной влажности). От стекловидности, в свою очередь, зависит количество энергии, затрачиваемое на размол партии зерна. Очевидно, что с помощью маятникового деформатора возможно проводить экспресс-анализ помольных партий зерна на стекловидность и, как следствие, устанавливать режим работы вальцовых станков. Стандартные методы испытаний (ГОСТ 10987-76) занимают достаточно продолжительное время и имеют большое расхождение результатов испытания, вследствие субъективности самих методов. Нетрудно заметить, что способ, основанный на прямом измерении энергозатрат на разрушение зерна заведомо более точен, по сравнению со стандартными методами.

Цель данной работы заключается в разработке технических средств для реализации способа определения энергозатрат на разрушение зерна.

Определение энергии разрушения основано на выявлении положения крайних точек маятниковой поверхности при затухающем колебательном процессе, в которых запасенная маятниковой поверхностью потенциальная энергия определяется однозначно.

Для расчета потерь на трение сначала определяется декремент затухания маятника, затем рассчитывается энергия рассеяния за один период с заданным начальным углом отклонения.

Известно, что для маятника:

$$E = m \cdot g \cdot l_m \cdot (1 - \cos\alpha),$$

где E – потенциальная энергия, запасенная маятником, m – масса маятника, l_m – приведенная длина маятника, α – угол отклонения маятника. Исходя из того, что декремент затухания маятника равен:

$$d = \ln\left(\frac{\alpha_1}{\alpha_2}\right) = \beta T,$$

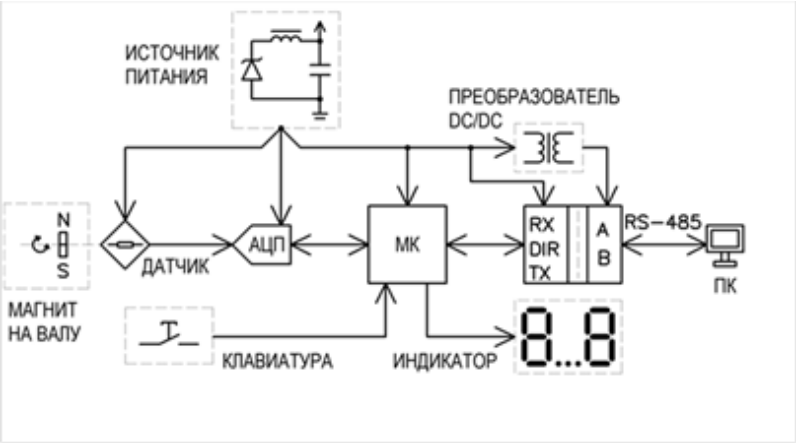
можно посчитать энергию, рассеиваемую за один период:

$$E_{тр} = m \cdot g \cdot l_m \cdot \left(\cos\left(e^{-\beta T}\alpha_1\right) - \cos\alpha_1\right).$$

Таким образом, определение энергии, затраченной на разрушение зерновки, находящейся на опорной поверхности маятникового деформатора, сводится к расчету декремента затухания и периода собственных колебаний маятника для заданного угла начального отклонения, а так же фиксации крайних положений маятниковой поверхности в процессе разрушения.

Для определения угла отклонения маятниковой поверхности используется магнитный датчик углового положения KMA200 фирмы NXP. Производителем была заявлена разрешающая способность не хуже 0,04° в цифровом режиме. В аналоговом режиме, при использовании внешнего АЦП разрешение составило 0.01°. Для преобразования аналогового сигналя в цифровую форму был разработан промежуточный контроллер, в состав которого вошло АЦП высокого разрешения AD7731 фирмы Analog Devices. Основой контроллера выступил микроконтроллер ATmega128A фирмы Atmel. Для связи контроллера с ПК была применена микросхема последовательного интерфейса RS-485 – ADM2483. В ходе работы было разработано программное обеспечение для контроллера на языке программирования C. Задачей ПО контроллера является получение данных с АЦП, пересчет их в значение угла и отправка их ПО верхнего уровня. Блок схема контроллера приведена на рисунке 1.

Рисунок 1. Блок-схема контроллера.



Программное обеспечение верхнего уровня

В ходе работы было разработано программное обеспечение верхнего уровня для ПК под управлением ОС Windows. ПО написано на языке программирования C++ в среде C++Builder XE2, и представляет собой приложение, отображающее графики испытания, а так же включающее набор инструментов для контроля испытаний.

Рабочее окно программы показано на рисунке 2:

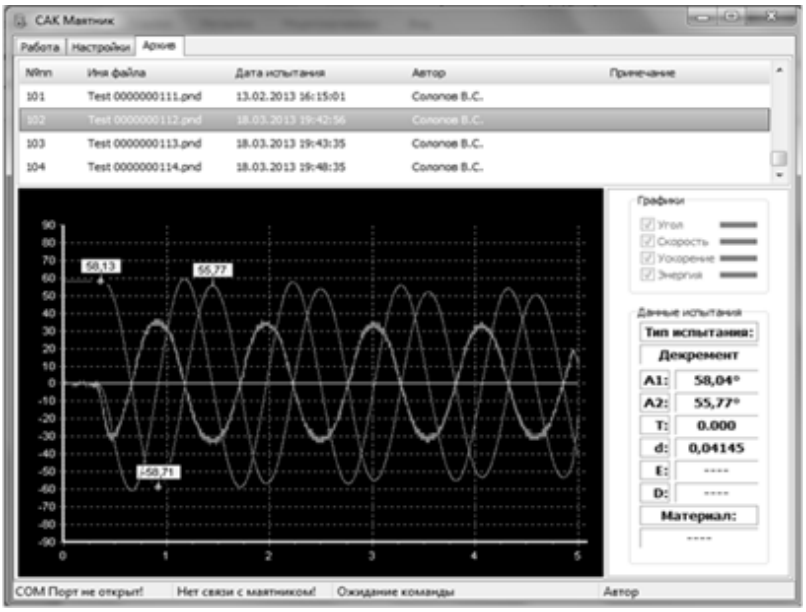


Рисунок 2. Внешний вид ПО верхнего уровня.

Выводы

В ходе работы был разработан контроллер бесконтактного определения угла положения маятниковой поверхности. Контроллер был изготовлен промышленным способом, для него было написано программное обеспечение и проведены реальные испытания на макетном стенде, которые доказали работоспособность устройства. Следующим этапом работы стала разработка ПО верхнего уровня.

В настоящий момент работа не закончена, идет постоянное совершенствование как механической части проекта, так и программной его составляющей, но уже с уверенностью можно говорить о большом потенциале и востребованности данной работы.

