ВЫБОР ОПТИМАЛЬНОЙ МОДИФИКАЦИИ ПРОТОКОЛА STP ДЛЯ КОНФИГУРИРОВАНИЯ ОБОРУДОВАНИЯ ПРОВАЙДЕРА

Алексеев Д.Р. - студент, Чугунов Г.А. – старший преподаватель
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Современные топологии связи оборудования в сети требуют множественных связей. Для увеличения пропускной способности каналов и повышения их надежности используется агрегирования каналов. Все это приводит к появлению петель на канальном уровне модели OSI. Для того что бы множественные связи привести к древовидной топологии, исключить циклы кадров был разработан протокол STP. Данный протокол имеет различные модификации и позволяет автоматически блокировать не нужные в данный момент для полной связности порты.

Spanning Tree Protocol — сетевой протокол, работающий на втором уровне модели OSI. Основной задачей STP является приведение сети Ethernet с множественными связями к древовидной топологии, исключающей циклы пакетов. Протокол описан в стандарте IEEE 802.1D.

Для разграничения физической и логической топологии используются VLAN. Среди различных вариантов протоколов STP встречаются стандарт 802.1Q. Стандарт 802.1Q, определяет, каким образом VLAN передаются внутри канала. Кроме того, он определяет один процесс STP для всех VLAN. BPDU по каналам передаются нетегированными (в native VLAN). Этот вариант STP известен как CST (Common Spanning Tree). Наличие только одного процесса для всех VLAN очень облегчает работу по конфигурированию и разгружает процессор коммутатора, но, с другой стороны, CST имеет недостатки: избыточные связи между коммутаторами блокируются во всех VLAN, что не всегда приемлемо и не дает возможности использовать их для балансировки нагрузки.

Cisco разработала свою собственную версию протокола STP — PVST (Per-VLAN Spanning Tree) — которая предназначена для работы в сети с несколькими VLAN. В PVST для каждого VLAN существует свой процесс STP, что позволяет независимую и гибкую настройку под потребности каждого VLAN, но самое главное, позволяет использовать балансировку нагрузки за счет того, что конкретная физическая связь может быть заблокирован в одном VLAN, но работать в другом. Минусом этой реализации является, конечно, проприетарность: для функционирования PVST требуется проприетарный же ISL канал между коммутаторами.

Также существует вторая версия этой реализации — PVST+, которая позволяет наладить связь между коммутаторами с CST и PVST, и работает как с ISL- каналом, так и с 802.1q. PVST+ это протокол по умолчанию на коммутаторах Cisco.

VLAN это довольно удобный инструмент для многих целей, и поэтому, их может быть достаточно много даже в небольшой организации. Некоторая избыточность вариаций с отдельным экземпляром STP для каждой VLAN состоит в том, что если топология нескольких VLAN совпадает, то соответствующие им экземпляры STP полностью повторяют работу друг друга. В таком случае в принципе ненужная работа по сути дублирующих друг друга экземпляров STP оборачивается ненужной дополнительной нагрузкой на процессор коммутатора, и в конечном счете может вынудить конструкторов оборудования для обеспечения его устойчивой работы выбирать более мощный процессор с большим энергопотреблением, что может повлечь за собой дополнительные затраты на электропитание и охлаждение, как при изготовлении оборудования, так и эксплуатации.

В этом отношении отдельно стоит Multiple STP (MSTP). В один экземпляр MST могут входить несколько виртуальных сетей, при условии, что их топология одинакова (в смысле входящих в VLAN коммутаторов и соединений между ними). Минимальное количество экземпляров MSTP соответствует количеству уникальных топологических групп VLAN в домене второго уровня (опять же на уровне коммутаторов и соединений между ними). MSTP накладывает важное ограничение: все коммутаторы, участвующие в MSTP, должны иметь

одинаково сконфигурированные группы VLAN (MST instances), что ограничивает гибкость при изменении конфигурации сети. RSTP (Rapid STP, англ. Rapid spanning tree protocol, быстрый протокол разворачивающегося дерева), он же IEEE 802.1W-2001 и IEEE 802.1D-2004— версия протокола STP с ускоренной реконфигурацией дерева, использующегося для исключения петель (исключения дублирующих маршрутов) в соединениях коммутаторов Ethernet с дублирующими линиями.

Принцип работы в общих чертах похож на STP: выбирается корневой коммутатор (англ. root switch), затем каждый коммутатор, участвующий в построении дерева, ищет кратчайший маршрут (с учётом пропускной способности канала) к корневому коммутатору через соседние коммутаторы (или напрямую). Линии, не попавшие в маршрут, переводятся в режим ожидания и не используются для передачи данных, пока работают основные линии. В случае выхода из строя основных линий, ожидающие линии используются для построения альтернативной топологии, после чего одна из линий становится активной, а остальные продолжают находиться в режиме ожидания.

В RSTP остались такие роли портов, как корневой и назначенный, а роль заблокированного разделили на две новых роли: Alternate и Backup. Alternate — это резервный корневой порт, а backup — резервный назначенный порт. Как раз в этой концепции резервных портов и кроется одна из причин быстрого переключения в случае отказа. Это меняет поведение системы в целом: вместо реактивной (которая начинает искать решение проблемы только после того, как она случилась) система становится проактивной, заранее просчитывающей “пути отхода” еще до появления проблемы. Смысл простой: для того, чтобы в случае отказа основного переключится на резервную связь, RSTP не нужно заново просчитывать топологию, он просто переключится на запасной, заранее просчитанный.

Ранее, для того, чтобы убедиться, что порт может участвовать в передаче данных, требовались таймеры, т.е. коммутатор пассивно ждал в течение означенного времени, слушая BPDU. Ключевым моментом RSTP стало введение концепции типов портов, основанных на режиме работы связи- full duplex или half duplex (типы портов p2p или shared, соответственно), а также понятия пограничный порт (тип edge p2p), для конечных устройств.

Исходя из вышесказанного, можно сделать вывод, что более удачной и подходящей модификацией протокола STP является протокол RSTP. Так как у него более удобная и простая конфигурация.

Список использованных источников:

1. Принцип работы протоколов STP/RSTP [Электронный ресурс] / Режим доступа: http://nsc-com.com/?page=155 , свободный.

2. STP [Электронный ресурс] / Режим доступа: http://xgu.ru/wiki/STP , свободный.

3. Обзор протокола RSTP [Электронный ресурс] / Режим доступа: http://www.akvilona.ru/serv/cisco/a_rstp.htm , свободный.

РАЗРАБОТКА МОДУЛЯ ДЛЯ КАРДИОДИАГНОСТИКИ НА БАЗЕ МИКРОСХЕМЫ ADS1298

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

Современная медицинская функциональная диагностика располагает самыми различными инструментальными методами исследования. Некоторые из них доступны только узкому кругу специалистов. Одним из распространенных и доступных методов исследования является холтер-мониторирование, используемое в основном в кардиологии [1-2]. Однако оно с успехом применяется и при исследовании больных с заболеваниями легких, почек, печени, эндокринных желез, системы крови, а также в педиатрии, гериатрии,

онкологии, спортивной медицине и в других случаях, когда заболевание может быть связано с проблемами в работе сердечно-сосудистой системы. Бывает и такая ситуация: у пациента есть жалобы, но они, допустим, возникают вечером (или в связи с какими-то событиями). Он записывается на прием к кардиологу, ему снимают электрокардиограмму (ЭКГ), и ничего не обнаруживают, потому что запись ЭКГ была проведена тот момент, когда особых жалоб у пациента не было. Дело в том, что стандартная запись ЭКГ - это как бы "моментальный снимок" деятельности сердца. На обычной ЭКГ может быть зафиксировано только несколько сокращений сердечной мышцы: от 3 до 10-20 (в зависимости от кардиографа). Но сердце человека делает около 100 тысяч сокращений в сутки. Людям, попавшим в такую ситуацию, когда симптоматика болезни проявляется эпизодически, или для постановки диагноза требуется длительное время наблюдения, может понадобиться холтеровский монитор (Холтер-монитор). Ежегодно с помощью холтеровского монитора производят обследования десятки тысяч больных. Этот метод в настоящее время стал достоянием широкого круга врачей – не только специалистов, занимающихся функциональной диагностикой, но и кардиологов, терапевтов, педиатров, спортивных врачей, физиологов и т. д.

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

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

Отличительные особенности и преимущества приборов серии ADS1298R заключаются в следующем.

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

Типовая схема включения ADS1298R приведена на рисунке 1. Для передачи данных с АЦП на ПК используется микросхема MCP2210, которая является преобразователем интерфейсов SPI в USB и типовая схема включения которой представлена на рисунке 2.

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

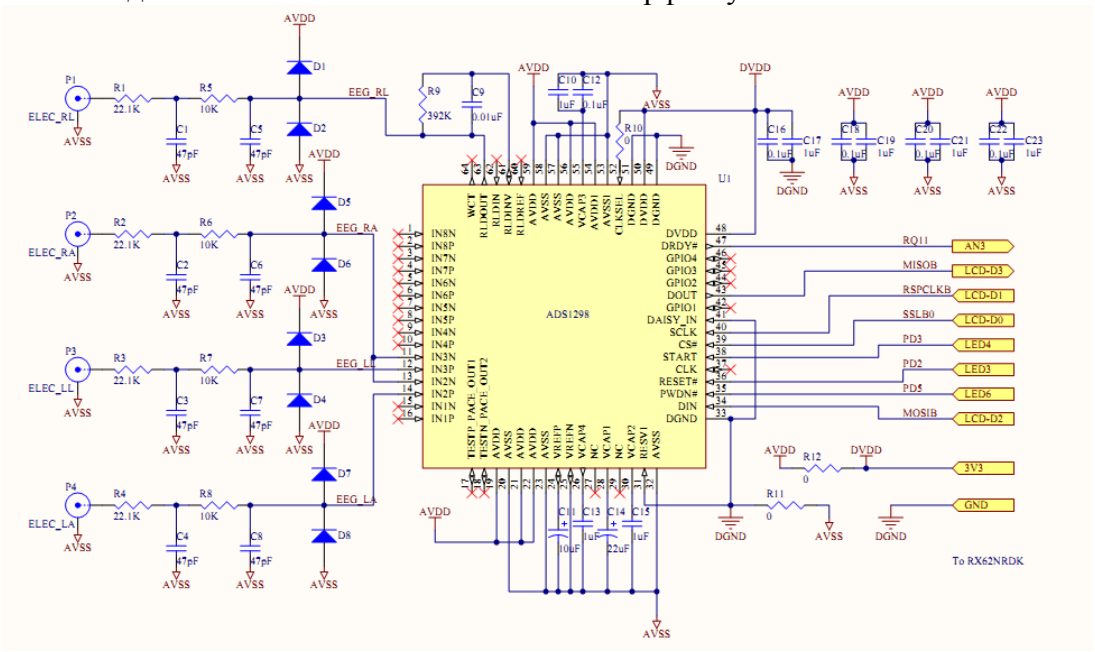


Рисунок 1. Рекомендуемая схема подключения АЦП.

