РАЗРАБОТКА НА БАЗЕ ARDUINO АВТОМАТИЧЕСКОЙ СИСТЕМЫ КОНТРОЛЯ СПОРТСМЕНА В ЦИКЛИЦЕСКИХ ВИДАХ СПОРТА

Бабин В.Ю. - магистрант, Борисов А.П. – к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

На протяжении многих веков люди стремятся в чем-то быть лучше других и одним из таких направления является спорт. Спортсмены, соревнуясь между собой, доказывают друг другу и всему миру кто самый быстрый, самый точный, самый выносливый, самый продуманный и т.д. Не так давно Россия приняла главное спортивное событие четырехлетия: Олимпийские и Паралимпийские игры. Одним из самый рейтинговых олимпийских видов спорта является биатлон. Кроме Олимпийских игр, соревнования по биатлону проводятся из года в год и Россия принимает этап кубка мира. Большинство зрителей покупает билеты с местами на стадионе, так как огневой рубеж является одним из ключевых мест в соревновании данного вида спорта. Несмотря на это, события активно развиваются на протяжении всей трассы, информацию о которых передают телекамеры. Однако визуальное представление зачастую бывает ложным и для большей картины по трассе расположены временные отсечки, проходя мимо которых, становится известно время лидера и отставание преследователей.

В Алтайском крае временная отсечка всего одна и та на финише, которую судьи фиксируют вручную и для тренеров и зрителей информация становится доступной только после формирования протокола, если комментатор не объявит раньше. Поэтому разработка автоматического процесса считывания информации о прохождении спортсменом временной отметки является одной из актуальных задач. Написание программного обеспечения, которое будет обрабатывать считанную информацию и формировать статистику по текущим данным является продолжением предыдущей задачи.

На рисунке 1 представлена лыжно-биатлонная трасса г. Барнаула с указанием планируемых мест временных отсечек и других объектов. На контрольных отсечках планируется установка оборудования, состоящая из следующих элементов: Arduino Pro Mini, изображение которого представлено на рисунке 2, RFID RC522, образ которого можно увидеть на рисунке 3 и радиомодем, изображенный на рисунке 4.

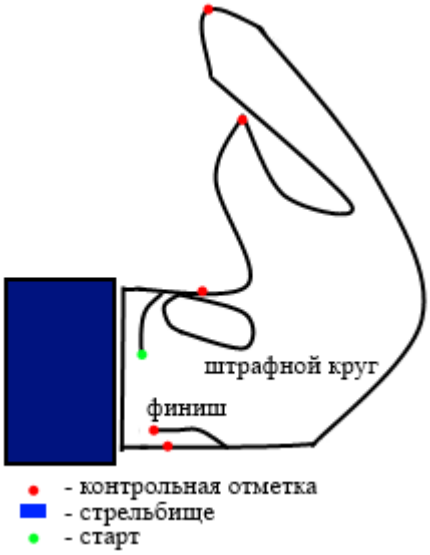


Рисунок 1 – Лыжно-биатлонная трасса

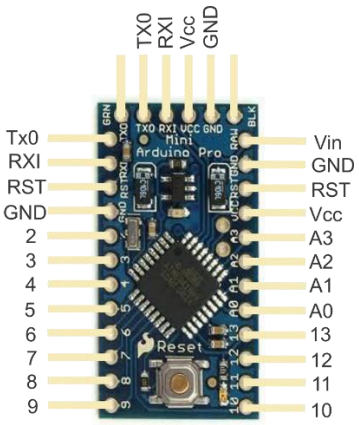


Рисунок 2 – Arduino Pro Mini

Рисунок 3 – RFID RC522

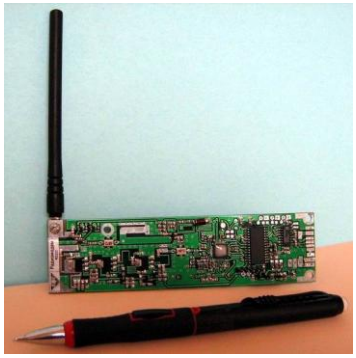


Рисунок 4 – Радиомодем

RFID [2] браслет, фотография которого приведена на рисунке 5, будет крепиться на ногу спортсмена, проходя мимо контрольной отсечки, за счет заряда RFID RC522 [3] передаст свой идентификатор, который, посредством радиомодема, отправится на станцию, установленную на финише, для дальнейшей обработки. RFID RC522 способен считывать до 200 различных идентификаторов в секунду, что сполна покрывает запросы системы. Данная технология находится на всех контрольных отметках.

На финишной станции вместо Arduino Pro Mini, используется Arduino mega 2560, представленная на рисунке 6. Использование представленной замены позволяет добиться необходимой производительности при обработке данных. Кроме того, к Arduino mega 2560 добавлен Ethernet модуль для передачи всех считанных данных на компьютер. Внешний вид Ethernet модуля представлен на рисунке 7.

Рисунок 5 – RFID браслет

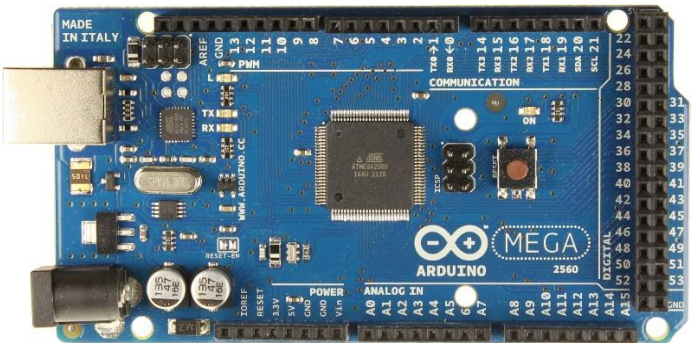


Рисунок 6 – Arduino mega 2560

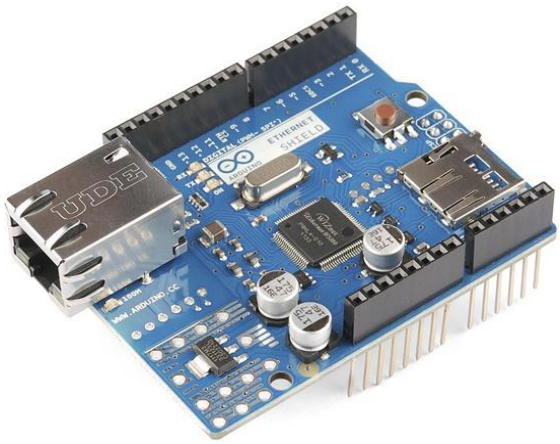


Рисунок 7 – Ethernet модуль

На компьютере данные будут обрабатываться написанным программным обеспечением, которое в свою очередь будет взаимодействовать с базой данных. При прохождении спортсменом контрольной отсечки считанный идентификатор передается на станцию расположенную в стартовом городке, которая пересылает данные на компьютер.

Программное обеспечение, находит в базе данных принятый идентификатор и формирует промежуточный результат с фамилией, временем и стартовым номером, в соответствии идентификатору. В базе данный хранится информация о спортсмене: фамилия, имя, отчетво, пол, регион, стартовый номер, возраст, идентификатор чипа, количество промахов (по рубежам), время каждой промежуточной отсечки и финишное время. Из полученной информации высчитывается время лыжного хода (без учета стрельбы), время потраченное на стрельбу и другая аналитическая информация. Правила IBU [1] гласят о нескольких видах нарушения, таких как: не выстреленный патрон, не прохождение штрафного круга, преждевременный старт (менее трех секунд и более трех секунд), последнее применяется в гонке преследования. По окончанию соревнований возможно внесение изменений в протокол, согласно перечисленным и другим нарушениям, с последующим его формированием и возможностью печати.

Таким образом планируется разработка автоматической системы контроля спортсменов, на примере соревнований по биатлону, оперативно передающую считанные данные на центральный компьютер, который в свою очередь занимается обработкой и выводит на экран интересующую информацию. Благодаря собранным данным представленной системы, тренер может тщательно анализировать передвижения спортсмена, время потраченной на огневые рубежи и на полагаясь на собранные данные внести коррективы в тренировочный процесс и усилить слабые стороны сортсмена.

СПИСОК ЛИТЕРАТУРЫ

1. Правила IBU [Электронный ресурс]. Режим доступа: URL: http://www.biathlonworld.com/media/files/rules_2013/IBU_Rules_2012_r_cap1_finish.pdf.

2. Д.Хант, RFID - A Guide to Radio Frequency Identification //Wiley, 2007

3. Барсуков В.С. RFID или не RFID? Вот в чем вопрос. // Специальная техника. 2005. - №6.

РАЗРАБОТКА МОДУЛЯ ПЕРЕДАЧИ И ЗАЩИТЫ ДАННЫХ НА БАЗЕ ARDUINO И МОДУЛЕЙ XBEE

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

В настоящее время подготовка специалистов в области информационных технологий должна проводиться с учетом все нарастающих темпов технического прогресса. От того насколько она будет отвечать этим темпам зависит не только будущее трудоустройство выпускников, но и возможно будущее ИТ в целом. Так методические рекомендации актуальные еще три года назад, сегодня уже не принесут должного эффекта и могут в некоторых случаях считаться устаревшими.

Глубокий анализ аппаратных и программных решений на рынке позволит определить тенденции развития технологий. На основании этого прогноза и необходимо строить те или иные методические рекомендации и курсы.

Так, например, технология ZigBee выходит за границы исследовательских лабораторий и начинает широко применяться на практике для создания беспроводных сетей датчиков, систем автоматизации зданий, устройств автоматического считывания показаний счетчиков, охранных систем, систем управления в промышленности [3].

Остановимся подробнее на использовании ZigBee для создания охранных систем. Опыт охраны объектов различных категорий показал, что наиболее эффективным и экономически выгодным ее видом является централизованная охрана с использованием систем передачи извещений. Последние годы характеризуются активным развитием и внедрением радиоканальных систем передачи извещений (РСПИ).

Внедрение охранных систем, использующих радиочастотные каналы связи, позволяет:

- расширить сферу деятельности как подразделений вневедомственной охраны, так и частных мониторинговых компаний путем организации охраны объектов, не имеющих надежные каналы связи, которые бы обеспечили оперативную передачу информации;
- повысить надежность систем охраны особо важных объектов за счет дублирования проводных каналов связи;
- обеспечить при необходимости оперативную установку оборудования на объекте, нуждающемся в охране.

Оценка возможностей применения современных технологий передачи извещений показала, что наиболее эффективной для систем ближнего радиуса действия является ZigBee.

Особенность ZigBee заключается в том, что в отличие от других беспроводных технологий она предназначена для реализации не только простых соединений "точка - точка" и "звезда", но также и сложных сетей с топологиями "дерево" и "ячеистая сеть", способных поддерживать ретрансляцию и поиск наиболее эффективного маршрута для передачи данных.

За счет реализованной ретрансляции в каждом элементе такой сети отпадает необходимость в прямом канале связи между оконечным устройством и пультом централизованного наблюдения (ПЦН), что в свою очередь позволяет значительно снизить мощность передатчика, а вместе с этим и его стоимость [1].

Сети ZigBee при относительно небольших скоростях передачи данных обеспечивают гарантированную доставку пакетов и защиту передаваемой информации.

Модули ZigBee могут быть подключены к микроконтроллерам, различным ARM, а также к такой аппаратно вычислительной платформе как Arduino с помощью модуля Xbee shield.

Анализ рынка показал, что самым простым и дешевым способом, при этом обладающим исчерпывающим функционалом, является подключение модулей ZigBee к Arduino.

Arduino – это инструмент для проектирования электронных устройств (электронный конструктор) более плотно взаимодействующих с окружающей физической средой, чем стандартные персональные компьютеры, которые фактически не выходят за рамки виртуальности. Это платформа, предназначенная для «physical computing» с открытым программным кодом, построенная на простой печатной плате с современной средой для написания программного обеспечения.

Arduino применяется для создания электронных устройств с возможностью приема сигналов от различных цифровых и аналоговых датчиков, которые могут быть подключены к нему, и управления различными исполнительными устройствами. Проекты устройств, основанные на Arduino, могут работать самостоятельно или взаимодействовать с программным обеспечением на компьютере (например Flash, Processing, MaxMSP). Платы могут быть собраны пользователем самостоятельно или куплены в сборе. Среда разработки программ с открытым исходным текстом доступна для бесплатного скачивания.

Язык программирования Arduino является реализацией Wiring, схожей платформы для «physical computing», основанной на мультимедийной среде программирования Processing [2].

Итак, использование Arduino дает следующие преимущества:
- низкая стоимость;
- кроссплотформенность;
- простая и понятная среда программирования;
- расширяемость;

В результате анализа параметров и цен была выбрана следующая элементная база для разработки модуля:
- Контроллер Arduino Nano (Atmega 328);
- Модуль связи Xbee shield [Nano], Freeduino;
- ZIGBEE радиомодем (модуль) XBEE-PRO S2, Digi International Inc;

Программное обеспечение для Arduino будет написано в одноименной программной среде. Также будет создана программа на языке C# для использования на ПК. Данное ПО будет осуществлять инициирование приема/передачи сообщений, а также обеспечение защиты передаваемой информации с использованием алгоритма шифрования AES-128.

При запуске приложения пользователю будет предложено выбрать COM – порт, к которому подключена плата Arduino, а также скорость передачи данных. Далее пользователь может либо сам напечатать текст передаваемого сообщения, либо загрузить его из файла. Далее в зависимости от поставленной задачи, может быть выбран режим включающий шифрование. При нажатии на кнопку «Отправить», сообщение по последовательному порту будет передано на Arduino, который в свою очередь передаст его на подключенный модуль Xbee. На принимающей стороне аналогичная связка - микроконтроллер и беспроводной модуль осуществляют прием передаваемого сообщения. Принятое сообщение появится в соответствующем окне программы, предварительно (если было включено шифрование) расшифрованное.

Для решения поставленных задач выбор программных и аппаратных средств являются наиболее рациональным.

В качестве целевой аудитории для выполнения лабораторных работ с использованием разрабатываемого модуля могут выступать группы направлений Информационная безопасность и Информатика и вычислительная техника в рамках соответствующих дисциплин. Для групп ИБ – Сети и системы передачи информации, для ИВТ – Микроконтроллерные системы сбора и обработки данных.

Использование разрабатываемого модуля не ограничивается рамками лабораторной работы. Например, путем внесения некоторых изменений он может быть адаптирован для использования в качестве приемопередатчика системы контроля управления доступа.

Список используемых источников

1. Международный форум Технологии безопасности [Электронный ресурс].
Режим доступа: http://www.secuteck.ru/articles2/firesec/ohrannye-samoorganizuyushiecya-radioseti - Загл. с экрана.
2. Arduino.ru [Электронный ресурс]. Режим доступа: http://arduino.ru – Загл. с экрана.
3. RTLS [Электронный ресурс]. Режим доступа: http://www.rtlsnet.ru/technology/view/3 - Загл. с экрана.

ЗАЩИТА ИНФОРМАЦИИ ПРИ ТЕЛЕФОННЫХ ПЕРЕГОВОРАХ ПУТЁМ СКРЕМБЛИРОВАНИЯ РЕЧЕВОГО СИГНАЛА

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

В современном обществе информация является товаром, соответственно имеет определённую ценность. Сохранение её от несанкционированного доступа (НСД) – основная работа специалиста по информационной безопасности. В наше время телефон представляет собой наиболее распространённый инструмент общения, следовательно, выступает как стратегически важный объект. Вот почему защита информации от перехвата при телефонных переговорах бесспорно актуальна на сегодняшний день.

Съём информации с телефонной линии возможен при контактном подключении, или через индукционный датчик. С каждым годом появляются всё более новые виды закладных устройств (ЗУ), пребывание которых в линии связи становится всё менее и менее заметным. Пассивные методы защиты и анализаторы телефонных линий не способны в полной мере защитить информацию от утечки, т.к. могут просто не опознать ЗУ. Для эффективной защиты необходимо использовать устройство, способное закодировать передаваемые в реальном масштабе времени данные. При этом злоумышленник сможет осуществить съём

зашифрованного сообщения, но пользы оно не принесёт, т.к. к моменту своего расшифровывания информация станет устаревшей, либо, её так и не удастся декодировать.

Таким образом, на сегодняшний день самым надёжным способом защиты информации при телефонных переговорах является скремблирование. Скремблеры способны зашифровать как входящее, так и исходящее сообщение (в отличие от односторонних маскираторов).

Специалистам по информационной безопасности необходимо иметь обширные знания в области технической защиты информации (ТЗИ), в частности защиты аналоговых телефонов от НСД к конфиденциальным сведениям. Целью данной работы является закрепление на практике знаний, полученных в теоретическом курсе по ТЗИ, для возможности применения их в профессиональной деятельности.

В задачи, необходимые для достижения поставленной цели входит:

- Анализ необходимости защиты аналоговых телефонных линий;
- Анализ способов защиты телефонных линий;
- Анализ схем скремблеров;
- Разработка программно-аппаратного комплекса для лабораторного практикума.

Процесс скремблирования может осуществляться двумя методами: аналоговыми или цифровыми преобразованиями речи. При этом возможно изменение исходных данных по трём параметрам: амплитуде, частоте, фазе. Основными методами преобразования речевого сигнала являются: частотные, временные и комбинированные преобразования.

При аналоговом скремблировании характеристики исходного сигнала изменяются таким образом, что конечный сигнал становится невозможно распознать, но он остаётся в исходной полосе частот. Это позволяет передавать сигнал по тем же каналам, что и обычную речь.

Цифровое скремблирование является более точным. При данном типе шифрования необходимо первоначально представить непрерывный аналоговый сигнал в виде дискретного, а после выполнять преобразования [1].

Процесс шифрования происходит следующим образом: исходное сообщение от первого абонента кодируется с помощью скремблера, восстановление информации происходит только на устройстве второго абонента (рисунок 1). Таким образом, на всей линии связи информация засекречена. Однако у данной системы есть минус, который заключается в необходимости установки клиентами совместного оборудования.

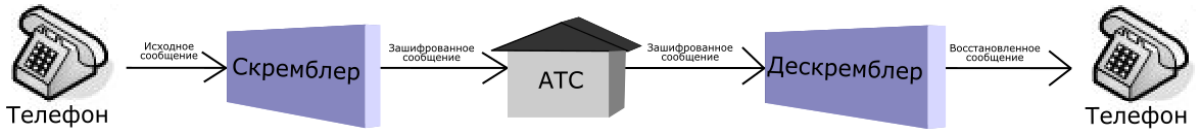
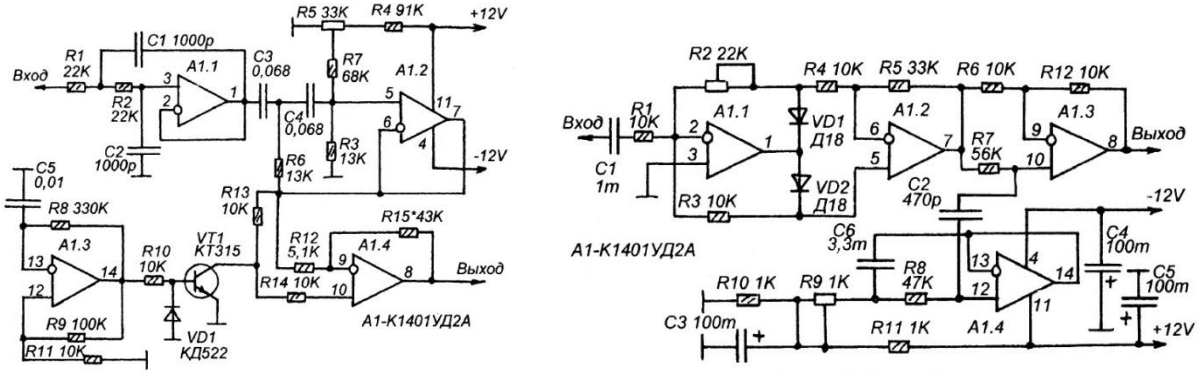


Рисунок 1 – Подключение скремблера и дескремблера к телефонной линии

В ходе разработки пособия будут подобраны схемы для самостоятельного воссоздания, согласно вариантам задания. В частности одна из схем представлена на рисунке 2.



а) б)

Рисунок 2 – Принципиальные схемы: а) скремблер; б) дескремблер

В представленном скремблере входной сигнал поступает на фильтр верхних частот (ФВЧ) второго порядка, затем на операционный усилитель (ОУ) А1.1. На ОУ А1.2 собран фильтр нижних частот (ФНЧ). Так как форманты, определяющие разборчивость речи при телефонных разговорах, расположены в полосе частот 0,3 – 3,4 кГц, остальные частоты могут быть отфильтрованы. На ОУ А1.3 настроен генератор прямоугольных импульсов. Генератор управляет знаком коэффициента усиления на ОУ А1.4 при помощи транзистора VT1. С выхода А1.4 снимается закодированный сигнал.

В декодере ОУ А1.1 и два диода реализуют инверсию и разделение полуволн на положительные и отрицательные. Отрицательные при прохождении через усилитель А1.2 инвертируются, положительные остаются неизменёнными. На ОУ А1.3 и А1.4 собран режекторный фильтр, настроенный на частоту кодирования скремблера [2].

Для более детального изучения материала необходимо продолжать работу в данном направлении, осваивая различные методы скремблирования. Итогом должно стать создание лабораторного комплекса по обеспечению конфиденциальности информации с помощью криптографических средств защиты при телефонных переговорах. Также необходимо создание программно-аппаратных средств ЗИ, реализованных в данном комплексе.

Список использованной литературы:

1. Каторин Ю.Ф., Куренков Е.В., Остапенко А.Н. Большая энциклопедия промышленного шпионажа. – СПб: ООО "Издательство Полигон", 200. – 896 с.

2. Уваров А.С. Скремблер [Текст] / А.С. Уваров // Радиоконструктор. – 2001. - №12. – с. 24-25.

ФОРМИРОВАНИЕ АЛГОРИТМА РАСЧЕТА УРОВНЯ СООТВЕТСТВИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРЕДИТНЫХ ОРГАНИЗАЦИЙ СТАНДАРТУ БАНКА РОССИИ

Будовских И.А. – студент, Алфёрова Л.Д. – старший преподаватель

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

Аудит информационной безопасности организации необходим для своевременного выявления, прогнозирования источников и характера внутренних, и внешних угроз информационной безопасности (ИБ), оценки рисков интересов субъектов информационных отношений, разработки и принятия мер оперативного реагирования на угрозы ИБ, проектирования и создания эффективной системы защиты.

Практически в каждой кредитной организации присутствует отдел информационной безопасности и именно на плечи его сотрудников ложатся обязанности проведения аудита, будь это внутренняя самооценка или организация и помощь в проведении внешнего аудита с привлечением аудиторской организации.

Зачастую не все руководители организаций воспринимают оценку рисков должным образом. Поэтому не всегда одобряют внешний аудит, так как он влечет за собой определенные риски и огромные финансовые затраты. В связи с этим специалистам по защите информации приходится проводить аудит своими силами, то есть проводить самооценку[1].

На сегодняшний день существует ряд определенных методик, по которым можно провести самооценку кредитной организации[1]. Одна из них принадлежит Банку России и носит название «Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС – 1.0 – 2014»[4].

Особенностью данной методики является то, что она основана на международном стандарте ISO 27001, который в свою очередь является сборником лучших мировых практик по управлению информационной безопасностью. Так же методика учитывает специфику кредитных организаций[1].

По данным центрального банка, на 1 января 2015 года, комплекс СТО БР ИББС ввели в действие 530 организаций (81%). Из них 40 проводили аудит с привлечением сторонних организаций и 304 в виде самооценки[2].

Данная статистика показывает, что методика оценки информационной безопасности является очень популярной, но и в то же время очень трудоемкой. Процесс подсчета групповых и частных показателей может затянуться не на один месяц, что приводит к менее актуальному определению итогового уровня соответствия ИБ кредитной организации требованиям стандарта. В связи с этим автоматизация данного процесса является очень актуальным вопросом.

На рисунке 1 представлен алгоритм расчета уровня соответствия ИБ кредитных организаций требованиям стандарта Банка России[3].

Данный алгоритм сформирован на основании методики СТО БР ИББС – 1.2 – 2014[4].

Описание блоков алгоритма:

1. Инициализация переменных:

-EV1 – степень соответствия текущего уровня ИБ организации;

-EV2 – степень соответствия менеджмента ИБ организации;

-EV3 – степень соответствия уровня осознания ИБ;

-EVM[34,60] – двумерный массив, содержащий значения всех частных показателей;

-KolPokaz[34] – одномерный массив, содержащий количество частных показателей в каждой группе;

-KolNO[34] – одномерный массив, содержащий количество частных показателей, которым присвоено значение «Н/О» (нет ответа) соответственно для каждой группы;

-KolZero[34] – одномерный массив, содержащий количество частных показателей, которым присвоено значение «0» соответственно для каждой группы;

-EVMmean[34] – одномерный массив, содержащий среднее значение частных показателей для каждой группы;

-Sum – вспомогательная переменная для вычисления степеней соответствия;

-k – корректирующий коэффициент (корректирует степени соответствия);

-EVbitp – степень соответствия банковского информационного технологического процесса;

-EVbptp – степень соответствия банковского платежного технологического процесса;

-EV2ozpd – степень выполнения требований регламентирующих защиту персональных данных в ИСПД, с учетом оценки степени выполнения требований по обеспечению ИБ при использовании СКЗИ;

-EVoopd – степень выполнения требований регламентирующих обработку персональных данных;

-R – итоговый уровень соответствия ИБ организации требованиям стандарта Банка России.

2. Второй блок отвечает за присвоение значений частным показателям (0; 0,25; 0,5; 0,75; 1; Н/О – частный показатель не относится к специфики организации).
3. Считается количество нулевых показателей и показателей со значением «Н/О» для каждой группы.
4. Определяются средние значения для каждой группы частных показателей.
5. Определяется текущий уровень информационной безопасности организации. Он определяется как минимальный из показателей EVbitp, EVbptp, EV2ozpd, EVoopd.
6. Определяется уровень менеджмента информационной безопасности организации EV2.
7. Определяется уровень осознания информационной безопасности EV3.
8. Определяется итоговый уровень соответствия информационной безопасности организации требованиям стандарта. Он определяется как минимальный из показателей EV1, EV2 и EV3.

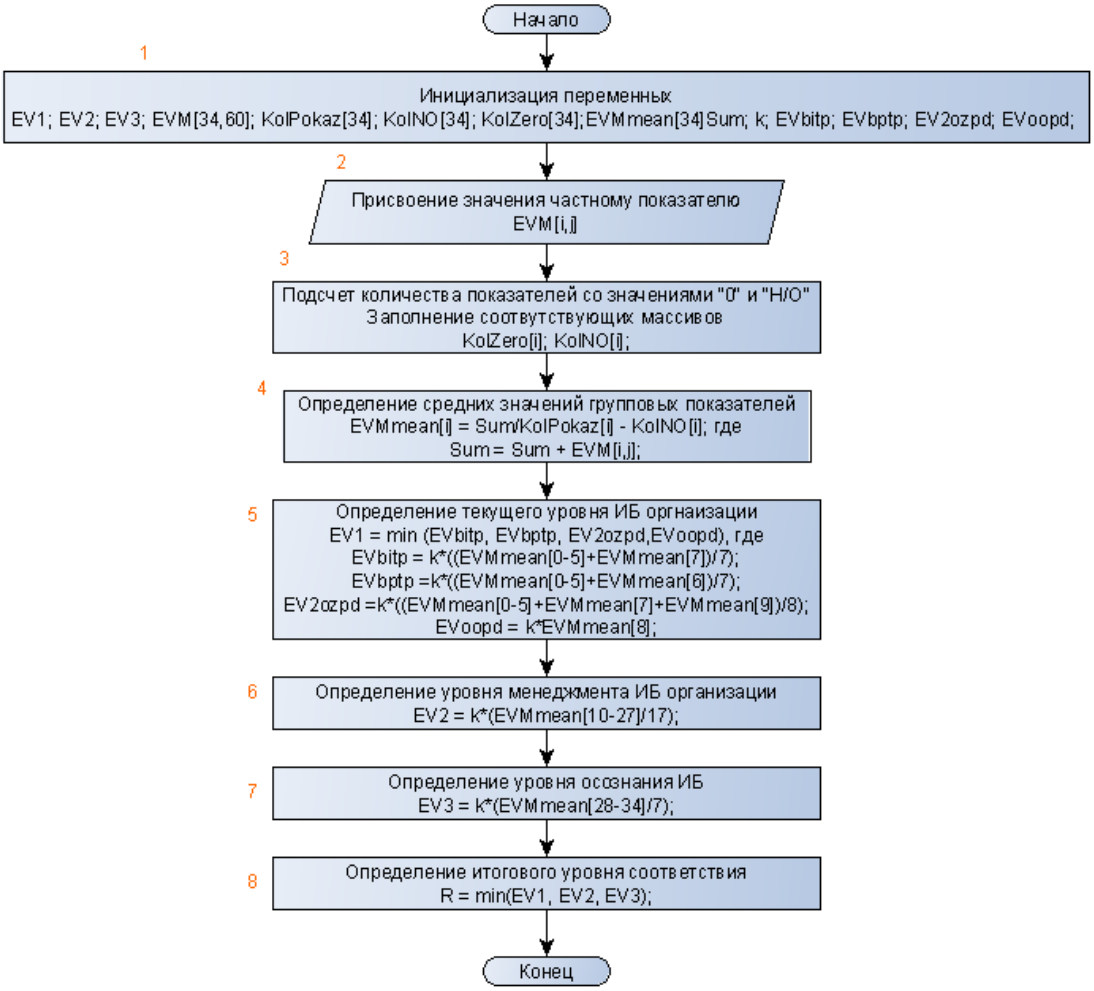


Рисунок 1 – Алгоритм расчета уровня соответствия ИБ кредитных организаций

Представленный алгоритм расчета позволяет сократить временные промежутки определения групповых и частных показателей, минимизировать затраты на проведения аудита, комплексно подойти к решению задач определения текущего и итогового уровней соответствия ОИ кредитной организации требованиям стандарта Банка России.

Список используемых источников

1. Лугацкий, А. Аудит информационной безопасности: какой, кому, за-чем? [Электронный ресурс] / Режим доступа: http://bosfera.ru/bo/audit-informatsionnoj-bezopasnosti

2. Центральный банк Российской Федерации. Информационная безопасность организаций банковской системы Российской Федерации [Электронный ресурс] / Режим доступа: http://www.cbr.ru/credit/Gubzi_docs/

3. Центральный банк Российской Федерации. Стандарты Банка России [Электронный ресурс] / Режим доступа: http://www.cbr.ru/credit/Gubzi_docs/main.asp?Prtid=Stnd

4. Стандарт СТО БР ИББС – 1.2 – 2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС 1.0 – 2014. – М. Изд-во стандартов, 2014. – 101 с.

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОЦЕНКИ РИСКОВ ИБ МЕТОДОМ ЛОГИКО-ВЕРОЯТНОСТНОГО МОДЕЛИРОВАНИЯ СЦЕНАРИЕВ РЕАЛИЗАЦИИ УГРОЗ

Воробьев О.Е. – студент, Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Одним из важнейших факторов при проектировании информационных систем является обеспечение безопасности их функционирования. В настоящее время это условие выполняется за счет внедрения системы менеджмента ИБ на уровне организации, основной задачей которой является выявление потенциальных факторов угроз и уязвимостей информации, которой оперирует данная ИС, и, в частности, как подсистему СУИБ, выделяют систему менеджмента риска ИБ, которая непосредственно реализует выполнение процедур анализа и оценивания рисков ИБ. Методики разработки и внедрения системы менеджмента ИБ и менеджмента риска содержатся в стандартах серии ГОСТ Р ИСО/МЭК 27001 и 27005, соответственно [1,2]. Стандарт ГОСТ Р ИСО/МЭК 27005-2010 содержит методику управления рисками, однако не содержит конкретных методик оценки риска, а существующие средства автоматизации уже устарели и их приобретение достаточно затратно для предприятий малого бизнеса.

Реальные результаты в проявлении угроз и уязвимостей, а также дальнейшее использованием полученной информации для реконфигурации защитных и управляющих механизмов ИС, может быть получено только на основе количественной оценки рисков ИБ, что существенно влияет на выбор методики, реализуемой в программном обеспечении предназначенным для этого.

Анализ методик оценки рисков, которые сосредоточены в ГОСТ Р ИСО/МЭК 31010-2011 [3], показал целесообразность использования методик анализа дерева неисправностей и анализа дерева событий для графического и аналитического описания ситуаций риска ИБ, для первичного описания же условий возникновения риска целесообразно использовать аппарат математической логики, методы теории вероятности и комбинаторные методы – для количественной оценки.

Выбранная методика оценки риска соответствует требованиям, изложенным в ГОСТ Р ИСО/МЭК 27005-2010, в описании процесса менеджмента риска ИБ, и, в частности, итеративному подходу к проведению оценки риска.

Исходя из выбранных критериев, была выбрана методология оценки рисков ИБ сценарным логико-вероятностным моделированием, которая изложена в [4].

Проведен анализ уже имеющегося на рынке доступного ПО для проведения оценки рисков (PTA, vsRisk, RMStudio, Гриф). Результат анализа: некоторые реализации данного вида программного обеспечения были выпущены достаточно давно, чтобы учесть все факторы, касающихся угроз и уязвимостей, актуальных на сегодняшний день, и соответственно их использование является крайне вынужденной мерой. Большинство программных продуктов имеет несоизмеримо с прибылью коммерческих организаций малого и среднего бизнеса стоимость, и в связи с этим последние не имеют возможности приобретения подобных программных продуктов. Исходя из данных выводов, целесообразно реализовать программное обеспечение для оценки рисков ИБ с актуальными базами угроз и уязвимостей, имеющее низкую стоимость, что делает его доступным для организаций малого и среднего бизнеса. Так же следует отметить, что заявленное ПО отличается логичным и простым управлением, что делает его использование в организациях с низким уровнем зрелости относительно вопросов ИБ.

Этапы вероятностной оценки рисков ИБ:

1. Определение факторов риска z_1, z_2, …, z_n. На данном этапе происходит построение фрагментов дерева событий ИБ в виде итерационного процесса, где каждое событие представляет собой сочетание характеристик угроз. На каждой итерации фрагменты проходят проверку путем вероятностной оценки событий, заключенных в данный фрагмент по заданному критерию пригодности (КПФ). После этого определяются потенциальные ситуации риска. На основе полученного перечня возможных ситуаций риска строится дерево нарушений; для каждого нарушения выявляются порождающие его причины, причем

нарушение описывается в виде сочетаний характеристик уязвимостей. Определяются вероятности причин нарушений для построения базисного вектора вероятностей аргументов Л – функции риска;

2. Построение Л-функции риска $y(z_1, z_2, \ldots, z_n)$. Используя математический аппарат алгебры логики строится сценарий ситуаций риска;

3. Определение В – полинома риска $P(y(z_1, z_2, \ldots, z_n))$. Построение многочлена расчетной вероятностной функции.