Список используемых источников:
1. Кантор С.А. Основы вычислительной математики: Учебное пособие. / Алт. госуд. технич. ун-т им. И.И.Ползунова. Барнаул, 2010. — 357с.
2. Analog Devices. Low Noise, High Throughput 24-Bit Sigma-Delta ADC: http://www.analog.com/static/imported-files/data_sheets/AD7731.pdf
3. Atmel. ATmega128A, Rev. 8151H–AVR–02/11: http://www.atmel.com/images/doc8151.pdf
4. ГОСТ 10987-76. Зерно. Методы определения стекловидности.

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ УДАЛЕННОГО МОНИТОРИНГА МЕТЕОДАННЫХ

Умбетов С.В. – студент, Якунин А.Г. – д.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Человеку необходимо иметь представление о погодных условиях, которые были, есть и, что особенно важно, будут сопровождать его существование на Земле. Без знания метеорологических условий невозможно правильно вести сельскохозяйственные работы, развивать и совершенствовать промышленность, обеспечивать нормальное функционирование транспорта, особенно авиационного и водного.

Современная урбанизация приводит к возникновению новых, в том числе метеорологических, проблем: например, проветриваемость городов и местное повышение температуры воздуха в них. В свою очередь, учет метеоусловий позволяет снизить вредное воздействие загрязненного воздуха , воды и почвы, на которые эти вещества осаждаются из атмосферы, на организм человека.

Основной задачей стало для нас создания недорого, но эффективного устройства для фиксирования ряда важных метеорологических данных с возможностью объединения этих устройств в сеть. Подобная сеть позволит охватить большие территории, что будет давать возможность делать комплексный анализ и прогнозировать ситуацию. Так при использовании подобного подхода к сбору и обработке данных возникает возможность их масштабирования в зависимости от исследуемой области.

Сбор данных начинается с физического явления, которое надо измерить. Таким физическим явлением является комнатная температура, интенсивность светового потока, давление, влажность и многие другие показатели. В нашем случае датчик конвертирует физическое явление в измеримый электрический сигнал, такой как напряжение.

Основной модуль представляет из себя компактное устройство, соединяемое с компьютером по интерфейсу usb, по нему же оно и получает питание. Задача модуля принять информацию с датчика, провести первичную обработку и переслать данные на компьютер. В случае если соединение с компьютером разорвано устройство переходит в автономный режим работы. Работая в заданном режиме устройство, опрашивая датчики, сохраняет информацию на специальном flash накопителе и при следующем подключении к компьютеру передает накопленные данные на него.

Система аварийного питания позволяет длительное время работать автономно, это достигается за счёт отключения не нужных узлов и перевода других узлов, например микроконтроллера в режим энергосбережения. Использование в основном модуле микроконтроллера семейства AVR (рисунок 1) обусловлено его невысокой стоимостью и полным набором необходимых функций [1].

Так как некоторые датчики генерируют слишком сложные сигналы, а зачастую и слишком опасные для измерения их напрямую то согласование сигнала, а именно приведение его в состояние, когда появляется возможность проведения безопасного и быстрого измерения повышает эффективность системы сбора данных.

Для прибора разрабатывается система выносных датчиков, а так же система экранирования от внешних воздействий основного блока.

Программное обеспечение трансформирует ПК в полностью завершенный механизм по сбору данных, их анализу и визуализации. Пользователь сможет в реальном времени наблюдать за динамикой изменения любого сигнала. Все данные собранные с разных датчиков отправляются на удаленный сервер, где уже происходит завершающий и самый ресурсоёмкий этап обработки и анализа сигналов. Подобный подход избавляет нас от нужды задействования в самом приборе мощных вычислительных ресурсов и переноса этих задач на удалённый сервер.

На данном этапе работы создан прототип устройства с набором датчиков и с возможностью коммутации с компьютером по usb (рисунок 2). В настоящее время ведется разработка программного обеспечения на языке C# [2] и ассемблере [3] для внутрисхемной прошивки бутлоадера и снятия показаний, осуществляется конфигурирование и поднятие сервера для работы с сетью датчиков. В дальнейшем планируется разработать систему экранирования основного модуля, увеличить диапазон измерений датчиков и расширить функционал ПО.

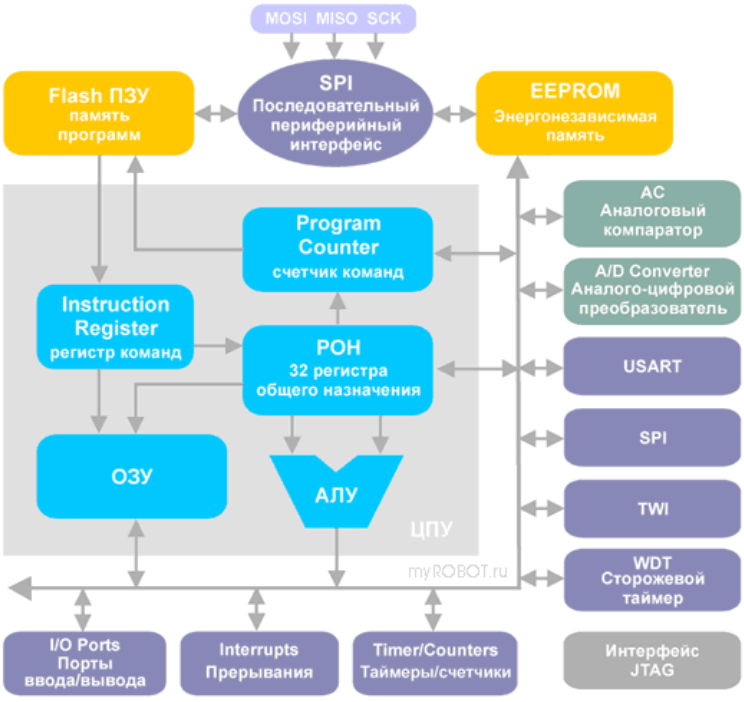


Рисунок 1 – Функциональная схема микроконтроллера.