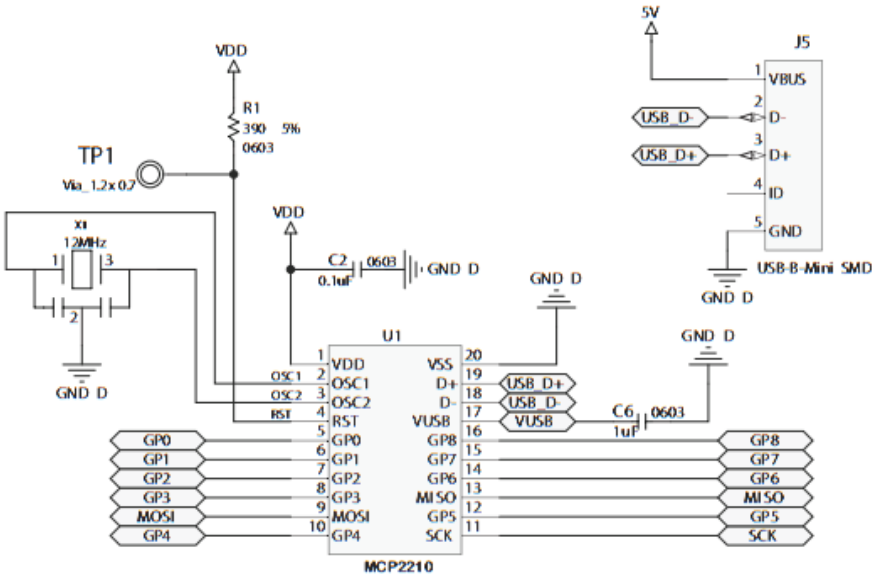


Рисунок. 2. Схема MCP2210.

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

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

ПРОТИВОДЕЙСТВИЕ КОМПЬЮТЕРНОМУ ТЕРРОРИЗМУ

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

Глобализация информационных процессов, а также современной экономики, насыщенность ее новыми информационно-телекоммуникационными технологиями, информатизация таких жизненно важных сфер деятельности общества, как связь, энергетика, транспорт, системы хранения газа и нефти, финансовая и банковская системы, водоснабжение, оборона и национальная безопасность, открыла не только доселе новые впечатляющие возможности для прогрессивного развития человечества, но и вызвала одновременно ряд качественно новых глобальных угроз. Появилась преступность, связанная с электронной обработкой данных, в том числе и преступность террористической направленности.

По мнению специалистов, терроризм с использованием последних достижений в сфере высоких технологий не менее опасен, чем ядерный или бактериологический терроризм.

Термин кибертерроризм был предложен в 1980-х годах старшим научным сотрудником Института безопасности и разведки США Барри Коллином. Кибертерроризм – это новая форма терроризма, которая для своих террористических целей использует компьютеры и электронные сети, современные информационные технологии. По своему механизму, способам совершения и сокрытия компьютерные преступления имеют определенную специфику, характеризуются высоким уровнем латентности и низким уровнем раскрываемости.

Кибертерроризм – это многогранный феномен, обусловленный во многом бесконтрольным использованием глобальных сетей, недостаточным вниманием со стороны государства, гражданского общества и спецслужб к данному сегменту политики, проявляющийся в атаках на компьютеры, компьютерные программы и сети или находящуюся в них информацию, с целью создания атмосферы страха и безысходности в обществе во имя достижения целей и интересов субъектов террористической деятельности, требующий объединения усилий мирового сообщества для эффективного противодействия ему [2].

Объектами кибератак в результате глобальной информатизации могут выступать практически все сферы человеческой жизни, но следует отличать действия обычных пользователей, которые используют сетевые ресурсы в целях пропаганды своих взглядов, нагнетания обстановки страха, напряженности и т.д., от действий хакеров-террористов.

Информационный террористический акт отличается от форм воздействия на киберпространство, прежде всего своими целями, которые остаются свойственными политическому террористическому акту. Средства осуществления информационно-террористических действий могут варьироваться в широких пределах и включать все виды современного информационного оружия. Некоторые из них: компьютерные программные закладки и вирусы, логические бомбы, троянские программы, программы-сниферы. В то же время тактика и приемы информационного террора существенно отличаются от тактики информационной войны и приемов информационного криминала. Главное состоит в том, чтобы террористический акт имел опасные последствия, стал широко известен населению и получил большой общественный резонанс [1].

В киберпространстве могут быть использованы различные приемы для совершения кибертеррakта:

1) получение несанкционированного доступа к государственным и военным секретам, банковской и личной информации;

2) нанесение ущерба отдельным физическим элементам информационного пространства, например, разрушение сетей электропитания, создание помех, использование специальных программ, стимулирующих разрушение аппаратных средств;

3) кража или уничтожение информации, программ и технических ресурсов путем преодоления систем защиты, внедрения вирусов, программных закладок и т.п.;

4) воздействие на программное обеспечение и информацию;

5) раскрытие и угроза публикации закрытой информации;

6) захват каналов СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;

7) уничтожение или активное подавление линий связи, неправильная адресация, перегрузка узлов коммуникации;

8) проведение инфомационно-психологических операций и т.п.

Эти приемы постоянно совершенствуются в зависимости от средств защиты, применяемых разработчиками компьютерных сетей.

Ущерб от террористических действий связан:

1) с человеческими жертвами или материальными потерями, вызванными деструктивным использованием элементов сетевой инфраструктуры;

2) с возможными потерями (в том числе гибелью людей) от несанкционированного использования информации с высоким уровнем секретности или сетевой инфраструктуры управления жизненно-важных (критических) для государства сферах деятельности;

3) с затратами на восстановление управляемости сети, вызванными действиями по ее разрушению или повреждению;

4) с моральным ущербом, как владельца сетевой инфраструктуры, так и собственного информационного ресурса;

5) с другими возможными потерями от несанкционированного использования информации с высоким уровнем секретности [3].

Решения проблемы компьютерного терроризма не просты и не однозначны. Кибертеррористы и их действия должны быть «привязаны» к законам. Это должно быть сделано в контексте как национальной, так и международной политики противодействия кибертерроризму. Серьезность террористической угрозы не может игнорироваться ни Россией, ни другими странами. Решимость принять необходимые меры может быть реализована в рамках новых эффективных международных законов и с новым воззрением на их действенность и применимость. Таким образом, решение проблемы борьбы с этими опасными явлениями на сегодняшний день это задача, которая требует объединения усилий, интеллектуального потенциала и доброй политической воли всего мирового сообщества.

Предупреждение кибертерроризма должно осуществляться одновременно в нескольких направлениях:

1) стратегическое направление, которое будет включать в себя долгосрочное прогнозирование кибертеррористической активности с определением возможных субъектов, также прогнозирование глобальных явлений и процессов в международном сообществе, обладающих кибертеррористическим эффектом;

2) выявление объектов и субъектов кибертерроризма, его причин, а также способов и иных обстоятельств, предотвращение кибертеррористических актов, которые могли бы быть совершены в ближайшее время или в недалеком будущем;

3) выявление и пресечение актов кибертерроризма по отношению к государственным и общественным деятелям, выявление и задержание кибертеррористов не только рядовых исполнителей и пособников, но и организаторов и вдохновителей террора, предание их к суду;

4) предупреждение, выявление, предотвращение и пресечение сходных с кибертерроризмом преступлений, как посягательство на жизнь лица, ведущего расследование кибердиверсии, киберэкстремизм.

В рамках ООН и ее учреждений принят ряд международно-правовых документов по различным аспектам предотвращения компьютерного терроризма. Совет Европы в 2001 г. принял Конвенцию «О киберпреступности». В течении 2001-2005 гг. Россия активно участвовала в разработке проекта Конвенции Совета Европы 2005 г. «О предупреждении терроризма» и первой ратифицировала ее 21 апреля 2006 г.

Указом Президента РФ от 15 января 2013 г. на ФСБ России возлагаются полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы РФ, информационные системы и информационно-телекоммуникационные сети, находящиеся на территории РФ и в дипломатических представительствах и консульских учреждениях РФ за рубежом.

Ведущие мировые державы признают, что угроза компьютерного терроризма является актуальной проблемой современности глобального характера, причем она будет неуклонно нарастать по мере развития и распространения информационных технологий. Поэтому эффективное международное сотрудничество в области предупреждения и ликвидации последствий кибератак имеет огромное значений.

Список использованной литературы:

1. Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия [Электронный ресурс]. – Режим доступа: http://www.tusur.ru/filearchive/reports-magazine/2010-1/41-45.pdf, свободный (дата обращения: 4.04.2014).

2. Голубев В.А. Кибертерроризм как новая форма терроризма [Электронный ресурс]. – Режим доступа: http://www.crime-research.org/library/Gol_tem3.htm, свободный (дата обращения: 4.04.2014).

3. Васенин В.А. Информационная безопасность и компьютерный терроризм [Электронный ресурс]. Режим доступа: http://www.crime-research.ru/articles/vasenin, свободный (дата обращения: 4.04.2014).

ПРИМЕНЕНИЕ ИНФОРМАЦИОННО-ПРАВОВЫХ СИСТЕМ ПРИ ЗАЩИТЕ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

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

С развитием человечества, появлением большого количества информации люди стали нуждаться в структурированных хранилищах данных, которые содержали бы в себе все документы и интерфейс был бы организован так, чтобы любому пользователю было удобно и просто работать с этими документами. Как результат такой потребности появился особый вид программного обеспечения, включающий в себя совокупность различных информационных технологий - информационные системы (ИС).

Термин «информационная система» можно рассматривать как в широком, так и в узком смысле слова. В широком смысле информационная система есть совокупность технического, программного и организационного обеспечения, а также персонала, предназначенная для того, чтобы своевременно обеспечивать надлежащих людей надлежащей информацией.

Также в достаточно широком смысле трактует понятие информационной системы Федеральный закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: «информационная система — совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств»

Одно из определений ИС дал М. Р. Когаловский: «информационной системой называется комплекс, включающий вычислительное и коммуникационное оборудование, программное обеспечение, лингвистические средства и информационные ресурсы, а также системный персонал и обеспечивающий поддержку динамической информационной модели некоторой части реального мира для удовлетворения информационных потребностей пользователей».

В узком смысле информационной системой называют только подмножество компонентов ИС в широком смысле, включающее базы данных, СУБД и специализированные прикладные программы. ИС в узком смысле рассматривают как программно-аппаратную систему, предназначенную для автоматизации целенаправленной деятельности конечных пользователей, обеспечивающую, в соответствии с заложенной в неё логикой обработки, возможность получения, модификации и хранения информации [1].

Информационная система накапливает и перерабатывает поступающую нормативную, плановую и учетную информацию в аналитическую информацию, которая служит основой для прогнозирования развития системы управления, корректировки целей и планирования нового цикла воспроизводства. К обработке информации в информационной системе предъявляются следующие требования:

- полнота и достаточность информации;
- своевременность представления информации;
- достоверность информации;
- экономичность обработки информации;
- адаптивность к изменяющимся информационным потребностям пользователей[2].