Для построения дерева событий (ДС) используются данные о составе активов, данные о угрозах и уязвимостях для этих активов. Вводятся интервальные значения пригодности фрагментов, которые позволят ограничить объем анализа ДС. Вероятностная оценка фрагмента ДС ИБ основана на представлении каждого события в виде сочетания характеристик угроз ИБ, определения их истинности и вычисления уровня угроз. Характеристиками угроз в данном случае являются: источник угрозы, объект воздействия, способ реализации, результат воздействия. Для каждой угрозы имеется некоторый перечень заданных характеристик, поэтому сочетания угроз представляют собой конъюнкцию от дизъюнкции множества характеристик каждого типа. Далее, выделяются нижняя и верхняя граничные оценки вероятности реализации угроз. Вероятность угрозы определяется как сумма из средних арифметических границ диапазона и характеристики относительной ошибки. В результате анализа ДС ИБ определяются ситуации риска, сценарии которых строятся в ходе анализа дерева нарушений (ДН) ИБ. При анализе ДН ИБ рассматриваются группы нарушений, наименьшая из которых при возникновении составляющих ее нарушений в надлежащей последовательности дает ситуацию риска; если этого не возникает – риск не реализуется. Вероятностная оценка причин возникновения нарушений ИБ основана на представлении каждого нарушения в виде сочетания характеристик уязвимостей системы. К ним относятся: метод использования, объект размещения, источник появления, результат использования, механизм защиты. Сочетания строятся на базе конъюнкции от дизъюнкции характеристик каждой группы. Определяются вероятности исходов сочетаний характеристик уязвимостей и на их основе строится базисный вектор вероятностей аргументов Л – функции риска.

Для определения функции Л – риска используется раскрытие всех функций нарушений ИБ и представление их в виде конъюнкций и дизъюнкций (возможно комбинирование) причин нарушений ИБ. Аргументы Л – функции проходят процедуру оценивания их веса (степени значимости). Вес есть не что иное как отношение булевой разности отдельно взятой причины нарушения к числу всех наборов m – мерного логического пространства, где m – мощность множества причин нарушений:

$$g_{z_i} = \sum_{f=1}^{k} 2^{-(r_f - 1)} - \sum_{j=1}^{l} 2^{-(r_j - 1)} \quad ,$$

где l и r – число и ранг ортогональных конъюнкций. Таким образом происходит ранжирование элементов ДН ИБ по степени их важности.

При построении расчетной вероятностной функции происходит переход от логических переменных к вероятностным, от булевых операций – к арифметическим. В результате будет получено выражение, численное значение которого есть вероятностная оценка возникновения ситуации риска.

На рисунке 1 представлена блок – схема алгоритма интерпретатора системы – он формирует ДС и ДН ИБ, Л – функцию и В – полином. Процедуры А и Б представляют собой алгоритмы анализа ДС ИБ и ДН ИБ, соответственно.

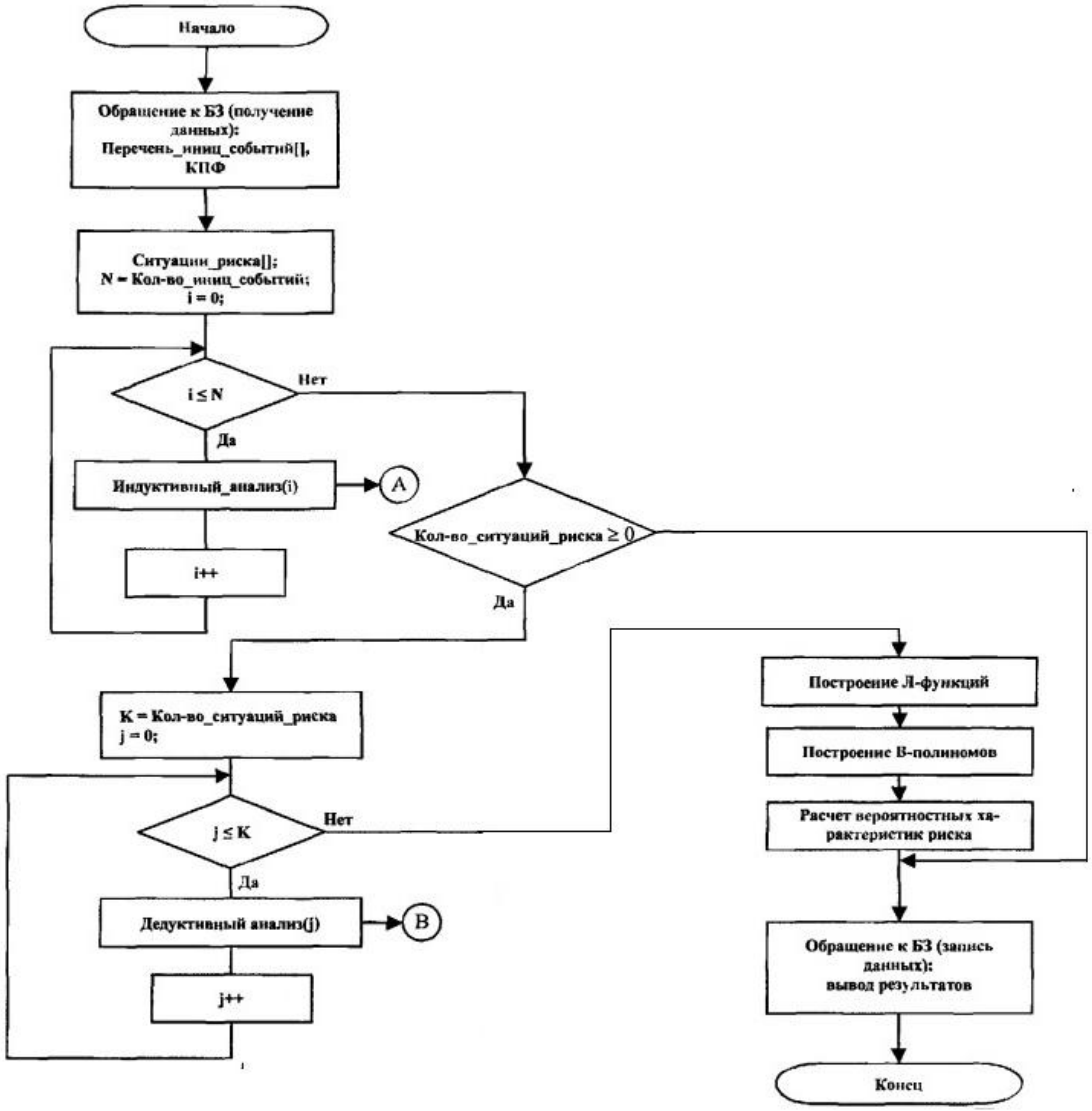


Рисунок 1 – Алгоритм работы интерпретатора

Для реализации заявленного программного обеспечения используется среда Microsoft Visual Studio 2013. В качестве языка программирования, на котором реализовано ПО, выбран язык C++ ввиду его гибкости и функциональности.

Список использованной литературы:

1. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Требования». http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii

2. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска ИБ». http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii

3. Национальный стандарт РФ ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска». http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii

4. Котенко А.Г. Метод оценки риска ИБ на основе сценарного логико-вероятностного моделирования. Санкт-Петербург: СПбГУ ИТМО, 2014. - 116 с.

БИОМЕТРИЧЕСКАЯ ЗАЩИТА НА ОСНОВЕ ПРОВЕДЕНИЯ АУТЕНТИФИКАЦИИ ПО ТЕМБРУ ГОЛОСА

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

Разграничение доступа к информации является одним из способов ее защиты. На данный момент в подавляющем большинстве случаев, для защиты данных используется различного рода парольные системы, либо системы, работающие с аппаратными ключами. Недостатком таких систем является то, что пароли часто не проходят по сложности или записываются на видных местах, а аппаратные ключи могут быть украдены или потеряны. Выходом из сложившейся ситуации может стать использование биометрических характеристик человеческого организма для аутентификации пользователя. Биометрические признаки сложно подделать, их практически невозможно потерять. Со стороны же пользователя процесс аутентификации становится прозрачным и естественным. Отдельно стоит выделить аутентификацию на основе тембра голоса. Значительным преимуществом является простота реализации аппаратной части системы, микрофоны являются неотъемлемой частью современных устройств, а развитие систем обслуживания пользователей по телефону делает системы аутентификации на основе тембра голоса актуальной областью развития компьютерной техники.

Целью работы является разработка программного средства осуществляющего разграничение доступа к ресурсам компьютера на основании проведения аутентификации по голосу.

Цель работы достигается при решении задач:

1. Реализация алгоритмов детектирования сигнала и его обработки.
2. Изучение методов извлечение признаков из звукового сигнала и реализация их в программе.
3. Изучение алгоритмов распознавания и их реализация.
4. Реализация подсистемы регистрации пользователя и хранение данных о нем в системе.
5. Реализация подсистемы разграничения доступа.

В работе таких систем можно выделить следующие этапы:

1. Получение данных.
2. Предобработка данных.
3. Извлечение признаков.
4. Постобработка признаков.
5. Распознавание, принятие решения.

Для получения данных используется микрофон компьютера и встроенная звуковая карта. Звуковая карта выступает в качестве аналого-цифрового преобразователя (АЦП). Для АЦП важными характеристиками является частота дискретизации и разрядность. Исходя из характеристик человеческого голоса и теоремы Котельникова, частоту дискретизации необходимо взять не ниже 8000Гц. При выборе разрядности следует руководствоваться значением отношения сигнал/шум. Для обеспечения соотношения сигнал/шум 36дБ требуется не менее семи разрядов, а для получения высококачественного цифрового кодирования не менее 11. На практике же используется 16, 24 и 32 разряда [1].

После детектирования, для упрощения последующей обработки, сигнал необходимо разделить на кадры, которые будут перекрывать друг друга. Необходимость перекрытия вызвана влияниями соседних амплитуд, не вошедших в кадр (фрэйм). Опытным путем установлено, что оптимальная длина фрейма является 10мс, прикрытие 50% [2].

Полученный сигнал необходимо обработать, для отчистки его от шумов, и увеличения в нем доли полезной информации. Для этого применяют КИХ – фильтр и оконное взвешивание. Фильтр с конечной импульсной характеристикой убирает сетевой шум 50Гц и увеличивает мощность сигнала на 20дБ, повышая эффективность анализа. Оконное

взвешивание необходимо применять в связи с тем, что кадр ограничен во времени, поэтому при переходе в частотную область будет происходить эффект просачивания спектра боковых лепестков. Оконное взвешивание призвано уменьшить этот эффект [2].

Основное назначение стадии извлечения признаков – это уменьшение объема входных данных без потери значимой информации – признака. В качестве признака аудио сигнала можно выделит следующие характеристики:

1. Основная частота.
2. Энергия сигнала.
3. Различные спектральные характеристики.

Основная частота – это определенная частота, с которой вибрируют голосовые связки человека во время речи. Раньше, в виду сложности её определения этой частотой часто пренебрегали в системах распознавания речи, но на данный момент существуют классы алгоритмов способных решить эту вычислительную задачу.

Использование, какого-либо вида измерения энергии в распознавании речи привлекательно, из-за простоты реализации. При подсчете энергии массив значения сигналов умножается на оконную функцию, затем энергия подсчитывается по известной функции поочерёдно, кадр за кадром. Саму энергию часто считают не напрямую, а по логарифмической шкале [2].

Одним из наиболее легких способов определения спектральных характеристик является банк Фурье-фильтров. Преобразование Фурье позволяет определить «весовую» составляющую частот спектра взвешенных соответствующими амплитудами. В компьютерной технике применяется дискретное преобразование Фурье (ДПФ), так как позволяет работать с конечными последовательностями. ДПФ работают за время $O(N^2)$, что достаточно долго. Алгоритмы быстрого преобразования Фурье (БПФ) позволяет произвести расчет за время O(Nlog(N)). Основной принцип данных алгоритмов заключается в разбиение последовательностей. Для примера, имея последовательность из N точек, БПФ для нее вычисляется за N^2. Если эту последовательность разделить на две, то вычисление этих двух последовательностей займет $\frac{N^2}{2}$. Разбиение исходной последовательности можно продолжать пока возможно ее деление на 2. Распространение получили алгоритмы прореживания по частоте и по времени [4].

После извлечения необходимых признаков сигнала для их дальнейшего использования производится нормализация признаков так, чтобы каждый компонент вектора признаков имел среднее значение 0 и стандартное отклонение 1.

Принятие решение о допуске человека к информации происходит на основе распознавания – сравнение образца речи введенного в систему в момент аутентификации, с шаблоном запомненным системой в момент регистрации пользователя. Во время регистрации пользователя происходит обучение системы – создание определенного класса. Классы объектов можно представить в виде областей в многомерном пространстве решений, это и есть шаблоны голоса пользователей системы, полученные на этапе их регистрации. Данные полученные в результате аутентификации пользователя можно представить в виде точки в этом пространстве, которую можно отнести к той или иной области с помощью того или иного алгоритма [3]. На данный момент наибольшее распространение получили системы, построенные на алгоритмах, которые можно разделить на пять больших категории:

1. Методы дискриминатного анализа, основанные на Байесовской дискриминации.
2. Скрытые модели Маркова.
3. Метод опорных векторов.
4. Динамическое программирование – временные динамические алгоритмы (DTW).
5. Нейронные сети.

На данном этапе работы были выполнены следующие задачи:

1. Реализация алгоритмов детектирования сигнала и его обработки.
2. Изучение методов извлечение признаков из звукового сигнала и реализация их в программе.

Впоследствии планируется завершить разработку программного средства реализующего аутентификацию на основе тембра голоса.

Список литературы:

1. Кинтцель Т. Руководство программиста по работе со звуком [Электронный ресурс]: Кинтцель Т. Руководство программиста по работе со звуком= A Programmer's Guide to Sound: Пер. с англ. - М.: ДМК Пресс, 2000. – Режим доступа: ftp://87.224.200.92/.../Кинтцель.%20Руководство%20программиста%.pdf

2. Методы моделирования сигнала в распознавании речи [Электронный ресурс]: Пикон Дз. Методы моделирования сигнала в распознавании речи = Proceedings if the IEEE: Пер. с англ. – К.: Кемерово, 2000. – Режим доступа: www.rusdoc.ru/material/raznoe/modelingrus.pdf

3. Обзор алгоритмов аудиоаналитики: [Электронный ресурс]: 3. Обзор алгоритмов аудиоаналитики – Режим доступа: http://habrahabr.ru/company/synesis/blog/250935/

4. Алгоритм быстрого преобразования Фурье FFT (fast Fourier transform). Принцип построения: [Электронный ресурс]: Алгоритм быстрого преобразования Фурье FFT (fast Fourier transform). Принцип построения – Режим доступа: http://www.dsplib.ru/content/fft/fft.html

ОПРЕДЕЛЕНИЕ СТЕКЛОВИДНОСТИ ЗЕРНА ПОСРЕДСТВОМ ОПРЕДЕЛЕНИЯ ЭНЕРГОЗАТРАТ ПРИ ИЗМЕЛЬЧЕНИИ МАЯТНИКОВЫМ ДЕФОРМАТОРОМ

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

В целях обеспечения максимально эффективного использования технологического оборудования для измельчения зерна или другой сельскохозяйственной продукции, в последнее время особо актуально встал вопрос об использовании лабораторных помолов на зерноперерабатывающих предприятиях. Стекловидность зерна имеет очень важное значение на мировом хлебном рыке, так как по нему судят о консистенции эндосперма, твердости зерна, его структуре и выходе муки. На данный момент стекловидность определяют классическим методом по ГОСТ 10987-76. Зерно. Методы определения стекловидности и ГОСТ 10987-76. Зерно. Методы определения стекловидности при помощи диафаноскопа и фаринотома. Данный метод полностью ручной и, ввиду человеческого фактора, неточный.

Наумовым И.А. [1] была выявлена зависимость между энергозатратами на измельчения зерна и стекловидностью, что дает основание на создание автоматизированного прибора, который при измельчении зерна выводил значения стекловидности, а сам метод определения основывался на ГОСТ 10987-76. Зерно. Методы определения стекловидности.

Для усовершенствования процесса лабораторного помола на кафедре МАПП АлтГТУ им. И.И. Ползунова, профессором Злочевским В.Л. была разработана лабораторная установка маятникового типа, позволяющая увеличить выход муки на 3%, а также изучать свойства зерна и кинематику маятниковых механизмов [2].

Основной целью создания данной системы является лабораторное исследование зернового (сельскохозяйственного) материала, необходимое для дальнейшей настройки измельчающих машин под определенный тип продукции. В данной работе решается важная и актуальная задача разработки программно-аппаратных средств, позволяющих осуществлять автоматическую работу системы предварительной подготовки зерна для последующего размола, передачу данных на компьютер, структурирование и предоставление полной информации о протекающих процессах пользователю. Для достижения поставленных целей необходимо разработать специальное программное обеспечение для системы автоматического управления процессом измельчения зернового материала маятниковым деформатором, а так же построить базы данных проведения эксперимента.

Принцип работы деформатора следующий: после захвата зернового материала начинается процесс упругой и пластической деформаций. Когда достигается предел прочности оболочки, она раскрывается. Такое разрушение должно происходить по самому ослабленному месту оболочки – бороздке. Очевидно, что такой процесс несравним с резанием зерновки, как это происходит на первых драных системах, использующих рифленые валки.

На текущий момент установка полностью механическая, за исключением датчика угла наклона маятника. Так как в настоящее время важную часть любого производства составляет автоматизация, которая позволяет сократить затраты времени, ресурсов и увеличить количество и качество выпускаемого продукта, поэтому основная задача состоит в создании средства управления в виде программы для персонального компьютера с интуитивно-понятным интерфейсом. Для этого необходимо реализовать связку «механика – электроника – микроконтроллер – программа для ПК».

Не все предлагаемые на рынке средства автоматизации, на основе программируемых логических контроллеров, подходят для использования в данном проекте, т.к. они имеют свои недостатки.

Данная работа отличается в первую очередь дешевизной, при том, что разрабатываемая система разрабатывается на современной элементной базе и имеет большие функциональные возможности, а так же надежности. Разрабатываемая система основана на универсальной платформе Raspberry Pi Model B+ и соответствует всем современным требованиям. В связи с данными фактами, была разработана своя система управления на персональный компьютер, которая полностью удовлетворяет всем функциональным и графическим требованиям, не имеет слишком сложной структуры, а так же не имеет лишней, ненужной функциональности.

Платформа Raspberry Pi Model B+ управляет подъемом маятниковой поверхности, дозирующим устройством, системой фиксации маятниковой поверхности, а также считывает данные с угла поворота и с трех веб камер.

Датчик угла поворота необходим для определения энергозатрат, которые определяются по формуле:

$$E = m \cdot g \cdot l_м \cdot (cos\alpha_2 - \cos(e^{-kT}\alpha_1))$$

где α_1 – угол отклонения; α_2 – угол выхода маятниковой поверхности.

Для определения работы маятникового деформатора используются три веб камеры. Данный метод основан на теории советского ученого П.А. Ребиндера [3], который предложил оценивать работу измельчения формулой

$$A_p = k_v \cdot k_n \cdot V_m + \alpha_{пов} \cdot \Delta S$$

где A_p – расход энергии на разрушение; k_v – коэффициент, учитывающий какая часть объема частицы деформируется; k_n – коэффициент, характеризующий физико-механические свойства разрушаемого тела; V_m - объем разрушаемого тела; $\alpha_{пов.}$ - удельная поверхностная энергия разрушаемого тела; ΔS - образованная при разрушении новая поверхность.

Таким образом, одна камера устанавливается над маятниковой поверхностью для определения площади зернового материала до измельчения, а две других – на вылете зернового материла в сборник, для определения площади после измельчения. Расчет работы производится в программе управления автоматически.

Приложение разработано на языке программирования C#. На рисунке 1 изображен главный экран программы.

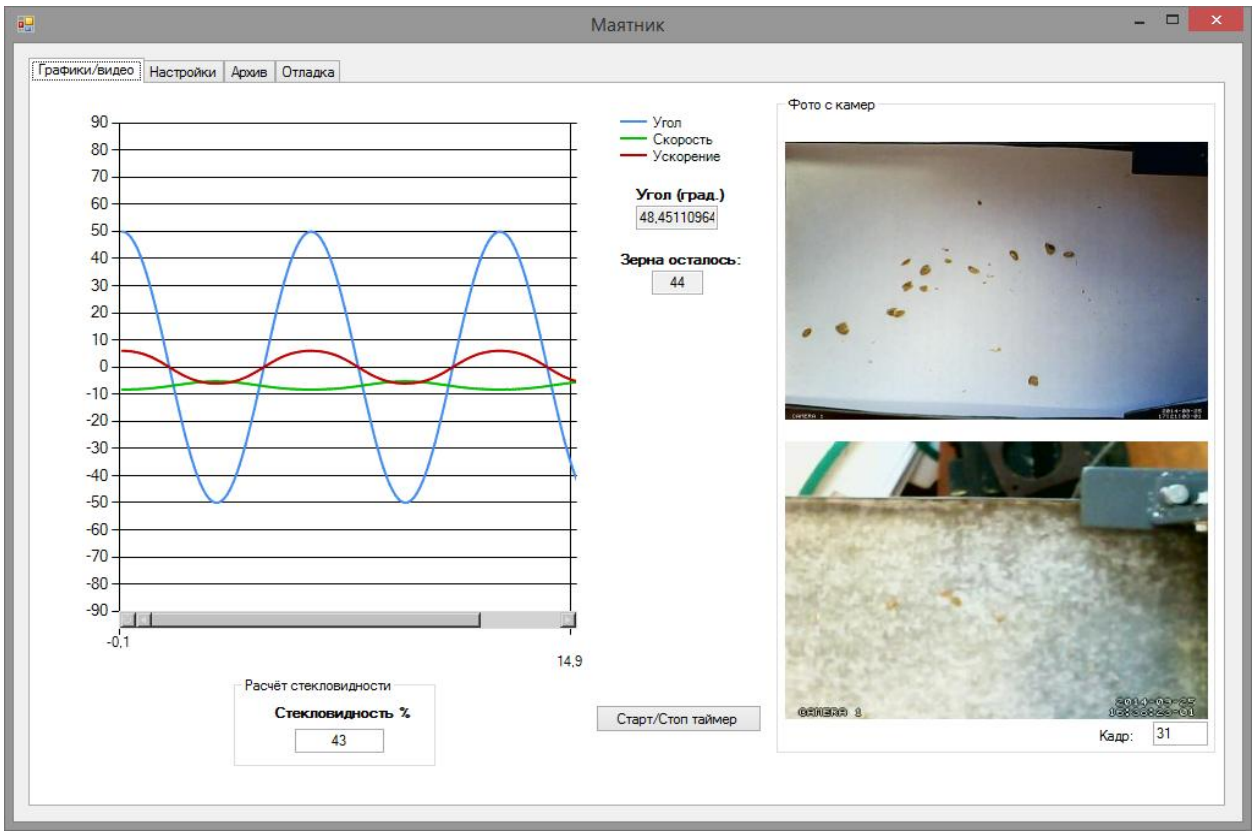


Рисунок 1 – Главный экран программы

Графики в данном окне отображают разные данные, а именно: угол, скорость и ускорение маятниковой поверхности. Процесс деформации зёрен будет отображаться на двух экранах, расположенных в правой части рабочей области. Будут показаны два основных состояния зерна: до деформации и после. Таким образом, будет удобней контролировать процесс деформации, и точно знать, насколько удачно прошёл размол. Так же на данном экране предоставлена информация о стекловидности зерна, количестве оставшихся зёрен, и угла наклона маятниковой поверхности.

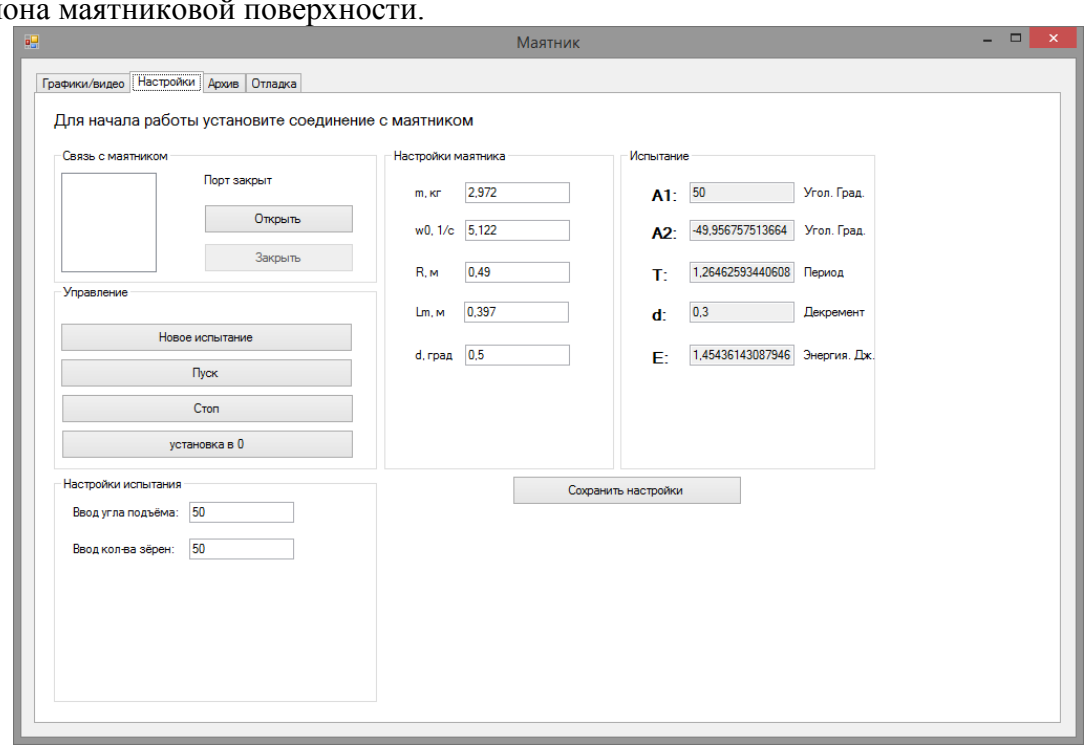


Рисунок 2 – Окно настроек программы

На вкладке «Настройки» будут представлены настройки всех узлов устройства, начальные характеристики маятника, управления маятниковой поверхностью в виде управляющих кнопок, соединение с микроконтроллером raspberry, и т.д.

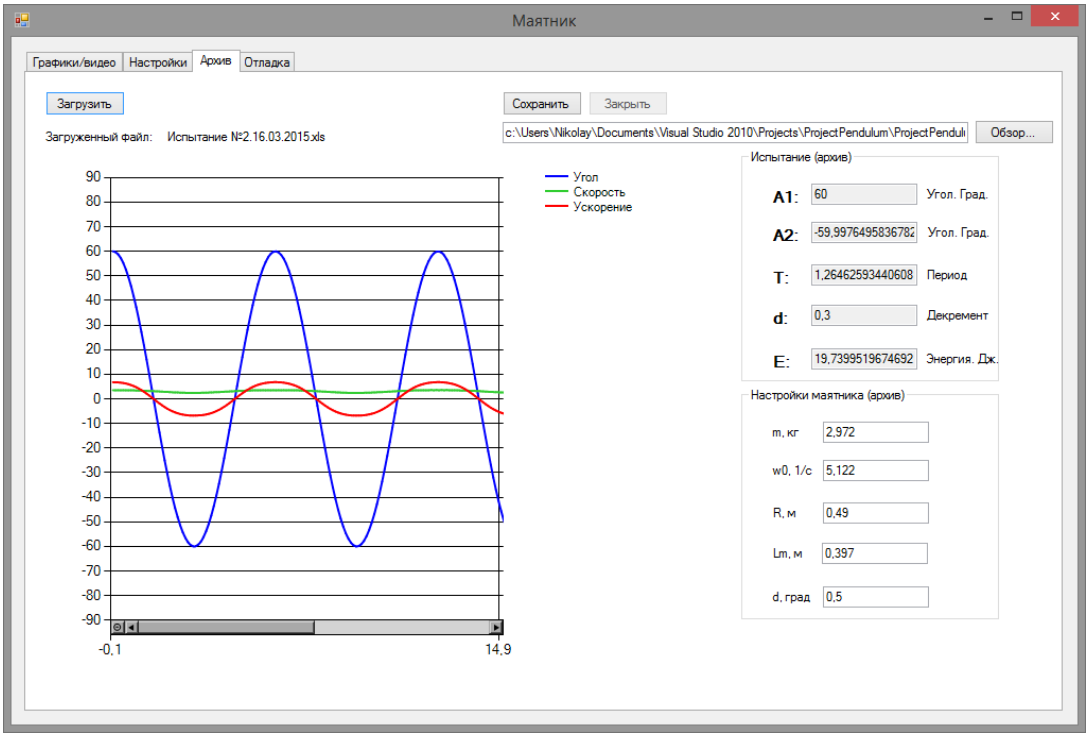


Рисунок 3 – Окно архива

Во вкладке «Архив» будут сохраняться все проведённые эксперименты а так же настройки маятникового деформатора, при которых был проведен данный тест.

Таким образом, разработанная система позволяет определять стекловидность по ГОСТ 10987-76. Зерно. Методы определения стекловидности, полностью автоматизирована и не требует специалистов высокого уровня для управления ею, так как разработанный интерфейс интуитивно понятен.

СПИСОК ЛИТЕРАТУРЫ

1. Наумов, И.А. Совершенствование кондиционирования и измельчения пшеницы и ржи / И.А. Наумов. – М.: Колос, 1975. – с.176

2. Пат. № 2263544 Российская Федерация, МПК B02C 19/16 Способ формирования зерновых продуктов размола / Злочевский Валерий Львович, Злочевский Алексей Валерьевич.; заявл. 16.02.2004; опубл. 10.11.2005.

3. Ребиндер, П.А. Исследование в области поверхностных явлений / П.А. Ребиндер // Труды Гипроцветметалл. – 1930, т.1.

РАСПРЕДЕЛЕННАЯ СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ OEM-МОДУЛЕЙ ARDUINO

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

Защита любого объекта включает несколько рубежей, число которых зависит от уровня режимности объекта. При этом во всех случаях важным рубежом является система контроля и управления доступом (СКУД).

Система контроля и управления доступом – совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-

выхода объектов (людей, транспорта) на заданной территории через точки контроля.

Точками контроля доступа могут быть двери, турникеты, ворота, шлагбаумы, места на парковке, лифты или другие физические преграды, где получение доступа может быть проконтролировано электроникой. Обычно точкой контроля доступа является дверь, а доступ контролируется магнитным замком и считывателем карт.

В настоящее время СКУД широко распространены. Такие системы встречаются каждый день: домофоны в подъездах, турникеты в университетах, автоматические ворота и шлагбаумы на въездах в предприятиях. СКУД являются одним из наиболее развитых сегментов рынка безопасности как в России, так и за рубежом.

По способу управления СКУД различаются на автономные, сетевые и универсальные. Наиболее распространены универсальные СКУД, они осуществляют обмен информацией с центральным пультом, в качестве которого обычно выступает персональный компьютер, но в то же время, при возникновении отказов управляющих компьютеров, сетевого оборудования или обрыве связи с контроллером СКУД переходят в автономный режим.

Основным признаком, по которому система принимает решение о разрешении доступа является идентификатор пользователя. В качестве идентификаторов используют автономные носители признаков допуска: магнитные карточки, бесконтактные карты, изображение радужной оболочки глаза, отпечаток пальца и многие другие физические признаки.

В СКУД каждому идентификатору ставится в соответствие информация о правах и привилегиях владельца идентификатора. Устройства идентификации (считыватели) расшифровывают информацию, записанную на контактных или бесконтактных картах, и передают ее в контроллер.

Контроллер является «сердцем» СКУД. Это устройство предназначено для обработки информации от считывателей идентификаторов, принятия решения, и управления исполнительными устройствами. Именно контроллер разрешает проход через пропускные пункты.

Среди исполнительных устройств контроля доступа наиболее распространены следующие запорные или управляемые преграждающие устройства: замки, защелки, турникеты и шлюзовые кабины, автоматические ворота и лифты.

На рынке существует большой выбор СКУД, начиная от самых простых, контроллер встраивается в исполнительное устройство, до дорогих систем со сканерами радужной оболочки глаза и интеграцией в охранную систему. Простые СКУД имеют ограниченный функционал и, обычно, не ведут журнал событий. Более сложные СКУД неоправданно дороги, и часто используют нестандартные типы идентификаторов, которые сложно достать.

Целью данной работы является создание программно-аппаратного обеспечения СКУД. Для достижения этой цели были решены следующие задачи: выполнен подбор современной элементной базы с низким энергопотреблением; выбраны языки программирования и ПО; разработано ПО сервера и веб-интерфейса; спроектирована и реализована база данных для системы; написаны прошивки для контроллеров и шлюза.

В контроллере установлен OEM-модуль Arduino Pro Mini, который имеет малые габаритные размеры (34x18), что позволяет уменьшить размеры конечного устройства. Модуль Arduino, а точнее микроконтроллер распаянный в нём является центром системы, именно он выполняет все операции по считыванию идентификатора, его поиска в собственной памяти, принимает решение о разрешении доступа и ведёт журнал событий.

В модуле Arduino Pro Mini используется микроконтроллер ATmega328P. Данный микроконтроллер обладает достаточным количеством оперативной и энергонезависимой памяти (2 КБ и 1 КБ соответственно) для выполнения поставленных перед ним задач. Также эта модификация микроконтроллера отличается пониженным энергопотреблением, что увеличивает время автономной работы системы.

В системе используется три типа считывателей: кодовая клавиатура, контактный считыватель Touch Memory и бесконтактный считыватель проксимити карт. Кодовая клавиатура является самым простым способом получить доступ. На данный момент

клавиатура используется для ввода одноразовых паролей. Контактный считыватель предназначен для каждодневного пользования. Ключи для него имеют низкую цену и широко распространены. Бесконтактный считыватель расширяет функционал, однако дороговизна считывателя мешает полному переходу системы на только бесконтактные карты. Контроллер поддерживает одновременное подключение от одного до трёх различных видов считывателей.

Для связи контроллеров между собой и между сервером используется отдельное устройство – конвертер сред или шлюз. Все контроллеры подсоединяются по интерфейсу I^2C к шлюзу (рисунок 1). Шлюз имеет большое количество постоянной памяти, которая позволяет принимать решения в автономном режиме. Также шлюз осуществляет пересылку событий системы серверу.

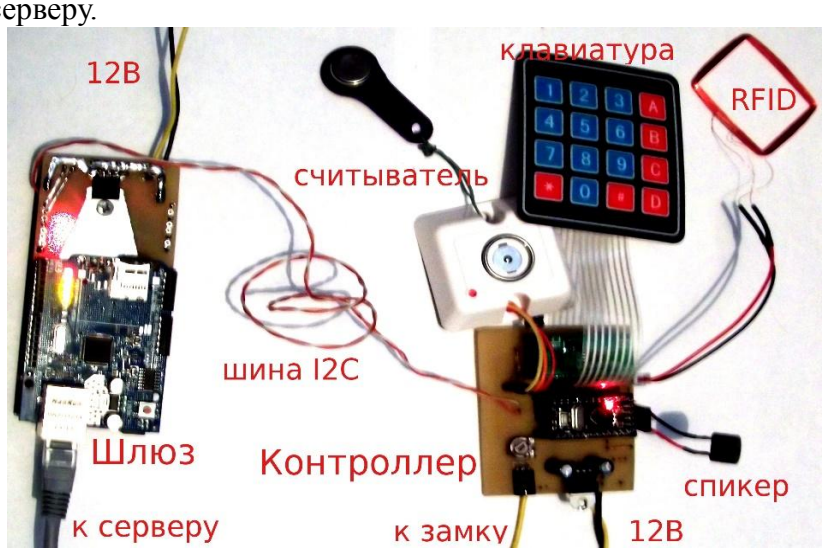


Рисунок 1 – Контроллер и шлюз

В основе шлюза также лежит OEM-модуль Arduino, только микроконтроллер, распаянный на плате имеет лучшие характеристики. Микроконтроллер ATmega2560 содержит 8 КБ оперативной памяти и 4 КБ энергонезависимой. Большое количество оперативной памяти требуется для буферизации событий системы перед отправкой их на сервер.

Сервер осуществляет обработку событий системы, хранение учетных данных пользователей и их личных идентификаторов. Также сервер осуществляет учёт статистики и обновление данных в контроллерах и шлюзе.