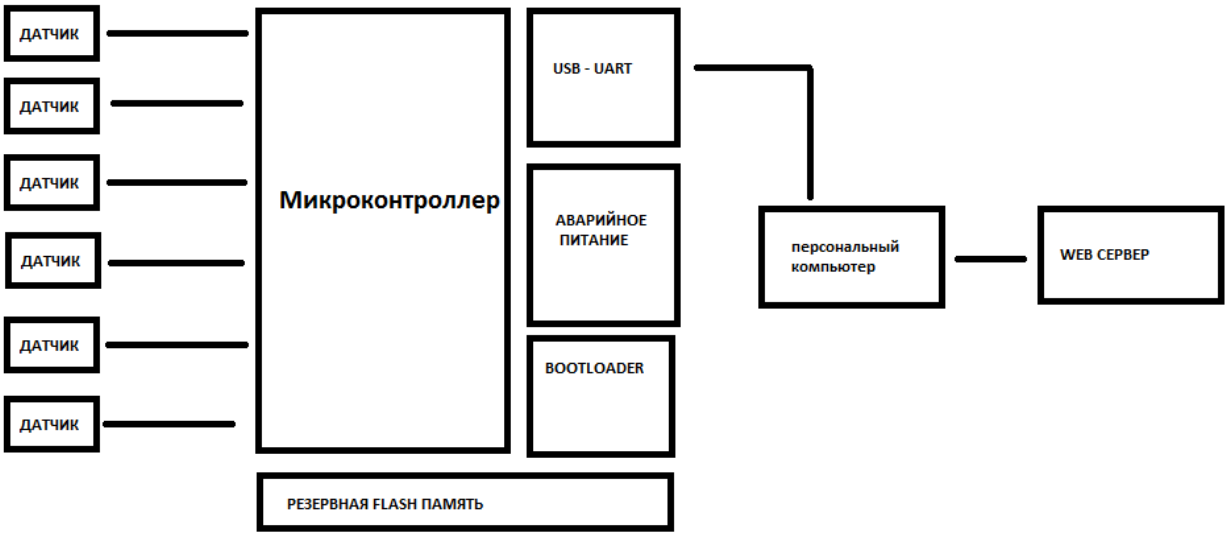


Рисунок 2 – Функциональная схема прибора

Список используемых источников:

1 Белов, А. Создаем устройства на микроконтроллерах [Текст]: учеб. пособие / А. Белов. – НИТ Спб, 2006. – 248 с.

2 Тролсен, Э. Язык программирования C# [Текст]: учеб. пособие / Э. Тролсен. – Москва, 2008. – 1344 с.

3 Зубков, В. Ассемблер для DOS, Windows и UNIX [Текст]: учеб. пособие / В. Зубков. – Москва, 2004. – 608 с.

DLP-СИСТЕМА КАК СРЕДСТВО ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ УТЕЧЕК

Химичева М.С. – студентка, Шарлаев Е.В. – к.т.н, доцент каф. ВСИБ
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В мировом сообществе уже давно сформировалось устойчивое отношение к информации, как к ценнейшему ресурсу. Объясняется это небывалым ростом объема информационных потоков в современном обществе. Развитие любой организации напрямую зависит от качества используемой информации, ее достоверности и полноты, оперативности и формы представления. Поэтому особое внимание должно уделяться проблемам формирования, использования и защиты информационных ресурсов на основе применения информационных и коммуникационных технологий.

Причинами утечек информации являются различные факторы: неосторожность или компьютерная неграмотность сотрудников, намеренная кража информации как собственными сотрудниками, именуемые иначе инсайдерами, так и мошенниками, использующими различные средства проникновения в корпоративную сеть, например, шпионские программы.

Существует множество способов борьбы с утечками конфиденциальных данных, как на уровне организационных процедур, так и на уровне программных решений. Одним из наиболее эффективных методов является внедрение системы защиты от утечек конфиденциальных данных Data Lock Prevention (DLP) - технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек.

Сегодня существует специализированный рынок программных решений для выявления и предотвращения утечек конфиденциальной информации. Представленные в этом сегменте

продукты различаются по методам работы, спектру покрываемых каналов утечки, наличию сопроводительных услуг и т.д. При выборе решения необходимо учитывать:

- параметр комплексности - покрывает ли продукт все возможные каналы утечки;
- возможность создавать и хранить архивы корпоративной корреспонденции;
- программной или программно-аппаратная реализация модулей, отвечающих за фильтрацию сетевого трафика.

Выполнение второго из представленных условий позволяет провести служебное расследование, не беспокоя сотрудников и не привлекая внимания.

Анализ проведенных исследований современного рынка технических средств позволяет отдать предпочтение комплексному решению InfoWatch Enterprise Solution (IES), который отвечает перечисленным выше критериям. Продукт поставляется российской компанией InfoWatch, разработчиком систем защиты от инсайдеров, позволяет обеспечить контроль над почтовым каналом и веб-трафиком, а также коммуникационными ресурсами рабочих станций, позволяет архивировать корпоративную корреспонденцию и абсолютно все пересылаемые по сети данные, таким образом обеспечивается комплексная защита всех каналов утечки. На сегодняшний день IES уже используется правительственными (Минэкономразвития, Таможенная служба), телекоммуникационными («ВымпелКом»), финансовыми (Внешторгбанк) и топливно-энергетическими компаниями (ГидроОГК, Транснефть).

Архитектуру комплексного решения InfoWatch можно разделить на две части: мониторы, контролирующие сетевой трафик, и мониторы, контролирующие операции пользователя на уровне рабочих станций. Первые устанавливаются в корпоративной сети в качестве шлюзов и фильтруют электронные сообщения и веб-трафик, а вторые развертываются на персональных компьютерах и ноутбуках и отслеживают операции на уровне операционной системы. Кроме того, следует выделить специальный модуль *Storage, который представляет собой хранилище всех входящих и исходящих сообщений, а также всего сетевого трафика. Схема работы InfoWatch Enterprise Solution представлена на рисунке 1.

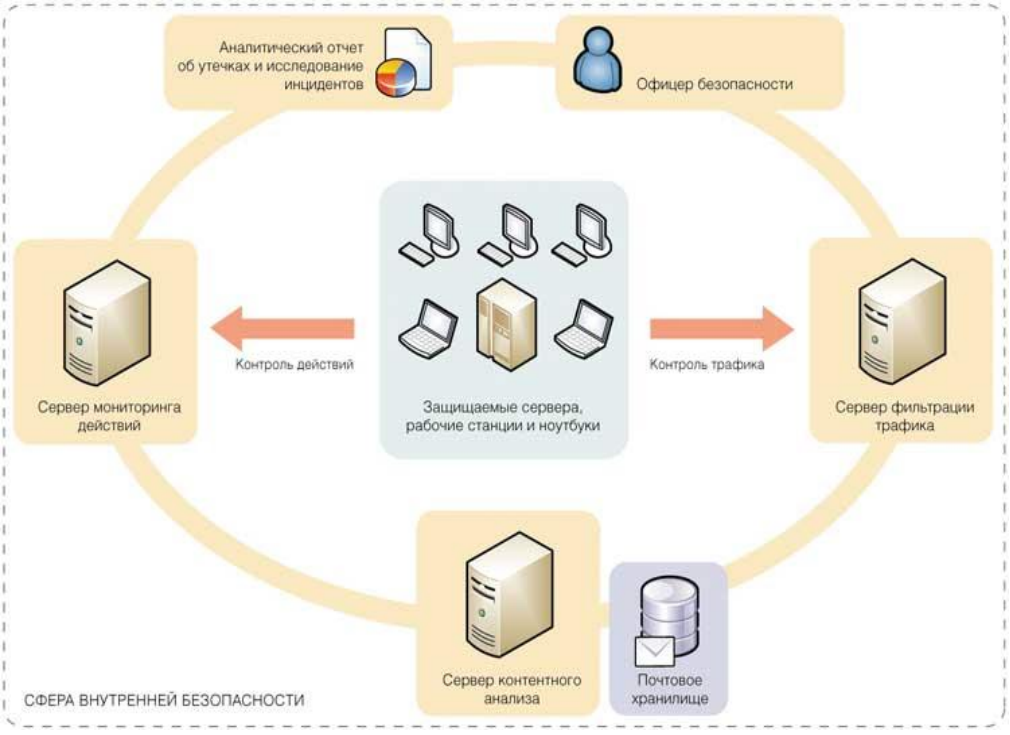


Рисунок 1 – Схема работы InfoWatch Enterprise Solution

Необходимо отметить, что сетевые мониторы могут быть реализованы в виде аппаратного устройства InfoWatch Security Appliance. Таким образом, заказчику

предлагается на выбор либо программное, либо аппаратное исполнение фильтров почты и веб-трафика.