Классификации информационных систем

Классификация по архитектуре

- настольные (desktop), или локальные ИС, в которых все компоненты (БД, СУБД, клиентские приложения) находятся на одном компьютере;
- распределённые (distributed) ИС, в которых компоненты распределены по нескольким компьютерам.

Классификация по степени автоматизации

- автоматизированные: информационные системы, в которых автоматизация может быть неполной (то есть требуется постоянное вмешательство персонала);
- автоматические: информационные системы, в которых автоматизация является полной, то есть вмешательство персонала не требуется или требуется только эпизодически.

Классификация по характеру обработки данных

- информационно-справочные, или информационно-поисковые ИС, в которых нет сложных алгоритмов обработки данных, а целью системы является поиск и выдача информации в удобном виде;
- ИС обработки данных, или решающие ИС, в которых данные подвергаются обработке по сложным алгоритмам. К таким системам в первую очередь относят автоматизированные системы управления и системы поддержки принятия решений [1].

Проводя обзор по видам ИС, можно выделить одно из направлений - справочно-правовое обеспечение. К таковым относиться система «Гарант».

«Гарант» — справочно-правовая система по законодательству Российской Федерации, разрабатываемая компанией «Гарант-сервис-университет», первая массовая коммерческая справочно-правовая система в России [3]

Казалось бы, как «Гарант» связан с информационной безопасностью? Но в законах множество статей, которые, так или иначе, связаны с информационной безопасностью, и при этом «Гарант» постоянно обновляет базу данных, и можно всегда обратиться к документу со всеми изменениями, например:

1. Федеральный закон от 3 апреля 1995 г. N 40-ФЗ "О федеральной службе безопасности"

Статья 11.2.

Обеспечение информационной безопасности

Обеспечение информационной безопасности - деятельность органов федеральной службы безопасности, осуществляемая ими в пределах своих полномочий:

- при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;
- при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, сетей связи специального назначения и иных сетей связи, обеспечивающих передачу шифрованной информации, в Российской Федерации и ее учреждениях, находящихся за пределами Российской Федерации.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ

Глава 28. Преступления в сфере компьютерной информации

Статья 272. Неправомерный доступ к компьютерной информации

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

3. Доктрина информационной безопасности Российской Федерации, 2000 год;

Таким образом, информационные системы, такие как, например система «Гарант», могут обеспечить качественный поиск интересующей информации, затрагивающей различные области деятельности человека и в первую очередь правовое обеспечение в области защиты информации и нахождение требований и рекомендаций при обеспечении технической защиты объектов информатизации.

Список использованной литературы:

1. Информационные системы [Электронный ресурс].-Электрон. текст. дан. – Режим доступа: http://ru.wikipedia.org/wiki/Информационная_система

2. Информационные системы – лекция [Электронный ресурс].-Электрон. текст. дан. – Режим доступа: http://webcache.googleusercontent.com/search?q=cache:http://edu.dvgups.ru/METDOC/ITS/STRPRO/INF_TEH_STR/METOD/SULDIN/frame/5.htm

3. Гарант (справочно-правовое обеспечение) [Электронный ресурс].-Электрон. текст. дан. – Режим доступа: http://ru.wikipedia.org/wiki/Гарант_(справочно-правовая_система)

РАЗРАБОТКА ОБУЧАЮЩЕЙ ПРОГРАММЫ ПО РАБОТЕ С СИСТЕМОЙ МОДЕЛИРОВАНИЯ ЭЛЕКТРИЧЕСКИХ СХЕМ

Бурмин Я.В. - студент, Борисов А.П. – к.т.н., доцент

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

Для обслуживания цифровой техники, тем более, для ее ремонта и разработки, требуются специалисты, досконально знающие принципы работы цифровых устройств и систем, базовые элементы цифровой электроники, типовые схемы их включения, правила взаимодействия цифровых узлов, способы построения наиболее типичных цифровых устройств.

В настоящее время были разработаны методические рекомендации для выполнения лабораторных работ для направления подготовки бакалавров «Информационная безопасность» по дисциплинам «Электротехника», «Электроника и схемотехника», «Основы радиотехники» [2-5] для программного обеспечения «NI Multisim».

На данный момент проведен анализ стандартов трех дисциплин: «Электротехника», «Электроника и схемотехника», «Основы радиотехники». Выполнены требования и

рекомендации к содержанию и организации лабораторных заданий и программного обеспечения. Выполнен анализ программных продуктов аналогового и цифрового схемотехнического моделирования. Произведен выбор программного обеспечения для выполнения лабораторных работ. Для успешного выполнения работ выбрано программное обеспечение для моделирования электрических схем TINA-TI [1] и Logisim. Logisim - инструмент позволяющий разрабатывать и моделировать цифровые электрические схемы используя графический интерфейс пользователя. TINA-TI представляет собой обычный SPICE-симулятор с простым, интуитивно понятным графическим интерфейсом, позволяющим освоить программу в кратчайшие сроки. Данный софт не имеет каких-либо ограничений на число используемых устройств и узлов, без проблем справляется с комплексными работами, идеально подходит для моделирования поведения различных аналоговых схем и импульсных источников питания. При помощи TINA-TI возможно «с чистого листа» создать проект любой сложности, объединить фрагменты уже готовых решений, проверить и определить некоторые качественные показатели схемы.

Также были разработаны лабораторные работы с использованием выбранного программного обеспечения по дисциплине «Электротехника» [6]. Общий вид программ TINA-TI и Logisim приведен на рисунке 1. Пример выполненной схемы в TINA-TI приведен на рисунке 2.

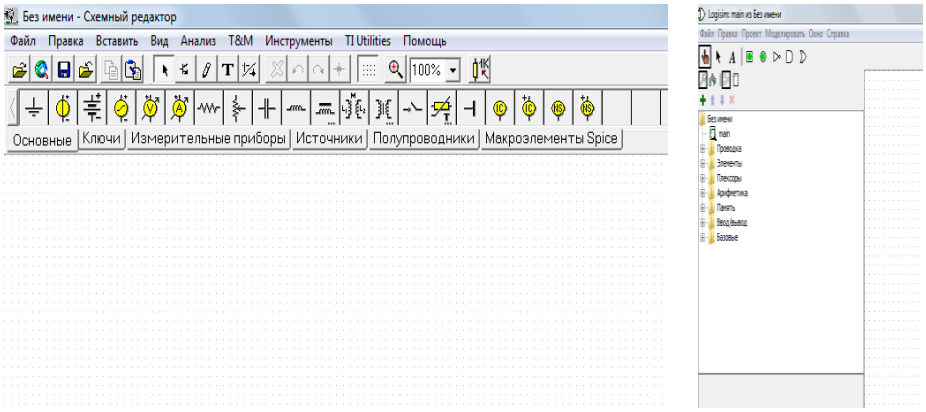


Рисунок 1 - Общий вид программ TINA-TI и Logisim

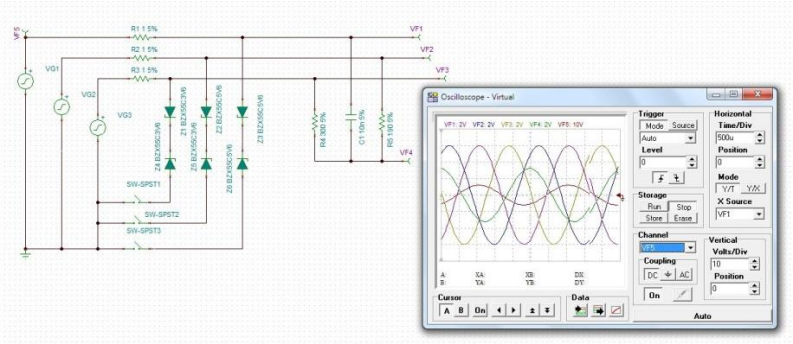


Рисунок 2 - Пример выполненной схемы в TINA-TI

Для разработки методических рекомендаций, удовлетворяющих требованиям стандартов, проведен их анализ и выявлены лабораторные, нуждающиеся в модернизации. Для разработки методических рекомендаций, удовлетворяющих требованиям стандартов, проведен их анализ и выявлены лабораторные, нуждающиеся в модернизации. Данные лабораторные работы должны проводиться в аудиториях, оборудованными рабочими стендами. Во время лабораторных занятий некоторые студенты не успевают выполнить предложенные лабораторные работы и чтобы невыполненные работы не остались у них долгом, им предлагается доделать эти лабораторные работы самостоятельно, с помощью программы для моделирования электрических схем. Для этого подобрана программа, которая является бесплатной и проста в использовании.

Данные программы являются простыми в своем использовании, с простым и интуитивно понятным графическим интерфейсом. Так же эти программы свободно-распространяемые, и пользователю не нужно будет плотить за их использование денежных средств.

Список использованной литературы:

1. Программное обеспечение TINA-TI [Электронный ресурс] / Режим доступа http://cxem.net/software/tina.php свободный.
2. Образовательный стандарт учебной дисциплины Б.3.Б.13 «Электротехника» 090900 Информационная безопасность.
3. Образовательный стандарт учебной дисциплины Б.3.Б.14 «Электроника и схемотехника» 090900 Информационная безопасность
4. Образовательный стандарт учебной дисциплины Б.3.Б.31. «Основы радиотехники» 090900 Информационная безопасность
5. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 090900 «Информационная безопасность» (квалификация (степень) «бакалавр»).
6. Опадчий Ю.Ф., Глудкин О.П., Гуров А.И. Аналоговая и цифровая электроника. /Полный курс/: Учебник для вузов /Под ред. Глудкина О.П. -М.: Горячая линия - Телеком, 2002. - 768 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)

По мере развития общества ценность информации неуклонно возрастает. Государственные секреты, наукоемкие ноу-хау, коммерческие, юридические и врачебные тайны все чаще доверяются компьютеру, который, как правило, подключен к локальным и корпоративным сетям. Популярность глобальной сети Интернет, с одной стороны, открывает огромные возможности для электронной коммерции, но, с другой стороны, создает потребность в более надежных средствах безопасности для защиты корпоративных данных от доступа извне. Но не смотря на это остается актуальным непосредственный контроль доступа в помещения, в которых осуществляется хранение и обработка информации. С этой задачей справляются системы контроля и управления доступом.

В настоящие время основным способом разграничения доступа в помещение являются обычные замки, или наличие охранников, или сторожей на входе в здание. По мере развития техники СКУД также развивались и на данный момент повсеместно вводят в эксплуатацию турникеты с бесконтактными картами, или электромеханические замки с использованием контактной памяти.

Основным недостатком таких систем является отчужденность носителя ключей от самого ключа (человека от ключа), или простота взлома замков, по средствам подмены или кражи ключей. Этого недостатка лишены системы работающие в отрыве от носителей, системы использующие биологические характеристики человеческого организма.

Термин "биометрия" обозначает измерение некоторых анатомических или физиологических параметров человека. Если обыкновенный пароль можно украсть или подобрать, то обмануть биометрическую систему практически невозможно. На текущий момент в качестве измеряемых параметров используют различные человеческие черты, такие как голос, отпечатки пальцев, радужная оболочка глаз, почерк и стиль нажатий на клавиши, а также внешний вид. Каждая из этих характеристик позволяет выделить конкретного человека из десятков, сотен и более людей. Также возможно комплексное использование нескольких параметров.