Веб-интерфейс (рисунок 2) имеет общую с сервером базу данных. Веб-интерфейс позволяет с лёгкостью администрировать систему, смотреть состояние системы, статистику, добавлять и удалять пользователей, их идентификаторы.

Рисунок 2 – Просмотр событий системы в веб-интерфейсе

В данной работе была спроектирована и реализована программно-аппаратная распределённая система контроля и управления доступом. Распределённая система остаётся работоспособной даже при обрывах связи между устройствами, при неисправности сети, при отключении электроэнергии гарантированное время автономной работы системы: 24 часа.

Список использованной литературы:

1) Arduino - Compare board specs – [Электронный ресурс]. – Режим доступа: http://arduino.cc/en/Products.Compare свободный. – Arduino.

2) Ворона , В.А. Обеспечение безопасности объектов . Системы контроля и управления доступом . - М.: Горячая линия - Телеком, 2010. - 272 е.: ил.

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ «ИТ СЕРВИС»

Ефимов А.С. – студент, Шарлаев Е.В. – к.т.н., доцент

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

Современный мир очень тяжело представить без средств коммуникации и вычислительной техники. Информационные технологии развиваются очень быстро, охватывая все более широкие области человеческой деятельности. Автоматизация предприятий влияет на её конкурентно способность и в тоже время является источником многочисленных угроз безопасности. Именно поэтому безопасность информационных технологий является одним их важнейших аспектов обеспечения их функционирования. Надежное обеспечение безопасности информации немыслимо без реализации комплексного подхода. Отсюда и вытекает потребность в создании системы защиты информации на предприятии [1].

Система защиты информации (СЗИ) — это комплекс организационных и технических мер, направленных на обеспечение информационной безопасности предприятия. Из этого определения следует, что для защиты информации нужны как организационные, так и технические меры, одно без другого существовать не может. Главной целью СЗИ является обеспечение непрерывности ведения бизнеса, устойчивого функционирования предприятия и предотвращения угроз его безопасности.

При построении СЗИ необходимо учитывать следующие факторы:

— информация защищается во всех формах и видах ее существования;

— информация защищается не только от несанкционированного доступа (НСД) к ней, но и от неправомерного вмешательства в процесс ее обработки, хранения и передачи;

— необходимо также принимать меры по защите информации от утечки по техническим каналам;

— должны быть обеспечены конфиденциальность, целостность и доступность информации.

Таким образом, защищаются все компоненты информационной структуры предприятия — помещения, аппаратура, документы на бумажных и электронных носителях и т.д.

При создании СЗИ выделяют три направления работ:

1. Методическое направление — создаются методологические компоненты СЗИ, разрабатывается замысел ее построения, прорабатываются правовые вопросы;

2. Организационное направление — заключается в разработке распорядительных документов, проводится обучение и инструктаж персонала и т.п.

3. Техническое направление — состоит в выборе, закупке и установке средств защиты информации [2].

При разработке СЗИ необходимо руководствоваться правовыми документами, которые обеспечивают защиту информации на правовой основе. Эти документы не являются самостоятельными мерами по защите информации, они лишь меры предупреждения для потенциальных нарушителей.

Угрозы для предприятия могут быть внешними и внутренними. К внешним угрозам относят действие российских конкурентов направленные на ослабление компании, деятельность государственных органов способных предпринять меры приводящие к ущербу предприятия, практические действия недобросовестных партнеров и т.д. Внутренними угрозами могут быть недобросовестность и недисциплинированность персонала, плохой морально – психологический климат на предприятии.

Структурная схема предприятия для которого разрабатывается СЗИ представлена на рисунке 1.

Рисунок 1 - Структурная схема предприятия

Модели информационных потоков – это физическое перемещение информации от одного сотрудника предприятия к другому, либо от одного подразделения к другому. Информационные потоки, подлежащие защите на рассматриваемом предприятии представлены на рисунке 2.

Каналы передачи информации представлены на рисунке 3. По этим каналам циркулирует как информация ограниченного доступа (ИОД), так и персональные данные (ПД). Для защиты этих данных следует модернизировать структуру сети. Во – первых на каждую из автоматизированных систем (АС) следует инсталлировать антивирусное программное обеспечение (ПО). Во – вторых разграничить права доступа субъектов к АС с помощью сертифицированных средств защиты информации (Secret Net, Dallas Lock и т.д.). В – третьих на сервер следует установить программный межсетевой экран (МЭ), либо вместо сервера использовать программно – аппаратный МЭ (VipNet, Cisco). Эти меры являются лишь начальными при проектировании СЗИ. Даже с ними безопасность на предприятии возрастет в несколько раз.

При внедрении СЗИ на объекте необходимо помнить, что защита информации – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированного и непреднамеренного доступа к ней. Исходя из вышесказанного можно сделать вывод, что мероприятия по защите информации необходимо осуществлять на объекте периодически, с целью совершенствования системы защиты, создания механизмов противодействия ранее не существовавшим угрозам, возникающим в связи с повышением уровня развития науки и техники.

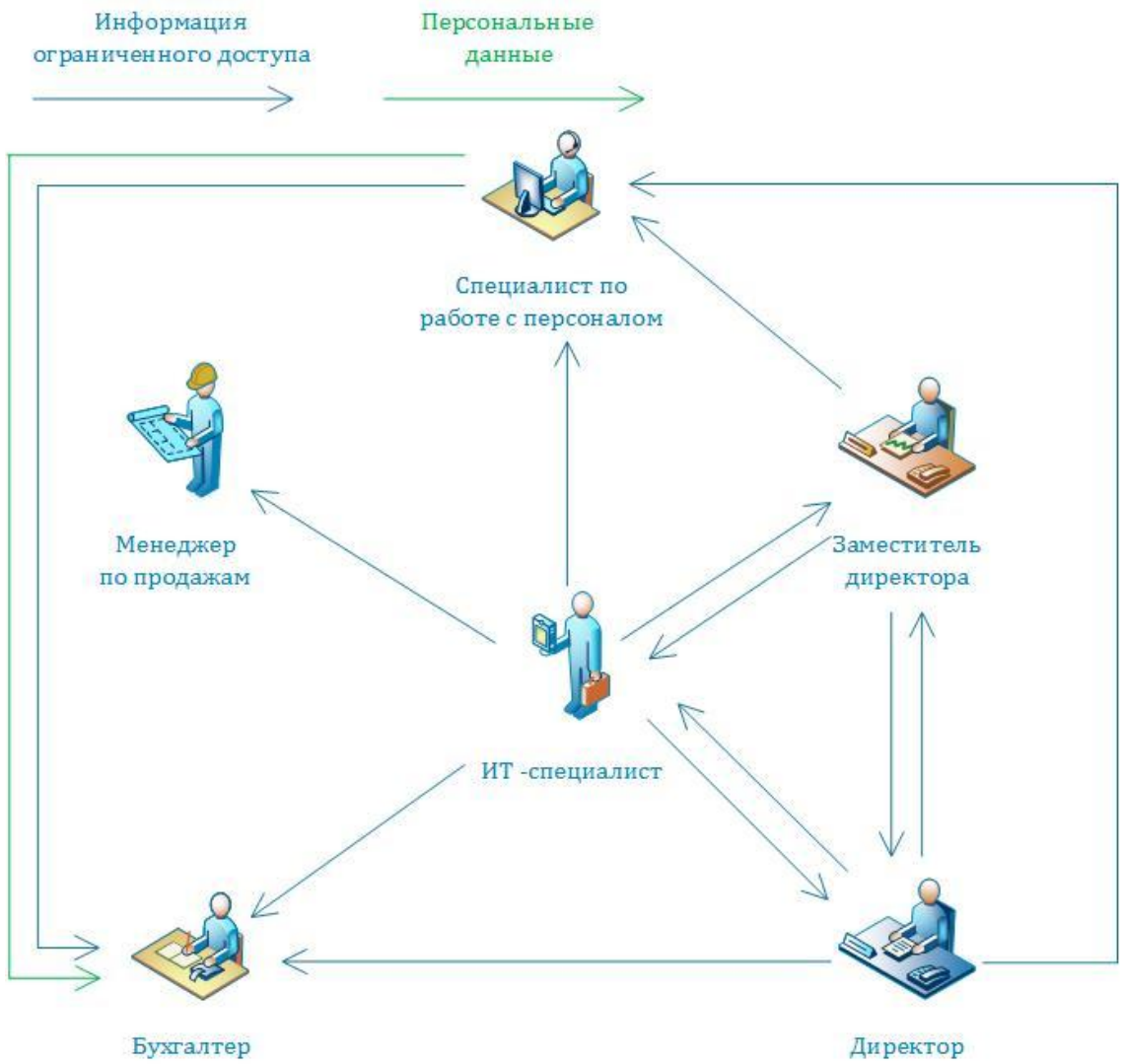


Рисунок 2 - Схема информационных потоков

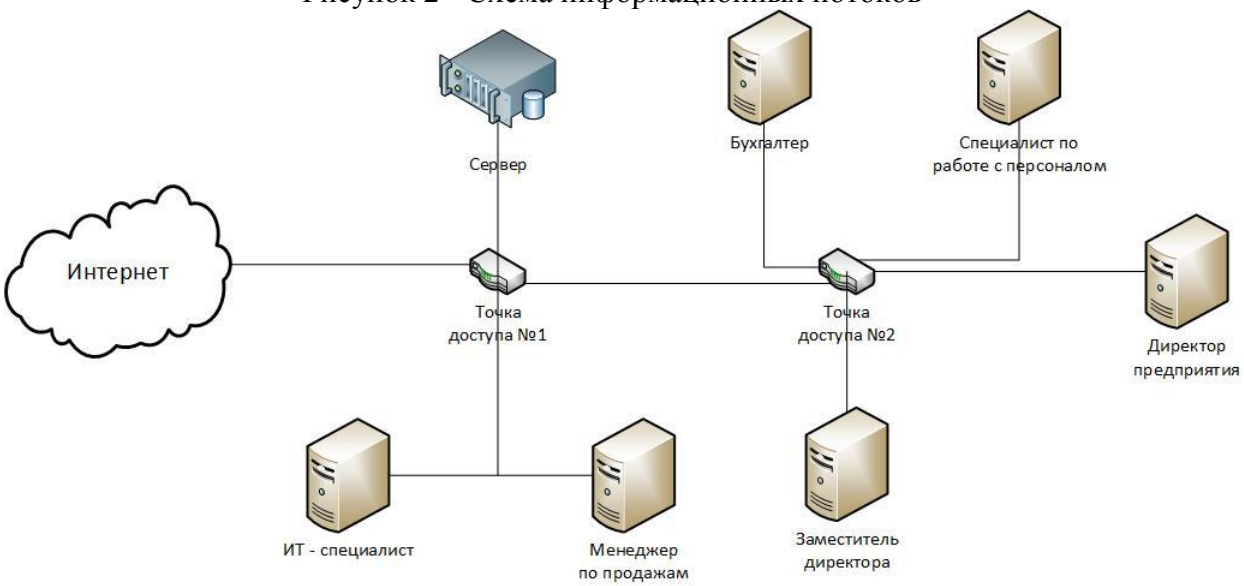


Рисунок 3 - Каналы передачи информации

Список источников

1. Грибунин В.Г. Комплексная система защиты информации на предприятии: учебник для студ. высш. учеб. заведений./ В.Г.Грибунин, В.В. Чудовский.- М.: Издательский центр «Академия», 2008.-320с.

2. Загинайлов Ю.Н. Комплексная система защиты информации на предприятии: учебно-методическое пособие / Ю.Н. Загинайлов и др., - Алт.гос.техн.ун-т им.И.И. Ползунова.- Барнаул: АлтГТУ.-2010-287с.

РАЗРАБОТКА КОМПЛЕКСА ДОКУМЕНТОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КРИПТОЗАЩИТЫ

Князев Б.В – студент, Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Защита персональных данных (ПДн) является одной из наиболее актуальных задач для большинства коммерческих компаний и государственных организаций [1]. В связи с этим организации оказывающие услуги по проектированию и внедрению систем защиты информационных систем персональных данных (ИСПДн) разрабатывают методики и средства автоматизации процессов проектирования, а также типизации этих процессов. Одним из таких процессов является типизация комплекса документов по защите ПДн в ИСПДн. Одним из вариантов типизации является вариант комплекса документов, когда для защиты ИСПДн используются средства криптозащиты. Такой комплекс был разработан и успешно применялся компанией ООО «ЦИБ – Сервис» в г. Барнауле и Алтайском крае [2].

Однако в связи со значительными изменениями в 2013-2014 годах законодательства РФ, нормативных и методических документов Правительства РФ, органов исполнительной власти уполномоченных в области информационной безопасности и технической защиты информации (ФСБ России и ФСТЭК России) для регулирования защиты ПДн потребовалась его существенная модернизация.

Эта цель была поставлена в рамках совместного проекта АлтГТУ и ООО «ЦИБ-сервис» по разработке комплекса типовых документов по защите ПДн в ИСПДн медицинского учреждения. Разработка пакета документов, в основу которых положена типовая система защиты ПДн в медицинском учреждении, была выполнена на базе Краевого государственного бюджетного учреждения здравоохранения «Детская городская поликлиника №2, г. Барнаул». В данной работе рассматривается одно из направлений - защита ПДн в ИСПДн медицинского учреждения с использованием средств криптозащиты.

Для достижения цели были поставлены следующие задачи:

– проанализировать законодательство РФ в области защиты персональных данных и применения средств криптографии для защиты информации;

– проанализировать нормативные и методические документы органов исполнительной власти уполномоченных в области информационной безопасности и технической защиты информации (ФСБ России и ФСТЭК России) в этой области;

– рассмотреть и выбрать существующие типовые пакеты документов по защите ИСПДн;

– переработать, откорректировать, дополнить разработанные ООО «ЦИБ-сервис» документы, необходимые для защиты ПДн в ИСПДн с использованием средств криптозащиты.

Необходимость обеспечения безопасности ПДн устанавливает Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», который обязывает оператора (любое физическое или юридическое лицо, осуществляющее обработку ПДн), получающего доступ к персональным данным, обеспечивать конфиденциальность таких данных (ст.7) .

Согласно статье 19 ФЗ-№152, «оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий».

Правила производства, разработки ,реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию ПД при их обработке в информационных системах устанавливает ФСБ России, но однозначного ответа о необходимости применения средства криптографической защиты информации (СКЗИ) не дают . Целесообразность их применения выясняется на этапе определения модели угроз. В том случае, если они признаются необходимыми, то применяемые СКЗИ должны соответствовать требованиям российского законодательства.

По криптографической защите персональных данных в Российской Федерации можно выделить три основных документа[3]:

1. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденные руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144 .

2. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622.

3. Приказ ФСБ № 378 от 10 июля 2014 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности». Зарегистрировано в Минюсте России 18 августа 2014г.

Приказ ФСБ № 378 от 10 июля 2014 г. это – главный документ в области криптографической защиты персональных данных, и его действие распространяется на все ИСПДн, в которых используются в качестве защиты КСЗИ. Приказом определены требования не только к криптографической защите, но и к режиму обеспечения безопасности помещений, порядок хранения носителей информации и другие организационные меры в зависимости от уровня защищенности системы. Отдельно указано, что оператору следует использовать СЗИ, прошедшие оценку соответствия – сертифицированные по требованиям безопасности. Защитные меры описаны очень подробно, включают в себя требования к оснащенности помещений (замки, приспособления для опечатывания, решетки на окна и т.д.).

В ходе анализа типового пакета документов созданного компанией ООО «ЦИБ-сервис» были определены локальные нормативно-правовые акты и нормативно-методические документы организации регулирующие вопросы защиты, связанные с обеспечением безопасности ПДн при их обработке в ИСПДн с использованием криптографических средств.

С учётом рассмотренных правовых, организационных, методических особенностей в законодательстве, нормативных и методических документах переработаны документы из пакета документов по защите ПДн в ИСПДн с использованием средств криптозащиты. В процессе переработки были учтены требования вступившего в силу Приказа ФСБ № 378. Всего таких 20 документов. К этим документам относятся:

– Приказ “О назначении ответственного пользователя криптосредств”

– Программа подготовки к самостоятельной работе со средствами криптографической защиты информации.

– Состав комиссии по допуску к самостоятельной работе со средствами криптографической защиты информации.

– Порядок работы со средствами криптографической защиты информации

– Порядок размещения специального оборудования, охраны и организации режима в выделенных (режимных) помещениях.

– Список лиц, допущенных к работе со средствами криптографической защиты информации.

– Список помещений, выделенных для установки средств криптографической защиты информации и хранения ключевых документов к ним.

– Порядок восстановления связи в случае компрометации действующих ключей к средствам криптографической защиты информации.

– Порядок заполнения «Журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов».

– 12 форм журналов, заявлений, актов.

– В качестве примера приведен Приказ “О назначении ответственного пользователя криптосредств”. На рисунке 1 представлен документ до и после переработки. Желтым цветом отмечены внесенные изменения:


РОССИЙСКАЯ ФЕДЕРАЦИЯ

{NAME_ORG_FULL.IP}

{TYPE_OF_DOCUMENT.IP}

От {DATE_OF_DOCUMENT} № {NUM}

О назначении ответственного пользователя криптосредств

В целях соблюдения положений «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» N 149/6/6-622, утвержденных руководством 8 Центра ФСБ от 21.02.2008, «Методических рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» N 149/54-144, утвержденных руководством 8 Центра ФСБ от 21.02.2008.

{TO_DO}:

1. Утвердить:

1.1. Программу подготовки к самостоятельной работе со средствами криптографической защиты информации (Приложение 1 к данному {TYPE_OF_DOCUMENT.DP}).

1.2. Состав комиссии по допуску к самостоятельной работе со средствами криптографической защиты информации (Приложение 2 к данному {TYPE_OF_DOCUMENT.DP}).

1.3. Порядок работы со средствами криптографической защиты информации (Приложение 3 к данному {TYPE_OF_DOCUMENT.DP}).

1.4. Порядок размещения специального оборудования, охраны и организации режима в выделенных (режимных) помещениях {NAME_ORG_SHORT.RP} (Приложение 4 к данному {TYPE_OF_DOCUMENT.DP}).

1.5. Список лиц, допущенных к работе со средствами криптографической за-

{NAME_ORG_FULL.IP}
{NAME_ORG_SHORT.IP}

{{TYPE_OF_DOCUMENT.IP}}

{{DATE_OF_DOCUMENT}} г. №
{{NUM}}
{{TYPE_OF_SETTLEMENT}} {{CITY}}

«О назначении Ответственного пользователя криптосредств»

В целях соблюдения положений «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» N 149/6/6-622, утвержденных руководством 8 Центра ФСБ от 21.02.2008, «Методических рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» N 149/54-144, утвержденных руководством 8 Центра ФСБ от 21.02.2008, приложения «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» к приказу ФСБ России N 378 от 10.07.2014 .

{{TO_DO}}:

1. Утвердить:

- программу подготовки к самостоятельной работе со средствами криптографической защиты информации (Приложение 1 к данному

Рисунок 1 - Приказ “О назначении ответственного пользователя криптосредств” до и после переработки

Список литературы

1. ЗАО «ДиалогНаука» [Электронный ресурс] – Режим доступа: www.dialognauka.ru/solutions/pdn/

2. Онлайн сервис подготовки документов [Электронный ресурс] – Режим доступа: https://safe-doc.com/.

3. Публикации по безопасности [Электронный ресурс] – Режим доступа: http://daily.sec.ru/2014/12/15/Personalnie-dannie-chto-bilo-chto-budet-na-chem-serdtse uspokoitsya-CHast-4-Kriptografiya.html.

АНАЛИЗ ПРОБЛЕМ ЗАЩИТЫ ИНФОРМАЦИИ СОСТАВЛЯЮЩЕЙ БАНКОВСКУЮ ТАЙНУ

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

Защита информации в наш век приобретает все большее значение. Появилось множество угроз, в связи с новыми способами обработки и передачи информации. Поэтому наиболее приоритетное развитие ИТ это обеспечение информации и компьютерных систем, которые ее обрабатывают. СЗИ находят все большее распространение, как в государственных, так и коммерческих учреждениях. Этому способствует несколько причин: комплексность защиты информации, контроль над рисками и ущербами и надежность. Что бы обеспечить наилучшую защиту требуется применение как программных, аппаратных, программно-аппаратных средств, так и мероприятия различного рода. Также необходимо учитывать и человеческий фактор, ведь какой бы хорошей не была система защиты, работают с ней люди и они могут допускать ошибки.

В банковской сфере вопрос защиты информации стоит особенно высоко, так как банки работают не только с персональными данными, но и с данными представляющими товарно денежные отношения. Банк предоставляет множество видов услуг, как физическим и юридическим лицам, так и малому и среднему бизнесу. Предоставляются такие услуги как: выдача кредитов, прием вкладом под проценты, производство и выдача банковских карт, дистанционное управление своим расчетным счетом и многие другие[1].

В настоящее время основными нормативными документами в банковской сфере являются:

1. Федеральный закон от 02.12.1990 N 395-1 (ред. от 29.12.2014) "О банках и банковской деятельности" от 02 декабря 1990 г.
2. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014)
3. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 — 2014» (СТО БР ИББС-1.2-2014)
4. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности СТО БР ИББС-1.1-2007» (СТО БР ИББС-1.1-2007).

В банковской среде необходим постоянный контроль информации циркулирующей как внутри банка, так и между отделами банковской сети так как разглашение, утечка или уничтожение такой информации могут привести к тяжелым последствиям как отдельных лиц и их денежных средств, так и всего денежного фонда банка. Деятельность организации банковской сферы Российской Федерации поддерживается входящей в ее состав информационной инфраструктурой, которая обеспечивает реализацию банковских технологий и может быть представлена в виде следующей иерархии:

— физический уровень (аппаратные средства и линии связи);
— сетевой уровень (точки доступа, роутеры, различные коммутаторы);
— уровень сетевых программ и приложений;
— операционный уровень (ОС);
— уровень СУБД;
— уровень банковских приложений и процессов;

— уровень бизнес процессов организации[2].

Наиболее актуальные источники угроз на физическом уровне, уровне сетевого оборудования и уровне сетевых приложений:

— внешние нарушители ИБ: лица, разрабатывающие/распространяющие вирусы и другие вредоносные программные коды; лица, организующие DoS, DDoS и иные виды атак; лица, осуществляющие попытки НСД и НРД;

— внутренние нарушители ИБ: персонал, имеющий права доступа к аппаратному оборудованию, в том числе сетевому, администраторы серверов, сетевых приложений и т.п.;

— комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие совместно и (или) согласованно;

— сбои, отказы, разрушения/повреждения программных и технических средств.

Наиболее актуальные источники угроз на уровнях операционных систем, систем управления базами данных, банковских технологических процессов:

— внутренние нарушители ИБ: администраторы ОС, администраторы СУБД, пользователи банковских приложений и технологий, администраторы ИБ и т.д.;

— комбинированные источники угроз: внешние и внутренние нарушители ИБ, действующие в сговоре

Наиболее актуальные источники угроз на уровне бизнес-процессов:

— внутренние нарушители ИБ: авторизованные пользователи и операторы АБС, представители менеджмента организации и пр.;

— комбинированные источники угроз: внешние нарушители ИБ (например, конкуренты) и внутренние, действующие в сговоре;

— несоответствие требованиям надзорных и регулирующих органов, действующему законодательству[2].

Хорошей практикой в организациях БС РФ является разработка моделей угроз и нарушителей ИБ для организации в целом, а также при необходимости для ее отдельных банковских процессов. Степень детализации параметров моделей угроз и нарушителей ИБ может быть различной и определяется реальными потребностями для каждой организации в отдельности. В организации банковской системы Российской Федерации рекомендуется устанавливать процедуры регулярного анализа необходимости пересмотра модели угроз и нарушителей ИБ.

Также не последнее место в защите информации в банковской сфере является аудит информационной безопасности. Мировой опыт в области обеспечения информационной безопасности определяет аудит ИБ как важнейший процесс в непрерывном цикле процессов менеджмента ИБ организации[3].

Банк России является сторонником регулярного проведения аудита ИБ в организациях БС РФ.

Основными целями аудита ИБ организаций БС РФ являются:

— повышение доверия к организациям БС РФ;

— оценка соответствия ИБ организаций БС РФ критериям аудита ИБ, установленным согласно требованиям стандарта Банка России СТО БР ИББС-1.0 “Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения” [3].

Список источников:

1. Федеральный закон от 02.12.1990 N 395-1 (ред. от 29.12.2014) "О банках и банковской деятельности" (02 декабря 1990 г.)

2. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014)

3. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности СТО БР ИББС-1.1-2007» (СТО БР ИББС-1.1-2007)

РАЗРАБОТКА СИСТЕМЫ АВТОМАТИЧЕСКОГО КОНТРОЛЯ УПРАВЛЕНИЯ ПРОЦЕССОМ ИЗМЕЛЬЧЕНИЯ НА МАЯТНИКОВОМ ДЕФОРМАТОРЕ

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

В современном производстве очень важное место занимают инновационные технологии, позволяющие сократить производственные затраты и вместе с тем повысить производительность, а также качество выпускаемой продукции.

Крупные системы в промышленности и энергетике, на транспорте, в различных государственных структурах строятся на принципах автоматизированного управления.

Однако предлагаемые готовые решения на базе программируемых логических контроллеров и SCADA имеют свои недостатки. Главным из них является недостаточная скорость обработки информации: колеблющаяся поверхность двигается очень быстро. Существенным недостатком также является стоимость приобретения подобных систем, развёртывания, отладки и сопровождения. Дополнительно существуют ограничение по их коммерческому использованию с объектами автоматизации. С другой стороны, широкие возможности готовых решений не всегда необходимы для реализации конкретных задач узкой направленности и поэтому их использование зачастую нерационально.

В данной работе решается важная и актуальная задача проектирования программно-аппаратного комплекса, позволяющего осуществлять автоматическое функционирование установки по измельчению зерна. Основным достоинством разрабатываемой системы управления является существенная разница в стоимости по сравнению с представленными на рынке системами. Однако она не уступает по своим функциональным возможностям при использовании совместно с маятниковым деформатором, в том числе, и по надёжности.

Принцип работы деформатора следующий: после захвата зернового материала начинается процесс упругой и пластической деформаций. Когда достигается предел прочности оболочки, она раскрывается. Такое разрушение должно происходить по самому ослабленному месту оболочки – бороздке. Очевидно, что такой процесс несравним с резанием зерновки, как это происходит на первых драных системах, использующих рифленые валки.

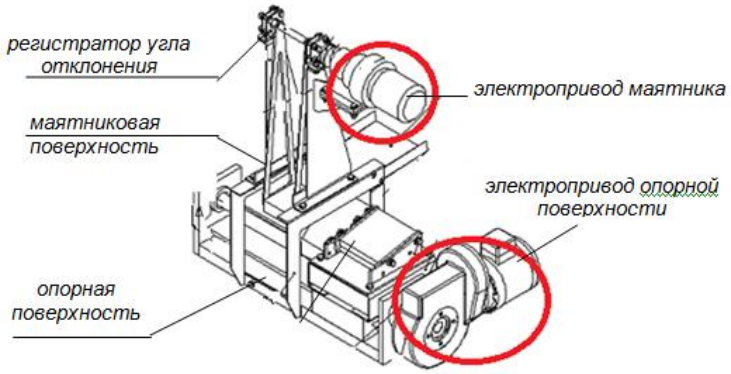


Рисунок 1 –Общий вид деформатора

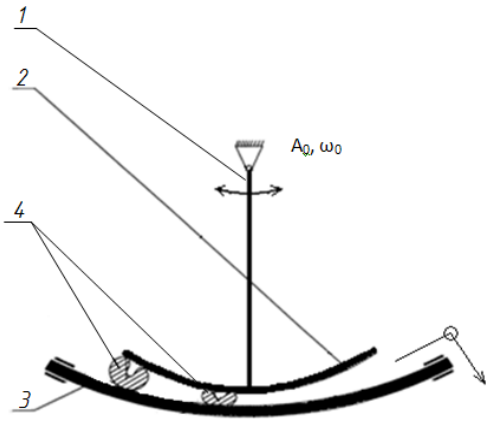


Рисунок 2 – Функциональная схема установки для измельчения зерна маятникового типа

На рисунке 2 приняты обозначения: 1 – маятник; 2 – криволинейная колеблющаяся поверхность; 3– опорная поверхность; 4 – зерновой материал;

—⊖→ измельченное зерно.

Установка для измельчения зерновых материалов при помощи колеблющейся криволинейной поверхности содержит подвижную опорную поверхность 3, на которой располагается зерновой материал 4, и закрепленную на маятнике 1 криволинейную колеблющуюся поверхность 2. Маятник 1 колеблется с амплитудно-частотной характеристикой A_0, ω_0. Криволинейная колеблющаяся поверхность 2 совершает одновременно колебания с амплитудно-частотной характеристикой маятника и вращение вокруг своей оси с частотной характеристикой. Между опорной поверхностью 3 и криволинейной колеблющейся поверхностью 2, имеющими определенную шероховатость, устанавливается необходимый зазор. Зерновой материал 4 подается на опорную поверхность 3 непосредственно в зону размола. Криволинейная колеблющаяся поверхность 2, проходя над зерновым материалом 4, воздействует на него с усилием, и за счет возникающих между ними сил трения зерновка поворачивается вокруг своей оси в сторону, противоположную своему колебательному движению. Таким образом, в зоне контакта криволинейной колеблющейся поверхностью 2 с зерновым материалом 4 возникает мгновенный центр скоростей, и усилия, с которым криволинейная колеблющаяся поверхность 2 действует на зерновой материал 4, сводятся к усилиям сжатия. По ходу движения криволинейной колеблющей поверхности 2 вправо или влево зерновой материал поступает на опорную поверхность 3 и выводятся продукты размола соответственно справа или слева.

В данной схеме используется привод с асинхронным двигателем.

Асинхронный двигатель имеет такие позитивные качества, как несложная технология изготовления, простота эксплуатации, высокая надежность и способность к перегрузкам, отсутствие искрения. Благодаря этим свойствам асинхронный двигатель нашел широкое применение в промышленности для привода станков и механизмов, а также сельскохозяйственных машинах разного назначения. Однако управление частотой вращения асинхронного двигателя в широком диапазоне значительно сложнее, чем двигателя постоянного тока.

Широкое распространение приводов с асинхронными двигателями на современном производстве объясняется следующими его достоинствами:

- относительно низкая стоимость двигателя;
- простота конструкции, несложная технология изготовления;
- простота обслуживания;
- высокая надежность;
- способность к перегрузкам;
- отсутствие искрения.

Но вместе со своими достоинствами асинхронный двигатель имеет следующие недостатки:

- изменение частоты вращения при изменении момента нагрузки;
- при регулировании скорости невозможность достижения малых скоростей.
- управление частотой вращения в широком диапазоне значительно сложнее, чем двигателя постоянного тока.

Последний недостаток ограничивает применение асинхронных двигателей в тех случаях, когда необходимо изменять частоту вращения двигателя в широких пределах (для этого нужен частотный преобразователь).

На текущий момент установка полностью механическая, за исключением датчика угла наклона маятника. Так как в настоящее время важную часть любого производства составляет автоматизация, которая позволяет сократить затраты времени, ресурсов и увеличить количество и качество выпускаемого продукта, поэтому основная задача состоит в создании средства управления в виде программы для персонального компьютера с интуитивно-понятным интерфейсом. Для этого необходимо реализовать связку «механика – электроника – микроконтроллер – программа для ПК».

Не все предлагаемые на рынке средства автоматизации, на основе программируемых логических контроллеров, подходят для использования в данном проекте, т.к. они имеют свои недостатки.

Данная работа отличается в первую очередь дешевизной, при том, что разрабатываемая система разрабатывается на современной элементной базе и имеет большие функциональные возможности, а так же надежности. Разрабатываемая система основана на универсальной платформе Raspberry Pi Model B+ и соответствует всем современным требованиям

Платформа Raspberry Pi Model B+ управляет подъемом маятниковой поверхности, дозирующим устройством, системой фиксации маятниковой поверхности, а также считывает данные с угла поворота и с трех веб камер.

Датчик угла поворота необходим для определения энергозатрат, которые определяются по формуле:

$$E = m \cdot g \cdot l_{м} \cdot (cos\alpha_2 - \cos(e^{-kT}\alpha_1))$$

где α_1 – угол отклонения; α_2 – угол выхода маятниковой поверхности.

Для определения работы маятникового деформатора используются три веб камеры. Данный метод основан на теории советского ученого П.А. Ребиндера [3], который предложил оценивать работу измельчения формулой

$$A_p = k_v \cdot k_n \cdot V_m + \alpha_{пов} \cdot \Delta S$$

где A_p – расход энергии на разрушение; k_v – коэффициент, учитывающий какая часть объема частицы деформируется; k_n – коэффициент, характеризующий физико-механические свойства разрушаемого тела; V_m - объем разрушаемого тела; $\alpha_{пов.}$ - удельная поверхностная энергия разрушаемого тела; ΔS - образованная при разрушении новая поверхность.

Таким образом, одна камера устанавливается над маятниковой поверхностью для определения площади зернового материала до измельчения, а две других – на вылете зернового материла в сборник, для определения площади после измельчения.

В соответствии с поставленной задачей необходимо разработать систему мониторинга процесса измельчения зерна, а именно – интерактивно получать данные в виде угла отклонения маятника от состояния покоя и передавать на ПК с целью дальнейшего использования в расчётах и ведения статистики.

В качестве регистратора угла используется бесконтактный магнитный датчик углового положения KMA200.

Также необходимо реализовать систему подъема маятниковой поверхности. Эта система должна выполнять подъем с точностью до градуса и выполнять остановку маятника после измельчения зерна. Она будет состоять из асинхронного двигателя, частотного преобразователя, электромагнитной муфты и реле.

Система имеет следующий вид:

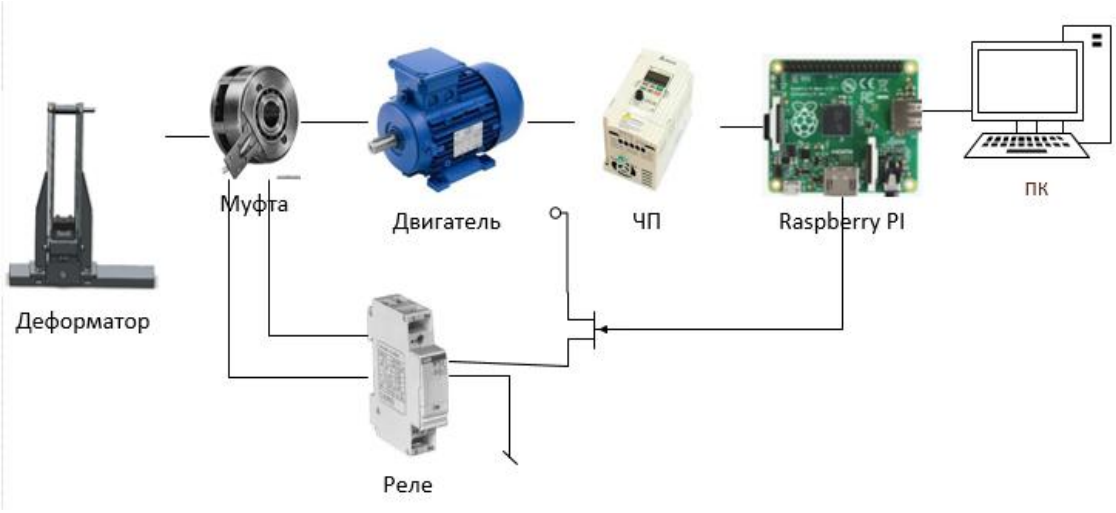


Рисунок 3 – Общий вид системы подъема

Алгоритм работы системы: в программе в специальной форме устанавливается необходимое значение угла. После этого, с программы посылается специальная команда на Raspberry PI, который преобразует эту команду в специальный сигнал для частотного преобразователя, к которому подключен двигатель. После этого двигатель поднимает маятник до того момента, пока не установится необходимый угол. Для того чтобы знать какой угол в данный момент установлен, в системе находится датчик Холла который, в реальном времени отправляет значение угла в Raspberry PI и уже далее в программу на ПК. Муфта необходима для остановки маятника. Она управляется с помощью реле, которое в свою очередь через транзистор подключено к Raspberry PI и можно в программе на ПК будет остановить маятник в любой момент.