Все мониторы, входящие в состав InfoWatch Enterprise Solution, способны блокировать утечку в режиме реального времени и сразу же оповещать об инциденте сотрудника отдела безопасности. Управление решением осуществляется через центральную консоль, позволяющую настраивать корпоративные политики. Предусмотрено также автоматизированное рабочее место сотрудника безопасности, с помощью которого специальный служащий может быстро и адекватно реагировать на инциденты.

Важной особенностью комплексного решения InfoWatch Enterprise Solution является возможность архивировать и хранить корпоративную корреспонденцию. Для этого предусмотрен отдельный программный модуль InfoWatch Mail Storage (IMS), который перехватывает все сообщения и складывает их в хранилище с возможностью проводить ретроспективный анализ. Таким образом, комплексное решение InfoWatch Enterprise Solution сочетает все аспекты защиты конфиденциальной информации от инсайдеров.

Список используемых источников:

1. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. -320с.

2. Защита конфиденциальной информации крупных организаций. Эл. ресурс. Реж. доступа http://www.infowatch.ru/solutions/information_security

SELECTING A SUITABLE TEMPERATURE SENSOR FOR ATMOSPHERIC TURBULENCE ANALYSIS

Hussein H. M. – teaching assistant , Yakunin A.G. – Ph.D, professor
Altai State Technical University (Barnaul)

This work aims at the selection of temperature sensors for the analysis of atmospheric turbulence. It answers the question, which sensor is suitable for temperature monitoring in atmospheric turbulence?

Many sensors have been considered. It seems that the sensor DS18S20, manufactured by DALLAS, is the best choice. Because it has a lot of great feature such as low price, acceptable temperature range, 1-Wire interface, sufficient accuracy and response time, etc.

Experiment result proves that, the sensor has suitable accuracy and stability.

Introduction

In many systems, temperature control is fundamental. There are a number of passive and active temperature sensors that can be used to measure system temperature, including: thermocouple, resistive temperature detector (RTD), thermistor and silicon temperature sensors. These sensors provide temperature feedback to the system controller to make decisions such as, over-temperature shutdown, turn-on/off cooling fan, temperature compensation or general purpose temperature monitor [1, 2].

Sensor Selection Criteria

To select an appropriate sensor many aspects should be observed [3, 4].

The selection criteria include:

- Temperature measurement range includes the minimum and maximum temperature that can be observed.
- Accuracy refers to how exactly the temperature of the thermal sensor matches that of its targeted measured environment.
- Stability includes the sensor's optimum operating environments, durability, and life expectancy.
- Probe type describes the unit which houses the temperature sensor. There are several different styles available, which are described on the GlobalSpec website [4].

- Termination style refers to how the user knows when the reading is completed.

The following table summarizes the different types of sensors and their Characteristics

Characteristic	Thermocouple	RTD	Thermistor	Temperature IC
Active Material	Two Dissimilar Metals	Platinum Wire	Metal Oxide Ceramic	Silicon Transistors
Temperature Range	-270 - 1800°C	-250 - 900°C	-100 - 450°C	-55 - 150°C
Accuracy	±0.5°C	±0.01°C	±0.1°C	±1°C
Linearity (Minimum order of polynomial, lesser the better)	4^{th} order polynomial	2^{nd} order polynomial	3^{rd} order polynomial	Linearization not required. Within ±1°C
Sensitivity	10s of µV/°C	0.00385 Ω / Ω /°C	Several Ω / Ω /°C	~1 mv/°C or ~1 uA/°C
Stability	Moderate	Excellent	Logarithmic, Poor	Excellent
Noise Susceptibility	High	Low	Low	High
Responsiveness	T_{res}<1s	1s<T_{res}<10 s	1s<T_{res}<5s	4s<T_{res}<60s
External Excitation Required	None	Current Source	Voltage Source	Supply Voltage
Special Requirements	Reference Junction	Lead Compensation	Linearization	None
Changing Parameter	Voltage	Resistance	Resistance	Digital/Current/ Voltage
Drift	1 to 2°F / year	± 0.01% /5 years	± 0.2 to 0.5°F/year	0.1°C / month
Cost	$1 to $50	$25 to $1000	$2 to $10	$1 to $10

Weather monitoring system requires a temperature sensor with the following characteristics:

- Temperature range -50 to 60 ° C.
- Accuracy better than 0.5.
- Response time <1 sec.
- Simple communication port.

After finding sensor which complies. It was found that the sensor DS18S20 (produced by DALLAS) is suitable.

Characteristics of the sensor DS18S20

Widespread chip digital thermometer DS18S20 (Figure 1), produced by DALLAS, provides a measurement of temperature in the range -55 .. +125 ° C with a resolution of 0,5 ° C. The cost of chips DS18S20 is about $ 2.

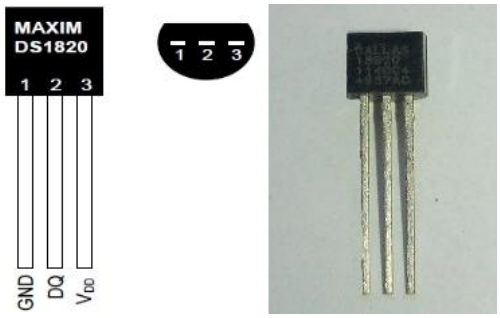


Figure 1 - Appearance chip digital thermometer DS18S20

Key Features for the DS18S20

- Unique 1-Wire Interface Requires Only One Port Pin for Communication.
- Each Device has a Unique 64-Bit Serial Code Stored in an On-Board ROM.
- Multidrop Capability Simplifies Distributed Temperature Sensing Applications.
- Requires No External Components.
- Can Be Powered From Data Line. Power Supply Range is 3.0V to 5.5V.
- Measures Temperatures from -55°C to +125°C (-67°F to +257°F).
- ±0.5°C Accuracy from -10°C to +85°C
- 9-Bit Thermometer Resolution.
- Converts Temperature in 750ms (max).
- User-Definable Nonvolatile (NV) Alarm Settings.
- Alarm Search Command Identifies and Addresses Devices Whose Temperature is Outside Programmed Limits (Temperature Alarm Condition)