Преимущества биометрических систем безопасности очевидны [2]: уникальные человеческие качества хороши тем, что их трудно подделать, трудно оставить фальшивый отпечаток пальца при помощи своего собственного или сделать радужную оболочку своего глаза похожей на чью- то другую. В отличие от бумажных идентификаторов (паспорт, водительские права, удостоверение личности), от пароля или персонального идентификационного номера (ПИН), биометрические характеристики не могут быть забыты или потеряны, в силу своей уникальности они используются для предотвращения воровства или мошенничества. Некоторые люди умеют имитировать голоса, но, это требует особых навыков, которые не часто повстречаешь в обыденной жизни. В качестве измеряемого параметра, используемого для идентификации, в данной работе будет использоваться голос человека.

В практической работе будет использована схема системы представленная на рисунке 1.

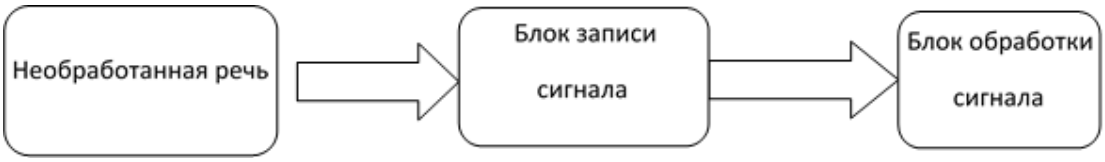


Рисунок 1 — Блок схема устройства

Для обработки голоса [1] необходимо предварительно его записать в оперативную память компьютера или машинный носитель, для этого предназначен блок записи сигнала. Он представляет собой устройство состоящие из микрофона с усилителем, фильтра и аналогово-цифрового преобразователя (рисунок 2).

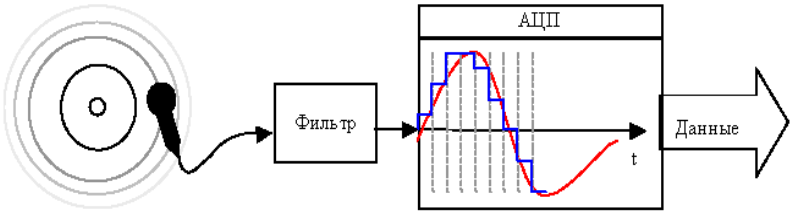


Рисунок 2 — Блок схема блока записи сигнала

Цифровой сигнал передается в память компьютера, на вход блока обработки сигнала. Блок обработки сигналов представляет собой программу схема, которой представлена на рисунке 3.

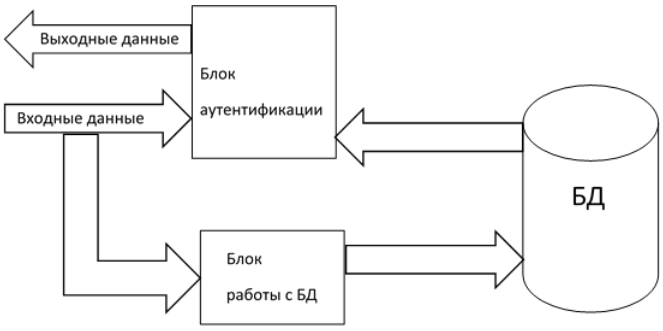


Рисунок 3 – Схема программы

На вход программы подается записанный голос. В зависимости от режима работы программы либо происходит запись в БД информации, либо происходит чтение из базы данных информации и сравнение ее с входными данными.

Блок аутентификации фильтрует входные данные от шумов, спектральное преобразование сигнала, фильтрация спектра, и наложение на него окна Кайзера, непосредственное сравнение с эталонными образцами в базе данных и выдача сигнала на оконечное устройство.

Блок работы с базой данных предназначен для добавления и удаления пользователей и просмотра статистики.

В базе данных программы хранится образец голоса, статическая информация о лицах, допущенных в помещение информация о пользователях системы.

В конце выполнения работы планируется создать законченное программно-аппаратное средство защиты информации – систему контроля и управления доступом на основе голосовой аутентификации. В комплекс будет входить оконечное устройство – блок записи сигналов и программа для работы администратора.

Список использованной литературы:

1. Идентификация пользователя по голосу [Электронный ресурс] – Режим доступа: habrahabr.ru/post/144580

2. Попов М. Биометрические системы безопасности [Электронный ресурс]/М. Попов. – Электрон. текстовые дан. 2002. – 20 мая. Режим доступа: http://daily.sec.ru/2002/05/20/print-Biometricheskie-sistemi-bezopasnosti.html

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМА НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

ДульцевД.В. – студент, Ленюк С.В. – к.ф.-м.н., доцент

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

В последнее время все больше и больше внедряются в нашу повседневную жизнь информационные технологии. Вместе с огромной пользой новые технологии приносят и новые проблемы. Одной из них является проблема защиты информации от несанкционированного доступа. В связи с этим развиваются технологии защиты информации, развитие которых с некоторой точки зрения гораздо более критично, чем развитие непосредственно информационных технологий. Способов защиты информации существует очень много, но рассматриваться будет шифрование информации. Зашифрованную информацию можно свободно распространять по открытым каналам связи без боязни ее раскрытия и нелегального использования. Хотя такая защита не абсолютно надежна, и каждый из способов шифрования характеризуется своей стойкостью.

На сегодняшний день большинство национальных организаций приняли стандарты цифровой подписи, а ряд западных регламентирующих институтов увязали эти стандарты с использованием эллиптических кривых.

Эллиптические кривые являются одним из основных объектов изучения в современной теории чисел и криптографии. Эллиптическая криптография образует самостоятельный раздел криптографии, посвященный изучению криптосистем на базе эллиптических кривых.

В целом асимметричная криптография основана на сложности решения некоторых математических задач. Криптосистемы с открытым ключом, такие как алгоритм RSA, безопасны благодаря тому, что достаточно сложно разложить составное число на простые множители. При использовании алгоритмов на эллиптических кривых полагается, что не существует субэкспоненциальных алгоритмов для решения задачи дискретного логарифмирования в группах их точек. При этом порядок группы точек эллиптической кривой определяет сложность задачи. Для достижения такого же уровня безопасности как и в RSA требуются группы меньших порядков, что уменьшает затраты на хранение и передачу информации [4].

Следовательно, можно выделить основные достоинства эллиптической криптографии:

1. Гораздо меньшая длина ключа по сравнению к «классической» асимметричной криптографией [2].
2. Скорость работы эллиптических алгоритмов гораздо выше, чем у классических. Это объясняется как размерами поля, так и применением более близкой для компьютеров структуры бинарного конечного поля [2].

3. Из-за маленькой длины ключа и высокой скорости работы, алгоритмы асимметричной криптографии на эллиптических кривых могут использоваться в смарт-картах и других устройствах с ограниченными вычислительными ресурсами [2].

Большинство криптосистем современной криптографии естественным образом можно "переложить" на эллиптические кривые. Такие криптосистемы как:

1. **RSA** — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.
2. **Протокол Диффи-Хеллмана** (англ. Diffie-Hellman, DH) — криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи.
3. **ГОСТ Р 34.10-94** – российский стандарт, описывающий алгоритмы формирования и проверки электронной цифровой подписи. В настоящее время стандарт недействителен. Ему на замену пришел **ГОСТ Р 34.10-2001** уже основанный на эллиптических кривых. Сейчас действительным является стандарт **ГОСТ Р 34.10-2012.**
4. **MQV** — это аутентификационный протокол, базирующийся на алгоритме Диффи-Хеллмана. MQV предоставляет защиту против активных атак путем сочетания статического и временного ключей.

Однако не для всех схем этот переход дает выигрыш в стойкости. Например, для системы RSA и родственных ей систем, основанных на сложности задачи факторизации, это не усиливает схему. В то же время для схем, основанных на сложности задачи логарифмирования в дискретных полях, переход на эллиптические кривые позволяет существенно увеличить стойкость.

Вот некоторые примеры криптосистем на эллиптических кривых:

1. **ECDSA (EllipticCurve DSA)** является аналогом алгоритма цифровой подписи DSA (DigitalSignatureAlgorithm), реализованным с помощью эллиптических групп.
2. **ECDH(EllipticcurveDiffie–Hellman)**– аналог криптографический протокол Диффи-Хеллмана, реализованный с помощью эллиптических кривых.
3. **ECMQV(EllipticCurve MQV)** – аналог аутентификационного протокола MQV, реализованный на эллиптических кривых.

Исходя из выше изложенного, была поставлена цель – реализовать один из алгоритмов на эллиптических кривых. Был выбран криптографический протокол ECDH. Программа позволяет сформировать общий секретный ключ для осуществления связи между сторонами.

Реализация выполнена в среде MicrosoftVisualStudio 2013, язык программирования - C#.

Актуальность данной работы заключается в том, что превосходство эллиптической криптографией над «современной» ассиметричной неоспоримо. «Современная» криптография полагается на сложность двух задач: факторизации целых чисел и дискретного логарифмирования. В недалеком будущем, возможно, данные задачи получат простые решения, выполняемые за полиномиальное время. Это поставит под удар широко распространённые протоколы и методы шифрования данных. Поэтому специалисты в области информационной безопасности призывают индустрию информационных технологий начать поддерживать эллиптическую криптографию уже сегодня [3].

Данный программный продукт можно будет использовать при изучении курса «Криптографии», для наглядного изложения материала.

В перспективе рассматривается возможность реализации других алгоритмов на эллиптических кривых и поиск своих эллиптических кривых для осуществления шифрования.

Список использованной литературы:

1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. – М: Стандартинформ, 2012.

2. Эллиптическая криптография: теория / Хабрахабр [Электронный ресурс]. Режим доступа: http://habrahabr.ru/post/188958/ - Загл. с экрана.
3. Эксперты призывают готовиться к криптоапокалипсису/ Хабрахабр [Электронный ресурс]. Режим доступа: http://habrahabr.ru/post/188846/- Загл. с экрана.
4. Н. Смарт. Криптография. / Смарт Н. – Москва: Техносфера, 2005. 528 с.

МЕНЕДЖЕР ПРОЦЕССОВ И ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ КАК СРЕДСТВО ОБЕСПЕЧЕНИИЯ БЕЗОПАСНОСТИ СЕРВЕРОВ НА ОСНОВЕ Clear OS

Егораев А.А., Мартынов Д.Б., Фишер В.А. - студенты, Шарлаев Е.В. – к.т.н., доцент
Алтайский государственный технический университет им И.И. Ползунова (г. Барнаул)

В условиях современной реальности уже трудно представить какую-нибудь крупную компанию без сосредоточенного информационного управляющего ресурса — сервера, так как с каждым днем человек все более и более стремиться автоматизировать весь процесс своей работы. В офисах появляются множество компьютеров, нормальное функционирование которых без сервера представить сложно - растут вычислительные мощности, объемы информации растут еще быстрее и обходиться без файлового сервера или же просто интернет шлюза очень сложно и зачастую просто неудобно.