СПИСОК ЛИТЕРАТУРЫ

1. Наумов, И.А. Совершенствование кондиционирования и измельчения пшеницы и ржи / И.А. Наумов. – М.: Колос, 1975. – с.176

2. Пат. № 2263544 Российская Федерация, МПК B02C 19/16 Способ формирования зерновых продуктов размола / Злочевский Валерий Львович, Злочевский Алексей Валерьевич.; заявл. 16.02.2004; опубл. 10.11.2005.

3. Ребиндер, П.А. Исследование в области поверхностных явле-ний / П.А. Ребиндер // Труды Гипроцветметалл. – 1930, т.1.

ИСПОЛЬЗОВАНИЕ РАДИОМОДЕМОВ ПРИ ОБУЧЕНИИ СТУДЕНТОВ БАКАЛАВРИАТА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Максимов А.А. – студент, Борисов А.П. –к.т.н., доцент, Черемисин П.С. – к.т.н., доцент, Тырышкин С.Ю. – к.т.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Беспроводная передача данных в настоящее время переживает бурное развитие. Ввиду продолжающейся компьютеризации 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 по цене, времени монтажа и самой возможности проведения. Поэтому беспроводные технологии связи являются востребованными решениями.

Среди беспроводных технологий применяются многие стандартизированные, закрепленные, например, институтом IEEE. Но кроме стандартизированных решений, имеется разработанное отдельными институтами и конструкторскими бюро собственное нестандартизированное оборудование, обеспечивающее радиосвязь большого или малого радиуса действия – радиомодемы.

Также стоит отметить следующий правовой аспект использования беспроводного обмена данными, особенность лицензирования радиосвязи в России. На основании решения ГКРЧ [1] выделены нелицензируемые радиочастотные диапазоны. Многие технологии и средства беспроводной связи иностранного производства, в том числе стандартизированные, не используют данные диапазоны, поэтому подлежат регистрации в соответствующих органах РФ.

Исходя из вышеназванного, будет уместным поместить ознакомление с радиомодемами в учебный план дисциплин, касающихся вычислительных комплексов и технологий в области связи. При этом практическому закреплению теоретической базы могут служить специальные аппаратно-программные средства. Помимо этого, бакалавр, а, тем более, специалист в области ИТ, несомненно, должен обладать кругозором, соответствующим получаемому высшему техническому образованию.

Радиомодемы серии RMD400 (рисунок 1) являются устройствами малого радиуса действия (до 10 км), используют непосредственное соединение между собой или через радиомодем-ретранслятор без подключения к сотовым сетям. Радиомодемы работают в диапазоне частот 433 МГц с выходной мощностью 10 мВт, что соответствует условиям нелицензируемого применения.

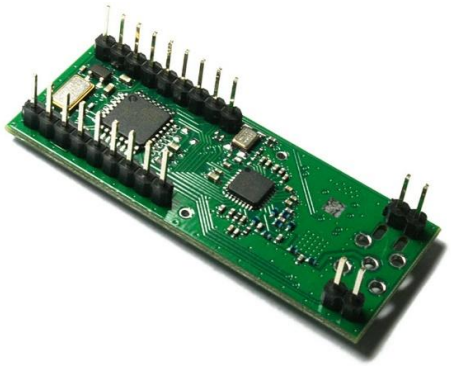


Рисунок 1 - Внешний вид печатной платы РМД400-ОЕМ

Радиомодем RMD400 [2] обладает высокой чувствительностью приёмника при низких скоростях передачи и возможностью компенсации потерь мощности сигнала в длинном фидере внешней антенны, что делает эффективным его использование для построения сетей сбора данных на большой территории.

Дальность радиосвязи радиомодемов РМД400 обусловлена использованием микросхемы приёмопередатчика CC1020 с узкополосным приёмником, обладающим высокой чувствительностью. При уменьшении скорости передачи в эфире пропорционально сужается и полоса пропускания приёмника, вплоть до 9,6 кГц при скорости передачи 1,2 кбит/с. Использование такой узкой полосы пропускания стало возможным благодаря высокой стабильности частоты сигнала передатчика и гетеродина приёмника, которая обеспечена компенсацией температурного ухода частоты опорного кварцевого генератора.

Высокая энергетическая эффективность радиомодемов серии РМД400 получена также за счёт использования каскадного кодирования с перемежением кодированных данных. В результате деперемежения и декодирования каскадного кода в приёмнике исправляются не только случайные шумовые ошибки, но и пакетные ошибки, вызванные импульсными помехами.

Радиомодемы серии РМД400 обеспечивают потоковую передачу поступающих на последовательный интерфейс данных с пакетированием и асинхронной передачей пакетов.

Асинхронная передача пакетов позволяет использовать преимущества синхронной передачи пакетированных данных в сочетании с удобством асинхронного ввода/вывода данных на интерфейсе.

С помощью радиомодемов серии РМД400 возможно построение как линии связи «точка-точка», так и производственно-технологические сети связи сложной конфигурации типа «звезда» или «дерево».

Для того чтобы осуществить связь между радиомодемом и компьютером, требуется разработать устройство сопряжения. Устройство сопряжения будет выполнять функции передачи пакетов от компьютера к радиомодему и обратно (шлюз), производить настройку радиомодема по команде компьютера (хоста), а также выполнять индикацию передачи данных светодиодами.

Устройство сопряжения связывает интерфейс UART радиомодема и порт USB компьютера. В данной работе решено не использовать последовательный порт COM для связи с компьютером по ряду немаловажных причин:

- в современных портативных компьютерах и ноутбуках крайне редко встречается порт COM (интерфейс RS-232);

- использование переходников или схем с преобразователями интерфейсов с RS232/TTL на COM с данным радиомодемом нерационально ввиду отсутствия гибкости и дополнительных возможностей;

- COM-порт имеет неудобства в использовании из-за отсутствия поддержки технологии «Plug and Play»: для работы с устройством по COM-порту компьютер зачастую следует перезагрузить;

- также у COM-порта низкая скорость, большие размеры разъемов, а также зачастую высокие требования к времени отклика ОС и драйвера. Высокое количество прерываний (одно прерывание на каждые 8 байт).

Вместо этого было принято решение сделать устройство сопряжения поддерживающим интерфейс USB, как более простой и дружественный для пользователей, пригодный для «горячего» подключения.

Для этого была использована схема со стабилитронами (рисунок 2).

Общая схема взаимодействия узлов системы «радиомодем-компьютер» представлена на рисунке 3.

Программное обеспечение лабораторной работы предназначено для использования в учебных и демонстрационных целях, поэтому требованиями к программе являются наглядный интерфейс и простота использования. Программа подает команды и данные на плату сопряжения с радиомодемом и принимает данные с платы.

Программа выполняет считывание и установку параметров радиомодема, а также производит настройку собственного режима работы. Программа защищена от ошибочных нажатий, зацикливаний и зависаний. Также предусмотрена защита от нажатий кнопок, запускающих действия, которые не могут быть выполнены в данный момент.

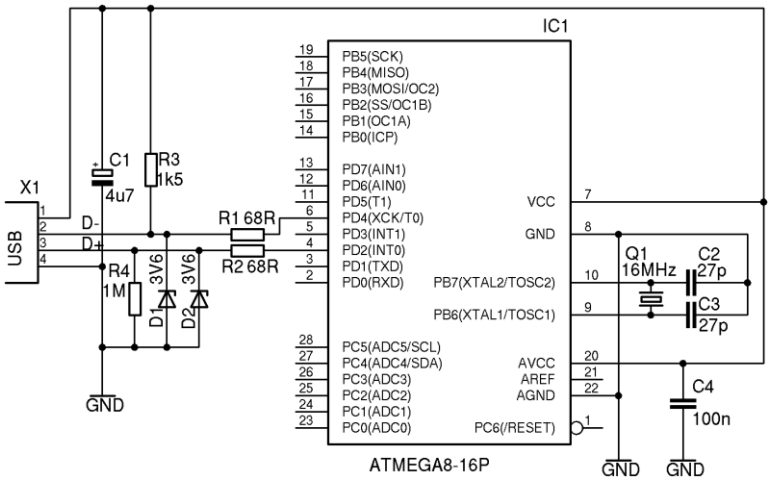


Рисунок 2 - Схема со стабилитронами. Питание МК от +5В

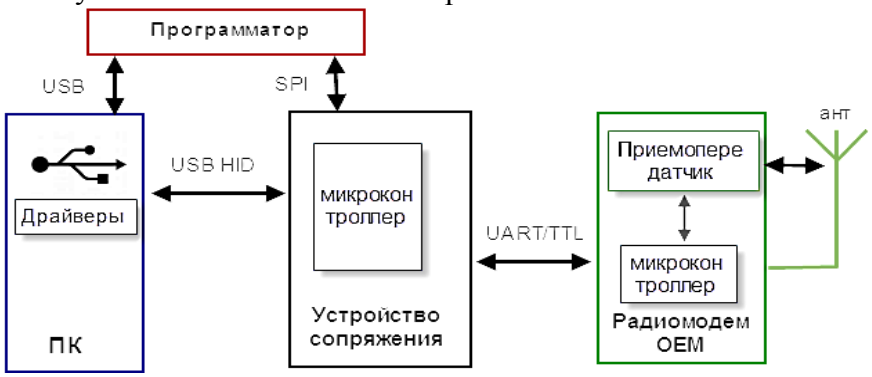


Рисунок 3 – Схема взаимодействия узлов системы «радиомодем-компьютер»

Программа взаимодействует с устройством сопряжения по интерфейсу USB класса HID с помощью Feature-репортов (специальных) на основе дескриптора USB репорта, предоставляемого устройством.

Для поддержки связи с радиомодемом программа периодически опрашивает устройство сопряжения на наличие данных от радиомодема, в положительном случае организовать их прием.

Перед передачей данных программа кодирует посылаемую информацию в последовательность байтов, а после приема – декодирует.

Общий вид программы и окна настроек представлен на рисунке 4 [3].

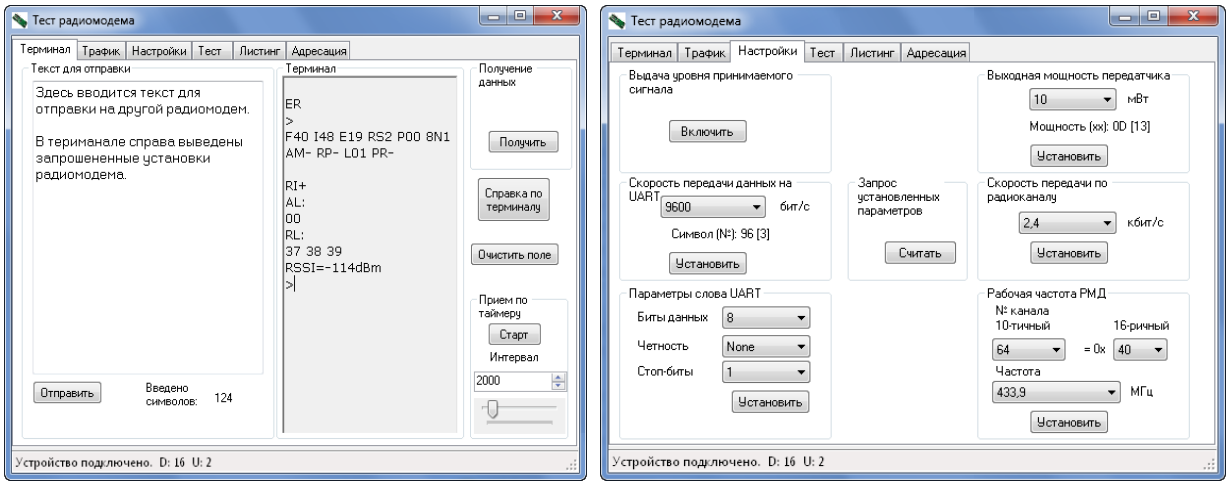


Рисунок 4 – Общий вид программы

Данное программное обеспечение, вместе с аппаратной частью подключения радиомодемов к ПК обеспечивает изучение принципов работы радиомодемов и шифрование при передаче данных.

Список литературы:

1. Решение ГКРЧ от 07.05.2007 № 07-20-03-001. О выделении полос радиочастот устройствам малого радиуса действия [Электронный ресурс]. – Режим доступа: http://rfcmd.ru/sphider/docs/GKRCh/GKRCh_07-20-03-001_ot_07_05_2007.htm.

2. КБ Марс РМД400-OEM – Компьютеры и оргтехника | Сетевое оборудование – www.db.am [Электронный ресурс]. – Режим доступа: http://computer.db.am/network/view/99029/.– Загл. с экрана.

3. Думнов, А.Н. Использование радиомодемов малого радиуса действия в учебном процессе дисциплины «Системы и сети связи» [Текст] / А.П. Борисов, А.Н. Думнов //

Горизонты образования: 10-я Всероссийская научно-техническая конференция «Наука и молодежь-2013». – Барнаул, АлтГТУ, 2013.

ОБЗОР МЕТОДОВ ПОСТРОЕНИЯ И АНАЛИЗА АЛГОРИТМОВ БЛОЧНОГО И ПОТОЧНОГО ШИФРОВАНИЙ

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

Сегодня в мире огромную популярность приобрели беспроводные сети, так как большое распространение получили различные мобильные гаджеты, а также ноутбуки, с которых пользователи передают разнообразную информацию, в том числе и не предназначенную широкому кругу пользователей, а соответственно, такая информация может быть перехвачена злоумышленниками. В связи с этим возникает проблема безопасности этих данных, решением которой является передача этой информации в зашифрованном виде. Данный способ реализуется с помощью различных алгоритмов шифрования.

В настоящее время методы построения беспроводных сетей изучаются, а методы построения и анализа алгоритмов блочного и поточного шифрования - нет, то есть методы шифрования используются как данность, что является большим упущением при подготовке специалистов в области информационной безопасности (ИБ). Поэтому актуально создание обучающего программного обеспечения в сфере методов блочного и поточного шифрования.

Поэтому целью работы это изучить симметричные алгоритмы шифрования и выдвинуть требования для создания программного обеспечения (ПО) для обучения студентов.

Для достижения данной цели, необходимо решить следующие задачи:

- Изучить алгоритмы блочных и поточных шифрований, их преимущества и недостатки, а также применение на практике.
- Изучить стандарты шифрования, используемые в беспроводных сетях.

Можно выделить два основных вида методов шифрования: симметричный и ассиметричный. Симметричный использует один и тот же ключ для шифрования и расшифровывания информации. Отправитель и получатель - единственные люди, которые знают этот симметричный ключ. Симметричные алгоритмы используются для шифрования данных передаваемых по беспроводным сетям, например Wi-fi. Выделяют два основных типа симметричного шифрования: блочный и поточный шифры.

Поточный шифр (рисунок 1) - это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого текста. Поточный шифр реализует другой подход к симметричному шифрованию, нежели блочные шифры.

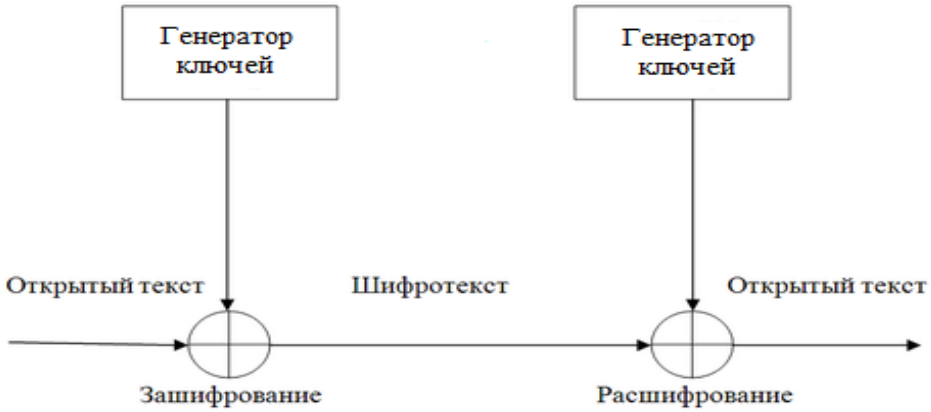


Рисунок 1 - Поточный шифр

На рисунке 1 представлена общая схема работы поточного шифрования. Генератор ключей выдает поток битов, которые будут использоваться в качестве гаммы. Источник

сообщений генерирует биты открытого текстах, которые складываются по модулю 2 с гаммой, в результате чего получаются биты зашифрованного сообщения [1].

Преимущества:

- Символ шифрованного текста получается из исходного текста на основе не только от используемого ключа, но и от его расположения в потоке открытого текста

- Высокая скорость шифрования, соизмеримая со скоростью поступления входной информации; поэтому, обеспечивается шифрование практически в реальном масштабе времени вне зависимости от объема и разрядности потока преобразуемых данных.

Недостатки: необходимость обмениваться с получателями секретными ключами.

Поточное шифрование широко применяется в различных системах защиты информации в компьютерных сетях (например, в протоколах SSL и TLS, алгоритме безопасности беспроводных сетей WEP и WPA).

Блочный шифр - разновидность симметричного шифра. Особенностью блочного шифра является обработка блока нескольких байт за одну итерацию (как правило 8 или 16). Блочные криптосистемы разбивают текст сообщения на отдельные блоки и затем осуществляют преобразование этих блоков с использованием ключа [2].

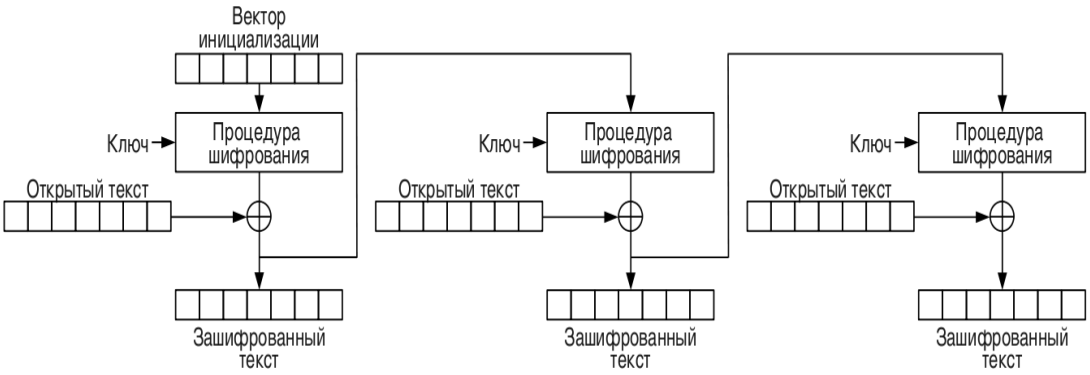


Рисунок 2 - Блочный шифр

Основные операции используемые при блочном шифровании:

-операция побитового сложения по модулю 2 с ключом шифрования;

-циклический сдвиг цепочки битов на определенного количество в право или влево;

-табличной подстановки;

-операции перемещения, то есть изменения порядка битов в блоке шифрования [3].

К достоинствам блочных шифров относят сходство процедур шифрования и дешифрования, которые, как правило, отличаются лишь порядком действий. Это упрощает создание устройств шифрования, так как позволяет использовать одни и те же блоки в цепях шифрования и дешифрования.

К недостаткам относится сложность обмена ключами. Для применения необходимо решить проблему надёжной передачи секретных ключей.

В России в качестве стандарта на блочные алгоритмы шифрования с закрытым ключом в 1989 году был принят ГОСТ 28147-89. Он рекомендуется к использованию для криптографической защиты данных. Симметричные алгоритмы шифрования используются также в американских стандартах DES, AES, RC4 и многих других. Алгоритм AES применяется для шифрования данных передающихся через беспроводные сети Wi-Fi. Алгоритм шифрования AES, действующий в качестве государственного стандарта в области шифрования данных в США с 2001 года. В основу стандарта положен шифр Rijndael. Шифр AES характеризуется размером блока 128 бит, длиной ключа 128, 192 или 256 бит и количеством раундов 10, 12 или 14 в зависимости от длины ключа.

Алгоритм AES основан на перестановках и заменах. Перестановка - это изменение порядка данных, а замена - замещение одного блока данных другим. В AES используется несколько видов перестановок и замен. Ядро алгоритма AES-шифрования образуют четыре

операции. AddRoundKey заменяет группы из 4 байтов, комбинируя их с итеративными ключами, которые генерируются по значению исходного ключа. SubBytes замещает отдельные байты в соответствии с таблицей замен. ShiftRows переставляет группы из 4 байтов, циклически сдвигая 4-байтовые строки. MixColumns заменяет байты результатами операций сложения и умножения элементов поля [4]. На рисунке 3 показана схема действия алгоритма AES.

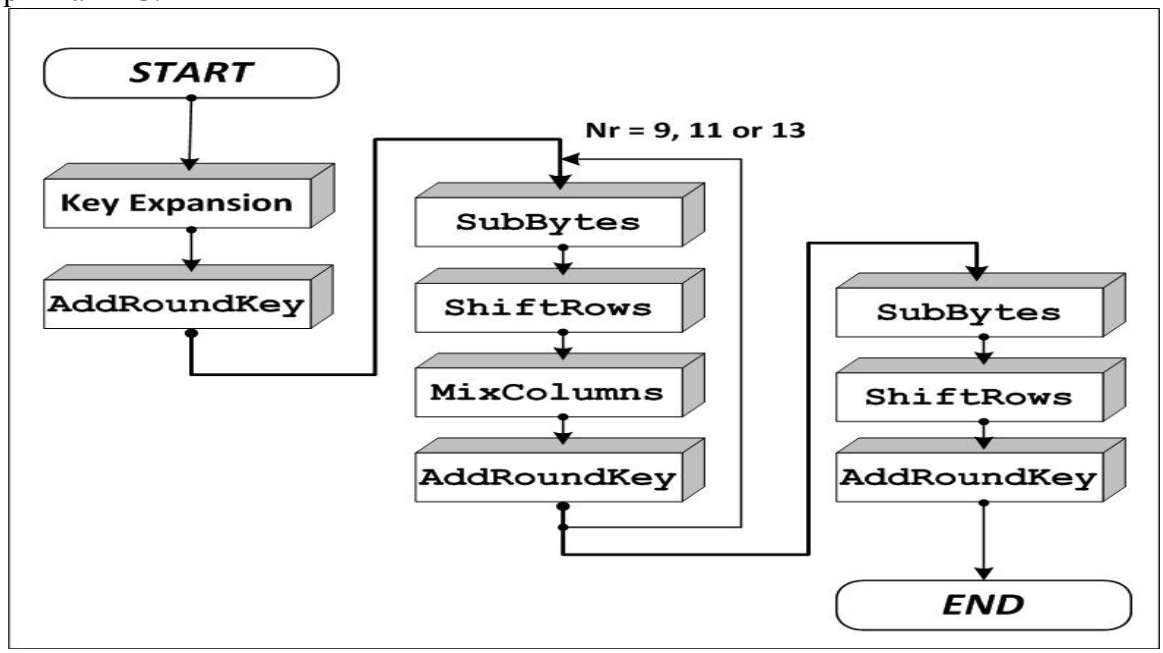


Рисунок 3 - Шифр AES

Согласно вышесказанному, область шифрования действительно является широко используемой во многих системах в том числе беспроводные сети Wi-Fi, поэтому существует необходимость написания ПО для обучения студентов по данной теме.

Список литературы

1.Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. — Москва.— Изд-во Горячая Линия-Телеком, 2005

2.https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%B2%D1%8B%D0%B9_%D1%88%D0%B8%D1%84%D1%80

3.http://www.intuit.ru/studies/courses/691/547/info

4.Баричев С.Г., Гончаров В.В., Серов Р.Е. 2.4.2. Стандарт AES. Алгоритм Rijdael // Основы современной криптографии. - М.: Горячая линия - Телеком, 2002

РАЗРАБОТКА УСТРОЙСТВА МОДЕЛИРОВАНИЯ КАНАЛА СВЯЗИ СТАНДАРТА GSM ДЛЯ ОБУЧЕНИЯ СТУДЕНТОВ НАПРАВЛЕНИЯ 10.03.01 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

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

Защита информационного пространства России на сегодняшний день является одним из приоритетных направлений национальной безопасности. Как заявил президент России Владимир Путин на открытии заседания Совета Безопасности РФ, надежная работа систем связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России в самом широком смысле этого слова.[6]

Обеспечение безопасности сетей связи – одна из важнейших задач в общем контексте мероприятий по обеспечению безопасности как на государственном уровне, так и для отдельно взятых организаций. Это один из приоритетов Доктрины информационной безопасности РФ.[9]

В этой связи подготовка бакалавров в области информационной безопасности должна включать в себя изучение принципов работы систем сотовой связи и приобретение практических навыков по обеспечению их безопасности.

Целью данной работы является создание модуля для проведения лабораторных работ по обеспечению безопасности телефонных переговоров сотовой связи для студентов направления 10.03.01 «Информационная безопасность».

Для достижения цели были выбраны следующие задачи:

- Проведение анализа образовательного стандарта учебной дисциплины Б.3.Б.7 «Сети и системы передачи информации»;
- Анализ особенностей обеспечения безопасности информации во время телефонных переговоров;
- Разработка стенда для осуществления звонков на мобильные телефоны и организации защищенной линии связи на основе модуля GSM Arduino применительно к учебному процессу.

На сегодняшний день большинство организаций для ведения переговоров (в т.ч. конфиденциальных) предпочитают системы подвижной связи телефонным сетям общего пользования. Порядка 100% рынка мобильной цифровой связи в России принадлежит стандарту GSM (как альтернатива данному стандарту есть связь CDMA, однако процент ее пользователей очень мал не смотря на то, что для данных систем характерна повышенная конфиденциальность обмена сообщениями). Этот стандарт был разработан в середине 90-х годов 20 века, и с тех пор система его защиты не претерпевала серьезных изменений.[7,11]

Защита GSM сетей обеспечивается тремя алгоритмами, использующими алгоритм шифрования RSA: A3 – алгоритм, отвечающий за аутентификацию и предупреждающий клонирование, A5 – алгоритм шифрования голосового трафика, и A8 – алгоритм генерации ключа из результата работы A3 в ключ A5, причем алгоритмы A3 и A8 чаще всего представляют собой обыкновенную хэш-функцию. Алгоритм A5 имеет несколько модификаций – A5/0 (без шифрования), A5/1 (для избранных стран), A5/2 (сильно ослабленная версия, используется в т.ч. в России) и A5/3 (разработан с цель заменить A5/1, однако используется только в 3GPP сетях).[5,8]

Схема аутентификации пользователя и шифрования приведена на рисунке 1.

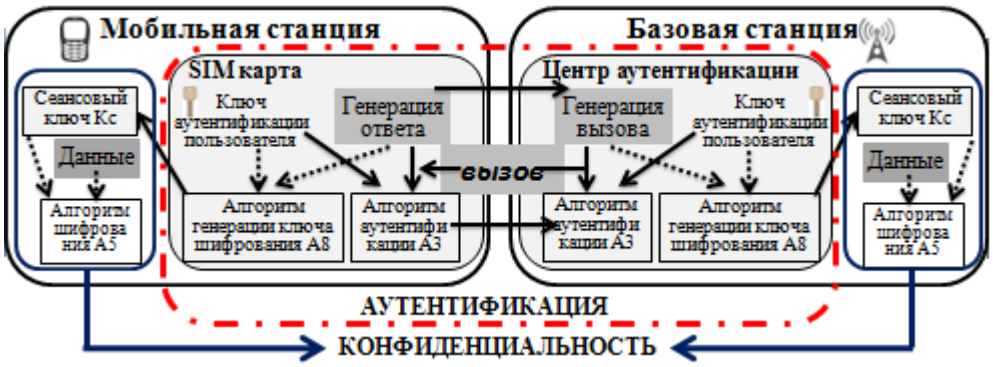


Рисунок 1 – Схема аутентификации пользователя и шифрования стандарта GSM

Как видно из представленной схемы, мобильные станции (телефоны) снабжены смарт-картой, содержащей A3 и A8, а в самом телефоне имеется ASIC-чип с алгоритмом A5. Базовые станции также снабжены ASIC-чипом с A5 и "центром аутентификации", использующим алгоритмы A3 и A8 для идентификации мобильного абонента и генерации сеансового ключа. В режиме реального времени производится шифрование сигнала с

помощью алгоритма А5 и его передача, а при приеме базовой станцией или телефоном производится обратный процесс – абонент слышит голос собеседника. Данная архитектура при надлежащем исполнении и надежных алгоритмах должна была обеспечить надежную защиту от прослушивания и клонирования абонентского номера, однако принципы работы алгоритмов довольно скоро стали известны и были опубликованы их криптосхемы. В результате еще в конце 90х годов прошлого века была реализована угроза клонирования абонентов и перехват и расшифровка голосового сообщения в режиме реального времени, а не так давно стала возможна подмена базовой станции. Эти уязвимости позволяют злоумышленникам получить доступ к конфиденциальной информации. Как результат – уровень потерь операторов мобильной связи от разного рода мошенничества и вредительства составляет в среднем 2 - 6% от общего объема трафика и может доходить до 25%.[2]

Теперь рассмотрим подробнее, какие угрозы возможно реализовать в сетях цифровой мобильной связи стандарта GSM благодаря существующим уязвимостям.

Поделим условно все угрозы на две группы: внутренние (существующие в канале GSM) и внешние. Внутренние угрозы могут быть реализованы на различных этапах передачи данных: в базовых станциях, в среде передачи и в мобильных телефонах. Внешние угрозы – это угрозы перехвата по акустическому, виброакустическому, акустоэлектрическому каналам. Прослушивание, перехват, дешифрование, клонирование осуществляются с помощью специальной аппаратуры, которая находится в свободном доступе в интернете. Производителями являются в основном иностранные компании, а цена таких устройств зависит от сложности реализации, дальности действия и надежности использования. К сожалению, российское законодательство никак не ограничивает продажу подобных средств, а мобильные операторы не собираются применять дополнительные средства для обеспечения безопасности данных своих абонентов. Не смотря на это, обеспечить конфиденциальность информации в сетях GSM могут сами пользователи. Рынок средств защиты информации оперативно реагирует на возникающие угрозы различными устройствами, которые можно условно поделить на средства технической защиты и средства криптографической защиты. К первой группе относятся глушители, поглотители сигналов, генераторы шума, экраны и т.д. Ко второй группе относятся устройства абонентского шифрования – скремблеры, криптофоны, шифраторы.[1-5,10-12]

Разработанное устройство моделирование канала представляет собой упрощенную модель канала связи GSM: базовая станция → среда передачи → мобильная станция. Оно позволит будущим специалистам по защите получить представление о принципах работы систем подвижной связи, а также даст возможность осуществлять перехват данных в сети связи. Программное обеспечение позволит осуществлять шифрование/дешифрование данных. Помимо пассивной защиты (шифрования) студенты получат представление о средствах активной защиты (перехват будет осуществляться со включенным генератором шума и без него). Схема генератора шума и устройство, представляющее собой базовую станцию, приведены на рисунках 2–3.

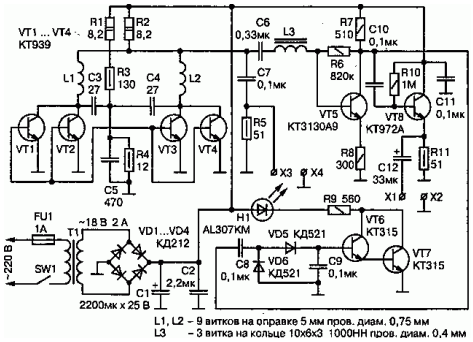


Рисунок 2 – Схема генератора подавления радиопередатчиков (30 МГц - 1гГц)

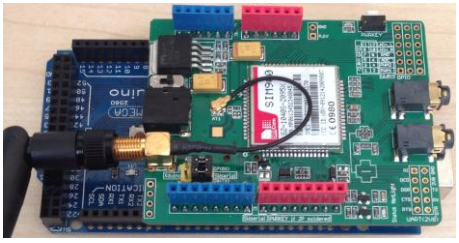


Рисунок 3 – Базовая станция лабораторной установки

Лабораторные занятия будут выполняться в рамках дисциплины Сети и системы передачи информации. Работы будут включать в себя изучение модели передачи данных в канале системы подвижной связи GSM, изучение угроз безопасности информации в сети, изучение активных и пассивных методов защиты (насколько повышается надежность передачи информации при использовании абонентского шифрования и средств зашумления). Данные занятия помогут будущему специалисту в формировании навыков решения профессиональных задач в рамках эксплуатационной, проектно-технологической и экспериментально-исследовательской деятельности, а также в формировании профессиональных компетенций.

Список литературы:

1. Jim Finkle, «GSM phones vulnerable to hijack scams – researcher» [Электронный ресурс]. Режим доступа: http://www.reuters.com/article/2011/12/27/us-mobile-security-idUSTRE7BQ05020111227

2. HackZone.RU - Описание GSM и ее взлом [Электронный ресурс]. Режим доступа: http://www.hackzone.ru/articles/vzlom_gsm.html

3. Lucky Green , "*More NSAKEY musings*", Crypto-Gram, September 15, 1999.

4. Безопасность GSM реальная или виртуальная [Электронный ресурс]. Режим доступа: http://www.bnti.ru/showart.asp?aid=957&lvl=04.02

5. Безопасность GSM сетей: шифрование данных [Электронный ресурс]. Режим доступа: http://habrahabr.ru/post/186838/

6. Заседание Совета Безопасности, посвящённое вопросам противодействия угрозам национальной безопасности в информационной сфере [Электронный ресурс]. Режим доступа: http://www.kremlin.ru/events/president/news/46709

7. Попов В.И. Основы сотовой связи стандарта GSM: Учебное пособие. [Текст] М.: «Эко-Трэндз», 2005г.

8. Скремблер – Описание GSM и ее взлом [Электронный ресурс]. Режим доступа: http://www.skrembler.ru/st10.html

9. Совет безопасности РФ. Доктрина информационной безопасности Российской Федерации [Электронный ресурс]. Режим доступа: http://www.scrf.gov.ru/documents/6/5.html

10. Способы и средства защиты информации [Электронный ресурс]. Режим доступа: http://www.analitika.info/zaschita.php?page=1&full=block_article88

11. Телекоммуникационные технологии. Введение в технологии GSM. С. Б. Макаров, Н. В. Певцов, Е. А. Попов, М. А. Сиверс. [Текст] М.: Академия, 2008 г.

12. Хорев А. А., Макаров Ю. К. Методы защиты речевой информации и оценки их эффективности. – Защита информации. Конфидент. – № 4.–2001г.–22-33 стр.

ПРАВОВЫЕ АСПЕКТЫ ОЦЕНКИ САЙТА В СЕТИ ИНТЕРНЕТ КАК ОБЪЕКТА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Небольсина М.В. – студент, Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Наличие сайта в сети Интернет (Интернет – сайта) год от года становится всё более значимым условием, залогом успеха для современной организации, её репутации [1]. Для большинства государственных организаций наличие интернет – сайта (страницы сайта) является обязательным требованием (например, образовательные учреждения, организации социального сектора, ст. 10 Федерального закона от 09 февраля 2009 года № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»). Для коммерческих организаций обеспечить конкурентоспособность без электронных средств, основу которых составляет Интернет - сайт практически невозможно. Таким образом, информация, размещённая на Интернет – сайте, является важным активом организации, а сам Интернет- сайт объектом обеспечения информационной безопасности организации.