Experimental results:

The sensor has been tested for more than two years in weather monitoring system, Figure 2 shows a sample for measured data from two sensors placed in two different places in the lab. The

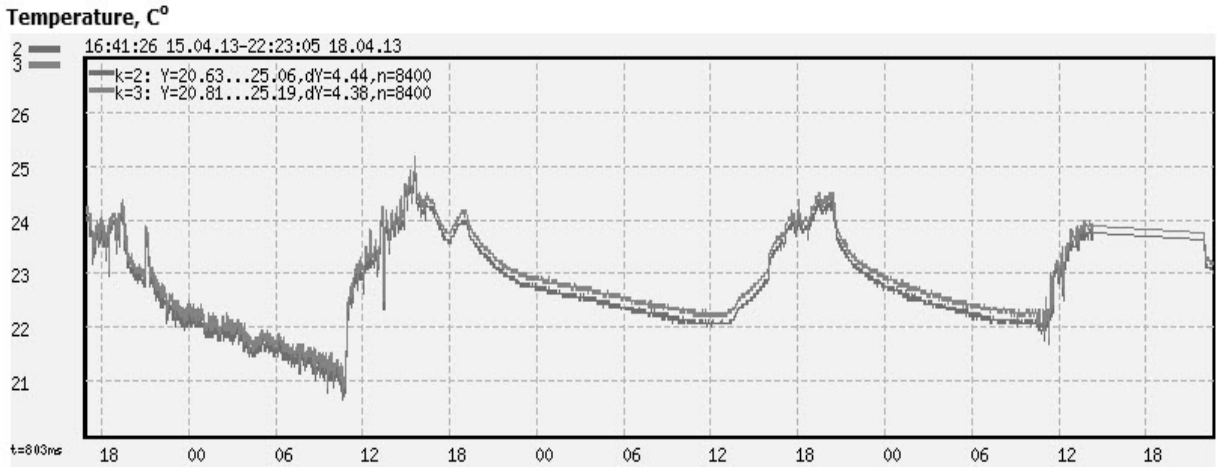


Figure 2 - Sample for measured data from two DS18S20 sensors

two readings are almost the same (the difference between them is less than 0.2°C). The gradient of the two readings appears in a similar way. So, this type of sensors has reasonable sensitivity and accuracy.

Conclusion

DS18S20 sensor has remarkable features. So it is suitable for monitoring the weather. Although other sensors may have a better performance, but the sensor DS18S20 has many advantages.

References

1. Microchip, “Temperature Sensor Design Guide,” Microchip Technology Inc., 2009.
2. Журнал "Компоненты и технологии", http://kit-e.ru/articles/sensor/
3. T. Al-Hawari, S. Al-Bo'ol, and A. Momani, “Selection of Temperature Measuring Sensors Using the Analytic Hierarchy Process,” Jordan Journal of Mechanical and Industrial Engineering, Vol. 5, No. 5, Oct. 2011, pp.451 – 459.
4. http://www.globalspec.com/.
5. http://www.maximintegrated.com/datasheet/index.mvp/id/2815

ЭЛЕКТРОННЫЙ УЧЕБНИК КАК СРЕДСТВО ПОЗНАВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ УЧАЩЕГОСЯ

Чурсин А.С. – студент, Загинайлов Ю. Н. – к.в.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Современная культурная и информационная ситуация требует существенного изменения концепции учебной литературы. Функция учебника не может сводиться к алгоритмизированному представлению информации, организованной в соответствии со стандартным шаблоном. Учебник должен учить справляться с разными видами «сырой», «необработанной» информации, приближая учебную ситуацию к условиям реального непрерывного самообучения, которое чаще всего носит неорганизованный, стихийный характер. В этой связи и структура учебника должна быть иной: линейному алгоритму бумажной книги следует противопоставить организованный хаос гипертекста, позволяющий работать с разными видами информации и вместе с тем требующий от учащегося существенной самостоятельности в выстраивании индивидуальной траектории обучения. В этой связи появление электронного учебника (ЭУ) является очень своевременным.

Электронный учебник – это обучающая программная система комплексного назначения, обеспечивающая непрерывность и полноту дидактического цикла процесса обучения, предоставляющая теоретический материал, обеспечивающая тренировочную учебную деятельность и контроль уровня знаний.

В самом общем виде идеальный ЭУ должен выступать основой для полноценного интегрированного учебно-методического комплекса, реализующего разнообразные по задачам и функциональному наполнению возможности мультимедиа. При этом ЭУ может включать в себя различные типы документов и интегрированных сред:

1)текстовые материалы;

2)графические материалы: таблицы, графики, диаграммы, иллюстрации;

3)аудиофайлы: устные учебные тексты, аудиодиалоги, учебные комментарии к виртуальным объектам, аудиохроника, музыка, звуки природных процессов и животного мира и т. п.;

4)видеофайлы: анимация, динамические модели явлений и процессов, постановочные видеосюжеты, фрагменты художественных фильмов, видеохроника;

5)коллекции документов и базы данных: полнотекстовые электронные библиотеки, каталоги, интегрированные словари, справочники, энциклопедии, глоссарии и т. п.;

6)игровые среды;

7)системы автоматического тестового контроля.

Очевидно, что этот набор может варьироваться в зависимости от особенностей содержания курса и поставленных задач. При этом такое разнообразие типов информации и способов работы с ней обеспечивает актуализацию различных видов познавательной активности учащегося, позволяя получить более полное и глубокое представление об изучаемом предмете.

Достоинств электронных учебников много. К ним можно отнести:

– Возможность адаптации и оптимизации пользовательского интерфейса под индивидуальные запросы обучаемого. В частности, имеется в виду возможность использования как текстовой или гипертекстовой, так и фреймовой структуры учебника, причем количество фреймов, их размеры и заполнение может изменяться.

– Возможность использования дополнительных (по сравнению с печатным изданием) средств воздействия на обучаемого (мультимедийное издание), что позволяет быстрее осваивать и лучше запоминать учебный материал. Особенно важным нам представляется включение в текст пособия анимационных моделей. Положительный эффект можно достигнуть и с помощью звукового сопровождения, соответствующего лекторскому тексту.

– Возможность построения простого и удобного механизма навигации в пределах электронного учебника. В электронном пособии используются гиперссылки и фреймовая структура, что позволяет, не листая страниц, быстро перейти к нужному разделу или фрагменту и при необходимости так же быстро возвратиться обратно. При этом не требуется запоминать страницы, на которых были расположены соответствующие разделы.

– Возможность встроенного автоматизированного контроля уровня знаний студента, и на этой основе автоматический выбор соответствующего уровню знаний слоя учебника, как указано в следующем пункте.