На серверах храниться множество информации, цену которой порой невозможно рассчитать, поэтому деятельность по обеспечению безопасности сервера выходит на первое место, ведь чем дороже на серверах информация, тем больше находиться желающих, которые хотят ею обладать. На сегодняшний день используются множество серверов, которые исполняют глобальное количество сервисов и процессов и далеко не секрет что практически каждый сервис имеет ту или иную уязвимость и найти ее дело времени. Уязвимости находят даже в тех сервисах, где их совсем и не ждешь. Без своевременного реагирования и устранения проблем, являющихся следствием ошибочно порождаемого программного продукта, о безопасности системы можно забыть.

Сложно представить какие страшные последствия понесет компания, если на ресурсы ее сервера проникнет злоумышленник. К наиболее вероятностным способам для проникновения злоумышленника на вычислительные ресурсы относиться выполнение задач, которые являются следствием не декларированных возможностей различного ПО, присутствия программных закладок или результатом действия вирусного программного обеспечения. Одним из возможных решений в обеспечении безопасности сервера является применение собственных менеджеров процессов, которые позволяют разграничить их между пользователями, контролировать действия, назначать привилегии и права. Однако использование менеджера процессов без связки с двухфакторной аутентификацией лишь немного затруднит и замедлит злоумышленника ведь количество эксплоитов и «дыр» растет и быть уверенным в том, что злоумышленник не сможет получить права суперпользователя, используя ту или иную «дыру» нельзя.

На сегодняшний день двухфакторная аутентификация [2] используется довольно часто в WEB сфере, но при удаленном доступе к данным сервера этот механизм защиты до сих пор является редкостью и как правило ограничивается лишь использованием электронных замков и Е-токенов.

Целью настоящего исследования является поиск наиболее безопасного соединения с удаленным сервером. В качестве объекта исследования выбрана вычислительная сеть на основе сервер на базе ClearOS с внешним подключением по SSH протоколу [1], т.е. использующее в качестве подключения клиента к серверу 22-ой программный порт.

Для начала необходимо сделать так, чтобы сервер при попытке подключения к нему клиента выглядел как обычный сервер, это поможет завести злоумышленника в заблуждение. Так же необходимо настроить подключение по SSH на контроль количества попыток ввода пароля, предпочтительно три раза, после чего отбрасываются все попытки соединения с

сервером, при этом необходимость занести ip-адресс устройства клиента, который пытался инициировать соединение в так называемый «бан лист» (черный список) на один час, что обезопасит от использования «брут перебора» неопытных атакующих и замедлит опытных, так как вызовет у них необходимость в использовании дополнительных промежуточных узлов составной сети, например прокси-серверов, для автоматизации и анализа каким образом сервер-цель сбрасывает соединение. Для усиления защитных механизмов также необходимо установить ограничение на количества одновременно подключенных клиентов. После применения данных настроек можно оставить конфигурирование SSH-параметров и перейти ко второй стадии защиты.

Вторым фактором усиленной аутоинтефикации является применение генерации случайных символов, а именно 6 символов. Программа реализована на языке C# с применением Mono. Это позволило реализовать универсальное приложение, которое можно использовать как на Unix платформах, так и на других. Приложение основано на клиент-серверной технологии. Серверная часть располагается непосредственно на самом сервере и работает как сервис, при ее запуске в конфигурационный файл записываются все запущенные приложения и закрывается к ним доступ ровно до того момента как сервис не пропустит к ним. Это позволяет оградить злоумышленника от интересующих файлов и ввести в легкое недоумение - ведь только что у него появилось окно приветствия подключения по SSH, а вслед за ним окно с 6 символами и окном ввода информации.

Рассмотрим работу серверной части поподробнее. Когда клиент подключается к серверу и проходит аутентификацию SSH, происходит генерация случайных символов, с комбинацией различных алгоритмов. Желательно использование не одного алгоритма генерации, а нескольких, в зависимости от времени или дня недели, например. День недели на мой взгляд намного лучше нежели время, так как его можно использовать как еще один символ, то есть у нас высвечивается на сервере окно с 6 символами плюс один скрытый который мы будем вводить после третьего видимого символа на нашем клиенте, при генерации кода на сервере это пройдет автоматически.

Обратим внимание на использование клиентского модуля. Клиентская часть используется как на Unix, так на Windows, но есть необходимость иногда подключиться к серверу моментально, используя, например, смартфон, поэтому клиентская часть адаптируется под андроид. Алгоритм работы клиентской части очень прост. Запускаем клиентскую часть, видим окно ввода, вводим в поля символы, которые представил нам сервер и не забываем, что после третьего символа должен идти символ, отвечающий за день недели, после чего клиентская часть выдает нам с генерированный по этим данным ключ для подключения. Вводим его в окно на сервере и получаем после этого доступ ко всем функциям системы. Подобрать такой с генерированный пароль довольно сложно, но все же лучше сделать следующее: ограничить количество попыток ввода двумя, после второй, неправильной попытки [3], будет происходить разрыв соединения с сервером и клиенту придётся заново осуществлять подключение и аутентификацию по SSH, при этом вновь произведётся генерация пароля уже нового, что сделает перебор невозможным

Данный способ прохождения аутентификации не делает сервер полностью безопасным, но он усложняет действия злоумышленников. А так как используется помимо двухфакторной аутентификации еще и менеджер процессов, то злоумышленнику придется потратить много времени и сил, чтобы проникнуть и получить нужные ему файлы.

Список использованной литературы:

1. Setting Up SSH Trust Between Two Servers [Электронный ресурс]. – Электрон. текст. дан. – Режим доступа:

http://www.clearcenter.com/support/documentation/clearos_guides/setting_up_ssh_trust_between_two_servers - Загл. с экрана.

2. Двухфакторная аутентификация [Электронный ресурс]. – Электрон. текст. дан. – Режим доступа: http://www.smspasscode.ru/product/two-factor-authentication - Загл. с экрана.

3. Контроль доступа [Электронный ресурс]. – Электрон. текст. дан. – Режим доступа: http://ru.wikipedia.org/wiki/Контроль_доступа_(информатика) - Загл. с экрана.

РАЗРАБОТКА СИСТЕМЫ АВТОМАТИЧЕСКОГО ДОЗИРОВАНИЯ ДЛЯ ЦИКЛОНА-ПЫЛЕОТДЕЛИТЕЛЯ

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

Современное мукомольное производство не может обойтись без автоматизации технологических процессов. Системы автоматического управления повышают производительность труда, безопасность производства, увеличивают выход продукции, снижают брак, экономят ресурсы. Используя современные средства автоматизации, можно на 10-15 лет продлить срок службы технологического оборудования. Но главное – без современных автоматических систем управления невозможно гарантировать качество выпускаемой продукции, а качество – это приоритетный критерий конкурентоспособности товара на рынке.

Инерционно-гравитационные пылеотделители (циклоны) применяются для сухой очистки больших объемов воздуха, конструктивные элементы которых обеспечивают вращательное или поступательное движение воздушного потока. По сравнению с другими пылеотделителями, циклоны обладают следующими преимуществами: простота конструкции, надежность и экономичность; удовлетворительная работоспособность, долговечность и ремонтопригодность; большая пропускная способность при сравнительно невысоких аэродинамических сопротивлениях.

Коэффициент очистки обычных циклонов может достигать 97%, а улучшенных и модернизированных конструкций на отдельных видах продукта даже 99% и выше. Следует отметить, что реальная эффективность очистки воздуха в циклонах в производственных условиях гораздо ниже (порядка 80%), что обусловлено различными причинами, одной из таких причин, например, может являться невыполнение условия по соответствию входной скорости оптимальному значению.

Дозирование сыпучих материалов [1] в настоящее время широко применяется в самых различных отраслях промышленности. В ряде технологических процессов дозирование является одной из основных операций. Качество готовой продукции и рациональное расходование исходных материалов во многом зависят от дозирования. В пищевой промышленности, например на весо-выбойных аппаратах, от дозирования зависит весь технологический процесс выбоя готового продукта.

Основным направлением в дозировании является максимальная механизация и автоматизация производственного потока, при обеспечении соответствующего сокращения цикла дозирования, повышения контроля за составлением смесей и точного соблюдения заданной рецептуры. Автоматизация дозирования способствует сокращению вспомогательного времени, обеспечивает более легкое управление дозирующими устройствами, снижает себестоимость продукции.

Экспериментальный циклон-пылеотделитель, разработанный на кафедре “Машины и аппараты пищевых производств” нашего университета, имеет коэффициент очистки более 99%, а также может применяться не только для очистки воздуха, но и для очистки муки от посторонних веществ, а также для разделения ее на фракции.

В общем виде состав системы автоматического управления можно представить следующим образом.

Программируемый логический контроллер (ПЛК) с управляющей программой является главным элементом системы. В качестве исполнительных устройств в системе служат два частотных преобразователя, позволяющие изменять скорости вращения вала асинхронного электродвигателя вентилятора и асинхронного электродвигателя дозатора соответственно.

Для успешной реализации системы было необходимо выбрать оборудование, соответствующее следующим требованиям:

– Программируемый логический контроллер должен обладать дисплеем, эргономичной клавиатурой, интерфейсом Modbus/RTU.

– Два асинхронных электродвигателя с числом номинальных оборотов, достаточных для управления процессами вентиляции и дозирования.

– Частотные преобразователи должны быть достаточной мощности для работы с выбранными асинхронными электродвигателями.

В качестве ПЛК был выбран SMH2010C [4] производства компании Segnetics - компактный, быстродействующий программируемый контроллер, предназначенный для операций управления в системах, требующих до 832 входов/выходов. Программное ядро, установленное на контроллере, позволяет при помощи специального инструментального пакета SMLogix [3], работающего под ОС семейства MS Windows, создавать пользовательские программы управления для контроллера на языке функциональных блоков (FBD) [2].

Для управления вентилятором был выбран асинхронный электродвигатель АДМ80А2У2 с номинальной мощностью 1,5 кВт и номинальными оборотами 2850 об/мин, а для управления дозатором - асинхронный электродвигатель АИМ63А4 с номинальной мощностью 0,5 кВт и номинальными оборотами 1350 об/мин. Оба двигателя имеют КПД 70%.

В качестве частотных преобразователей были выбраны преобразователи производства компании Delta серии VFD-E [5]. Данные преобразователи подходят для работы с выбранными электродвигателями.

Схема системы с учетом выбранных компонентов приведена на рисунке 1.

Рисунок 1 - Схема системы

Управляющая программа для ПЛК была разработана в среде SMLogix. Общий вид программы управления приведен на рисунке 2.