Современное обеспечение информационной безопасности организации, как по международным, так и по Российским стандартам и технологиям, базируется на комплексном применении правовых, организационных, технических, криптографических, физических способов и средств защиты информации [2] в отношении всех информационных ресурсов и применительно ко всем объектам защиты (информационным системам и информационно-телекоммуникационным сетям), обеспечивающим её функционирование по предназначению: обеспечение государственных функций, обеспечение бизнес-процессов, обеспечение общественных интересов.

Применение технических (программных и программно-аппаратных) способов и средств защиты исследовано достаточно полно и отражено в современной и учебной литературе. А вот правовые аспекты требуют дополнительных исследований, в том числе и в связи с тем, что законодательство в этой области в 2012-2014 годах претерпело немалые изменения.

Это определило необходимость решения в процессе исследования следующих задач:

1) выполнить анализ существующих подходов к определению, структуре сайта как объекта защиты информации в научной и учебной литературе, законодательстве РФ;
2) определить структуру сайта как объекта защиты информации;
3) выполнить анализ правовых норм законодательства по защите сайта и его составляющих (элементов);
4) определить правовые аспекты, которые необходимо учесть при оценке сайта как объекта обеспечения информационной безопасности организации.

Анализ научной литературы некоторых зарубежных стран англо-саксонской правовой системы показал, что там преимущественно преобладает «описательный» подход к определению понятия сайта. Акцент делается на защите отдельных охраняемых объектов, представленных на Интернет-сайте, как объектов авторского права, а не сайта в целом (например, [3]).

Анализ научных работ российских авторов последнего десятилетия показал, что они выполнены в области юридических наук и рассматривают Интернет – сайт как объект права и, в частности, как сложный объект интеллектуальной деятельности и исключительных прав. Например, в [5] Интернет-сайт определяется как предназначенный для размещения в сети Интернет результат интеллектуальной деятельности, состоящий из статичной основы (базового элемента сайта), представляющей собой программный (объектный) код и порождаемые им визуальные отображения (дизайн сайта), и динамичного содержания (контента), представляющего собой совокупность разнородных объектов исключительных прав и иных материалов, системно расположенных в пределах базового элемента сайта.

Интернет-сайт является с одной стороны «составным» объектом права, так как состоит из значительного числа объектов права, охраняемых или не охраняемых исключительными

правами. Базовым видом правоотношения, в котором участвует Интернет-сайт, является его создание, в процессе которого определяются охраноспособность составных частей Интернет-сайта, их правообладатели и владельцы, правообладатель и «владелец» Интернет-сайта, и др.

В 2012 году Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 21.07.2014) "Об информации, информационных технологиях и о защите информации) официально определил сайт следующим образом. Сайт в сети "Интернет" - совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети "Интернет" по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети "Интернет". Страница сайта в сети "Интернет" - часть сайта в сети "Интернет", доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет" [5].

Сайт - система электронных документов (файлов данных и кода) частного лица или организации в компьютерной сети под общим адресом (доменным именем или IP-адресом) [4]. С учётом вышеизложенных особенностей сайта как объекта права и его правового определения в законодательстве РФ можно представить структуру сайта следующим образом (технические (программно-аппаратные) элементы сайта):

Непосредственные элементы сайта:

– веб-приложение (программа для ЭВМ на гипертекстовой разметке);

– контент - любое информационное наполнение ресурса (веб-сайта), загружаемое в соответствии с законом (О рекламе, о персональных данных, об авторском праве (ГК РФ ч.4)) [5-6].

Опосредованные элементы сайта:

– информационно –телекоммуникационная сеть (ИТКС) - (Закон об «Информации…» ст.2, п.4.);

– доменное имя (Закон об «Информации…» ст.2, п.15;

– сетевой адрес (Закон об «Информации…» ст.2, п.15.);

– сервер - специализированный компьютер и/или специализированное оборудование для выполнения на нём сервисного программного обеспечения [1];

– браузер — прикладное программное обеспечение для просмотра веб-страниц [1].

Анализ правовых норм законодательства по защите сайта и его составляющих (элементов) выполнен с учётом рассмотрения норм правовой охраны и норм правового регулирования относительно этих элементов. Результаты имеют табличный вид (таблица 1).

Таблица 1 – Фрагменты анализа правовых норм для элементов сайта

Элемент сайта	Правовая охрана (УК РФ,КО АП, ГК РФ, ФЗ)	Правовое регулирование (ФЗ, НПА Прав-ва, ФОИВ)
Сайт в целом	КОАП РФ Статья 13.18. ч.2 Воспрепятст-вование работе сайтов в сети "Интернет"	С.15.1, ст.15.3 закона «Об информации…»
Доменное имя	Статья 1485. Знак охраны товарного знака	Ст.1484 ч. 2.п5. ГК РФ ч.4 Исключительное право на товарный знак

Правовые аспекты оценки сайта в сети интернет как объекта обеспечения информационной безопасности организации определяются следующим образом.

1. Контент сайта в части рекламы должен формироваться в соответствии с требованиями законодательства РФ «О рекламе». Ответственность за это несёт организация (юридический отдел).

2. При использовании на сайте или странице сайта общедоступных персональных данных их статус «общедоступности» должен быть проверен и подтверждён в соответствии с ФЗ «О персональных данных» юридической службой (юристом) организации.

3. При использовании на сайте или странице сайта, или с использованием сайта персональных данных, должна быть обеспечена их защита в соответствии с ФЗ «О персональных данных» и требованиями нормативно-правовых актов Правительства РФ, нормативных и методических документов ФСБ России и ФСТЭК России.

4. Размещение персональных данных россиян на сайте или странице сайта, или с использованием сайта вне России (на сервере) в ближайшем будущем запрещается.

5. Запрет на размещение информации, распространение которой в Российской Федерации запрещено, должен быть закреплён в локальном нормативно-правовом акте организации.

6. Контент сайта, использующий объекты интеллектуальной собственности (авторские права), должен формироваться в соответствии с нормами гражданского законодательства РФ в этой области и норм международного права.

7. Доменное имя в части товарного знака могут быть (должны быть) защищены свидетельством.

8. Обязанности по обеспечению безопасности в отношении сайта должны быть отражены в договоре с администратором домена или хостинг-провайдером.

Все эти аспекты оценки сайта как объекта обеспечения ИБ организации должны быть отражены в локальных нормативных актах и методических документах организации (рисунок 1).

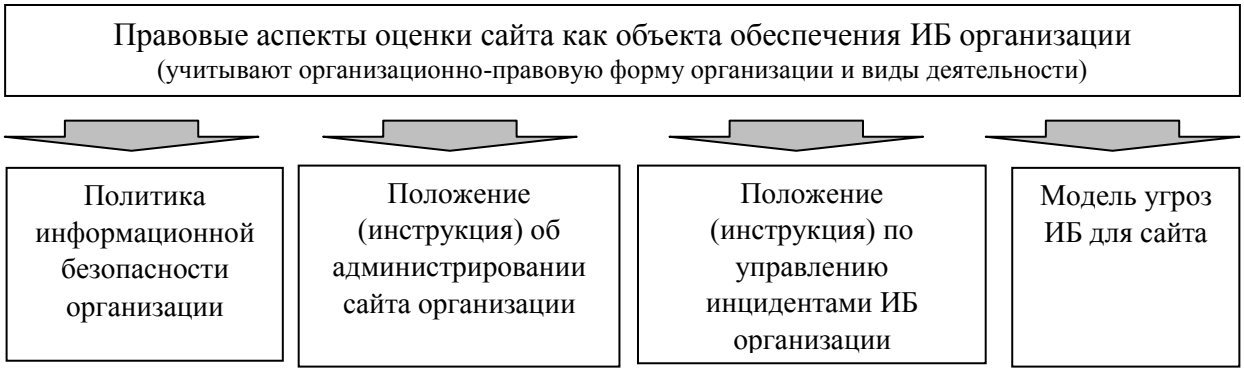


Рисунок 1 - Локальные нормативные акты и методические документы организации

Полученные результаты исследования планируется использовать при разработке организационно-технической (субъектно-объектной) модели сайта, как объекта обеспечения информационной безопасности организации, в рамках НИР «Информационная безопасность организации», выполняемой на кафедре ИВТиИБ.

Список использованной литературы:

1. Нурбеков К.Н. Интернет-сайт как объект гражданских прав и средство коммуникации // Московское объединение студентов-юристов. – М., 2008. С. 1-6.

2. Загнайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие / Ю.Н. Загинайлов; Алт. гос. техн. ун-т им. И.И. Ползунова. – Барнаул: АлтГТУ, 2011 – 252 с.

3. Bell T.W. Intellectual Property // Internet Law. [Электронный ресурс] // URL: http://www.tomwbell.com/NetLaw/Ch07.html.

4. Википедия: свободная электронная энциклопедия: на русском языке [Электронный ресурс] // URL: http://ru.wikipedia.org (дата обращения: 03.04.2015).

5. Федеральный закон РФ от 29 июля 2004 года (ред. 24.11.2014) №149 ФЗ «Об информации, информационных технологиях и защите информации» (с изм. и доп., вступающими в силу с 1.01.2016).

6. Энциклопедия SEO [Электронный ресурс] // URL: http://www.hmx.ru (дата обращения 04.04.2015).

АНАЛИЗ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ РАЗРАБОТКИ ОБУЧАЮЩЕГО СТЕНДА

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

Информационные технологии непрерывно развиваются и совершенствуются, и этот факт не мог бы обойтись без появления негативных явлений, таких как промышленный шпионаж, компьютерные преступления и несанкционированный доступ к секретной и конфиденциальной информации через каналы утечки информации. Чтобы гарантировать высокую степень защиты информации, необходимо постоянное регулирование, разработка и совершенствование средств ее защиты, в том числе технических.

Целью данной работы является: изучить классификации технических каналов утечки информации и проанализировать имеющееся оборудование, предназначенное для разработки лабораторного стенда с использованием средств технической защиты от несанкционированного доступа.

Для достижения поставленной цели, были выделены некоторые задачи:

- Изучить технические каналы утечки информации и способы их защиты
- Классифицировать имеющееся оборудование и ознакомиться с принципом его работы
- Выдвинуть требованию к созданию лабораторного стенда

Каналы утечки информации.

Основная задача технической защиты информации - выявить и блокировать каналы утечки информации. Канал утечки информации – это методы и пути утечки информации из информационной системы.

Существуют следующие группы каналов утечек информации: организационные, технические, системно-программные, инфо-телекоммуникационные и комбинированные. Технические каналы утечки информации - каналы, несанкционированный перенос информации в которых осуществляется с использованием технических средств защиты.

Существует несколько классификаций технических каналов утечки информации: по типу обрабатываемой информации и по физической природе носителя.

По типу обрабатываемой информации технические каналы утечки информации делятся на два вида: каналы для перехвата телекоммуникационной информации (электрические, электромагнитные, параметрические) и каналы для перехвата речевой информации (акустические, акустоэлектрические, виброакустические, оптико-электронные, параметрические).

Технические каналы утечки по физической природе носителя бывают:

- радиоэлектронные (электромагнитный и электрический)
- визуально-оптические (фотографический, оптико-электронный)
- акустические (виброакустические, акустоэлектрический, гидроакустический)
- материально-вещественные

Т.к. большинство каналов можно отнести как к одной классификации, так и к другой, более подробно рассмотрим только одну классификацию – по физической природе носителя.

В *радиоэлектронном канале* утечки конфиденциальной информации носителям информации могут являться электрические, магнитные и электромагнитные поля в радиодиапазоне, а так же электрический ток, распространяющийся по металлическим проводам. Такой канал образуется в результате излучений, издаваемых самим объектом

информатизации, а так же за счет побочных, паразитных излучений и наводок. Радиоэлектронные каналы делятся на электромагнитный и электрический каналы утечки информации.

К электромагнитным каналам утечки информации можно отнести перехват побочных электромагнитных излучений (ПЭМИ) элементов технических средств передачи информации (ТСПИ), ПЭМИ на частотах работы высокочастотных генераторов и на частотах самовозбуждения усилителей низкой частоты.

Электрические канал утечки информации включают в себя съем информационных сигналов ТСПИ и вспомогательных технических средств и систем с линий электропитания или с цепей заземления, съем информации путем установки в ТСПИ электронных устройств перехвата информации.

В *акустическом канале* утечки информации носителем информации являются механические упругие акустические волны в определенных диапазонах частот, распространяющиеся в атмосфере, воде и твердой среде. Такие каналы подразделяются на акустоэлектрические и виброакустические каналы утечки информации.

В акустоэлектрических каналах утечки информации акустические сигналы распространяются в воздухе. Для перехвата таких сигналов используются портативные диктофоны, проводные микрофонные системы, акустические сетевые, телефонные и инфо-коммуникационные закладки.

В виброакустических каналах утечки информации средой распространения акустических сигналов являются ограждающие конструкции зданий, сооружений (стены, потолок, пол), трубы водоснабжения и т.д. Для перехвата акустических сигналов пользуются контактными микрофонами, электронными стетоскопами, радиостетоскопами.

В *оптическом* канале носителем информации является электромагнитное поле в диапазоне 0,46-0,76 мкм (видимый свет) и 0,76-13 мкм (инфракрасные излучения). Доступ к информации осуществляется с помощью средств визуально-оптической, фотографической и оптико-электронной разведки. К таким устройствам относятся различные фотокамеры и видеокамеры, приборы ночного видения, приборы наблюдения (бинокли, монокуляры, телескопы), тепловизоры, рентгеновские аппараты и т.д.

В *материально-вещественном канале* утечки информации носителем информации является материалы и вещества (твердые, жидкие, газообразные). В виде отходов или некачественных промежуточных продуктов такие вещества и материалы переносятся за пределы охраняемой зоны сотрудниками организации, воздушными массами атмосферы, жидкой средой, излучениями радиоактивных веществ.

Технические средства защиты информации - важный компонент в изучении обеспечения информационной безопасности, поэтому в будущем планируется разработка лабораторного стенда с использованием средств технической защиты информации.

На данный момент большинство имеющихся устройств блокирует именно материально-вещественный канал утечки информации. Это различные пульты контроля и управления С2000-КС, С2000-АСПТ, Pyronix Conqueror, DSC, охранно-пожарные контрольные панели РС 585RUS H и Vista, представленные на рисунке 1, бесконтактные считыватель С2000-Proxy и считыватель проксимити карт Proxy-3A (рисунок 2), точечные, звуковые и оптико-электронные пожарно-дымовые извещатели ИП 212-45, ИП 212-3СУ, ИП 114-5-А2 (рисунок 3).

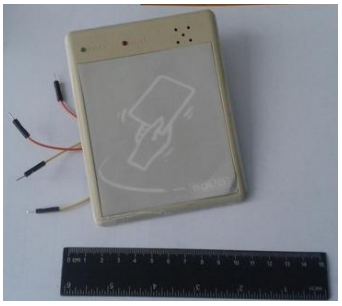


Рисунок 1- Бесконтактный считыватель С2000-Proxy

Рисунок 2- Пульты контроля и управлени Pyronix Conqueror,DSC

Рисунок 3- Оптико-электронный пожарно-дымовой извещатель ДИП-34А-01-02

Так же имеется оборудование, блокирующее перехват информации с акустических каналов (микрофон Шорох 1) и оптических каналов утечки информации (датчик движения PYRONIX COLT QUAD PI ПИК детектор).

Так же хотелось бы отметить, что планируемый стенд будет не только наглядным, но и практически полезным, т.к. все устройства будут взаимосвязаны и студент с помощью проводов сможет собирать различные варианты схемы. Такой стенд не только облегчит усваивание технической защиты информации, но и сделает обучение более интересным и занимательным.

Список литературы

1. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие/ Ю.Н.Загинайлов; Алт. гос. техн. ун-т И.И. Ползунова.- Барнаул: АлтГТУ, 2011.-252с.

2. Технические средства и методы защиты информации: учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

3. Классификация и краткая характеристика каналов утечки информации http://www.analitika.info/

РАЗРАБОТКА ЛАБОРАТОРНОГО КОМПЛЕКСА ДЛЯ ИЗУЧЕНИЯ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ НА БАЗЕ ТЕХНОЛОГИИ NFC

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

Система контроля и управления доступом (СКУД) — совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода»: двери, ворота, контрольно-пропускные пункты (КПП) [1]. Поэтому, для подготовки бакалавров в области защиты информации изучение СКУД является особо актуальным.

СКУД признаны одним из наиболее эффективных методов решения задач комплексной безопасности для объектов и поэтому на рынке представлено множество различных устройств, основанных на различных способах контроля и управления доступом.

В настоящее время быстрыми темпами развивается технология NFC, которая имеет один из способов применения, как система контроля управления доступом. NFC (Near Field Communnication) - технология беспроводной высокочастотной связи малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на расстоянии около 10 сантиметров. Эта технология — простое расширение стандарта бесконтактных карт (ISO 14443) [3].

Так как технология только получает свое развитие, то она еще не используется в учебном процессе и отсутствуют какие-либо обучающие материалы по данной тематике. Соответственно, выпускники направлений «Информационная безопасность» и «Информатика и вычислительная техника» могут столкнуться с проблемами при разработке данных устройств.

Поэтому целью данной работы является разработать комплекс по изучению СКУД на базе NFC. Для достижения данной цели, необходимо решить следующие задачи:

- Подобрать материально-техническое обеспечение.
- Проанализировать существующие СКУД.
- Разработать техническое обеспечение для лабораторного практикума.
- Разработать программное обеспечение для лабораторного практикума.

Для разработки данного стенда был использован Arduino Due совместно с модулем PN532 NFC RFID (рисунок 1). Был рассмотрен микроконтроллер ATmega, но данный

микроконтроллер был бы сложен в использовании – для его корректной работы с модулем пришлось бы изучить и написать несколько библиотек, тогда как данные библиотеки уже существуют для Arduino Due. Модуль PN532 NFC RFID имеет несколько функций, за счет этого с его помощью можно реализовать не только рассматриваемый лабораторный модуль, но и придумать на его основе какой-либо другой.

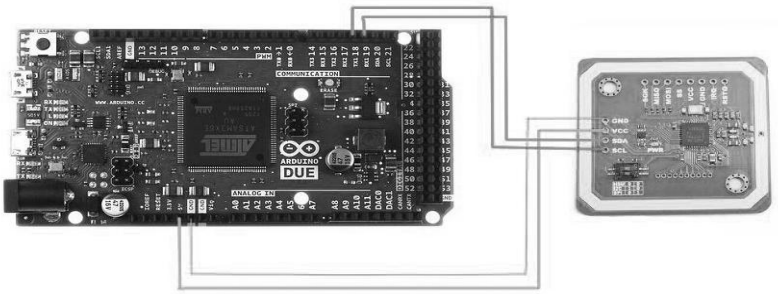


Рисунок 1 – Схема подключения модуля PN532 к Arduino Due

Принцип работы данного СКУД будет заключаться в следующем:

1. Человек подходит к точке доступа, где находится считыватель, запускает приложение на смартфоне (с поддержкой NFC) и подносит мобильное устройство к считывателю. При контакте отсылается уникальная последовательность битов, однозначно идентифицирующая данное устройство, а следовательно, и его владельца.

2. Считыватель обрабатывает полученный сигнал от смартфона и проверяет наличие такого идентификационного номера в базе данных. Если есть совпадение, то на мобильное устройство отсылается случайная последовательность цифр. В обратном случае в доступе отказывается.

3. Владелец мобильного устройства из полученного набора вводит цифры по заранее определенному алгоритму. Например, пользователь получает всегда набор из десяти цифр, по своему алгоритму, записанному в базе данных, ему нужно ввести третью, пятую, первую и седьмую цифры. Он выбирает именно эти цифры из полученной последовательности и вводит их на экране мобильного в обозначенном порядке. Затем полученный PIN-код отсылается на считыватель.

4. Считыватель обрабатывает полученный PIN-код, проверяет соответствие введенного PIN-кода и PIN-кода полученного в ходе применения алгоритма пользователя к полученной последовательности. При совпадении PIN-кодов человек допускается на режимный объект, в ином случае – запрещается.

Двухфакторная идентификация (ID, отсылаемый смартфоном, и PIN-код, вводимый человеком) предусматривает случай кражи или утери мобильного устройства – злоумышленнику не достаточно иметь смартфон, нужно знать алгоритм. Перехватить данные во время обмена довольно затруднительно за счет малого радиуса действия NFC, порядка 10-20 см.

Для управления данной системой контроля управления и доступа планируется написать приложение для телефона, программу для компьютера и составить базу данных.

При первом запуске приложение на телефон у пользователя будет запрошен ID, который будет выдаваться пользователю администратором и иметь определенную длину и сложность. Идентификационный номер будет записан в память приложения. Далее приложение при запуске будет отправлять персональный ID, не спрашивая для этого разрешение у пользователя. Пользователь сразу увидит полученную последовательность цифр и поле для ввода PIN-кода.

База данных будет включать в себя одного администратора и неограниченное количество пользователей. Для каждого пользователя будет отдельная запись, где будут уточнены его персональные данные (ФИО), персональный ID и алгоритм создания PIN-кода.

Также планируется использовать веб-сайт для управления базой данных и на данном ресурсе будет размещена краткая информация, как и в принципе о системах контроля

управления доступом, так и конкретно о данной СКУД. Регистрация на сайте будет закрытой, по приглашению администраторов, тогда как информационная часть будет открыта для любого пользователя сети интернет. На данном ресурсе зарегистрированный пользователь сможет посмотреть алгоритм создания PIN-кода, либо поменять его в случае необходимости.

Таким образом, студенты специальностей «Информационная вычислительная техника» и «Информационная безопасность» смогут на практике изучить технологию NFC и потом использовать ее в дальнейшем.

Список использованной литературы:

1. Система контроля и управления доступом /[Электронный ресурс] : - Режим доступа : - https://ru.wikipedia.org, – Загл. с экрана

2. Система контроля управления доступом на базе технологии NFC/ Николаева В.К., Борисов А.П. // Новые задачи технических наук и пути их решения, г.Уфа. – 2015. – с. 72-74.

3. Near Field Communication /[Электронный ресурс] : - Режим доступа : - https://ru.wikipedia.org, – Загл. с экрана

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ВИДЕО ОХРАНЫ ДЛЯ ПОДГОТОВКИ БАКАЛАВРОВ ПО НАПРАВЛЕНИЮ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

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

Система видеонаблюдения — это программно-аппаратный комплекс (видеокамеры, объективы, мониторы, регистраторы и др. оборудование), предназначенный для организации видеоконтроля как на локальных, так и на территориально-распределенных объектах.

Видеонаблюдение уже давно закрепилось компонентом технической защиты предприятия в рамках комплексной защиты объекта информатизации, а иногда, основным или единственным средством обеспечения безопасности на множестве объектов. Это связано с его высокой эффективностью при защите и охране территории, имущества и обеспечения собственной безопасности.

Видеонаблюдение решает вопрос безопасности контролируемого объекта на самом высоком уровне. Современные системы видеонаблюдения успешно справляются со следующими задачами:

- позволяют контролировать ситуацию в нескольких точках одновременно;
- служат источником дополнительной информации о работоспособности предприятия (контроль за персоналом, перемещение материальных ценностей и т.п.).
- предоставляют возможность увидеть один и тот же объект в различных ракурсах;
- предоставляют возможность создания информационных архивов, необходимых для видеоаналитики и видеомониторинга;
- позволяют предотвратить утечку конфиденциальной информации;
- препятствуют проникновению на охраняемую территорию посторонних лиц.

Именно эти задачи определяют необходимость подготовки специалистов в области видеонаблюдения.

Компания Axis, мировой лидер рынка систем сетевого видеонаблюдения, поддержала инициативу по подготовке специалистов в сфере безопасности, предложенную российским производителем систем безопасности PERCo, предоставив возможность использовать свое оборудование в лабораториях вузов, участвующих в программе. Ряд ведущих вузов уже активно работает с PERCo, а программа, предложенная компанией, успешно реализуется с ноября 2012 года.

На данный момент камерами Axis оборудуют лаборатории российских вузов, таких как: МГТУ им. Баумана, Москва; Университет телекоммуникаций им. Бонч-Бруевича, Санкт-

Петербург; Московский Университет МВД; Воронежский Институт МВД; Университет Государственной Пожарной Службы, Санкт-Петербург; Уральский Федеральный Университет, Екатеринбург; Новосибирский ГТУ; Казахский Национальный Университет, Алмата; Белорусский Государственный Университет Информатики и Электроники, Минск.

Система видеонаблюдения и видеорегистрации позволяет вести круглосуточное визуальное наблюдение как за периметром вокруг объекта, так и за обстановкой внутри него с возможностью записи интересующей информации на жесткий диск центрального компьютера или специализированный видеомагнитофон. Кроме этого, такие системы дают возможность определять местоположение любого сотрудника или его перемещения внутри здания.

Системы видеонаблюдения очень хорошо помогают защитить конфиденциальную информацию, но многие компании не могут позволить сразу взять готовые комплексные решения в силу высокой стоимости. Например, компания Nstor предлагает IP-видеонаблюдение в рамках комплексного решения для небольших организаций на пять IP-видеокамер. Такая версия подходит для малых офисов, магазинов и павильонов. Стоимость комплекта из пяти видеокамер составляет 69 750 рублей.

Во избежание больших затрат, предлагается создать учебно-методический комплекс систем видеонаблюдения, используя следующее оборудование: компактный четырехканальный видеорегистратор с одним каналом аудио; IP-видеорегистратор; линия Effio 4x25 Hybrid IP; жёсткий диск SATA-III 1Tb; видеокамера цветная купольная INNOVI; антивандальная IP-камера; уличная IP-камера; купольная IP-камера. С помощью данного оборудования студенты будут не только разобраться со способами установки и настройки систем видеонаблюдения, но и научатся объединять различные существующие системы на предприятии и создавать готовые решения.

Целями создания учебно-методического комплекса для изучения систем видеонаблюдения является:

- Подготовка учебно-методического обеспечения, формирование учебно-методического комплекса по дисциплине «Технические средства защиты информации»;
- Оснащение учебного процесса учебно-методическими, справочными и другими материалами, улучшающими качество подготовки специалистов;
- Создание инструмента планирования и организации работ по совершенствованию учебно-методической базы кафедры защиты информации;
- Обеспечение стопроцентной оснащенности учебного процесса учебно-методическими комплексами.
- Освоение знаний и закрепления их на практике, способы подключения и использования средств для видеонаблюдения.

Анализ структуры учебно-методического комплекса:

Учебно-методический комплекс (УМК) - это программно-аппаратный продукт, обеспечивающий возможность студенту самостоятельно или с помощью преподавателя освоить учебный курс или его раздел, объединяющий в себе свойства учебника, справочника, задачника. Использование электронных учебно-методических комплексов позволяет сделать процесс обучения студента более эффективным, дающим новые современные возможности в освоении материала и получении профессиональных знаний и навыков.

УМК состоит из двух учебных модулей (УМ), включающих в себя аппаратную и программную часть.

Логика выделения учебных модулей соответствует логике преподавания учебного курса и разрабатываются с учетом временных затрат студента на проработку и усвоение раздела.

Учебно-методические материалы, включаемые в УМК, должны отражать современный уровень развития науки, содержать использование современных методов и технических средств интенсификации учебного процесса, позволяющих студентам глубоко осваивать учебный материал и получать навыки по его использованию на практике.

Список использованной литературы:

1. Информационная безопасность и видеонаблюдение [Электронный ресурс]. – Режим доступа: http://www.ohrana-kremlin.ru/uslugi-i-czenyi/informaczionnaya-bezopasnost-i-videonablyudenie.html, свободный (дата использования 12.03.15)

2. Системы безопасности – информация о видеонаблюдении, контроле доступа [Электронный ресурс]. – Режим доступа: http://www.secuteck.ru/main.php, свободный (дата использования 10.03.15)

3. Видеонаблюдение в системах охраны периметра видеонаблюдение [Электронный ресурс]. – Режим доступа: http://www.video-group.ru/videonabliudenie-v-sistemach-ochrani-perimetra, свободный (дата использования 17.03.15)

4. Пескин А.Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации. — "Горячая линия-Телеком", 2013.

СПОСОБЫ ВТОРЖЕНИЯ В КОРПОРАТИВНУЮ СЕТЬ ЧЕРЕЗ СРЕДСТВА БЕСПРОВОДНОЙ СВЯЗИ

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

На сегодняшний день невозможно уже представить существование компаний без использования в своей инфраструктуре локальной сети для реализации своей деятельности. Информация, обрабатываемая внутри сети, может иметь огромное значение для компании, и в случае кражи информации или отказа сети довольно сложно оценить нанесённый ущерб.

Многие компании используют средства беспроводной связи (в частности wi-fi), которые могут представлять реальную угрозу как информационному обмену так и функционированию всей технологической системы поддерживающей деятельность организации. Особое внимание заслуживает угрозы на примере уязвимого роутера, который функционирует во внутреннем периметре сети. Из многообразия типовых угроз можно выделить три ситуации:

1) Ошибки конфигурации оборудования:

- web-интерфейс, видимый во внешнем периметре сети, с паролем и именем пользователя по умолчанию;
- использование ненадёжных паролей или алгоритмов шифрования (например: wep) для беспроводной сети;
- несвоевременное обновление прошивки беспроводного устройства;
- отсутствие фильтрации клиентов по mac адресам и разделения гостевого и внутреннего трафика;

2) Ошибки допущенные создателями сетевого оборудования:

- возможность использования эксплойтов;

3) Уязвимости, внесённые в базовую конфигурацию роутера злоумышленниками намеренно:

- выставленные в настройках роутера по умолчанию dns-сервера, возвращающие заведомо ложные адреса интернет ресурсов;
- отправка на удалённый сервер параметров сети для удалённого доступа к устройству и последующему проникновению в сеть.

Подробное внимание, в качестве объекта исследования, уделено нестандартным способам вторжения в корпоративную сеть, которые стали целью работы.

Чаще всего роутер стоит между внешним периметром сети и внутренним, т.е между интернетом и внутренней сетью, из-за этого задача существенно упрощается.

Так как базовые возможности обычного роутера ограничены, возможно установить на роутер альтернативную прошивку с расширенным функционалом DD-WRT настройки. В качестве эксперимента было сконфигурировано устройство таким образом, чтобы его

параметры нельзя было изменить пользователю из web интерфейса, а роутер при этом отправлял на выделенный сервер информацию о своём ip адресе в зашифрованном формате. Настройки роутера позволяют осуществить возможность отправки по беспроводному каналу связи, чтобы в дальнейшем можно было подключиться удалённо к роутеру по принципу VPN шлюза, а затем проникнуть во внутренний сегмент сети для проведения несанкционированных действий. Данная процедура занимает не так уж много времени, таким образом, подключив такой роутер, к сети нам будет достаточно времени, чтобы закрепиться в ней. Если развивать эту идею дальше, то существует возможность использовать не только wi-fi роутер но и другое сетевое оборудование, которое можно перепрошить.

Данный способ проникновения используется на сегодняшний день довольно часто, например, при ведении информационных войн между конкурирующими компаниями. На рынке также есть подобные устройства со схожим функционалом, однако, к сожалению, ценовая доступность оставляет желать лучшего. На рисунке 1 приведена простейшая схема реализации роутера-закладки.

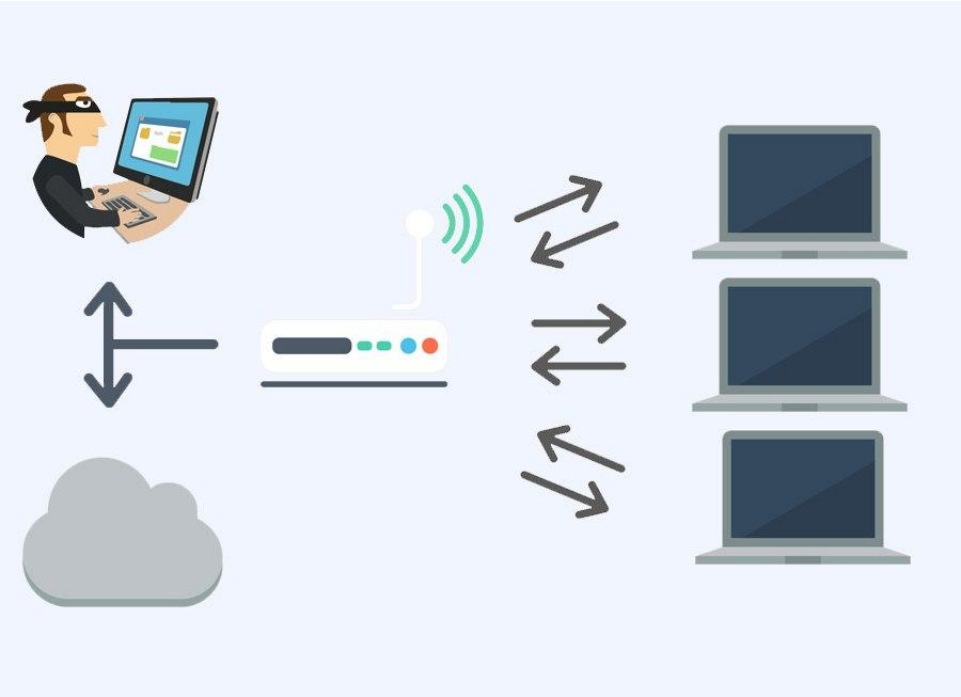


Рисунок 1 Схема реализации "роутер-закладка"

Другой сценарий развития – установка wi-fi точки доступа, в места, где сигнал, создаваемый штатным оборудованием наиболее низкий или отсутствует, с тем же именем что и атакуемая (см. рис. 2). За счет перенаправления всех устройств подключившихся к ресурсу происходит заражение клиентов вирусом эксплуатировщиком написанным конкретно для модели функционирующей на постоянной основе. При подключении заражённой машины к корпоративной wi-fi сети происходит выполнение вредоносного сценария, изменяющего настройки оборудования корпоративной сети согласно сценария злоумышленника.

Рисунок 2. Схема реализации "Заражённый клиент"

Из анализа различных ситуаций проникновения в корпоративную сеть можно сделать вывод о том, что данная проблема актуальна сегодня и требует внимания при выборе производителя оборудования, а также корректной настройки и контроле со стороны потребителей.

Библиографический список.

1. Камайкин А.Г., Осипов И.Е., Шумарин О.Е. Корпоративные сети Wi-Fi / ТЕХНОЛОГИИ И СРЕДСТВА СВЯЗИ No 1 февраль–март, 2006г: [Электронный ресурс]. – Режим доступа: http://www.dateline.ru/resources/Публикации/corporate-wifi-networks-osipov.pdf

2. DD-WRT Official forum[Электронный ресурс]. – Режим доступа: http://www.ddwrt.com/

ПОДГОТОВКА ИСХОДНЫХ ДАННЫХ ПО АТТЕСТАЦИИ ЗАЩИЩАЕМОГО ПОМЕЩЕНИЯ

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

С развитием информационных технологий возрастает важность обеспечения защиты информации. В организации на ряду с использованием автоматизированных систем в обработке информации, речевая информация представляет собой коммерческую или иную ценность и нуждается в защите. Обеспечение защиты возможно, если процесс обработки этой информации не выходит за пределы защищаемого помещения (ЗП), предназначенного специально для проведения мероприятий с обработкой речевых сведений. Такое помещение характеризуется выполнением требований по безопасности информации (определено в [6]), подтвержденных аттестатом соответствия. Получение аттестата представляет собой установленную процедуру, одним из этапов которой является подготовка и предоставление исходных данных по помещению в уполномоченный орган по аттестации.