– Возможность адаптации изучаемого материала к уровню знаний студента, следствием чего является улучшение восприятия и запоминания информации. Адаптация основана на использовании слоистой структуры издания, причем в соответствии с результатами тестирования студенту предоставляется слой, соответствующий уровню его знаний.

– Главное преимущество электронного учебника это возможность интерактивного взаимодействия между студентом и элементами учебника. Уровни ее проявления изменяются от низкого и умеренного при перемещении по ссылкам до высокого при тестировании и личном участии студента в моделировании процессов. Если тестирование подобно собеседованию с преподавателем, то участие в моделировании процессов можно сопоставить с приобретением практических навыков в процессе производственной практики в реальных или приближенных к ним условиях производства.

– Интерактивность раскрывает характер и степень взаимодействия между преподавателем и студентом. Данное свойство проявляется при выполнении тестов, практикумов в электронных учебниках и вызывает активность обучающихся студентов к активным действиям в познании и усвоении нового материала.

– Адаптивность позволяет создавать, изменять и приспосабливать версии учебника индивидуально для группы студентов, под конкретный уровень подготовленности группы. Электронный учебник должен допускать адаптацию к нуждам конкретного пользователя в процессе учебы, позволять варьировать глубину и сложность изучаемого материала и его прикладную направленность в зависимости от будущей специальности учащегося, применительно к нуждам пользователя генерировать дополнительный иллюстративный материал, предоставлять графические и геометрические интерпретации изучаемых понятий и полученных учащимся решений задач.

– Интеллектуальность - свойство, превращающее электронный учебник в партнера обучаемого, реагирующего на действия обучаемого и корректирующего его действия в процессе обучения. Очевидно, что степень интеллектуальности может меняться в широких пределах от подсказок при выполнении контрольных упражнений до имитации виртуальным собеседником разумного поведения партнера, наставника, учителя.

Список используемых источников:

1.Башмаков А. И., Башмаков И. А. Разработка компьютерных учебников и обучающих систем. М., 2003.

2.Беспалько В. П. Образование и обучение с участием компьютеров (педагогика третьего тысячелетия). М., 2002.

3.Буга П. Г. Создание учебных книг для вузов. М., 1987.

4.Мальченко Н. С., Елисеев А. Б., Бессарабова В. В. «Организация самостоятельной работы студентов с использованием информационно-образовательной среды вуза». Минск: Изд-во Минский филиал МГУ, 2012. – 6 с.

ПРОБЛЕМА ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Штрошенко А.В. - студент, Загинайлов Ю.Н. – к.в.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В современном мире все чаще открываются совместные предприятия: российские организации активно сотрудничают с международными фирмами. При проведении совместных работ обе стороны должны быть уверены в том, что предоставляемая партнеру информация будет надежно защищена. Уровень доверия к обеспечению безопасности информации на предприятии прямо пропорционален квалификации сотрудников, занимающихся данным вопросом. Следовательно, компаниям все чаще требуются высококвалифицированные специалисты в области информационной безопасности. В связи с этим остро встает вопрос о подготовке таких специалистов.

Основным инструментом подготовки специалистов в области ИБ являются высшие учебные заведения. Однако, в российских университетах отсутствуют механизмы контроля актуальности предоставляемых сведений, вследствие чего, выпускник-специалист не может быть уверен, что сможет применить полученные знания и навыки на практике. Также не каждый выпускник умеет видеть, анализировать, учитывать современные тенденции в области информационной безопасности, к примеру, ее активную привязку к бизнесу, бизнес-процессам и менеджменту. Уровень знаний выпускников не позволяет им чувствовать себя готовыми к практической профессиональной деятельности, делая их непригодными для конкуренции [3]. А исключение России из конкурентной борьбы в области информационной безопасности на мировом рынке - непозволительно как для экономического и стратегического развития, так и для имиджа страны.

Существует несколько способов решения проблемы подготовки специалистов (рисунок 1), например, изменение программы обучения. Программа должна быть адаптирована под современные технологии, тенденции, должна учитывать такие темы, как безопасность приложений (например, ERP, CRM, SCM, биллинг и т.п.), Web-сервисов, телефонии (в т.ч. и VoIP), систем хранения данных (SAN, NAS, DAS) и многих других технологий, без которых современное предприятие немыслимо.

Рисунок 1 – Пути решения проблемы

Схожим с первым является такой способ, как повышение уровня практических навыков выпускников, например, за счет увеличения количества практических занятий, а также оснащение лабораторной базы ВУЗа современными стендами и оборудованием.

Наиболее реальным способом является получение сертификатов в области информационной безопасности в международных центрах сертификации, поддерживаемых основными вендорами в области ИБ.

В настоящее время, профессиональная сертификация в области информационной безопасности постепенно трансформируется из программ повышения квалификации отдельных компаний в обязательное требование рынка для специалистов, особенно пытающихся выйти на мировой уровень.

Ценность сертификации состоит из ее востребованности на рынке, способности подтвердить квалификацию обладателя и ее адекватности технологии, применяемой или предлагаемой кандидатом и работодателем.

Два основных аспекта, в которых проявляется полезность сертификации, это - во-первых, подготовка к экзамену помогает специалисту систематизировать свои знания, и, во-вторых, работодателю проще найти подходящего работника [2].

Важность сертификаций для специалистов в области информационной безопасности, по версии журнала Information Security за 2012 год, можно объяснить следующими причинами:

– подтверждение собственной квалификации;
– стремление к уважению со стороны работодателя и коллег;
– повышение заработной платы;
– большие возможности карьерного роста;
– приобщение к сообществу специалистов [1].

Сертификация может стоить очень дорого – как в денежном выражении, так и по затратам времени. Многие схемы сертификации предусматривают несколько экзаменов. Некоторые сертификации высокого уровня требуют очных экзаменов, которые длятся не один день. Для каждого экзамена может потребоваться прохождение очного или электронного обучения. Несмотря на высокие затраты на получение сертификатов, инвестиции в сертификацию специалиста окупаются достаточно быстро, хотя бы за счет повышения имиджа компании в глазах клиентов.

Основными преимуществами от получения сертификатов являются такие, как:

– повышение заработной платы за счет повышения привлекательности специалиста для работодателей;
– получение новых знаний и навыков в процессе подготовки;
– подтверждение своей квалификации на мировом уровне;
– гарантия компетентности и профессионализма специалиста (рисунок 2) [2].