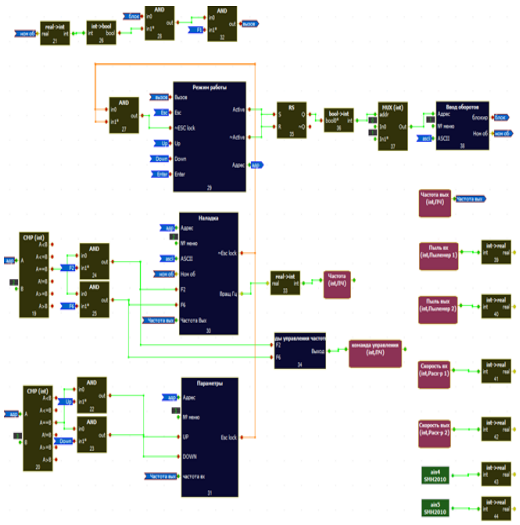


Рисунок 2 - Общий вид программы управления

При включении системы на экране ПЛК появляется приветственный диалог (рисунок 3), из которого с помощью нажатия кнопки F1 осуществляется переход в главное меню (рисунок 4). Основными элементами программы управления являются макросы: «Номинальные обороты», «Пуск двигателей», «Параметры», реализующие одноименные меню.

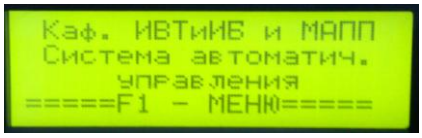


Рисунок 3 - Приветственный экран

Рисунок 4 - Главное меню

В меню «Номинальные обороты» осуществляется ввод номинальных оборотов двигателей. Осуществляется проверка корректности введенного значения. В меню «Пуск двигателей» имеется возможность установить желаемую скорость вращения валов двигателей и с помощью кнопок F2 и F3 запустить двигатели. В меню «Параметры» в ходе работы системы отображаются различные ее параметры.

Разработанная система автоматического дозирования позволяет обеспечить легкое и быстрое управление процессом дозирования с помощью циклона-пылеотделителя.

Список использованной литературы:

1. Видинеев Ю. Д. Автоматическое непрерывное дозирование сыпучих материалов. Библиотека по автоматике, выпуск 516. – М: Энергия, 1974. – 120 с.

2. Петров, И. В. Программируемые контроллеры. Стандартные языки и приемы прикладного проектирования [Текст] / И. В. Петров ; под ред. В. П. Дьяконова. – М. : СОЛОН-Пресс, 2004. – 256 с.

3. Программное обеспечение SMLogix [Электронный ресурс] / Режим доступа: http://segnetics.com/smlogix, свободный.

4. Панельный контроллер SMH 2010C [Электронный ресурс] / Режим доступа: http://segnetics.com/main.aspx?Page=229, свободный.

5. Приборы и средства промышленной автоматизации [Электронный ресурс] / Режим доступа: http://www.delta-vfd.ru, свободный.

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ОБУЧАЮЩЕГО КОМПЛЕКСА ШИФРОВАНИЯ НА ОСНОВЕ АЛГОРИТМА RIJNDAEL

Заварзин А.В. – студент, Ленюк С.В. – к.ф.-м.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Проблема обеспечения безопасности информации при ее хранении, обработке и передаче по сетям связи на сегодняшний день является актуальной. Актуальность данной проблемы обуславливается стремительным развитием информационно-телекоммуникационных технологий и объемом передаваемой по сетям связи информации. В связи с этим встает вопрос о подготовке специалистов в области обеспечения информационной безопасности.

В настоящее время существуют различные способы защиты информации, такие как метод физического преграждения доступа к защищаемой информации, управление доступом, шифрование, стеганографические методы защиты информации и др. [1]. При передаче информации по каналам связи шифрование является самым надежным способом. Оно имеет ряд ключевых преимуществ, таких как высокая защищенность и относительная быстрота преобразования данных.

В настоящее время в информационно-телекоммуникационных системах широко используется симметричный алгоритм шифрования AES.

В разработанном программном комплексе представлен стандарт шифрования AES, основанный на алгоритме Rijndael. На сегодняшний день данный алгоритм является достаточно стойким и имеет различные варианты использования длин ключей в зависимости от степени конфиденциальности информации [2].

Rijndael – симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128, 192, 256 бит), разработанный в 1997 году известными бельгийскими криптографами Йоном Даменом и Винсентом Рэменом и принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Алгоритм состоит из 10 раундов различных преобразований, таких как SybBytes, ShiftRows, MixColumns и AddRoundKey. Этот алгоритм хорошо проанализирован и сейчас широко используется. Национальный институт стандартов и технологий США опубликовал спецификацию AES 26 ноября 2001 года после пятилетнего конкурса, в ходе которого были созданы и оценены 15 кандидатур. 26 мая 2002 года AES был объявлен стандартом шифрования США. По состоянию на 2009 год AES является одним из самых распространенных алгоритмов симметричного шифрования [3].

Так как программный комплекс имеет обучающую функцию, было реализовано шифрование с длиной ключа 128 бит.

Разработанное программное обеспечение предназначено для проведения практических занятий со студентами, отработки практических умений и навыков студентов по шифрованию и расшифрованию информации с помощью алгоритма Rijndael.

Главное окно программы показано на рисунке 1.

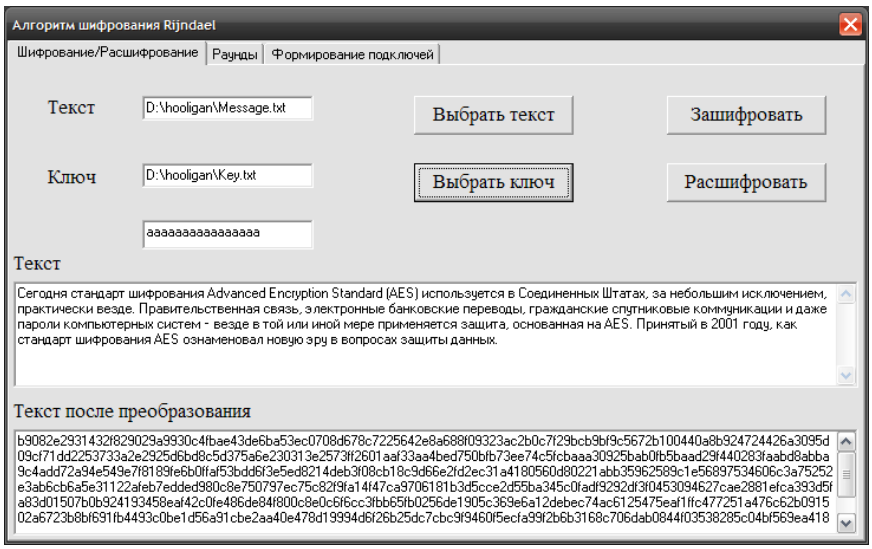


Рисунок 1 – главное окно программы

Отличительной особенностью программного продукта является вывод всех промежуточных результатов шифрования, расшифрования и формирования подключей.

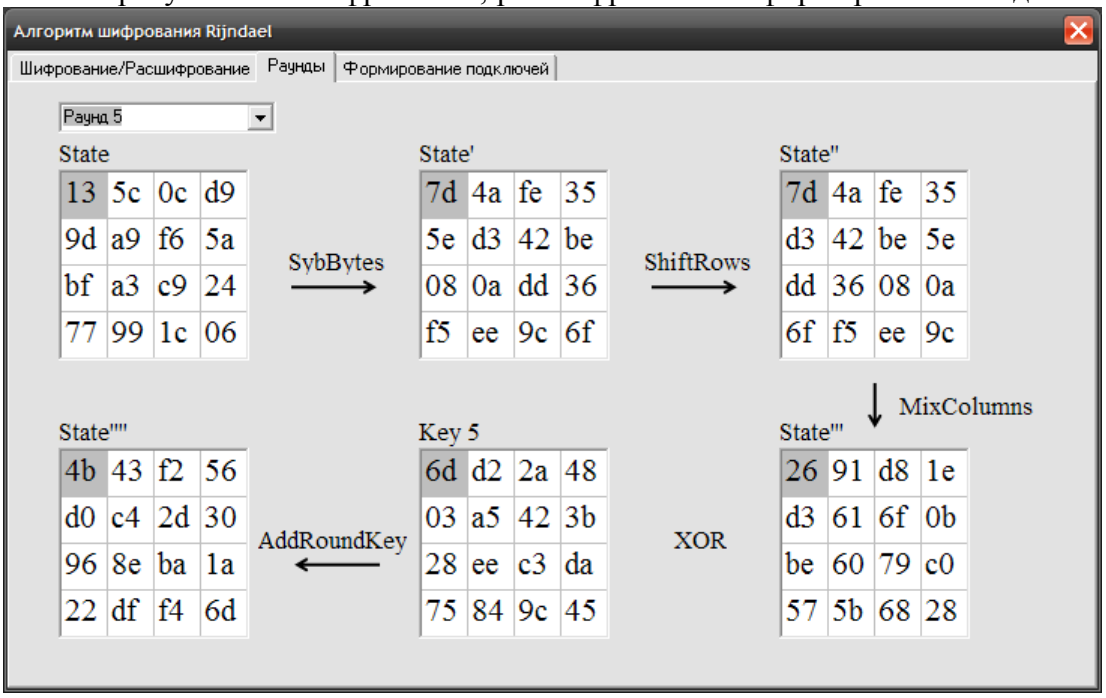


Рисунок 2 – вывод промежуточных результатов 5 раунда шифрования

Программа состоит из 3 основных модулей: шифрование, расшифрование, формирование подключей, каждый из которых состоит из отдельных процедур.

При шифровании текст разбивается на блоки по 128 бит, при необходимости последний блок дополняется нулями до необходимого размера. Каждый блок преобразуется по таблице символов ASCII в число в 16-ричном формате и проходит 10 раундов преобразований, состоящих из отдельных преобразований: замена байт S-блоком, сдвиг строк, перемешивание столбцов, сложение с ключом. Результатом шифрования является шифротекст, записанный в 16-ричном формате.

Расшифрование является обратным действием шифрования. Шифротекст разбивается на блоки по 16 чисел в 16-ричном формате. Каждый блок проходит инверсные преобразования функций SubBytes, ShiftRows, MixColumns и AddRoundKey, но в обратном порядке. В результате обратного преобразования по таблице символов ASCII восстанавливается

исходный открытый текст. Такую функцию расшифрования называют функцией обратного расшифрования.

Но алгоритм Rijndael позволяет использовать процедуру прямого расшифрования, в которой последовательность преобразований совпадает с примененной в процедуре шифрования. Это достигается путем изменения массива подключей и двумя свойствами алгоритма:

1) Процедуры SubBytes и ShiftRows коммутативны. То есть, результат выполнения процедуры SubBytes непосредственно после процедуры ShiftRows будет эквивалентен результату выполнения процедуры ShiftRows непосредственно после процедуры SubBytes. То же верно и для инверсий этих процедур – InvSubBytes и InvShiftRows.

2) Операции перемешивания в столбце – MixColumns и InvMixColumns – являются линейными по отношению к данным, расположенным в столбце, что означает InvMixColumns(State XOR RoundKey) = InvMixColumns(State) XOR InvMixColumns(RoundKey).

Согласно этим свойствам порядок выполнения процедур InvSubBytes и InvShiftRows можно изменять на обратный. Порядок выполнения процедур AddRoundKey и InvMixColumns тоже можно инвертировать, если при этом слова в последовательности подключей будут изменены с помощью процедуры InvMixColumns.