Объектом исследования является ЗП, подлежащее аттестации по требованиям безопасности.

Предмет исследования представляет собой процесс подготовки исходных данных по аттестуемому помещению.

Целью работы является определение порядка подготовки исходных по ЗП. Исходя из цели поставлены следующие задачи:

- анализ нормативно-правовых документов;
- определение общих положений аттестации;
- определение сторон, участвующих в аттестации и их обязанностей;
- определение процесса и правил подготовки исходных данных по ЗП.

Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации [4]. В рамках работы объектом информатизации является ЗП (понятие ЗП определено [5]).

Аттестация ЗП проводится до мероприятий с использованием защищаемой информации, и носит добровольный характер (в отличие от сведений, составляющих государственную тайну [3]), так как предполагаемая речевая информация не содержит сведений, составляющих государственную тайну. В аттестации участвуют заказчик, орган по аттестации и испытательные центры.

Для проведения аттестационных мероприятий органу по аттестации необходимо изучить объект. Для этого аттестующему органу заказчик предоставляет заявку на проведение аттестации и приложенную к ней информацию по ЗП. Такая информация в процессе её подготовки и оформления должна отвечать следующим требованиям и правилам, а именно:

- соответствовать нормативно – правовым документам;
- являться достаточной;
- быть понятной и обладать возможностью анализа органом по аттестации.

Соответствие нормативно-правовым документам предполагает, что получение, комплектование и оформление исходных данных основывается на перечне определенных вопросов. Полный перечень вопросов определен в положении по аттестации [4] и включает в себя организационные, правовые и технические аспекты обеспечения безопасности информации.

Достаточность подготовленных данных по ЗП подразумевает, что они в полной мере описывают все аспекты обработки информации в ЗП, и обеспечения её безопасности как в ЗП, так и в пределах контролируемой зоны. Данные также должны наиболее точно и полно содержать в себе сведения об аттестуемом объекте и о самой защищаемой информации [2]. Таким образом достаточность предполагает полное описание ЗП и всех сторон выполняемых им функций.

Раз подготовленная заказчиком информация предназначена для органа по аттестации, то она должна следовать правилам, обеспечивающим ее успешную обработку. Данные о ЗП необходимо предоставлять в понятном, структурированном, просто изложенном и грамотно оформленном виде.

Соблюдение требований и правил подготовки исходных данные актуально как для заказчика, так и для органа по аттестации. Это объясняется следующим:

1) Если заказчик, обратившийся в орган по аттестации, предоставил им исходные данные по ЗП, которые были собраны, подготовлены и оформлены в соответствии с вышеперечисленными требованиями, то органу по аттестации нет необходимости выполнять дополнительные действия, направленные на дальнейшее ознакомление с объектом, так как вся необходимая информация им уже получена. В результате
   - снижаются затраты заказчика на проведение аттестации;
   - уменьшается время, необходимое на проведение всех мероприятий аттестации.
2) Для аттестационного органа проще и быстрее составить и согласовать схему проведения аттестации и программу аттестационных испытаний, так как:
   - имеется исчерпывающая информация об объекте;
   - форма представления данных позволяет обрабатывать и анализировать их быстрее и качественнее.

В настоящее время определенные норма и форма представления исходных данных не установлены нормативно – правовыми документами. Имеется лишь перечень вопросов, на основании которых такие данные должны быть подготовлены и предоставлены. Для некоторых из них возможно составить типовую форму представления, позволяющую структурировать и оформить собранную информацию. Поэтому имеет смысл целью выпускной работы взять разработку типовых документов для подготовки и оформления исходных данных по аттестации ЗП.

На данный момент на основании нормативно-правовых документов [1-6] был определен и сформирован состав исходных данных, подлежащих дальнейшему исследованию. На основании этих данных планируется разработать типовые документы для их оформления, сформированные в соответствии с принципами построения документов.

Список источников:

1) Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации

2) Указ президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 года № 188.

3) Закон РФ от 21.07.1993 №5485-1 «О государственной тайне».

4) Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.

5) Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Москва 2001.

6) ГОСТ Р 50.1.053- 2005 «Информационные технологии, основные термины и определения в области технической защиты информации».

ПЕРСОНАЛЬНЫЕ ДАННЫЕ НА ПРЕДПРИЯТИЯХ МАЛОГО БИЗНЕСА

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

С развитием демократии открывается очень много новых предприятий малого и среднего бизнеса, таких как ИП, ООО и прочих. Такие предприятия дают возможность многим людям работать и зарабатывать. Так как среди работников об анонимности не может идти и речи, то необходимо позаботиться о том, чтобы не пострадала частная жизнь работников. В современном демократическом обществе права человека и, в частности, право на неприкосновенность частной жизни имеют первостепенное значение. Особым институтом права на неприкосновенность частной жизни в условиях автоматизации и развития новых информационных технологий является институт персональных данных.

Исходя из 152 ФЗ «О персональных данных», под понятие «Персональные данные» попадают такие данные о человеке, как фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, информация о доходах и многое другое [1]. Большинство этих данных о работниках в том или ином виде имеют место быть на предприятии. Кроме того, в настоящее время на предприятиях по оказанию услуг при заказе тех или иных услуг создается индивидуальная заявка, которая, как правило, содержит те или иные персональные данные, например, ФИО, адрес, телефон и прочее. То есть система защиты персональных данных нужна таким организациям не меньше чем остальным.

В условиях развития информационных технологий необходимо обеспечивать защиту персональных данных в информационных системах персональных данных. Требования же по защите определены в следующих документах:

—152 ФЗ «О персональных данных».

—Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите ПДн при их обработке в ИСПДн».

—Приказ ФСТЭК России N 21 от 11.02.2013г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн».

Данные требования предусматривают, в том числе:

—идентификация и аутентификация субъектов доступа и объектов доступа;

—управление доступом субъектов доступа к объектам доступа;

—ограничение программной среды;

—защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

—регистрация событий безопасности;

—антивирусная защита;

—обнаружение (предотвращение) вторжений;

—контроль (анализ) защищенности персональных данных;

—обеспечение целостности информационной системы и персональных данных;

—обеспечение доступности персональных данных;

—защита среды виртуализации;

—защита технических средств;

—защита информационной системы, ее средств, систем связи и передачи данных;

—выявление инцидентов [2].

Идентификация и аутентификация субъектов доступа, управление доступом субъектов, а так же регистрация событий безопасности для защиты персональных данных может предусматривать только настройку средств защиты, встроенных в ОС на АРМ сотрудников. Так же, эти требования могут быть реализованы сторонними программами, такими как SecretNet 7 совместно с ПАК «Соболь». Антивирусная защита должна обеспечиваться сертифицированными антивирусными средствами, например антивирусом «Kaspersky».

Если сеть организации взаимодействует с сетями общего пользования или же в организации предоставлена в общее пользование беспроводная сеть (которая может использоваться и самими работниками) необходимо межсетевое экранирование. Причем, каждое АРМ сотрудника, входящее в сеть организации должно содержать в своем составе индивидуальные межсетевой экран. При наличии администратора безопасности можно использовать межсетевые экраны с централизованным управлением, такие как VipNet.

Остальные требования должны выполняться администратором безопасности, а так же быть учтены в таких документах как политика безопасности организации, инструкции операторов, обрабатывающих персональные данные, инструкции администраторов безопасности и прочие.

Литература:

1. Общие понятия безопасности персональных данных [Электронный ресурс]. Режим доступа: http://www.intuit.ru/studies/courses/680/536/lecture/12090?page=2

2. Приказ ФСТЭК России N 21 от 11.02.2013г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн».

ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ПОРТАТИВНЫХ УСТРОЙСТВ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

Современный процесс защиты информационного пространства уже давно превратился в искусство противостояния обладателя объекта с одной стороны и «злоумышленника», желающего владеть ценностями, с другой стороны с целью получения материальной или моральной выгоды. Всяческие попытки совершенствования технических и программных средств с целью совершенствования системы безопасности порой приводит к появлению новых уязвимостей, дающих возможность для реализации угрозы информационной безопасности.

Для построения информационных систем передачи данных, в том числе с применением мобильных устройств, необходимо выполнение требований по защите информации, а также разрешение на эксплуатацию систем от регуляторов, таких как: ФСТЭК, ФСБ, Роскомнадзор. Для уменьшения риска возникновения реализации угроз информационной безопасности, при построении комплексной системы обеспечения безопасности, необходимо разработать модель нарушителя.

В настоящее время при построении модели нарушителя возможно применение методики определения актуальных угроз ПДн при их обработке в ИСПДн ФСТЭК и методических рекомендаций по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации ФСБ.

Предполагаем: информационная система – ИСПДн сотрудников, актуальные угрозы – угрозы 3-го типа, объем – менее 100000 субъектов ПДн.

В соответствии с Постановлением Правительства РФ №1119 от 1 ноября 2012 года «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» уровень защищенности соответствует УЗ 4.

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

- Организация режима обеспечения безопасности помещений, в которых размещена информационная система.
- Обеспечение сохранности носителей ПДн.
- Утверждение руководителем перечня лиц, доступ которых к ПДн, необходим для выполнения ими служебных (трудовых) обязанностей.
- Использование сертифицированных средств защиты информации [1].

В таблице 1 представлен общий перечень групп угроз, которые можно использовать как исходные данные при построении модели нарушителя, и которые соответственно необходимо нейтрализовать [2].

Таблица 1 – Общий перечень угроз

№ п/п	Угрозы безопасности информации
1	Угрозы утечки информации по техническим каналам
2	Угрозы НСД к информации
3	Угрозы, реализуемые в ходе загрузки операционной системы
4	Угрозы, реализуемые после загрузки операционной системы
5	Угрозы, реализуемые при запуске прикладных программ
6	Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия
7	Угрозы, реализуемые через халатность сотрудников

Показатели исходной защищенности представлены в таблице 2.

Таблица 2 – Показатели исходной защищенности ИСПДн

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	высокий	средний	низкий
1. По территориальному размещению			
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)	-	-	+
2. По наличию соединения с сетями общего пользования			
ИСПДн, имеющая одноточечный выход в сеть общего пользования	-	+	-
3. По встроенным (легальным) операциям с записями баз персональных данных			
чтение, поиск	+	-	-
4. По разграничению доступа к персональным данным			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн	-	+	-
5. По наличию соединений с другими базами ПДн иных ИСПДн			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации - владельцу данной ИСПДн	+	-	-
6. По уровню обобщения (обезличивания) ПДн			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	-	+	-
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки			
ИСПДн, предоставляющая часть ПДн	-	+	-

Актуальность угрозы определяется параметрами: опасность угрозы и возможность реализации угрозы [3].

В процессе определения актуальных угроз выявлено относительно «Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия»:

1. Угроза анализа сетевого трафика: возможность реализации - высокая; опасность – средняя; актуальность – актуальная.
2. Угроза сканирования сети: возможность реализации – высокая; опасность – низкая; актуальность – актуальная.
3. Угроза выявления пароля: возможность реализации – низкая; опасность – высокая; актуальность – актуальная.
4. Угроза подмены доверенного объекта сети: возможность реализации – средняя; опасность – высокая; актуальность – актуальная.
5. Угроза навязывания ложного маршрута сети: возможность реализации – средняя; опасность – высокая; актуальность – актуальная.
6. Угроза внедрения ложного объекта сети: возможность реализации – средняя; опасность – высокая; актуальность – актуальная.
7. Угроза «Отказ в обслуживании»: возможность реализации – средняя; опасность – средняя; актуальность – актуальная.
8. Угроза удаленного запуска приложений: возможность реализации – средняя; опасность – низкая; актуальность – неактуальная.
9. Угроза внедрения по сети вредоносных программ: возможность реализации – низкая; опасность – низкая; актуальность – неактуальная.

Физические лица, имеющие доступ к техническим и программным средствам информационной системы, разделяются на 2 категории:

Категория I – лица, не имеющие права доступа в КЗ информационной системы.

Категория II – лица, имеющие право постоянного или разового доступа в КЗ информационной системы [4].

Разделение представлено в таблице 3.

Таблица 3 - Категорирование нарушителей

Категория I	Категория II
Разведывательные службы	Администратор безопасности
Интернет-провайдер	Персонал работающий с ПДн
Разработчик криптосредства	Системный администратор
Поставщики оборудования	Руководство

Разделение нарушителей на внутренних (только Категория II) и внешних (как Категория I, так и Категория II).

Таблица 4 – Разделение нарушителей

Внутренний нарушитель	Внешний нарушитель
Руководство	Поставщики оборудования
Администратор безопасности	Разработчик криптосредства
Системный администратор	Разведывательные службы
Персонал работающий с ПДн	Интернет-провайдер

Привилегированные пользователи информационной системы: Администратор безопасности и Системный администратор.

Из числа потенциальных нарушителей исключаются лица, разрабатывающие криптосредства и разведывательные службы, так как средства проходят обязательную сертификацию, а компания-разработчик получает лицензию на осуществление криптографических видов деятельности. Обрабатываемая информация не несет критичного характера для разведывательных служб.

Поставщики оборудования и уволенный администратор безопасности могут быть в сговоре. Дополнительные возможности, которые появляются у этих нарушителей: знание «backdoor-ов», топологии сети и используемого прикладного программного обеспечения, дополнительные финансовые возможности на изучение и проведения экспериментов.

Основные каналы атак:

1. Каналы связи.

Возможны атаки путем подмены точки доступа беспроводной локальной сети, атаки типа «человек посередине», а также пассивные атаки: сканирование сети и анализ сетевого трафика.

2. Штатные средства.

Увеличение привилегий пользователя до root-а, путем перепрошивки устройства.

Вспомогательные каналы атак:

1. Каналы непосредственного доступа к объекту атаки.

Возможно при использовании специальных средств съема информации, а также при непосредственной близости с объектом атаки. Использование атаки типа «социальная инженерия». Халатность сотрудников.

2. Мобильные устройства, выведенные из употребления.

При смене мобильного устройства не произошла его утилизация, а также стирание информации ограниченного доступа.

3. Технические каналы утечки.

4. Канал утечки за счет электронных устройств негласного получения информации.

При ремонте устройства у организаций, предоставляющих ремонт мобильных устройств, возможна установка «закладок» различного типа.

В таблице 5 представлены типы нарушителей, полученные в ходе проведенных исследований.

Таблица 5 – Типы нарушителя

Нарушитель	Предположения о сведениях	Предположения об средствах	Тип нарушителя
Руководство	Н2	Н3	Н3
Интернет-провайдер	Н3	Н1	Н3
Администратор безопасности	Н3	Н3	Н3
Системный администратор	Н3	Н3	Н3
Внешний нарушитель	Н1	Н1	Н1
Поставщик оборудования	Н2	Н3	Н3
Персонал работающий с ПДн	Н2	Н2	Н2

На основании модели типов нарушителя имеем: уровень криптографический защиты – КС3, уровень специальной защиты каналов ПЭМИМ – КС, уровень защиты от НСД – АК3.

В соответствии с приказом ФСБ № 378 от 10.07.2014 г. состав и содержание организационных и технических мер, необходимых для выполнения установленных Правительством РФ требований к защите ПДн для УЗ 4, необходимо выполнение следующих требований [5]:

1. Организация пропускного режима в помещения, в которых размещена критически важная информация (СКЗИ, носители ключевой, аутентифицирующей, парольной информации), препятствующего нахождению в них лиц, не имеющих права доступа.
2. Обеспечение сохранности носителей.
3. Утвержденный руководителем документ, определяющий перечень лиц, которым необходим доступ для выполнения ими своих служебных обязанностей.
4. Использование сертифицированных СЗИ, когда применение таких средств необходимо для нейтрализации актуальных угроз [6].

Библиографический список

1. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 1 ноября 2012 г., № 1119. – М., 2012. – 4 с.
2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г. – ФСТЭК., 2008. – 69 с.
3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Утверждена заместителем директора ФСТЭК России 14 февраля 2008 г. – ФСТЭК., 2008. – 10 с.
4. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации: Утверждены руководством 8 Центра ФСБ России от 21 февраля 2008 г., № 149/54-144. – ФСБ., 2008. – 20 с.
5. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности: Приказ ФСБ России от 10 июля 2014 г., № 378. – М., 2014. – 1 с.
6. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации

требований к защите персональных данных для каждого из уровней защищенности: Приложение к приказу ФСБ России от 10 июля 2014 г., № 378. – М., 2014. – 6 с.

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО СРЕДСТВА ДЛЯ СОПРЯЖЕНИЯ ОХРАННО-ПОЖАРНОГО ПРИБОРА С СОТОВЫМ ТЕЛЕФОНОМ

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

В настоящее время наблюдается повсеместное проникновение информационных технологий практически во все сферы жизни человека. Исключением не становятся и общеобразовательные учреждения, где, помимо использования информационных технологий в процессе обучения, с их помощью ведётся и обработка персональных данных сотрудников, учеников и их родителей, необходимость защиты которых установлена требованиями Федеральных законов РФ.

Помимо персональных данных сотрудников обработке подлежат также персональные данные учеников и их родителей, следовательно, информационная система гимназии является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Для общеобразовательного учреждения актуальны угрозы 3-го типа, т.к. для него актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

В гимназии необходимо обеспечивать 4-й уровень защищенности персональных данных.

Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Согласно приказа ФСТЭК от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» для обеспечения 4 уровня защищенности персональных данных применяются:

– средства вычислительной техники не ниже 6 класса;

– системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;

– межсетевые экраны 5 класса.

Также при обеспечении безопасности информации важно предусмотреть полный комплекс мер для ее защиты. Особое внимание стоит уделять защите помещений, где проводятся работы, связанные с обработкой защищаемой информации, или же осуществляется ее хранение, в том числе защите с использованием средств охранно-пожарной сигнализации.

Охранно-пожарная сигнализация представляет собой интегрированный комплекс систем пожарной и охранной сигнализации, объединяющий функции защиты от проникновения на охраняемый объект и функции раннего обнаружения очагов возгорания и автоматического пожаротушения.

Разработанное программно-аппаратное средство служит дополнением к прибору приемно-контрольному охранно-пожарному "Кварц" – законченному электронному устройству, предназначенному для опроса состояний подключенных к нему охранных шлейфов, снабженных охранными извещателями, анализа этих состояний и формирования соответствующих сигналов путем размыкания контактов выходных реле. Оно и позволяет автоматически передавать сигнал тревоги по сотовому телефону. Данное средство предназначено для использования в частности в МБОУ «Гимназия №74», предметом деятельности которой является образовательная деятельность, включающая в себя осуществление образовательного процесса через реализацию образовательных программ и обеспечение содержания и воспитания обучающихся.

Приставка имеет возможность не только звонить в случае тревоги по номеру, заранее занесённому в память телефона, но и принимать входящие звонки, позволяя в любое время дистанционно следить за состоянием охраняемого объекта. Она автоматически распознаёт, находится ли ППКОП в режиме охраны, контролируя шлейф (или цепь датчиков) на размыкание и замыкание, а также следит за исправностью и состоянием сотового телефона. Этого не могут обеспечить простые сигнализаторы.

При необходимости приставку можно использовать как автономное охранное устройство, не подключая к ППКОП. С ней сможет работать практически любой сотовый телефон.

При приёме входящего звонка автоматический отбой не предусмотрен, его должен дать сам звонящий.

Основой приставки является восьмивыводной микроконтроллер PIC12F683 с программой, анализирующей состояние реле ПЦН1 ППКОП и управляющей сотовым телефоном. После включения питания программа сначала проверяет, находится ли ППКОП в режиме "Охрана".

Сигнал состояния телефона снимается с его кнопки "Вызов". Если телефон выключен, программа включает его, имитируя 3-секундное нажатие на кнопку "Вкл./Выкл." телефона. Затем программа проверяет, включился ли телефон. Если нет, делается новая попытка его включить, всего до пяти попыток. Убедившись, что телефон включён, программа отменяет приём всех поступивших входящих вызовов и сообщений SMS. Затем выполняется набор номера, заранее заложенного в память телефона. По истечении 50 секунд приставка переходит в режим "Охрана".

В этом режиме периодически проверяется, поступает ли на приставку напряжение 5 В от внешнего сетевого источника питания.

Далее программа проверяет, не поступает ли в данный момент на телефон входящий вызов.

Пока ППКОП остаётся в режиме "Охрана", не подавая сигнала тревоги, проверки наличия напряжения питания и входящего вызова повторяются циклически.

Обнаружив переход ППКОП в режим "Тревога", начинается выполнение исходящих вызовов. Каждый длится 30...40 секунд в зависимости от расхода времени на соединение. Затем программа даёт отбой и после 15...20 секунд вызов повторяется. Количество звонков – 5.

Если ППКОП в системе охраны отсутствует, проводной шлейф или замкнутые в отсутствие тревоги контакты охранного датчика подключают непосредственно к приставке. Телефон позвонит по заданному номеру при обрыве шлейфа или размыкании контактов датчика.

Если после выполнения пяти звонков целостность шлейфа будет восстановлена, приставка автоматически возвратится в дежурный режим.

Таким образом, был определен класс защищенности персональных данных и разработано программно-аппаратное средство, позволяющее автоматически передавать сигнал тревоги по сотовому телефону в случае обнаружения нарушения безопасности здания: несанкционированного проникновения, возгорания и т.д.

Список использованных источников:

1. Прибор приемно-контрольный охранно-пожарный «Кварц», вариант 1, руководство по эксплуатации, САПО.425513.060-01РЭ;

2. А. Ковтун. Сопряжение охранно-пожарного прибора с сотовым телефоном. Радио, 2012, №10, 42-43;

3. Официальные сведения о гимназии [Электронный ресурс] – http://g74.ucoz.ru/index/oficialno/0-154/.

4. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 [Электронный ресурс]- http://www.ispdn.info/laws/postanovlenie-pravitelstva-rf-ot-1-noyabrya-2012-g-n-1119/;

5. СЗПДн. Анализ. Проекты новых ПП РФ по защите ПДн 2;

6. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 [Электронный ресурс]- http://fstec.ru/normativnye-pravovye-akty-tzi/110-deyatelnost/tekushchaya/tekhnicheskaya-zashchita-informatsii/normativnye-pravovye-akty/prikazy/692-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21

РАЗРАБОТКА УЧЕБНОЙ ПРОГРАММЫ ДЛЯ ИНТЕРПРЕТАЦИИ КОНСТРУКЦИЙ МОДЕЛЬНОГО ЯЗЫКА С РАЗЛИЧНЫМИ СЕМАНТИЧЕСКИМИ ТИПАМИ ДАННЫХ

Тарасенко А.Н. – студент, Сучкова Л.И. – к.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В настоящее время существует множество языков программирования, как компилируемых, так и интерпретируемых. Существование этих языков было бы невозможно без наличия отвечающих современным требованиям средств трансляции. В связи с этим программисты все чаще сталкиваются с потребностью в знании теории языков программирования и построения компиляторов.

На начальном этапе изучения теории формальных языков и компиляторов у студентов часто возникают проблемы связанные с построением таблиц компилятора. Существует два варианта построения данных таблиц. Первый вариант построения - в виде массива (статическая), реализация которого достаточно проста. Подходит для небольших программ и языков вследствие чего, мало востребована. Другим же вариантом является представление таблиц в виде дерева (динамическая). Наиболее используемый вид таблиц, сокращающий время поиска элементов и не ограниченный по размеру. Сложность реализации гораздо выше, чем у массивов.

Студенту не понятна логика занесения в дерево различных данных, и дальнейшая их обработка. В связи с этим возникла потребность в программе, которая бы позволила визуализировать процесс построения дерева и отслеживать вызываемые для вставки и поиска функции по ходу интерпретации, введенного студентом кода.

Целью данной работы является разработка программного продукта, визуализирующего процесс построения семантических таблиц компилятора для структурного языка, не требующего от студентов особых навыков, и показывающего полную картину работы по

созданию дерева разбора для заданного кода. Сегодня, на рынке программного обеспечения нет универсального и гибкого продукта для реализации данных задач.

Для создания данного продукта был разработан учебный модельный язык, модули, выполняющие лексический, синтаксический и семантический анализ. Самой важной частью программы является модуль визуализации, работающий в комплексе с модулем интерпретатора и транслятора.

Модель языка содержит целые, дробные и символьные типы данных, выполняет арифметические операции (+, - , *, /, ++, --), сравнения (>, <, !=, ==, >=, <=) и логические (&&, ||). Операндами выступают простые переменные, массивы, константы и структуры. Включает операторы присваивания, if, for, while, do while. Для описания последовательности команд разработана формальная грамматика, описывающая язык модели в форме Бэкуса-Наура. Данный комплекс средств модельного языка в полной мере позволяет увидеть процесс построения наиболее значимых участков дерева разбора.

Архитектура программного продукта

После анализа предметной области и постановки задач, была спроектирована архитектура программного продукта, полностью удовлетворяющая всем поставленным требованиям (рисунок 1).

Для обработки текста программы был разработан лексический анализатор, осуществляющий проверку правильности таких действий как присваивание переменных или объявление структур, построения условных и иных операторов. Были разработаны блоки синтаксического, семантического анализа и интерпретатор. Модуль построения и вывода дерева по исходному коду, работает через лексический анализатор, обрабатывая каждую лексему и принимая решение построения согласно заданному алгоритму.

Перспективы развития

В дальнейшем данная программа должна включить в себя обработку дополнительных конструкций модельного языка. Так же должны быть реализованы дополнительные опции для пошагового вывода применяемых в анализе функций и возможность настройки интерфейса пользователя. Так же будет сформирован справочный материал, описывающий возможности модельного языка и применяемые для его анализа функции, который будет доступен вместе с программным продуктом

Рисунок 1 - Архитектура программного продукта

Заключение

В результате проделанной работы автором был создан программный продукт для визуализации процесса построения таблиц компилятора в виде дерева по средствам создания учебных модельных языков, на основе которых был создан модуль интерпретации, работающий в комплексе с модулем визуализации.

Список литературы

1. Сучкова, Л.И. Абстрактный и структурный синтез автоматов: учебное пособие по дисциплине «Теория автоматов» [Текст]/ Л.И. Сучкова; АлтГТУ им. И.И. Ползунова. – Барнаул, Изд-во АлтГТУ, 2009. – 162с., ил.

2. Никлаус Вирт, Построение компиляторов/ Пер. с англ. Борисов Е.В., Чернышов Л.Н. - М.:ДМК Пресс, 2010 - 192с.:ил.

ПРОТИВОДЕЙСТВИЕ SQL-ИНЪЕКЦИЯМ В АСПЕКТЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

Теплюк П.А. – студент, Шарлаев Е.В.- к.т.н., доцент
Алтайский государственный технический университет им. И.И.Ползунова (г. Барнаул)

Исследования в области информационной безопасности [1] показывают, что организации несут большие убытки вследствие разных видов сетевых атак, и немалую роль при потерях играет недостаточная защищенность информации, хранящейся в базах данных (БД). В настоящее время критически важная для государственных и коммерческих компаний информация обрабатывается с применением веб-приложений [2], где БД входят в число ключевых компонентов. Одним из способов взлома веб-сайтов и приложений, работающих с базами данных, являются SQL-инъекции – атаки, реализуемые посредством внедрения злонамеренного кода (операторов) на языке SQL (Structured Query Language).

Чтобы понять суть рассматриваемой атаки, необходимо определить недостаток программного обеспечения (ПО), приводящий к ее реализации, и причину, а также рассмотреть простейшую атаку с внедрением произвольных операторов на языке SQL.

Недостаток ПО в данном случае – это возможность внедрения операторов SQL. К причине реализации SQL-инъекции следует отнести некорректную обработку входных данных. В результате бреши программного обеспечения, работающего на стороне сервера, пользователь может изменить структуру запроса к базе данных.

Схема простой атаки с использованием SQL-инъекции приведена на рисунке 1.

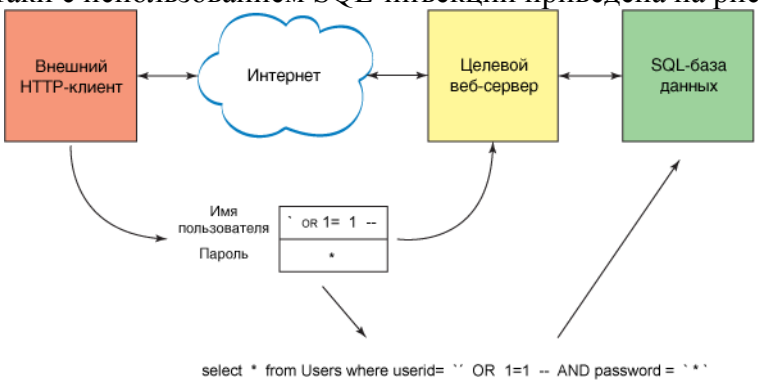


Рисунок 1 - Схема реализации SQL-инъекции

С точки зрения архитектуры пользователь при помощи веб-клиента взаимодействует по прикладному протоколу HTTP с фронтендом веб-сервера, который, в свою очередь, взаимодействует с бэкэндом в виде SQL-сервера (сервера БД). В ситуации входа пользователя в систему этот фронтенд веб-сервера применяет предоставляемую пользователем информацию при построении SQL-запроса. Как правило, защищенный веб-сервер требует от каждого пользователя, чтобы он аутентифицировал себя в системе,

представив имя пользователя и пароль. В самом простейшем случае веб-сервер выполняет следующую SQL-операцию (в которой uname и pword являются входными переменными):

*select * from Users where userid='uname' AND password='pword';*

Введя в веб-форму определенным образом подобранную информацию, злоумышленник может обойти намерения разработчика и модифицировать исполняемый запрос. В примере на рисунке 1 было изменено условие запроса, чтобы получить все записи. Для этого было использовано логический оператор OR (которое всегда имеет значение true) и с помощью комментария была деактивирована проверка пароля.

Приведенный пример позволяет увидеть, как данные, вводимые в форму на веб-странице, способны эксплуатировать уязвимость при обмене с внутренней системой в виде SQL-базы данных (MySQL, PostgreSQL). Результатом выполнения показанной выше операции является список всех записей, удовлетворяющих введенному выражению, т. е. база данных всех пользователей.

Как правило, реализация SQL-инъекций может привести к нарушению основных свойств защищаемой информации:

1. Конфиденциальности.
2. Целостности.
3. Доступности.

Нарушение конфиденциальности данных. Злоумышленник может получить полный доступ к базе данных, «скачать» ее, чтобы в дальнейшем получить материальную выгоду.

Нарушение целостности данных. Злоумышленник может изменить данные в БД.

Нарушение доступности данных. Злоумышленник может удалить данные. В итоге приложение не сможет обрабатывать запросы клиента.

Также путем SQL-инъекции возможно нарушение целостности приложения. Если сервер БД работает на одном узле с веб-сервером, сервером приложений, и если привилегии сервера баз данных позволяют записывать в каталог веб-приложения и изменять его файлы, то возможна модификация скриптов, добавление собственных файлов, изменение логики функционирования веб-приложения.

Необходимо подробнее остановиться на мерах защиты от вероятных последствий эксплуатации SQL-инъекций. Основная контрмера – это использование т.н. подготовленных выражений (prepared statement). Фиксируется структура запроса, и указываются те места, куда будут передаваться параметры. При этом задача парсера и драйвера по работе с СУБД - корректно экранировать данные, поступающие в качестве значений параметров.

Пример скрипта:

```
$stmt=$dbh->prepare("INSERT INTO TABLE_NAME(value, name) VALUES (?,?)");
$stmt->bindParam(1,$name);
$stmt->bindParam(2,$value);
$name='one';
$value=1;
$stmt->execute();
```

С целью минимизации последствий SQL-инъекций требуется:

1. Использование наименьших привилегий для подключений к СУБД. Если веб-приложению требуется считывать данные только из некоторой таблицы, то необходимо создать отдельного пользователя с привилегиями, позволяющими ему получать данные только из этой таблицы; установить запрет на модификацию данной таблицы и получение доступа к другим таблицам.
2. Вынесение сервера СУБД на отдельный узел.
3. Контроль целостности приложения. Применение контрольных сумм к файлам, директориям приложения позволит отслеживать несанкционированное их изменение [3].

Таким образом, использование приведенных выше мер предотвращения, либо минимизации последствий позволяет обеспечить должный уровень защиты веб-приложений

от SQL-инъекций, негативные последствия от которых, в лучшем случае, будут на уровне данных в БД, в худшем скажутся на логике работы непосредственно приложения.

Список используемых источников

1. Лихоносов А. Г. Безопасность баз данных. Учебное пособие [Текст] / А.Г. Лихоносов. - М.: 2010.

2. Теплюк П.А., Шарлаев Е.В. Угрозы безопасности веб-приложений // Сборник статей Международной научно-практической конференции «Новые задачи технических наук и пути их решения». – Уфа: Аэтерна, 2015. – с.83-85.

3. Лекции по курсу «Практические аспекты сетевой безопасности». Уязвимости в веб-приложениях. Часть I: SQLi [Электронный ресурс]. – Режим доступа: http://course.secsem.ru/lections, свободный (дата обращения 28.03.2015).

РАЗРАБОТКА КОМПЛЕКСА ДОКУМЕНТОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ ПРИ ИХ АВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ

Турубаров А.Е – студент, Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Разработка комплекса документов по защите персональных данных (ПДн) в информационных системах, обрабатывающих персональные данные (ИСПДн) медицинского учреждения является одним из элементов проектирования систем защиты информации (СЗИ). Законодательство Российской Федерации не определяет нормы и содержание документов. Документы Правительства и органов исполнительной власти ФСТЭК России и ФСБ России так же не определяют перечень локальных нормативно правовых актов организации для регулирования вопросов защиты информации в ИСПДн. Задачу конкретных типов и видов документов решают сами операторы или специализированные организации, оказывающие услуги в области информационной безопасности с учётом Законодательства РФ нормативных и методических документов ФСБ России и ФСТЭК России.

В Алтайском крае разработкой комплексов документов по защите ПДн организаций, занимается ООО «ЦИБ-сервис»[1]. Эта компания разработала онлайн-сервис подготовки пакета документов в соответствии с требованиями Федерального закона №152-ФЗ "О персональных данных"[4]. Сервис позволяет формировать инструкции, приказы, регламенты и журналы, всего номенклатура включает около 100 документов. Однако этот пакет не позволяет решить указанную задачу, поскольку он не учитывает специальные категории персональных данных, а именно обработку ПДн в медицинских информационных системах.

Поэтому в рамках совместного проекта АлтГТУ и ООО «ЦИБ-сервис» решена задача по разработке комплекса типовых документов по защите ПДн в ИСПДн медицинского учреждения. Выявлены основные направления, а именно: защита ПДн при автоматизированной обработке, неавтоматизированной обработке и криптографическими методами. Разработка пакета документов, в основу которых положена типовая система защиты ПДн в медицинском учреждении, была выполнена на базе Краевого государственного бюджетного учреждения здравоохранения «Детская городская поликлиника №2, г. Барнаул». В данной работе рассматривается одно из направлений - защита ПДн при автоматизированной обработке в медицинском учреждении.

Для достижения цели работы были определены конкретные задачи:

– анализ нормативно-правовых актов и нормативно-методических документов РФ, регулирующих отношения, связанные с обеспечением безопасности ПДн при их обработке в ИСПДн;

– анализ законодательства РФ в области здравоохранения и систематизация полученных знаний для реализации поставленной задачи;

– анализ типового пакета документов созданного компанией ООО «ЦИБ-сервис» по регулированию защиты ИСПДн;

– разработка типовых документов для регулирования защиты ИСПДн в медицинских учреждениях.

В ходе анализа законодательства РФ были определены нормативно-правовые акты и нормативно-методические документов РФ, регулирующие отношения, связанные с обеспечением безопасности ПДн при их обработке в ИСПДн:

– Конституции Российской Федерации;

– Трудового кодекса Российской Федерации;

– Федерального закона [4];

– Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Постановления Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановления Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Приказа ФСТЭК России от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– и другие.