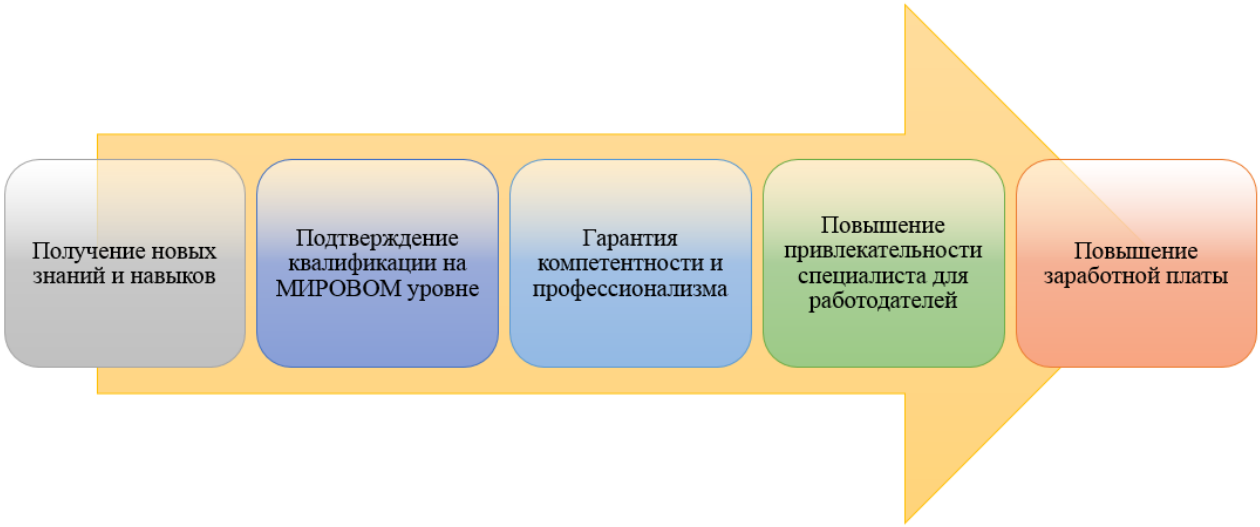


Рисунок 2 – Преимущества от получения сертификатов

Исходя из приведенных фактов, можно сделать вывод: подготовка действительно достойных специалистов, способных составить конкуренцию на мировом рынке, важна как государству в целом, так и представителям бизнеса. Выход специалиста на мировой уровень возможен лишь при документальном подтверждении его знаний, навыков, умений, при чем эти знания должны опираться на мировой опыт, а не концентрироваться на достижениях Российской Федерации.

Список используемых источников:

1. *И. Сачков* Особенности и проблемы сертификации специалистов по информационной безопасности [Электронный ресурс]. – Электрон. текст. дан.- Режим доступа: http://www.itsec.ru/articles2/control/osoben_probl_sertif_spec_inform_bezopasn – Загл. с экрана

2. Журавлев, Р. Одежка по уму, или Кому и зачем нужна сертификация специалистов и руководителей ИТ// «Директор информационной службы». 2010, № 05

3. Станкевич В. Будущее профессии ИБ-специалиста и индустрии IT-образования// Журнал "Information Security/ Информационная безопасность". 2012, №1

ПОДХОДЫ К МИНИМИЗАЦИИ ВОЗДЕЙСТВИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА БИЗНЕС-ПРОЦЕССЫ ОРГАНИЗАЦИИ

Штрошенко А.В. - студент, Пивкин Е.Н. – к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

На современном этапе развития экономики существование многих бизнес-процессов невозможно без информационных технологий: возрастает использование программного обеспечения, информационных систем, различных сервисов, компьютерных сетей, при чем они не ограничиваются рамками одной организации, а соединяют бизнес-партнеров и обеспечивают связь с внешним миром.

Бизнес становится более уязвимым из-за технических сбоев, человеческих ошибок, действий злоумышленников, хакеров и взломщиков, компьютерных вирусов из-за возрастающей сложности ИТ-инфраструктуры. Вследствие чего требуется управленческий подход, который позволит снизить негативные воздействия инцидентов в области информационной безопасности на бизнес-процессы организации.

Возможно несколько подходов к решению данной проблемы, такие как организация процесса управления инцидентами, организация системы управления информационной безопасности, реализация структурного подхода к управлению инцидентами ИБ. Сравнительная характеристика подходов приведена в таблице 1.

Таблица 1 – Сравнительная характеристика управленческих подходов

Название	Цель	Преимущества	Недостатки
1	2	3	4
Организация процесса управления инцидентами	- уменьшение или исключение отрицательного воздействия нарушений в предоставлении ИТ-услуг [1]	- наиболее быстрое восстановление работы пользователей [1]	- инциденты в области информационной безопасности рассматриваются в совокупности со всеми инцидентами => возможность неправильной оценки степени воздействия и срочности
Организация	- выбор	- фокусировка на	- система

системы управления информационной безопасности	адекватных и пропорциональных средств обеспечения информационной безопасности, которые защищают информационные активы и придают уверенность заинтересованным сторонам [3]	информационной безопасности в целом и инцидентах в области ИБ в частности [3]	управления информационной безопасности не может существовать изолировано => необходима организация общей системы менеджмента => трудоемкая, ресурсозатратная работа

Продолжение таблицы 1

1	2	3	4
Реализация структурного подхода к управлению инцидентами ИБ	- обеспечение обнаружения и эффективной обработки событий ИБ - идентификация и оценка инцидентов ИБ - минимизация воздействий инцидентов на бизнес-процессы - извлечение уроков с целью повышения шансов предотвращения инцидентов в будущем [2]	- улучшение информационной безопасности - усиление внимания к предотвращению инцидентов - сбор качественных данных для идентификации и определения характеристик различных угроз и уязвимостей - предоставление данных о частоте возникновения идентифицированных типов угроз - более быстрое устранение последствий инцидентов [2]	- разработка и документация политик, «Плана реагирования» => трудоемкая, ресурсозатратная работа

Анализ преимуществ и недостатков каждого метода и их сравнение позволяют сделать вывод, что реализация структурного подхода к управлению инцидентами ИБ является наиболее приемлемым методом на начальном этапе организации работы с подобными инцидентами. Организация системы управления информационной безопасности является логичным развитием и дополнением структурного подхода. Организация процесса управления инцидентами необходима при использовании информационных технологий, информационных систем, сервисов, сетей как способ уменьшения влияния различных событий на бизнес в целом.

Рисунок 1 – Модель PDCA (Plan – Do – Check - Act)

Для результативного и эффективного ввода управления инцидентами информационной безопасности на основе структурного подхода необходимо разработать и утвердить политику управления инцидентами ИБ, а также разработать подробную документацию, которая будет включать в себя описание необходимых процедур. В последующем, можно автоматизировать часть процедур или весь процесс управления [2].

Так как организации и их информационные системы меняются, деятельность в рамках управления инцидентами информационной безопасности должна постоянно пересматриваться с целью обеспечения эффективности защиты [2]. Поэтому целесообразно данную деятельность осуществлять на основе модели PDCA (Plan – Do – Check - Act) (рисунок 1).