Существование двух способов расшифрования является отличительной особенностью алгоритма Rijndael.

Формирование подключей – это расширение из одного 128-битного ключа до 11 128-битных подключей, используемых в различных раундах алгоритма. Первый подключ является используемым ключом, при формировании остальных 10 подключей используются функции RotWord и SubWord [4].

Разработанный программный комплекс имеет значительную практическую ценность при подготовке специалистов в области защиты информации. Позволяет более детально изучить особенности алгоритма и является инструментом самостоятельной проверки знаний будущих специалистов в процессе обучения. Ключевым достоинством данного комплекса является вывод всех промежуточных результатов шифрования, расшифрования и формирования подключей. Данное программное обеспечение может быть использовано для обучения студентов, связанных с направлением защиты информации.

Список использованной литературы:

1. Методы и средства защиты информации [Электронный ресурс] – Режим доступа: http://abc.vvsu.ru/Books/inform_tehnolog/page0025.asp, свободный – Загл. с экрана. – Яз. рус.

2. Advanced Encryption Standard [Электронный ресурс] – Режим доступа: http://ru.wikipedia.org/wiki/Advanced_Encryption_Standard, свободный – Загл. с экрана. – Яз. рус.

3. Конкурс на Advanced Encryption Standard [Электронный ресурс]. – Режим доступа: http://bibliofond.ru/view.aspx?id=550637, свободный. – Загл. с экрана. – Яз. рус.

4. Описание алгоритма Rijndael [Электронный ресурс]. – Режим доступа: http://kaf401.rloc.ru/Criptfiles/Rijndael/Rijndael.htm, свободный. – Загл. с экрана. – Яз. рус.

РАЗРАБОТКА ГЕНЕРАТОРА СИГНАЛОВ НА БАЗЕ DDS-МОДУЛЯ AD9833

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

Алтайский Государственный Университет им. И.И. Ползунова осуществляет подготовку кадров по направлению 090900 «Информационная безопасность» и 230100 «Информатика и вычислительная техника» (квалификация (степень) «бакалавр»). Обучение, по данным специальностям, предусматривает ряд предметов ориентированных на изучение

электроники. Подобными дисциплинами являются «Электроника и схемотехника» и «Сети и системы передачи информации» [1].

Учебный план курса указывает на необходимость выполнения лабораторных работ по дисциплинам бакалавриата, однако, для проведения работ необходимо наличие помещений оснащённых дорогостоящим специализированым измерительным оборудованием. Актуальной задачей является разработка аппаратуры имеющей достаточную функциональность для выполнения практических занятий. Одним, из которых является лабораторный генератор сигналов.

Целью данной работы является решение проблемы разработки лабораторного генератора сигналов, входящим в комплектацию оборудования учебных мест, для направления подготовки бакалавров «Информационная безопасность» по дисциплине «Сети и системы передачи информации» и «Информатика и вычислительная техника» по дисциплине «Сети и системы передачи информации» [2].

Для достижения цели необходимо выполнить следующие задачи:

– выдвинуть требования к объекту разработки;
– выполнить анализ существующих средств генерации сигналов;
– произвести подбор радиоэлементов соответствующих требованиям;
– собрать и исследовать опытный образец.

Генератор должен обеспечить формирование сигналов прямоугольной и синусоидальной формы, возможность настройки частоты в диапазоне 20Гц-1МГц.

Для создания устройства (рисунок 1) будет использован микроконтроллер компании Atmel, который будет управлять DDS-генератором на базе AD9833. Данный компонент является малопотребляющим, программируемым генератором колебаний. Частота и фаза выходного колебания управляются программно, что упрощает настройку генератора. Регистры частоты имеют разрядность 28 бит. При частоте тактового сигнала 1 МГц разрешение настройки AD9833 составляет 0,004 Гц.

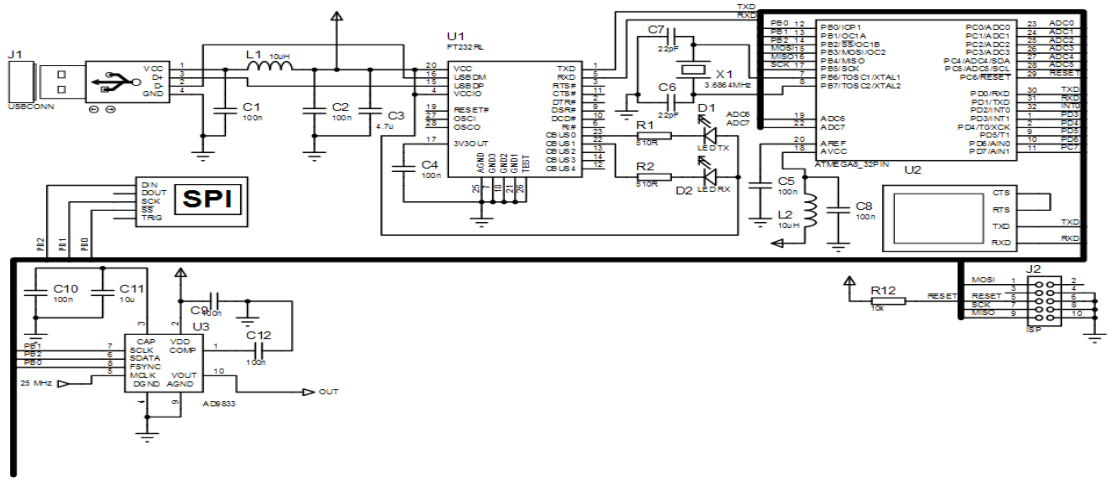


Рисунок 1 – Схема электрическая принципиальная

Режим работы устройства заключается в формировании сигнала одной из трёх форм: прямоугольного, синусоидального и треугольного. Форма, частота а так же фаза определяется DDS генератору по шине SPI с помощью ATmega8. Необходимая для контроллера информация выдаётся компьютером на USB порт. Для дальнейшего

преобразования USB – RS232 информация проходит преобразователь FT232RL, после чего поступает на контроллер [3-6].

В процессе данной работы выполнена разработка аппаратной части системы и организация связи между стендом генератора сигналов синусоидальной прямоугольной треугольной формы и компьютером с установленным программным обеспечением.

Список использованной литературы:

1. Образовательный стандарт учебной дисциплины Б.3.ДВ.20.2 Системы и сети связи 230100 Информатика и вычислительная техника. [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.

2. 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.

3. 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

4. РадиоЭлПриборы справочная информация // измерительные генераторы сигналов – щбщие сведения [Электронный ресурс]: справочная информация – 2011-2013. – Режим доступа: http://radioelpribori.ru/izmeritelnyie-generatoryi-signalov-obshhie-svedeniya.html

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

6. 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

ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ В ПОМЕЩЕНИИ ДЛЯ КОНФИДЕНЦИАЛЬНЫХ ПЕРЕГОВОРОВ

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

В современных условиях информация играет решающую роль как в процессе экономического развития, так и в ходе конкурентной борьбы на внутреннем и внешнем рынках.

Одним из источников важной информации организации являются совещания, на которых представляются материалы по имеющимся результатам и планам работ. Присутствие большого количества людей и большие размеры помещений ставят перед этими организациями проблему сохранения коммерческой тайны.

Таким образом, защита информации при проведении совещаний с участием представителей сторонних организаций имеет актуальное значение и основными задачами по обеспечению информационной безопасности является выявление и своевременная локализация возможных технических каналов утечки акустической информации.

В настоящее время существует масса возможностей снять речевую информацию. Один из самых простых способов - это прослушивание разговора с помощью микропередатчиков, установленных в офисе. Другой распространенный способ - прослушивание помещений с

помощью микрофона телефонного аппарата. Еще один очень распространенный метод - это прослушивание звуковых волн разговорной речи, передающихся через перегородки, стены, стекла, батареи отопления. Для прослушивания помещений, имеющих окна могут применяться устройства, работающие в оптическом диапазоне - лазерные детекторы [1].

Набор технических средств для съема акустической информации не ограничивается перечисленными выше средствами. Однако рассматриваемая техника является основной для съема акустической информации.

Проблема защиты конфиденциальных переговоров решается комплексно с применением различного рода мероприятий и с использованием разных технических средств. При этом учитываются все перечисленные выше обстоятельства образования каналов утечки информации.

Для решения обозначенных проблем в ходе данной работы были применены:

1)Устройство с генератором аккустической помехи - наиболее безопасным и надежным способом сохранения конфиденциальности переговоров является маскировка звукового поля разговорной речи участников совещания непрерывно излучаемым широкополосным сигналом, полоса частот которого совпадает с полосой частот речевого сигнала. Уровень излучаемого шума выбирается таким, чтобы в любой точке помещения для переговоров речь участников переговоров была бы неразборчива, а характеристики шума - такими, чтобы полученный по любому каналу речевой сигнал не поддавался шумоочистке [2].

2)Детектор электромагнитного поля - данные устройства весьма эффективны при поиске активных радиопередатчиков со стандартными каналами передачи [3].

3)Генератор виброакустического шума – эти устройства применяются для защиты речевой информации от утечки через перегородки, стены, стекла, батареи отопления. Они зашумляют звуковые волны разговорной речи с помощью вибро- и пьезодатчиков, которые располагают на стенах, окнах и батареях центрального отопления [4].

Таким образом, предложенные устройства помогают защитить информацию при проведении конфиденциальных переговоров в закрытом помещении.

Список использованной литературы:

1. Защита информации в выделенных помещениях [Электронный ресурс]. Режим доступа: http://www.analitika.info/stati2.php?page=1&full=block_article217

2. Радиоэлектронный принцип работы генератора акустических помех [Электронный ресурс]. Режим доступа: http://www.zondir.ru/articles/radioelektronnyj-princip-raboty-gjenjeratora-akusticjeskikh-pomekh.htm

3. Бюро научно-технической информации [Электронный ресурс]. Режим доступа: http://www.bnti.ru/showart.asp?aid=960&lvl=04.01.01.

4. Системы виброакустической маскировки [Электронный ресурс]. Режим доступа: http://www.vrsystems.ru/stati/sistemi_vibroakusticheskoi_maskirovki.htm

ЗАЩИТА ОТ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА БАЗЕ ТЕХНОЛОГИЙ DATA LOSS PREVENTION

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

Распространение информационных технологий и тенденция подключения государственных информационных систем (ГИС) к информационно-телекомуникационным сетям общего пользования являются порождающим фактором увеличения риска реализации инсайдерских угроз информационной безопасности организаций. Согласно нормативно-правовым актам (НПА) в области обеспечения защиты информации в ГИС, таких как ФЗ №152 «О персональных данных», Постановление правительства 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах

персональных данных», Указ Президента РФ от 17.03.2008 N 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена", Приказ ФТЭК от 13.02.2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказ ФСТЭК 18.02.13 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и Руководящие документы ФСТЭК, необходимо использование сертифицированных по требованиям безопасности средств защиты информации. Делая акцент на увеличение количества утечек конфиденциальной информации в сеть, следует предпринимать своевременные меры по нейтрализации данного типа угроз посредством разработки, внедрения и эксплуатации DLP – систем. Использование данной технологии в совокупности с профессиональной настройкой системы, опираясь на перечень сведений конфиденциального характера, выполненной по требованиям НПА, позволяет сократить уровень риска утечки КИ до приемлемого уровня и существенно упростить технические мероприятия по расследованию возможных инциндентов.