Согласно Федерального закона [4] ст. 10 п.3-4 ПДн в медицинских учреждениях подпадают под специальные категории персональных данных. Обработка ПДн осуществляется для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн. В медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка ПДн осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством РФ сохранять врачебную тайну. В информационных системах медицинских учреждений оператор, кроме документов указанных выше, должен осуществляет обработку ПДн на основании следующих нормативно-правовых актов РФ[2]:

– Федеральным законом [3], ст.ст. 85-90 ТК РФ;

– Приказами Минздравсоцразвития;

– Нормативными актами (приказами (распоряжениями) Главного управления Алтайского края по здравоохранению и фармацевтической деятельности, приказами учреждения)

В результате анализа законодательства РФ в области здравоохранения были определены особенности по обработке ПДн в медицинских учреждениях. Оператор в медицинском учреждении должен руководствуется принципами и условиями касающиеся соблюдения врачебной тайны, которые описаны в ФЗ [3] ст. 13.

На основании этих особенностей в типовой пакет документов созданного компанией ООО «ЦИБ-сервис», который соблюдает нормативно-правовые акты и нормативно-методические документы РФ, регулирующих отношения, связанные с обеспечением безопасности ПДн при их обработке в ИСПДн, были введены добавление в пункты касающиеся:

– сведений о третьих лицах, участвующих в обработке ПДн;

– срока обработки ПДн;

– принципов и условий обработки ПДн;

– правовых оснований обработки ПДн;

– целей обработки ПДн;

– категорий обрабатываемых ПДн, источников их получения, сроках обработки и хранения;

– плана обучения правилам защиты информации;

– формы заявления на обработку ПДн пациента;

На рисунке 1 представлен один из документов подвергшихся изменениям. Красным цветом отмечены добавленные пункты.

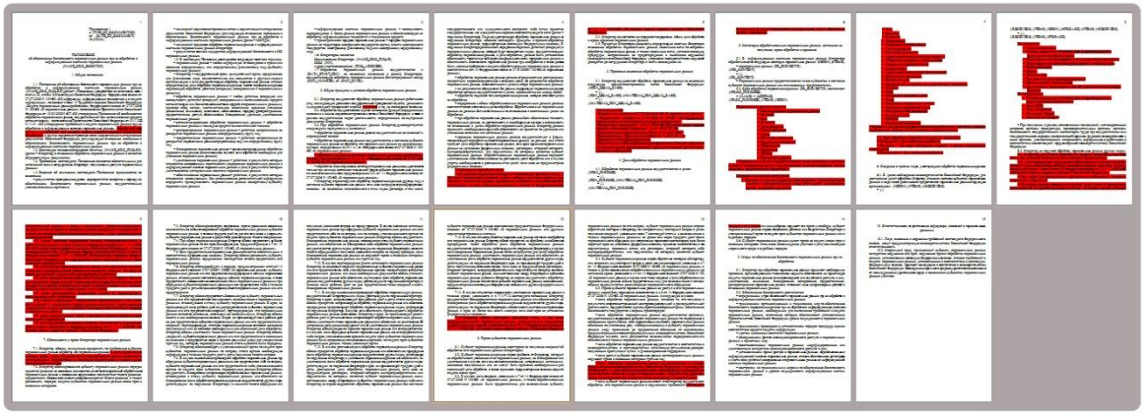
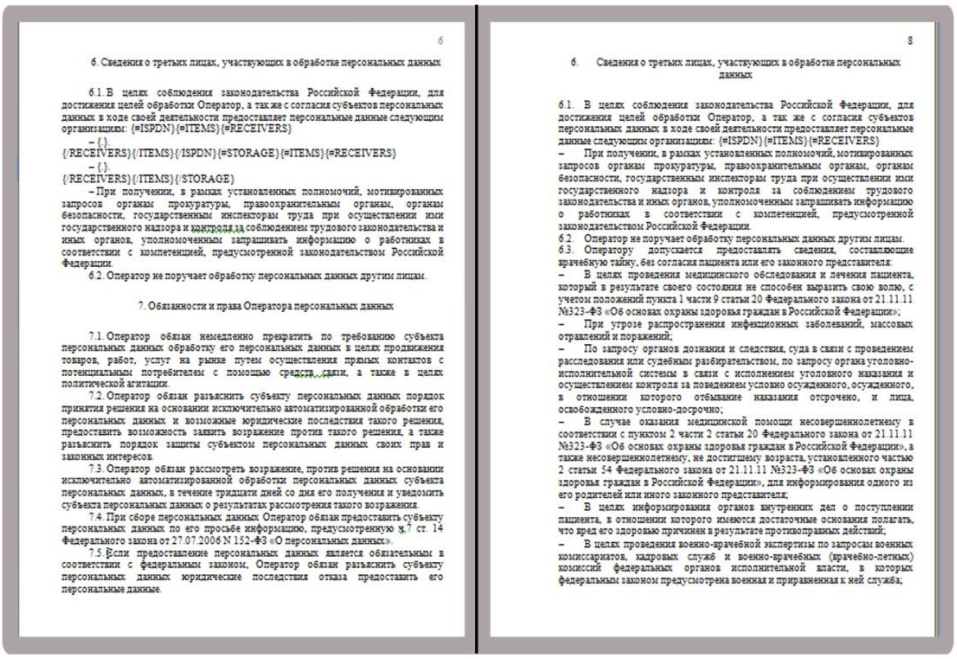


Рисунок 1 - Пример изменения документа

На рисунке 2 представлен шестой пункт документа «Об обеспечении безопасности персональных данных при их обработке в ИСПДн». Слева изображен документ до изменения, справа после.



6

6. Сведения о третьих лицах, участвующих в обработке персональных данных

6.1. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки Оператор, а так же с согласия субъектов персональных данных в ходе своей деятельности предоставляет персональные данные следующим организациям: {#ISPDN}{#ITEMS}{#RECEIVERS}

– {},

{/RECEIVERS}{/ITEMS}{/ISPDN}{#STORAGE}{#ITEMS}{#RECEIVERS}

– {}.

{/RECEIVERS}{/ITEMS}{/STORAGE}

– При получении, в рамках установленных полномочий, мотивированных запросов органам прокуратуры, правоохранительным органам, органам безопасности, государственным инспекторам труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства и иных органов, уполномоченных запрашивать информацию о работниках в соответствии с компетенцией, предусмотренной законодательством Российской Федерации.

6.2. Оператор не поручает обработку персональных данных другим лицам.

7. Обязанности и права Оператора персональных данных

7.1. Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации.

7.2. Оператор обязан разъяснить субъекту персональных данных порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты субъектом персональных данных своих прав и законных интересов.

7.3. Оператор обязан рассмотреть возражение, против решения на основании исключительно автоматизированной обработки персональных данных субъекта персональных данных, в течение тридцати дней со дня его получения и уведомить субъекта персональных данных о результатах рассмотрения такого возражения.

7.4. При сборе персональных данных Оператор обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную ч.7 ст. 14 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных».

7.5. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Оператор обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

8

6. Сведения о третьих лицах, участвующих в обработке персональных данных

6.1. В целях соблюдения законодательства Российской Федерации, для достижения целей обработки Оператор, а так же с согласия субъектов персональных данных в ходе своей деятельности предоставляет персональные данные следующим организациям: {#ISPDN}{#ITEMS}{#RECEIVERS}

– При получении, в рамках установленных полномочий,мотивированных запросов органам прокуратуры, правоохранительным органам, органам безопасности, государственным инспекторам труда при осуществлении ими государственного надзора и контроля за соблюдением трудового законодательства и иных органов, уполномоченным запрашивать информацию о работниках в соответствии с компетенцией, предусмотренной законодательством Российской Федерации.

6.2. Оператор не поручает обработку персональных данных другим лицам.

6.3. Оператору допускается предоставлять сведения, составляющие врачебную тайну, без согласия пациента или его законного представителя:

– В целях проведения медицинского обследования и лечения пациента, который в результате своего состояния не способен выразить свою волю, с учетом положений пункта 1 части 9 статьи 20 Федерального закона от 21.11.11 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

– При угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

– По запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

– В случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 Федерального закона от 21.11.11 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 Федерального закона от 21.11.11 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», для информирования одного из его родителей или иного законного представителя;

– В целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

– В целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых федеральным законом предусмотрена военная и приравненная к ней служба;

Рисунок 2 - Документ до изменения и после

В результате проведенной работы разработан комплекс документов по защите ПДн в ИСПДн медицинского учреждения при их автоматизированной обработке. Существенным изменениям подверглось 20-30% типовых документов. Данный комплекс документов применяется в Краевом государственном бюджетном учреждении здравоохранения «Детская городская поликлиника №2, г. Барнаул».

Список литературы:

1. ООО «ЦИБ-Сервис» [Электронный ресурс]. – URL: https://safe-doc.com/

2. PC Week Review: ИТ в медицине, октябрь 2009 [Электронный ресурс]. – URL: http://www.pcweek.ru/security/article/detail.php?ID=120407

3. Федеральный закон от 21.11.11 №323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» – URL: http://www.rg.ru/2011/11/23/zdorovie-dok.html

4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс] – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi ?req=doc;base=LAW;n=166051.

ОХРАННО-ИНФОРМАЦИОННОЕ УСТРОЙСТВО НА ОСНОВЕ КОМПЬЮТЕРА

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

При охране помещений актуальной является задача не только обнаружения несанкционированных проникновений, но и своевременного оповещения о таких инцидентах.

Организация ООО «Лель-сервис» занимается продажей кассовых аппаратов, расходных материалов к ним, а также послепродажным обслуживанием.

В рассматриваемой организации обрабатываются персональные данные сотрудников и клиентов, подлежащие обязательной защите в соответствии с законодательством РФ.

Также в организации обрабатывается иная конфиденциальная информация, которая возникает, например, при платежах в банк, маркетинговых исследованиях, а также сведения о системе защиты и сети.

При изучении текущего состояния защиты информации в организации было выявлено, что основным каналом утечки является несанкционированный доступ (НСД). Для обеспечения безопасности помещения предлагается использовать охранно-информационное устройство на основе компьютера.

В настоящее время охранно-информационные устройства строят на основе GSM-передающих устройствах, таких как телефоны или специализированные модули. Обычно такие решения требуют существенных материальных затрат или требуют дополнительной доработки и часто являются довольно сложными в исполнении.

Данная система выполняется на основе обычного компьютера, а информирующие сообщения передаются на сотовый телефон через сеть Интернет с помощью SMS-шлюза.

Предлагаемая система способна постоянно контролировать состояние семи датчиков, например, как показано на рисунке 1, датчики движения для дверей и окон, датчики для пожарной сигнализации, а также отправлять SMS-сообщения различного содержания на 5 номеров, например при постановке или снятии с сигнализации, а также при сигналах тревоги. Существует возможность подключения элементов световой или звуковой сигнализации к трем выходам системы [1].

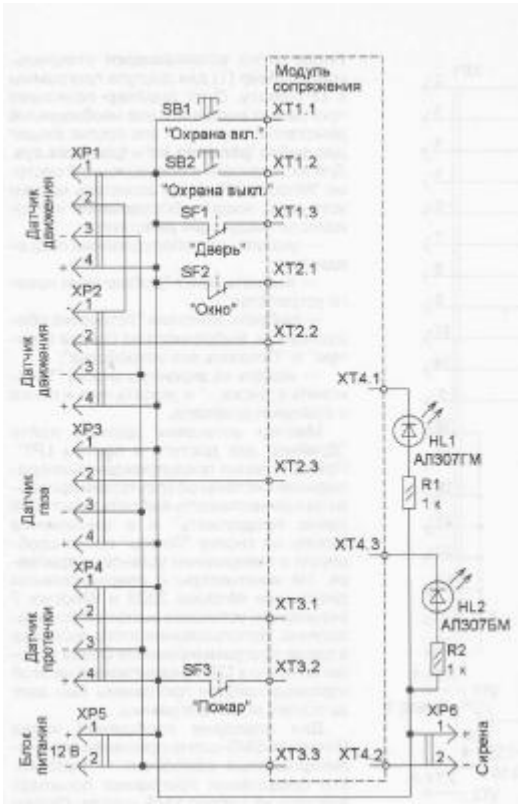


Рисунок 1 - Общая схема устройства

Все элементы модуля сопряжения смонтированы на печатной плате из фольгированного с двух сторон стеклотекстолита.

В данной системе для подключения датчиков охраны и сигнализации был выбран LPT-порт компьютера [2].

Управление охранно-информационной системой осуществляется с помощью специализированной программы. Для доступа к LPT-порту программы управления устройством предварительно необходимо установить драйвер. Для передачи сообщений через интернет также необходим специальный компонент, средствами которого программа будет посылать запросы на сервер SMS-шлюза. Программа управления устройством позволяет установить желаемую продолжительность работы сирены в режиме тревоги и интервалы времени на вход и выход. Также можно установить время, в течение которого система будет находиться в режиме "Охрана сработала" после срабатывания датчиков. По истечении этого времени система перейдёт в режим "Тревога". Программа предоставляет возможность установить режим "Задержка на выход", то есть интервал, в течение которого следует покинуть охраняемую зону после включения режима "охрана". После установки указанных настроек по свечению светодиодов и программных индикаторов можно проверить работу датчиков и модуля.

Информация о всех событиях, произошедших во время работы системы, автоматически сохраняется в log- файле, в каждой строке которого записывается событие, а перед ним системные дата и время. Эта же информация может выводится в окне программы.

Светодиоды выполняют функции индикатора состояния контактов датчиков, с его помощью можно быстро проверить работоспособность и исправность цепи датчика. Различные режимы работы светодиодов (кратковременные/длительные вспышки, постоянное свечение, выключено) отображают текущее состояние системы (выключено, в состоянии охраны, тревога).

Таким образом с помощью данной охранно-информационной системы можно эффективно отслеживать состояние защищаемого помещения, своевременно предупреждать

попытки несанкционированного доступа, а так же осуществлять контроль за пожарной сигнализацией.

Список используемых источников:

1. Красносельский Д. Охранно–информационная система на основе компьютера. Радио, 2012, № 8, 36-39.
2. Программируем порты - это очень просто ![Электронный ресурс]- valery-us4leh.narod.ru/PortCoding/cod01.html

ЗАЩИТА ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ИНТЕРНЕТ-ПРОВАЙДЕРА

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

На сегодняшний день, интернет-технологии является неотъемлемой частью нашего общества. Без них мы уже не можем представить свою жизнь. Интернет нужен нам для учебы, работы, развлечений, шопинга, коммуникаций и многого другого. Очень часто нам необходимо предоставлять персональные данные, например, для оплаты коммунальных платежей, получения государственных услуг, оплаты покупок с помощью банковской карты, защита которых обязательна по требованию законодательства. Всё вышеперечисленное создаёт потребность в усиленной защите данных при использовании сети Интернет.

Так как услуги по предоставлению доступа во всемирную сеть осуществляют Интернет-провайдеры, то именно на них ложится большая часть ответственности за безопасность пользовательских данных. Поэтому создание системы защиты информации является обязательной составляющей деятельности организации Интернет-провайдера. Также комплексная система защиты информации позволит обеспечить бесперебойное функционирование сервисов, предотвратить прямые материальные потери от утечки или утраты конфиденциальной информации, а также предотвратить возможный ущерб репутации компании.

Создание системы защиты информации позволит всесторонне защитить информацию с помощью таких мер, как правовые, инженерно-технические, криптографические, организационные, программно-аппаратные.

Для того, чтобы определить целесообразность создания системы защиты информации, зону и глубину её охвата следует провести детальный анализ организации, включающий:

- Анализ деятельности предприятия
- Положение организации на рынке
- Выявление конфиденциальной информации и защищаемых ресурсов
- Анализ угроз, уязвимостей и потенциального ущерба от реализации угрозы

На основе полученной информации о деятельности организации и уязвимых местах в действующей системе защиты необходимо составить техническое задание на создание комплексной системы защиты информации.

Исходя из существующего технического задания, следует определить практические меры для его реализации. Совокупность этих мер составит проект внедрения комплексной системы защиты информации.

Для создания системы защиты информации необходимо:

- Выявить требования, предъявляемые к создаваемой комплексной системе защиты информации
- Составить детальный список мероприятий, необходимых для внедрения комплексной системы защиты информации
- Назначит ответственных за проводимые мероприятия
- Произвести оценку затрат ресурсов на внедряемые мероприятия
- Оценить эффективность проводимых мероприятий

На первом этапе производится анализ информационной системы предприятия. Определяется кол-во АРМ и серверов, их техническая составляющая, используемое программное обеспечение, обрабатываемая информация.

На следующем этапе проверяется состояние фактической защищенности организации. Исследуются права доступов сотрудников, места хранения защищаемой информации, наличие охранных систем.

На основании проведенного анализа фактической защищенности необходимо составить перечень требований к создаваемой комплексной системе защиты информации. Данные требования должны соответствовать реальному состоянию защищенности информации в организации. Требования должны быть оформлены в виде Технического задания на создание комплексной системы защиты информации.

Последним этапом должно стать выявление всевозможных рисков, с которыми мы можем столкнуться во время реализации проекта, а также определение мер минимизации данных рисков.

Библиографический список:

1. Федеральный закон от 27 июля 2006 г. N 152-ФЗ О персональных данных
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ Об информации, информационных технологиях и о защите информации.
3. Указ Президента Российской Федерации от 17 марта 2008 г. N 351 О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена

РАЗРАБОТКА ГЕНЕРАТОРА СИГНАЛОВ НА БАЗЕ ЦИФРОВОГО ВЫЧИСЛИТЕЛЬНОГО СИНТЕЗАТОРА AD9851 ДЛЯ УЧЕБНОГО СТЕНДА

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

Одной из часто встречающихся задач в рамках дисциплин «Электротехника, электроника и схемотехника», «Радиотехника» и «Измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения» [4] является рассмотрение принципов действия электронных компонентов и простых схем на однофазном переменном токе, для которых необходим генератор различного вида сигналов с большим спектром частот

На данный момент в лаборатории используется генератор сигналов (ГС) на базе звуковой карты компьютера. Он обладает следующими характеристиками: диапазон регулируемых частот составляет 1Гц – 20кГц; генератор сигналов выполнен на звуковой карте персонального компьютера; настройка частоты производится через графический интерфейс; Настройка амплитуды напряжения производится через графический интерфейс и делитель напряжения непосредственно на стенде; выбор типа генерируемого сигнала производится с помощью графического интерфейса на ПК.

Данный ГС имеет следующие недостатки:

1) низкая максимальная частота, что не всегда является достаточным для изучения принципов модуляции;
2) маленькая амплитуда напряжения, не всегда достаточная для выполнения практических задач в рамках учебных курсов;
3) отсутствие возможности функционирования без персонального компьютера;
4) отсутствие трехфазного тока;
5) отсутствие частотомера, позволяющего контролировать смоделированную генератором частоту тока.

Имеет преимущества:

1) на данный момент таким генератором оборудованы все лабораторные стенды;

2) генерирует три вида сигнала: синусоидальный, треугольный и прямоугольный, но не всегда корректно.

После анализа приведённых недостатков и преимуществ была поставлена цель: Разработать генератора сигналов, исключающий недостатки существующих лабораторных стендов.

Вектор цели направлен следующими задачами:

1) ГС должен обеспечивать генерацию сигналов различных форм и заданной частоты от 1Гц до 40МГц.

2) ГС должен быть полностью независимым от персонального компьютера, либо иметь поддержку косвенного управления для задания сложных форм сигналов.

3) ГС должен быть встраиваемым в стенд.

4) ГС должен иметь достаточный уровень безопасности для эксплуатации на территории ВУЗа.

5) иметь достаточно простую элементарную базу, что позволит обслуживать и ремонтировать генератор в случае сбоя/неисправности;

Есть три возможных пути достижения поставленной цели:

1) приобрести новый многофункциональный генератор сигналов (ГС);

2) улучшить имеющийся ГС;

3) разработать новый ГС, отвечающий необходимым требованиям.

При выборе первого варианта решения проблемы существует финансовая проблема – стоимость профессиональных генераторов сигналов с необходимым уровнем безопасности колеблется на уровне в 15 000 рублей, кроме того, возникает проблема с встраиванием в стенд, а так же может возникнуть проблема с обслуживанием, в случае выхода из строя ГС [2].

Если попытаться улучшить имеющийся генератор сигналов, то возникает проблема повышения частоты, после её решения, возникнет потребность коррекции формы сигнала, которая приведёт к необходимости проектировки фильтров. Среди этих проблем выделяется основная – в существующем ГС нет возможности обеспечения функционирования устройства без персонального компьютера, что является одной из поставленных задач.

Поэтому, исходя из анализа, наилучшим решением будет конструирование нового генератора сигналов.

Для решения данной задачи были определены основные модули проектируемого устройства, предварительно просчитана экономическая эффективность проектируемого устройства и определён порядок действий для разработки.

Параллельно был разработан код программы для микроконтроллера «Atmega8» на языке СИ в среде «Code Visual AVR» с тестированием в симуляторе «Proteus». В процессе разработки выявилась необходимость использования шифратора для подключения всех кнопок, был изучен принцип передачи данных по параллельному интерфейсу.

На данный момент разработана следующая версия принципиальной схемы (рисунок 1), не являющаяся итоговой, но на которой будет основана остальная часть работы. В схему будут добавлены: трехзвенный фильтр нижних частот на выходе AD9851, усилители и транзисторы в той же области [1,3].

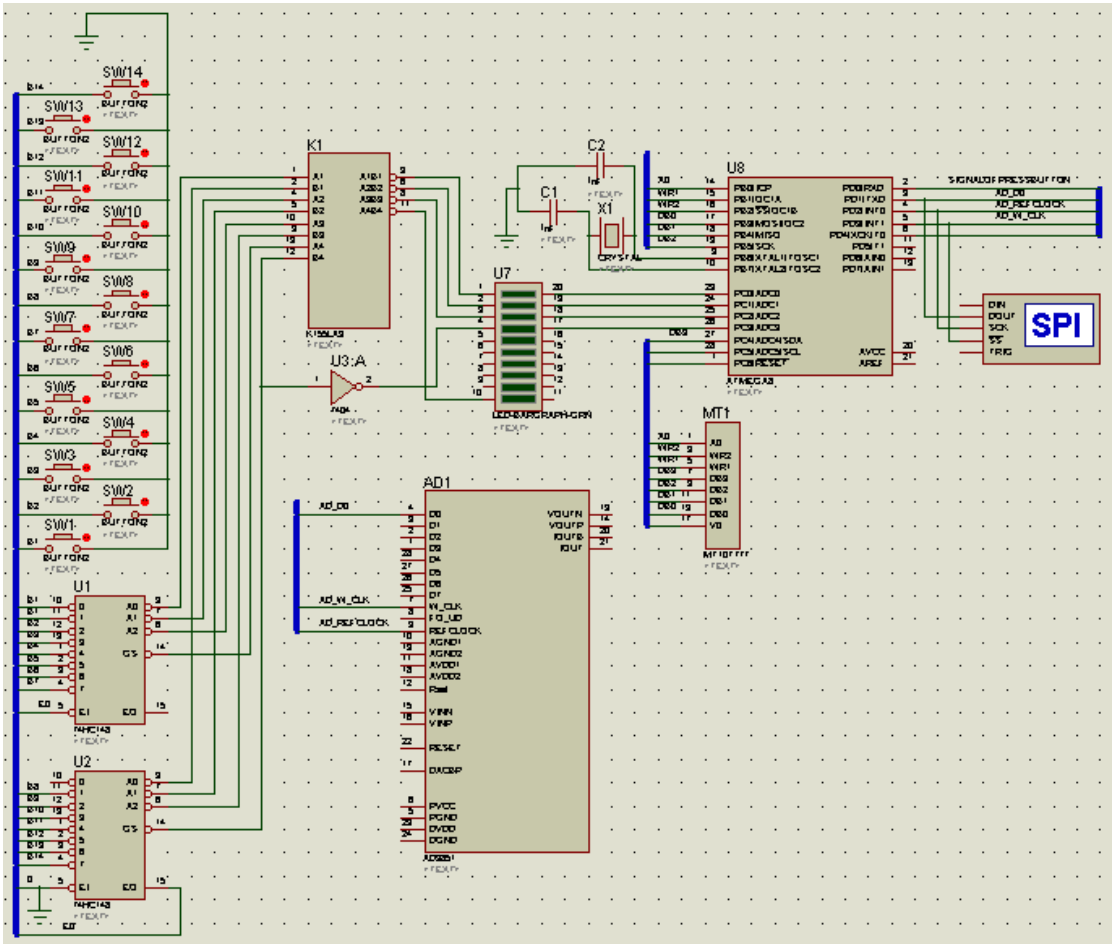


Рисунок 1 – Принципиальная схема генератора

На представленной схеме тестируются последовательности кодов, генерируемых микроконтроллером «Atmega» и передаваемых по SPI интерфейсу в случае нажатия одной из кнопок. Модуль AD9851 смоделирован только частично – лишь сопоставлены контакты модели и корпуса в ARES, что несколько осложняет разработку.

Также в среде ARES 7 Proteus была создана 3D модель будущей печатной платы устройства, представленная на рисунке 2, позволяющая увидеть расположение компонентов и смоделировать расположение платы в стенде.

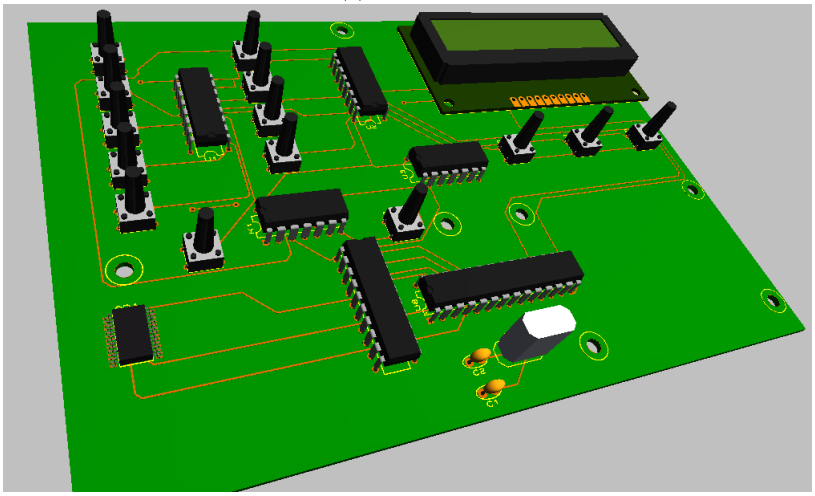


Рисунок 2 – Внешний вид черновой 3D модели печатной платы.

В данной работе был проведен анализ генераторов сигналов, был сделан вывод о том, что для более качественного решения необходимо разработать собственный генератор сигналов на базе ATMega8 и AD9851 и написан первый вариант кода для данной схемы. При

дальнейшей разработке необходима корректировка кода, расчет фильтров и подбор транзисторов, а также написание документации – руководства по использованию и ремонту для выполнения поставленной задачи по обеспечению стенда ячейкой генератора сигналов.

Список литературы

1. Журнал «Контрольно-измерительные приборы и системы» // Измерительный генератор [Электронный ресурс]: журнал, – город Москва – 2000-2013. – Режим доступа: http://www.kipis.ru/info/index.php?ELEMENT_ID=20943

2. Компания астена // измерительные приборы и оборудование // генераторы [Электронный ресурс]: интернет магазин – г. Рязань – 2005. – Режим доступа: http://www.astena.ru/pr_7.html

3. Радио лоцман // Схемы // Генераторы // Версия DDS генератора на микросхеме AD9833 и микроконтроллере AT90USB162 [Электронный ресурс]: журнал – 2012. – Режим доступа: http://www.rlocman.ru/op/tovar.html?di=56282&/ANR-1002

4. Образовательный стандарт учебной дисциплины Б.3.Б.14 «Электроника и схемотехника» 090900 Информационная безопасность. [Текст]: Разработан кафедрой вычислительных систем и информационной безопасности Алтайского государственного технического университета им. И. И. Ползунова. / Алтайский государственный технический университет имени Ивана Ивановича Ползунова. – Барнаул. – Неопубликованные материалы.

РАЗРАБОТКА САЙТА КАФЕДРЫ ИНФОРМАТИКИ, ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Шигин А.И. - студент, Якунин А.Г. - д.т.н., профессор
Алтайский государственный технический университет им. И. И. Ползунова

На сегодняшний день практически все учебные заведения используют Интернет в различных целях, например, для привлечения абитуриентов, рекламы, увеличения эффективности методической работы, обеспечения информацией и т.д. Хотя у каждого вуза имеется сайт, он не способен отражать интересы всех кафедр, оперативно предоставлять информацию кафедрального уровня в требуемом формате. В настоящее время многие кафедры различных вузов создают собственное представительство в сети Интернет отдельно от учебных заведений для повышения эффективности своей деятельности.

Подобное веб - приложение будет необходимо как сотрудникам кафедры, так и студентам, и абитуриентам. В связи со всем вышесказанным очевидна актуальность разработки кафедрального web-сайта. Об этом свидетельствует и огромное количество таких сайтов в Интернете, некоторые из которых были тщательно изучены.

Представительство кафедры ИВТ и ИБ в сети Интернет позволит добиться выполнения сразу нескольких целей:

- привлечение абитуриентов;
- увеличение эффективности учебного процесса;
- привлечение к сотрудничеству заинтересованных организаций;
- улучшение взаимодействия между студентами и преподавателями.

В результате анализа требований к данному веб приложению было выявлено главное отличие подобных сайтов от большинства других. Во-первых, это система разграничения доступа к ресурсам веб - приложения. Преподаватели и сотрудники кафедры должны быть активными создателями контента сайта, в связи с чем, должно быть реализовано следующие уровни доступа:

- гости, например, абитуриенты — права только для чтения;
- пользователи - студенты — права для чтения и просмотра ресурсов, комментирования, обмена информацией с преподавателями и другими студентами;

- пользователи - сотрудники (преподаватели и вспомогательный персонал) кафедры — права добавления и редактирования некоторых разделов сайта, участие в общении со студентами и другими преподавателями;
- пользователи – бывшие выпускники кафедры – права добавления и редактирования разделов сайта, касающихся вопросов трудоустройства, их личных отзывов о качестве обучения, обмена впечатлениями, связанными с профессиональной деятельностью;
- пользователи – работодатели – права добавления и редактирования разделов сайта, касающихся вопросов подбора персонала, описания специфики их производственной деятельности, трудоустройства и отзывов о качестве обучения со стороны работодателя;
- администратор (разработчик) — полные права;

На основе опроса сотрудников и преподавателей кафедры были сформулированы основные функциональные требования и структура разделов разрабатываемого сайта. Основные разделы:

- Новости
- О кафедре
- События
- Абитуриентам
- Студентам
- Выпускники
- Преподаватели
- Работодатели
- Личный кабинет
- Обратная связь

При этом сотрудники кафедры должны иметь возможность создавать и редактировать новости, объявления (о приеме долгов и времени консультаций, переносе занятий и проч.), свое расписание, информацию о себе (преподаваемые дисциплины, тематику научных исследований, свои публикации, награды), информацию о связях и о работе.

Также необходимо настроить систему общения и обмена файлами между студентами и преподавателями. Это необходимо для осуществления рассылки объявлений всем студентам, или студентам одной группы, курса, потока, всем преподавателям или одному конкретному человеку или группе лиц. Очень полезным в такой системе будет также модуль оповещения о входящих сообщениях и изменениях на сайте на почтовый ящик, который в настоящее время есть абсолютно у каждого.

В данный момент подобный функционал имеется у стандартного личного кабинета преподавателя и личного кабинета студента, однако у него имеется ряд недостатков, которые будут учтены в разрабатываемом веб приложении.

Реализовать требуемый функционал планируется с использованием web - сервера Apache, СУБД MySQL, языка гипертекстовой разметки HTTP, таблиц стилей CSS, а также таких языков программирования как PHP и JavaScript.

В настоящее время проект находится в стадии разработки модели базы данных, сбора и анализа информации от студентов, абитуриентов и преподавателей кафедры. Следующим этапом будет создание макета сайта и разработка его функционала. Затем после проведения различного рода тестирований проект будет выложен в сеть интернет и станет общедоступным ресурсом.

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СТЕГАНОГРАФИЧЕСКИХ И КРИПТОГРАФИЧЕСКИХ МЕТОДОВ

Шустов Д.В. – студент, Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

С развитием интернет-технологий цифровая информация (текст, изображение, звуковой или видео файл) может быть очень легко передана по сети [1]. В современной жизни часть информации, передающаяся по сети интернет, имеет конфиденциальный характер, например, сведения, составляющие личную или семейную тайну. Существующие средства безопасности среды интернет не обеспечивают полной гарантии конфиденциальности, что часто приводит к появлению во всемирной паутине личной информации людей. Поэтому вопрос о том, как обеспечить конфиденциальность информации во время ее передачи и хранении, остается актуальным.

Одним из основных методов защиты цифровой информации является криптография. Ее цель - сокрытие содержимого сообщения при помощи шифрования. При шифровании происходит повышение безопасности сообщения или файла, при котором их содержимое преобразуется так, что оно может быть прочитано только пользователем, обладающим соответствующим ключом шифрования для расшифровки содержимого. Однако криптография не обеспечивает секретность передачи информации. Переданное зашифрованное сообщение будет легко обнаружено злоумышленником, пытающимся получить конфиденциальную информацию.

Задачу скрытия факта передачи именно секретного сообщения решает такая наука, как стеганография. В древности стеганография являлась искусством передачи сообщения тайным образом, чтобы только получатель знал о существовании секретного сообщения[1]. В современном же мире появилась компьютерная стеганография. Компьютерная стеганография позволяет дополнить криптографию, то есть сам факт передачи зашифрованного секретного сообщения будет неизвестен.

Современные методы компьютерной стеганографии представляют собой процесс замены несущественных или неиспользуемых блоков данных в цифровых файлах на конфиденциальную информацию. Таким образом, после некоторых преобразований можно получить компьютерный файл, почти не отличающийся от оригинала, с секретным сообщением [2].

В данной работе рассматриваются стеганографический и криптографический алгоритмы защиты информации, а ее целью является программная реализация рассмотренных алгоритмов.

Для реализации программного средства защиты нужно решить несколько задач, а именно:

1) выбор криптографического алгоритма;

2) выбор стеганографического алгоритма;

3) разработка программного обеспечения реализующего крипто и стегоалгоритмы.

Криптографическая составляющая позволит обезопасить конфиденциальную информацию пользователя от раскрытия ее содержания в случае извлечения сообщения из переданного файла. Также при шифровании изменяются статистические характеристики сообщения, повышается его энтропия. Зашифрованное сообщение становится похожим на случайные данные с таким же распределением, как и в пустом контейнере. Именно шифрование не позволяет злоумышленнику однозначно установить факт передачи информации.

В статье [2] был проведен анализ современных симметричных криптографических алгоритмов, что позволило принять решение: выбран алгоритм шифрования AES(Rijndael).

Rijndael – это итерационный блочный шифр, имеющий архитектуру «Квадрат». Шифр имеет переменную длину блоков и различные длины ключей. Длина ключа и длина блока

могут быть равны независимо друг от друга 128,192 или 256 битам. В стандарте AES определена длина блока данных, равная 128 битам[3].

В качестве стеганографического алгоритма используется метод замены наименее значащего бита (НЗБ, LSB - Least Significant Bit). Популярность данного метода обусловлена его простотой и тем, что он позволяет скрывать в относительно небольших файлах достаточно большие объемы информации (пропускная способность создаваемого скрытого канала связи составляет при этом от 12,5 до 30%). Основной недостаток данного метода – высокая чувствительность к малейшим искажениям контейнера[4]. Основной принцип метода показан на рисунке 1. Извлечение секретного сообщения из изображения происходит в обратном порядке.