Таким образом, после организации управления инцидентами в области информационной безопасности на основе структурного подхода заметно снизятся негативные воздействия инцидентов в области информационной безопасности на бизнес-процессы организации, а, следовательно, организация избежит финансовых убытков, нарушения хода бизнес-операций, потери престижа в глазах бизнес-партнеров и клиентов.

Список используемых источников:

1. Бон, Я.В. Введение в ИТ сервис-менеджмент/ Я.В. Бон, М.Ю. Потоцкий. – 2003.
2. ГОСТ Р ИСО\МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – Москва: Стандартинформ, 2009.
3. ГОСТ Р ИСО/МЭК 27001-2005 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Москва, 2008.

МИКРОКОНТРОЛЛЕРЫ И ИХ ПРИМЕНЕНИЕ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Шулаков Е.А. - студент, Борисов А.П. - к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Использование в современном микроконтроллере достаточного мощного вычислительного устройства с широкими возможностями, построенного на одной микросхеме вместо целого набора, значительно снижает размеры, энергопотребление и стоимость построенных на его базе устройств.

Микроконтроллеры используются во всех сферах жизни человека, основные сферы их использования представлены на рисунке 1.

Чаще всего используются простейшие микроконтроллеры с четко запрограммированным назначением.

Рисунок 1 – Сферы применения микроконтроллеров

Для того, чтобы микроконтроллер выполнял необходимые функции должным образом, программистами выполняется большой объем работ по разработке и тестированию прошивок. Все известные компиляторы C/C++ для микроконтроллеров представлены на рисунке 2.

Микроконтроллеры получили широкое распространение в информационной безопасности (ИБ), так как устройства ИБ на основе микроконтроллера гораздо дешевле аналогов, без использования микроконтроллера. Таким образом можно сэкономить на стоимости компонентов, сделать устройство компактным и энергонезависимым. Поэтому специалистам в области ИБ очень важно получение знаний в области программирования и использования микроконтроллеров в ИБ.

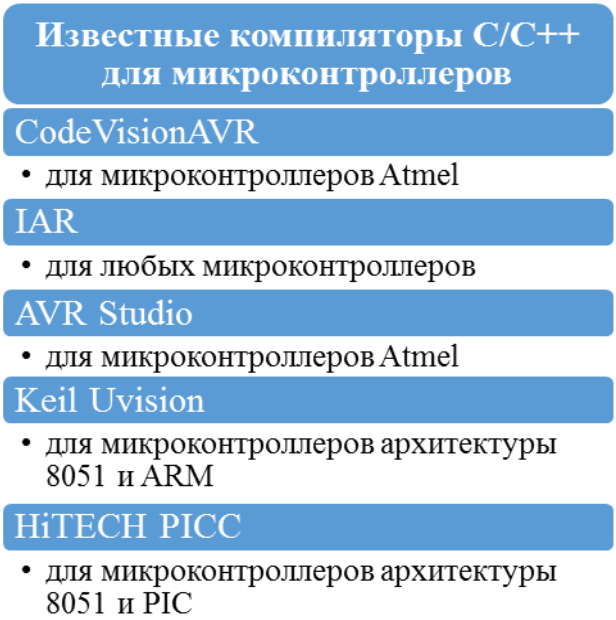


Рисунок 2 - Компиляторы C/C++ для микроконтроллеров

Для получения базовых и углубленных знаний в области программирования микроконтроллеров, студентам специальности 090900 «Информационная безопасность» предлагается изучение дисциплины «Микроконтроллеры и их применение в

информационной безопасности». Данная дисциплина входит в вариативную (профильную) часть учебного цикла. [1]

Для дисциплины «Микроконтроллеры и их применение в информационной безопасности» были разработаны лабораторные задания, рассчитанные на выполнение параллельно теоретическим занятиям в седьмом и восьмом семестрах. [2]

Выполнение лабораторных заданий осуществляется в среде программирования AVR Studio. Главная причина выбора данного ПО – это достаточно широкая распространённость микроконтроллеров фирмы Atmel, благодаря большому выбору как недорогих, так и Hi-End моделей микроконтроллеров по высоким ценам и широкими возможностями. Кроме того, среда программирования AVR Studio напрямую поддерживается фирмой Atmel.

Основные характеристики AVR Studio представлены на рисунке 3. [3] Интегрированный Ассемблер дает возможность написания прошивки на языке ассемблер. Интегрированный симулятор позволяет тестировать прошивку на компьютере, не загружая её в микроконтроллер. Благодаря поддержки компилятора GCC, есть возможность написания прошивки на языке C/C++.

Рисунок 3 - Основные характеристики AVR Studio

В ходе 7 семестра учебного курса специальности 090900 «Информационная безопасность» студентам необходимо выполнить ряд заданий в среде программирования AVR Studio. Задания выполняются, как языке программирования C/C++, так и на языке программирования низкого уровня «ассемблер». [2]

Предполагается выполнение лабораторных работ на следующие темы:

- Лабораторная работа №1,2. «Основы программирования микроконтроллеров»;
- Лабораторная работа №3,4. «Прерывания»;
- Лабораторная работа №5,6. «Цифровые входы/выходы»;
- Лабораторная работа №7. «Таймер/счетчики»;
- Лабораторная работа №8. «Использование аналогового компаратора в микроконтроллере».

Также был разработан стенд на базе микроконтроллера фирмы Atmel. На стенде предусмотрено выполнение лабораторных заданий в ходе 8 семестра учебного курса специальности 090900 «Информационная безопасность».

Процесс выполнения лабораторного задания в 8 семестре проводится в два этапа:

1) Написание и отладка прошивки в среде программирования AVR Studio;
2) Загрузка и тестирование прошивки непосредственно на стенде.

Предполагается выполнение лабораторных работ на следующие темы:

- Лабораторная работа №1. «Сборка USB программатора для микроконтроллера Atmel»;

- Лабораторная работа №2. «Таймер/счетчики»;
- Лабораторная работа №3. «Аналого-цифровой преобразователь (АЦП) в микроконтроллере»;
- Лабораторная работа №4. «Использование аналогового компаратора в микроконтроллере».

Таким образом, разработанные курс заданий и программно-аппаратное обеспечение будет иметь практическое применение, как в рамках лабораторного практикума по дисциплине «Микроконтроллеры и их применение в информационной безопасности», так и в дальнейшей работе по обеспечению информационной безопасности с помощью микроконтроллеров.

Список используемых источников:

1. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 090900 «Информационная безопасность» (квалификация (степень) «бакалавр»).

2. Образовательный стандарт учебной дисциплины Б.3.ДВ.27.2. «Микроконтроллеры и их применение в информационной безопасности» 090900 Информационная безопасность.

3. Atmel Corporation - Microcontrollers, 32-bit, and touch solutions [Электронный ресурс] : Официальный сайт. – Режим доступа: http://www.atmel.com/default.aspx.