Цифровое изображение представляет собой матрицу пикселей. Как известно, пиксель – единичный элемент изображения. Для представления цвета в пикселе используется цветовая модель RGB. Каждому цвету соответствует интенсивность, которая изменяется от 0 до 255. Младший значащий бит в изображении несет меньше всего информации. Известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически, НЗБ – это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения. Каждый пиксель кодируется 3 байтами (24 бит). Чтобы записать информацию и при этом не исказить изображение, необходимо записывать данные в младшие биты цветов изображения. Например, в изображение размером 512x512 можно встроить примерно 32кБайт информации[4].

На основании описанных алгоритмов было разработано программное обеспечение на языке программирования C#. Программа позволяет шифровать секретное сообщение, встраивать шифрованную последовательность в изображение, а так же извлекать и расшифровывать конфиденциальную информацию.

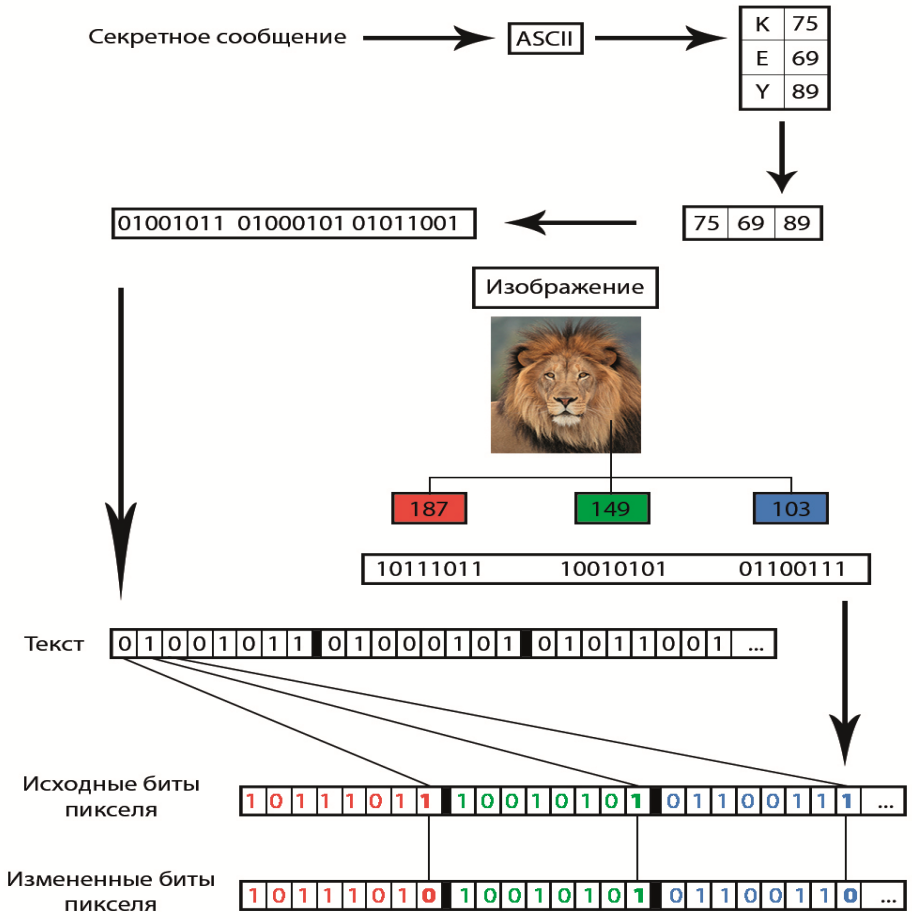


Рисунок 1 - Принцип метода НЗБ

Программное обеспечение работает под операционной системой Windows. Для работы с ПО потребуется:

1) персональный компьютер с ОС Windows xp или выше;
2) установленное программное обеспечение .net framework версии 4 или выше
3) 32 мегабайта оперативной памяти;
4) 2 мегабайта места на жестком диске;
5) процессор с тактовой частотой 400 мегагерц или более.

Портативная версия не требует инсталляции. Интерфейс программы изображен на рисунке 2.

Программа снабжена простым и интуитивно понятным интерфейсом, при помощи которого пользователь может максимально эффективно использовать данное программное обеспечение. При работе с программой следует учитывать, что малейшее искажение контейнера приводит к невозможности извлечения секретного сообщения.

Программное обеспечение может быть использовано:

1) при обучении студентов;
2) в личных целях, для скрытой передачи конфиденциальной информации.

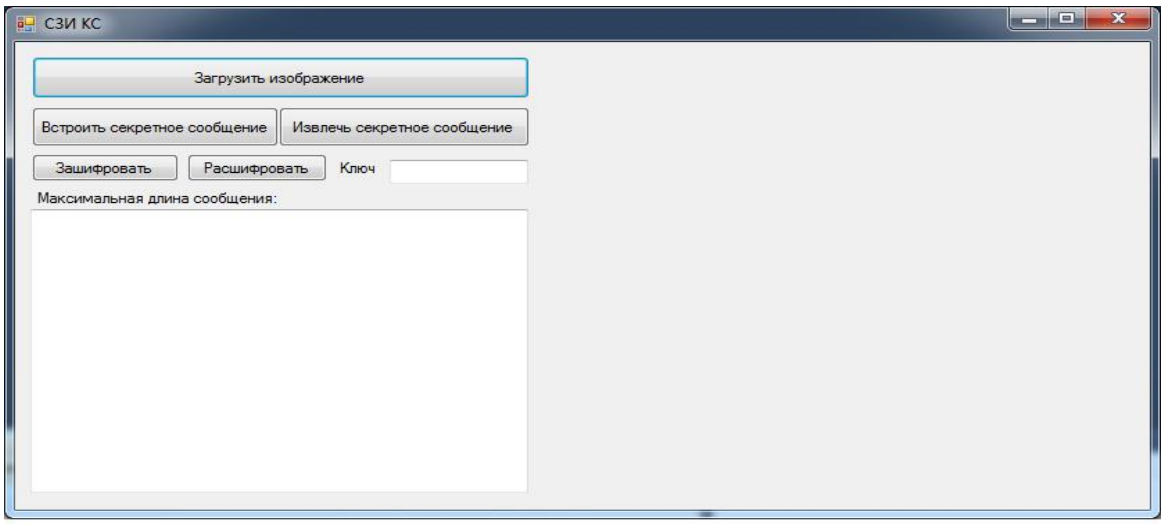


Рисунок 2 – Интерфейс программы

Список литературы

1. Lee Y. K., Chen L. H., 2004, "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement", Proceedings of the Ninth National Conference on Information Security, Taiwan, 8-15 // http://debut.cis.nctu.edu.tw/Publications/

2. Кобелев С.Ю. Загинайлов Ю.Н. Разработка средства защиты информации на основе криптостеганографической системы // V Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых "Наука и молодежь − 2008". Секция «Информационные и образовательные технологии». Подсекция «Безопасность информационных технологий и защита информации». / Алт. гос. техн. ун-т им. И.И.Ползунова. – Барнаул: изд-во АлтГТУ, 2008. – 15 с.

3. Стандарт криптографической защиты – AES. Конечные поля. / Под ред. М.А. Иванова – М.: «КУДИЦ-ОБРАЗ»,2002. – 176 с.

4. Коханович Г. Ф. Компьютерная стеганография. Теория и практика. / Г. Ф. Коханович – К.: «МК-Пресс», 2006. – 288 с.

РАЗРАБОТКА СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ В КОМИТЕТЕ ПО ОБРАЗОВАНИЮ ГОРОДА БАРНАУЛА

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

Комитет по образованию города Барнаула (далее - Комитет) является органом местного самоуправления, уполномоченным в сфере управления образованием. Основными видами деятельности комитета является организация предоставления общедоступного и бесплатного начального общего, основного общего, среднего (полного) общего образования по основным общеобразовательным программам, организация предоставления дополнительного образования и общедоступного бесплатного дошкольного образования на территории городского округа, а также отдыха детей в каникулярное время, разработка стратегии развития системы образования в городе и обеспечение ее корректировки [1].

Такая деятельность подразумевает обработку персональных данных учащихся детских садов и школ, а также сотрудников комитета. В соответствии с Федеральным законом РФ от 27.07.2006 №152-ФЗ «О персональных данных» доступ в помещения, где ведется обработка персональных данных, должен быть ограничен, а также должны быть приняты комплекс

технических и организационных мероприятий по защите персональных данных в соответствии с руководящими документами.

Поэтому доступ к помещениям, в которых ведется обработка персональных данных, необходимо ограничивать особенно тщательно. Чтобы допустить к работе в таких помещениях только специально обученный персонал, необходимо наличие специальных систем контроля и управления доступом. Поэтому существует основной задачей является разработка и внедрение подобных систем.

В настоящее время на рынке существует масса продуктов систем разграничения доступа к помещениям различного рода. Для офисных помещений популярными решениями данной проблемы являются электронно-механические замки. Вариаций таких замков много: замки с цифровой клавиатурой для набора уникального кода; замки со специальными считывателями электронных карт, таблеток, токенов и т.д; радиоэлектронные замки, для которых применяются радиоключи, настроенные на радиочастоту замка; замки с проверкой биометрических параметров, таких как отпечатки пальцев, сетчатка глаза, проверка голоса и т.д [2].

У каждого типа замков, описанных выше, имеются свои достоинства и недостатки. Замки с цифровой клавиатурой уязвимы тем, что код можно подсмотреть, подслушать, подобрать перебором, да и кнопки клавиатуры быстро стираются и приходят в негодность. Замки со специальными считывателями более совершенны и стойки ко взлому, но электронный ключ, карту или токен легко потерять, а получить копию зачастую бывает проблематично и затратно. Радиоэлектронные замки уязвимы к перехвату радиосигнала от ключа к замку злоумышленником и подделке сигнала. Замки с проверкой биометрических параметров наиболее стойкие ко взлому, но зачастую их цена противоречит принципу, что ценность средств для защиты информации не должна быть выше ценности самой информации.

Наиболее рациональным решением для разграничения доступа в офисное помещение комитета по образованию города Барнаула, в котором обрабатываются персональные данные, выбран электромеханический замок со считывателем RFID карт стандарта Mifare S50 с частотой 13,56 МГц. Карты данного стандарта отличаются трехступенчатой аутентификацией по протоколу ISO/IEC 9798, шифрованием передаваемой информации и её передачи по ВЧ-каналу, наличием транспортного ключа для доступа к внутренней памяти карты EEPROM объемом 1 кб, а также уникальным серийным номером каждой карты, что в совокупности позволяет достичь высокого уровня безопасности от подделки карты.

Система состоит из пластиковой карты со встроенным чипом и антенной, контроллера, а также исполнительного устройства с источником питания. Схема устройства системы контроля доступа представлена на рисунке 1.

В качестве управляющего элемента выбран микроконтроллер Atmega8 фирмы AVR. Для индикации используется жидкокристаллический дисплей. Индикатор выбирался большой - 4 строки по 20 символов для возможности отображения большого количества информации при сохранении карточек в память устройства. ЖК дисплей подключается к микроконтроллеру по четырех битной системе. Переменный резистор R2 необходим для регулировки контраста символов на дисплее. Подсветка ЖК дисплея организована через вывод "A" и "K" на плате дисплея. Подсветка включается через резистор, ограничивающий ток - R1. При помощи кнопок S1 - S4 происходит запись и сохранение RFID карточек в память микроконтроллера. Для питания схемы используется микросхема линейного стабилизатора L7805. Далее 5 вольт стабилизируются другой микросхемой - AMS1117 в исполнении, дающей на выходе 3,3 вольта. В этой схеме 5 вольт используется для питания дисплея, далее вся схема питается от напряжения 3,3 вольта. Для управления исполнительным устройством используется цепь с реле. При разрешении доступа по карточке на выводе PB0 микроконтроллера появится высокий потенциал на 5 секунд, транзистор T1 откроется и замкнет цепь катушки реле. Диод VD1 предохраняет транзистор от выхода из строя при выключении катушки - в этот момент ЭДС самоиндукции может пробить транзистор без диода. Для общего питания схемы

используется отдельный блок питания на 12 вольт. Он же и используется и для питания электромеханического замка. Для считывания RFID карточек применен модуль на базе микросхемы RC522 [3].

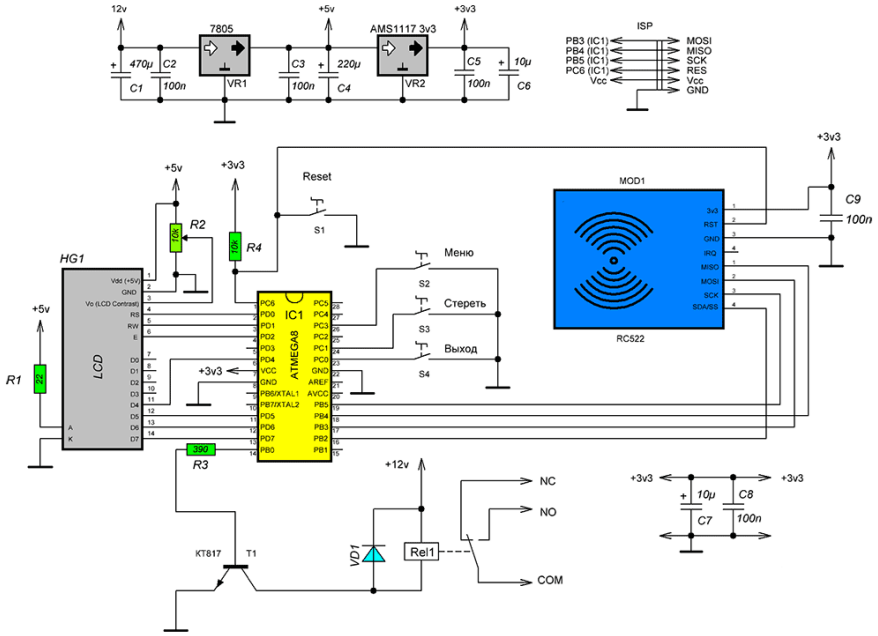


Рисунок 2 – схема устройства системы контроля доступа

В ходе работы был изучен принцип действия системы контроля и управления доступом со считывателем RFID карт стандарта Mifare S50, состоящей из карты доступа, контроллера и исполнительного устройства.

Список используемых источников

1. Положение о комитете [Электронный ресурс]. – Электрон. текст. дан.- М., 2007.- Режим доступа: http://www.barnaul-obr.ru/kpmo/ - Загл. с экрана.

2. Как выбрать СКУД [Электронный ресурс]. – Электрон. текст. дан.- М., 2007.- Режим доступа: http://hardbroker.ru/pages/skud - Загл. с экрана.

3. Система доступа на RFID картах [Электронный ресурс]. – Электрон. текст. дан.- М., 2014.- Режим доступа: http://cxem.net/guard/3-77.php - Загл. с экрана.

ОСОБЕННОСТИ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА КАК ОБЪЕКТА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Эрнст М.Е. – студент, Паршукова Т.П.- ст.преподаватель,
Загинайлов Ю.Н. – к.в.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Применение систем электронного документооборота и делопроизводства (СЭД) началось с середины 1990-х годов. Однако внедрение СЭД в государственном масштабе получило широкое распространение только в последние пять лет. Основным стимулом тут стало распоряжение Правительства РФ от 12.02.2011 № 176-р, утвердившее План мероприятий по переходу федеральных органов исполнительной власти на безбумажный документооборот и Постановление Правительства РФ от 06.09.2012 № 890 «О мерах по совершенствованию электронного документооборота в органах государственной власти» [1]. В соответствии с этим планом мероприятий Минкомсвязи РФ были подготовлены и утверждены требования к СЭД [2].

Кроме этого, фактически произошло изменение парадигмы защиты информации в системах электронного документооборота [3]. Если раньше защищались сами электронные

документы или информационные ресурсы, содержащие документы (т.е. системы электронного документооборота как объект защиты рассматривались как прикладное программное обеспечение), то теперь изменяется основной вектор атак и соответственно изменяется объект защиты. Электронный документооборот как объект защиты является в современных условиях процессом и поэтому объектом становится взаимодействие «человек – электронный документ», «человек – информационный ресурс» [3] откуда следует, что защищать надо не документы, а сами системы передачи, обработки и хранения электронных документов при доступе легальных пользователей систем к работе с электронными документами. Также важна и непосредственно организация самого доступа пользователя к системе, к инструментам обработки и непосредственно к документам. Таким образом для исследования информационной безопасности необходимо учесть человеческий (субъективный) фактор, связанный с инсайдерством и объективный (технический) фактор, связанный с уязвимостью аппаратных и программных элементов информационной системы, что обусловливает необходимость детального исследования этих вопросов как специфических особенностей СЭД.

Основной идеей построения защищённого ЭД является то, что к задаче защиты СЭД надо подходить классически с точки зрения защиты информационной системы, когда система включает правовые, организационные, технические, криптографические и физические средства защиты. А именно, кроме известных уже среди разработчиков СЭД задач по защите электронных документов, таких как: аутентификация пользователей и разделение доступа, подтверждение авторства электронного документа, контроль целостности электронного документа, конфиденциальность электронного документа, обеспечение юридической значимости электронного документа, – для организации современного ЭД необходимо использовать механизмы, обеспечивающие: контроль целостности используемого программного обеспечения, регистрацию событий в информационных системах, криптографическую защиту, межсетевое экранирование, построение виртуальных частных сетей, антивирусную защиту, аудит информационной безопасности, – которые хорошо известны специалистам по защите информации.[3]

Однако разработка и построение систем защиты информации СЭД с учётом новой парадигмы невозможны без достаточно полного анализа уязвимостей и угроз безопасности объекту защиты – СЭД. Под системой электронного документооборота понимается организационно-техническая система, обеспечивающая процесс создания, управления доступом и распространения электронных документов в компьютерных сетях, а также обеспечивающая контроль над потоками документов в организации [2].

В настоящее время СЭД классифицируют следующим образом [4]: универсальные «коробочные» СЭД (имеют стандартный набор функций), индивидуально разрабатываемые СЭД (максимально персонифицированная система), комбинированные СЭД (базовая платформа, к которой разрабатываются необходимые дополнительные модули).

Структуру СЭД можно представить на основе «коробочной» СЭД «Дело», нашедшей наибольшее распространение в России (49%) от всех СЭД.

Она включает следующие компоненты (подсистемы):

– ДЕЛО-WEB Опция «ДЕЛО-WEB» — решение для предприятий с территориально распределенной структурой.

– ЭЦП и шифрование. Электронная цифровая подпись (ЭЦП) является необходимым условием для полноценной реализации защищенного электронного документооборота. Криптосрдства сертифицированы.

– Сканирование и поточное сканирование.

– Защита от несанкционированного доступа. Задача обеспечения безопасности хранимой информации решена с помощью Secret Disk Server NG компании Aladdin.

– Подсистема управления процессами. Подсистема позволяет проектировать и создавать произвольные документоориентированные приложения.

– Подсистема интеграция СЭД «ДЕЛО» и системы 1С. Решение позволяет упорядочить работу с финансовыми документами.

– Мастер паролей. Мастер Паролей — программно-аппаратный комплекс, разработанный компанией «Рускард».

– Мониторинг документов. Мониторинг документов — приложение, разработанное компанией «Корпоративные Системы-Консалтинг».

– Подсистема «Повестки заседаний». Повестки заседаний - дополнительный компонент системы электронного документооборота «ДЕЛО».

1.1.1 Серверная часть системы «ДЕЛО» 14.2 (2014 г.) работает на платформе Windows Server 2012, а клиентская часть поддерживает Windows 8.1. В новую версию СЭД добавлена поддержка СУБД MS SQL Server 2012, MS SQL Server 2014, Oracle 12c. Коллективная работа пользователей реализована также через «Личные папки».

1.1.2 Из анализа структуры СЭД на примере СЭД «Дело» можно сделать вывод, что особенностями СЭД как информационной системы и в частности её технической (программно-аппаратной) основы будет наличие сервера централизованного управления, сервера баз данных и автоматизированных рабочих мест (АРМ), сети передачи данных. Эти составные части СЭД имеют собственные уязвимости которые могут быть идентифицированы с использованием базы данных уязвимостей на сайте ФСТЭК России.

При использовании организацией СЭД возникает сложная система внутренних и внешних связей. Кроме того, что документы циркулируют между структурными подразделениями организации, обмен информацией происходит и с государственными учреждениями, и возможно с различными коммерческими организациями. Таким образом, для того, чтобы построить наиболее эффективную систему защиты для СЭД необходимо разобраться в том, какие субъекты учувствуют в процессе создания и использования электронного документа. Для визуализации связей при электронном документообороте можно использовать упрощённую модель взаимодействия субъектов СЭД (Рисунок 1). Она отражает информационные потоки а также позволяет определить и выделить конфиденциальные информационные потоки, в которых присутствует конфиденциальная информация: служебная тайна, персональные данные, коммерческая тайна.

Вид тайны будет определять современную систему требований к системе защиты информации (СЗИ) СЭД. Так при наличии в СЭД служебной тайны (служебной информации ограниченного распространения) необходимо применять Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утв. приказом ФСТЭК России 2013 г. № 17) а таже [2].

При наличии в СЭД персональных данных необходимо применять Требования к защите персональных данных при их обработке в информационных системах персональных данных (утв. постановлением Правительства РФ от 1 ноября 2012 г. N 1119) а также документ « Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. приказом ФСТЭК России 2013 г. № 21).

При наличии в СЭД информации, составляющей коммерческую тайну могут использоваться как требования, применяемые для государственных информационных системах (утв. приказом ФСТЭК России 2013 г. № 17), так и требования стандартов серий ГОСТ Р ИСО/МЭК 27000 (27001, 27005 и др.) и ГОСТ Р ИСО/МЭК 15408.

Определённые особенности СЭД как объектов обеспечения ИБ организации планируется использовать в научных исследованиях и учебно-методических материалах в АлтГТУ.

Рисунок 1 – Общая модель взаимодействия субъектов СЭД

Перечень использованной литературы

1. Кузнецов С.Л. / Требования к системам электронного документооборота. Источник: журнал "Управление персоналом"http://www.klerk.ru/buh/articles/397298/

2. Требования к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающие в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения (Приложение к Приказу Министерства связи и массовых коммуникаций Российской Федерации от 02.09.2011 N 221) http://www.consultant.ru/search/?q=02.09.2011

3. Сабанов А.Г. Комплексная защита электронного документооборота . Оборонный комплекс. - научно-техническому прогрессу россии 1.2009. http://elibrary.ru/item.asp?id=180

4. Система автоматизации документооборота. Википедия. https://ru.wikipedia.org/wiki/D0

ЗАЩИЩЕННОЕ ХРАНЕНИЕ ДАННЫХ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ АЛЬТЕРНАТИВНЫХ ПОТОКОВ ФАЙЛОВОЙ СИСТЕМЫ NTFS В ОПЕРАЦИОННЫХ СИСТЕМАХ СЕМЕЙСТВА WINDOWS

Яковенко Р.А – студент, Сучкова Л.И. – к.т.н., профессор
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

В современном мире сложно представить жизнь без глобальной сети интернет. В последние годы с развитием интернета всё больше набирают популярность различные онлайн-сервисы в совершенно разных отраслях жизнедеятельности.

Современный человек стал активнее использовать ресурсы интернета, поэтому ему приходится регистрироваться на разных сайтах, что увеличивает угрозы потерь и утечек секретных данных, а также несанкционированного доступа к личным данным со стороны злоумышленников и мошенников.

На сегодняшний день самой востребованной операционной системой в мире является Windows 7. Статистика от Net Applications за сентябрь 2014 года показывает, что 52,71% рынка занимает именно эта операционная система. Поэтому проблема защищенного хранения данных в системах семейства Windows является актуальной.

Исходя из вышеизложенного, была поставлена цель – реализовать надежное и удобное в использовании хранилище секретных данных в файловой системе NTFS в операционных системах семейства Windows.

Хранение данных можно организовать по-разному, и каждый способ имеет свои достоинства и недостатки:

1) Хранение информации в файлах является распространенным способом, однако тогда увеличивается риск реализации угроз несанкционированного воздействия на файл [1].

2) Хранение данных в реестре затрудняет обнаружение ценной информации, но и не исключает возможности воздействия на нее со стороны злоумышленника [2].

3) Хранение защищаемой информации на съемном носителе не исключает угроз хищения и потери самого носителя, данные которого позже могут быть вскрыты [3].

4) Хранение данных в так называемых альтернативных потоках (Alternate Data Streams), файловой системы NTFS является достаточно надежным способом хранения секретных данных, хотя и допускает утечку информации [4]. Альтернативные потоки данных – это метаданные, связанные с объектом файловой системы NTFS.

Предложен способ защищенного хранения секретных данных на основе имеющейся особенности системного файла $Repair в системном каталоге $RmMetadata файловой системы NTFS операционной системы Windows 7.

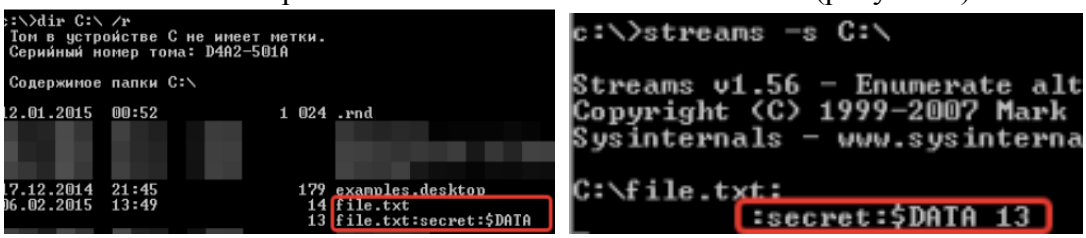
В Windows 7, а также Vista, на разделе NTFS имеется набор системных файлов, которые скрыты, и доступ к которым запрещён. Например, скрытыми системными файлами в корне диска C являются $AttrDef, $Bitmap, $Boot, $LogFile, $MFT, $Secure, $Volume, $Extend.

Интерес для защищенного хранения представляет системный файл $Repair, который размещается в системной папке $RmMetadata.

Вообще говоря, доступ к системным файлам, а также к их альтернативным потокам, блокируется на уровне драйвера ntfs.sys. Однако альтернативные потоки файла $Repair доступны как для чтения, так и для записи. Тогда возможно хранить в защищённой системной папке свои данные, пусть даже не в виде файлов, а в виде метаданных.

При помощи системных команд Windows echo и more существует возможность реализации ввода и вывода информации в альтернативные потоки системного файла $Repair. Для выполнения таких операций необходимо знать наименование альтернативного потока.

Было проведено исследование по обнаружению наименований потоков в обычном файле. Для этого на диске C был создан файл file.txt и к нему поток secret. В результате, метаданные были обнаружены командой dir с атрибутом /R, утилитой streams.exe, программами NTFS Stream Explorer 2.1.1 и AlternateStreamView 1.50 (рисунок 1).



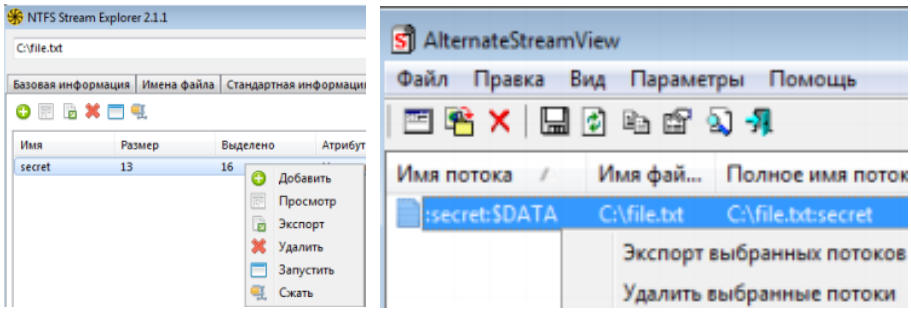


Рисунок 1 – Обнаружение метаданных обычного файла

Было проведено исследование по обнаружению наименований потоков системного файла $Repair, который размещен по пути «C:\$Extend\$RmMetadata». Для этого также был создан поток secret в $Repair. В итоге, никакой программой не удалось обнаружить метаданные системного файла на прикладном уровне операционной системы (рисунок 2).

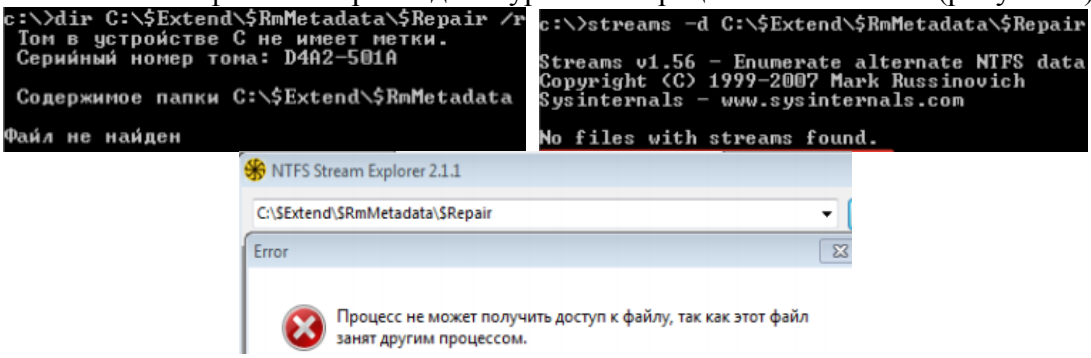


Рисунок 2 – Отказ в обнаружении ADS файла $Repair

Преимущество хранения информации в альтернативных потоках системного файла $Repair заключается в том, что потоки не доступны для обнаружения ни при помощи командной строки (CMD), ни программами streams, NTFS Stream Explorer, AlternateStreamView и другими.

На прикладном уровне отсутствует возможность получения сведений о наименовании потоков $Repair. Однако существует угроза вскрытия данных системного файла при помощи программных средств низкоуровневого доступа к памяти: WinHex, DiskEdit, DMDE и другие. Такая проблема решаема при помощи шифрования содержимого альтернативных потоков и маскировка их наименований под символы иероглифов, как показано на рисунке 3.

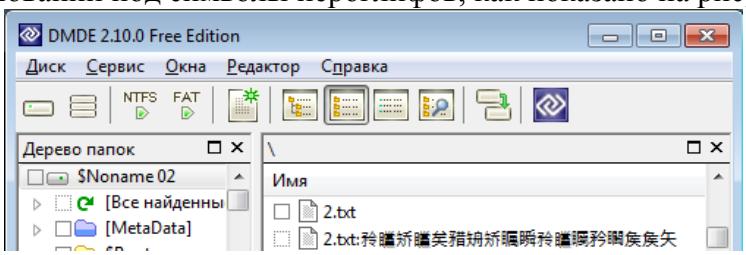


Рисунок 3 – Отображение имен метаданных, заданных иероглифами

Если наименования будут в виде иероглифов, то злоумышленнику придется искать и подбирать определенные иероглифы, что существенно затрудняет доступ нарушителя.

Определены важные требования к защищенному хранению секретных данных:

1) Обеспечение конфиденциальности информации, что гарантирует недоступность защищаемых данных сторонним лицам;

2) Обеспечение целостности информации, что гарантирует недопустимость повреждений и искажений защищаемых данных со стороны злоумышленника;

3) Обеспечение доступности информации, что гарантирует своевременный беспрепятственный доступ пользователей к интересующей их своей информации.

Очевидно, что все три критерия выполнены в силу того, что имена потоков не могут быть известны. А известная атака перебора «грубой силой», возможна только лишь при коротких именах.

В результате, был сделан вывод о том, что системный файл $Repair является достаточно надежным защищенным хранилищем секретных данных, потому что, если не знать наименования потока, то невозможно будет получить его данные.

Так как надежное хранилище данных выявлено, то необходимо наличие программы, которая бы смогла выполнять процедуры чтения и записи информации в отношении хранилища данных. Поэтому была разработана программа на языке программирования C# с удобным графическим интерфейсом.

При помощи данной программы пользователь может добавить секретные данные в защищенное хранилище данных. Графический интерфейс разработанного приложения показан на рисунке 4.

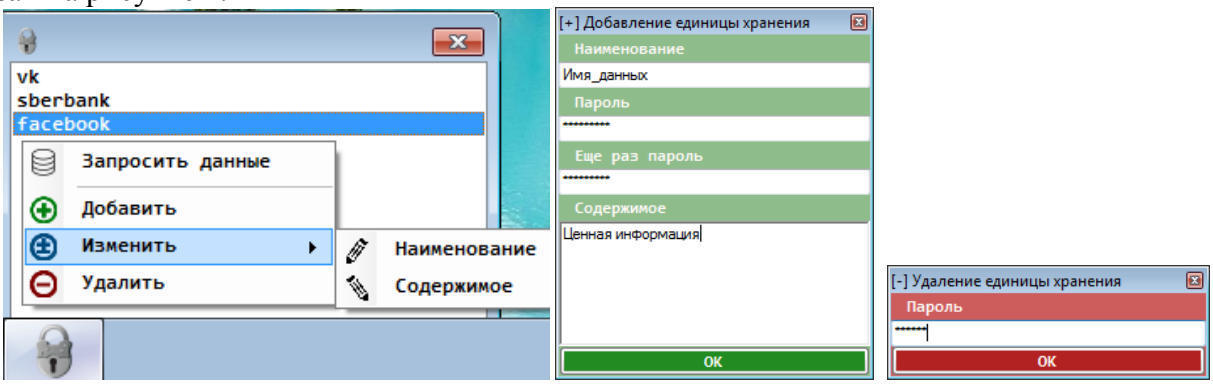


Рисунок 4 – Графический интерфейс разработанной программы

В программе реализованы механизмы шифрования алгоритмом DES-256 и маскировка имен альтернативных потоков под символы иероглифов.

Созданная программа позволяет не запоминать множество паролей к многочисленным аккаунтам. Например, пользователь сервиса сбербанк онлайн получил распечатку с учётными данными в свой личный кабинет. Каждый раз, когда нужно зайти в личный кабинет, он вынужден, если не помнит пароль, обращаться к распечатанным идентификационным данным. В этом есть два недостатка. Во-первых, хранение паролей на бумажных носителях подразумевает принятие мер по сокрытию носителя от сторонних лиц. Во-вторых, возможна потеря распечатанных данных. Поэтому решением таких проблем является размещение паролей в защищенном хранилище.

Чтобы получить данные достаточно запустить программу, затем в списке выбрать имя нужной единицы хранения и нажать Enter, затем ввести пароль, и секретные данные помещаются в буфер обмена данных. В программе предусмотрена очистка данных. При создании единиц хранения в качестве пароля можно использовать свой пароль, который всегда известен.

Таким образом, разработано приложение, позволяющее защищено хранить данные в альтернативных потоках файловой системы NTFS в операционных системах семейства Windows.

Список использованной литературы:

1. Как хранить настройки программ [Электронный ресурс]. – Электрон. текст. дан. – Режим доступа: http://www.codenet.ru/progr/delphi/stat/config.php - Загл. с экрана.

2. Безопасность и реестр (Visual Basic) [Электронный ресурс]. – Электрон. текст. дан. – Режим доступа: https://msdn.microsoft.com/ru-ru/library/2fehd64c.aspx - Загл. с экрана.

3. Как хранить файлы [Электронный ресурс]. – Электрон. текст. дан. – Режим доступа: http://takbezopasno.ru/kak-hranit-faily - Загл. с экрана.

4. Альтернативные потоки данных в NTFS или как спрятать блокнот [Электронный ресурс]. – Электрон. текст. дан. – Режим доступа: http://geektimes.ru/post/46935/ - Загл. с экрана.