Предотвращение утечек (Data Loss Prevention, DLP) — технологии предотвращения утечек конфиденциальной информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек [4]. DLP-системы строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется. Распознавание конфиденциальной информации в DLP-системах производится двумя способами: анализом формальных признаков (например, грифа документа, специально введённых меток, сравнением хэш-функции) и анализом контента.

К основным задачам DLP – систем относятся следующие:

– предотвращение передачи конфиденциальной информации за пределы информационной системы;

– архивирование пересылаемых сообщений на случай возможных в будущем расследований инцидентов;

– выявление инсайдеров внутри компании;

– повышение эффективности работы отдела по защите информации;

– предотвращение передачи нежелательной информации не только изнутри наружу, но и снаружи внутрь информационной системы;

– оптимизация загрузки каналов, экономия трафика;

– контроль присутствия работников на рабочем месте;

– отслеживание благонадёжности сотрудников.

Основными методами детектирования конфиденциальной информации являются:

1) Сигнатуры – поиск в потоке данных некоторой последовательности символов. Достоинство: простота пополнения словаря запрещённых терминов. Недостаток: лингвистическое разнообразие словесных форм.

2) Цифровые отпечатки – детектирование на основе хэшей шаблонов. Достоинство: простота добавления новых шаблонов, высокую степень детектирования и прозрачность алгоритма технологии для сотрудников подразделений по защите информации. Недостаток: необходимость постоянного обновления базы данных «цифровых отпечатков».

3) Метки – расстановка специальных «меток» внутри файлов. Достоинство: высокое качество детектирования. Недостаток: значительная перестройка инфраструктуры внутри сети и введение множества новых правил и форматов файлов для пользователей.

4) Регулярные выражения – нахождение совпадения по форме данных. Достоинства: позволяют детектировать специфичный для каждой организации тип контента. Недостаток:

ограниченная сфера применения в рамках DLP – систем и невозможность применения независимо от других технологий.

5) Лингвистические методы – основаны на лингвистическом анализе текста. Достоинства: высокая степень эффективности при намного меньших трудозатратах на внедрение и поддержку. Недостаток: зависимость от языка.

6) Ручное детектирование – фильтрация контента специалистом по защите информации. Достоинства: высокое качество детектирования. Недостаток: ограниченный объём контента.

Современные DLP – системы имеют следующие функции:

1) Контроль доступа к устройствам и интерфейсам. Обеспечение контроля доступа пользователей и групп к портам ввода-вывода, адаптерам WiFi и Bluetooth, любым типам принтеров, мобильным устройствам и дисководам.

2) Контроль сетевых коммуникаций. Обеспечение детектирования коммуникационных приложений и их селективную блокировку.

3) Мониторинг и фильтрация трафика. Информация анализируется на предмет соответствия корпоративным политикам безопасности.

4) Централизованное управление. Полная интеграция централизованного управления в групповые политики Windows.

5) Контроль по типу файлов. Разрешение и запрет доступа к определенным типам файлов.

6) Контроль буфера обмена. Предотвращение утечки данных при намеренном или случайном копировании между различными приложениями и документами через встроенный в ОС Windows буфер обмена.

7) Межсетевое экранирование.

8) Белый список носителей и сетевых протоколов. Для каждого пользователя или группы можно задать свой "белый" список, доступ к которым будет всегда разрешен.

9) Аудит. Протоколирование всех действий пользователей с устройствами и файлами.

10) Централизованное хранение журналов аудита и теневого копирования.

В качестве объектов сравнительного анализа были взяты три DLP - системы российских разработчиков: DeviceLock, InfoWatch Traffic Monitor Enterprise и Дозор Джет.

Рассмотренные системы имеют модульную структуру.

Комплекс DeviceLock Endpoint DLP Suite [3] состоит из взаимодополняющих функциональных модулей — DeviceLock, NetworkLock, ContentLock и DeviceLock Search Server.

1) DeviceLock Service — агент DeviceLock, устанавливаемый на каждый защищаемый компьютер и работающий на уровне ядра Microsoft Windows.

2) Компонент NetworkLock обеспечивает контекстный контроль каналов сетевых коммуникаций на рабочих компьютерах, включая распознавание сетевых протоколов независимо от используемых портов, детектирование коммуникационных приложений и их селективную блокировку.

3) Компонент ContentLock реализует механизмы контентного мониторинга и фильтрации файлов и данных, передаваемых с/на сменные носители и в каналах сетевых коммуникаций.

4) DeviceLock Search Server (DLSS) — дополнительный компонент (необязательный), используется для индексирования и полнотекстового поиска по содержимому файлов теневого копирования и журналам, хранящимся в базе данных DeviceLock Enterprise Server.

Состав комплекса InfoWatch Traffic Monitor Enterprise [1]:

1) Модуль для защиты периметра корпоративной сети - InfoWatch Traffic Monitor.

2) Модуль для защиты рабочих станций - InfoWatch Device Monitor.

3) Модуль для контроля информации в общедоступных сетевых хранилищах - InfoWatch Crawler.

4) Модуль централизованного архивирования и управления - InfoWatch Forensic Storage.

Состав комплекса Дозор Джет [2]:

1) Система архивирования и анализа.
2) Система пассивного перехвата сообщений.
3) Система инспекции файловых ресурсов.
4) Система активного контроля.
5) Модуль контроля рабочих станций.

Для проведения сравнительного анализа DLP - систем были выбраны следующие критерии [5]:

1) Позиционирование системы на рынке.
2) Системные требования.
3) Используемые технологии детектирования.
4) Контролируемые каналы передачи данных.
5) Возможности контроля подключаемых внешних устройств.
6) Мониторинг агентов и их защита.
7) Управление системой и обработка инцидентов.
8) Отчетность.
9) Интеграция с решениями сторонних производителей.

Рассмотренные DLP – системы полностью удовлетворяют требованиям российского законодательства и имеют идентичные функциональные возможности по основным критериям анализа. Ключевым фактором выбора средства защиты информации является наличие свободно распространяемой полнофункциональной демонстрационной версии, так как разработка и внедрение проекта системы защиты от утечки конфиденциальной информации будет реализовано в виртуальной среде. Услуга по предоставлению демо-версий доступна только для продуктовой линейки DeviceLock 7 Endpoint DLP Suite. При последующем внедрении проекта в автоматизированную информационную систему важным элементом является стоимость DLP – системы. Очевидное преимущество комплекса DeviceLock заключается в возможности активации лицензий только на необходимые компоненты в зависимости от потребностей организации.

Проанализировав функционал DLP – систем, можно сделать вывод о том, что данная технология обладает высокой эффективностью и имеет перспективы развития. Становится очевидно, что блокирование доступа в интернет является нерациональным способом ограждения информационных систем от существующих угроз, так как это влечёт за собой усложнение или полный отказ информационного взаимодействия посредством телекоммуникационных сетей общего пользования. Поэтому DLP – системы становятся необходимым элементом в системе защиты информационных систем и используются в совокупности с СЗИ от НСД, МЭ и антивирусными средствами.

Список использованной литературы:

1. INFOWATCH TRAFFIC MONITOR ENTERPRISE «Естественное и искусственное освещение» [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/products/traffic_monitor_enterprise/

2. Комплекс защиты от утечек информации Дозор Джет [Электронный ресурс]. – Режим доступа: http://www.dozor-jet.ru/

3. DeviceLock защита от инсайдеров [Электронный ресурс]. – Режим доступа: http://www.devicelock.com/ru/

4. DLP – Википедия [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/DLP

5. Сравнение систем защиты от утечек [Электронный ресурс]. – Режим доступа: http://www.anti-malware.ru/comparisons/data_leak_protection_2014_part1

ОРГАНИЗАЦИЯ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ

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

Для современной российской рыночной экономики обязательным условием успеха предпринимателя в бизнесе, получением прибыли и сохранением в целостности созданной им организационной структуры, является обеспечение экономической безопасности его деятельности. Одной из главных составных частей экономической безопасности является информационная безопасность.

В настоящее время существует множество различных способов перехвата информации, начиная от прослушивания помещений для переговоров и заканчивая атаками на информационные сети [2]. Поэтому к защите необходимо подходить не только с технической стороны, но и с инженерной.

В данный момент существует огромное множество различных систем инженерно-технической защиты, например охранные системы (сигнализации), системы видеонаблюдения, системы разграничения доступа в помещения, криптографические средства [3].

Однако в связи со стремительным развитием GSM технологий, у злоумышленников начало появляться большое количество различных подслушивающих устройств, работающих в данном частотном диапазоне. Поэтому необходимость обеспечения защиты информации от ее перехвата по каналам GSM не менее важна чем, ее защита от утечки по другим каналам.

На рынке существует большое количество приборов, разработанных для защиты информации от ее утечки по каналам GSM. К таким устройствам относятся генераторы белого шума. Данные устройства способны защитить не только от утечки информации по GSM каналу, но и от ее утечки по каналам ПЭМИН. Несмотря на то, что для большинства руководителей предпринимательских структур утечка конфиденциальной информации из используемой ВТ через ПЭМИН кажется маловероятной, такой канал перехвата информации все же существует, а это значит, что рано или поздно кто-то им все-таки воспользуется. Особую остроту эта проблема приобретает для коммерческих фирм, офисы которых занимают одну или несколько комнат в здании, где кроме них размещаются другие организации [1].

Ниже приведены некоторые генераторы шумов, представленные на рынке:

1. SEL SP-21 "Баррикада" Генератор шума маскировки ПЭМИН

Генератор с регулируемым уровнем излучения SEL SP-21 "Баррикада" предназначен для маскировки и предупреждения перехвата информативных побочных электромагнитных излучений и наводок от средств вычислительной техники путём создания в широкой полосе частот активных маскирующих помех (типа "белый шум").

2. SEL SP-113 "Блокада"

Устройство защиты информации от утечки по каналу ПЭМИН "Блокада" предназначено для активной защиты информации, обрабатываемой на объектах информатизации, включая вычислительную технику, от утечки за счёт побочных электромагнитных излучений и наводок от них на цепи электропитания и проводные слаботочные линии.

3. "Соната-РК2"

Данное устройство является комбинацией фильтра поглощающего типа, генераторов шумового тока с корректировкой спектра и регулировкой интегрального уровня и элементов антенной системы.

Изделие предназначено для защиты информации, обрабатываемой основными техническими средствами и системами до 1 категории включительно, от утечки за счет ПЭМИН путем постановки маскирующих помех в линиях электропитания и заземления, а также путем пространственного зашумления и частичного поглощения информативных сигналов, распространяющихся по линиям электропитания и заземления [4].

Данные устройства можно купить на рынке, но они дороги, поэтому возникла необходимость собрать генератор белого шума и разобраться в принципе его работы. За основу которого был взял генератор SEL SP-21 "Баррикада". Схема данного генератора представлена на рисунке 1 [5].

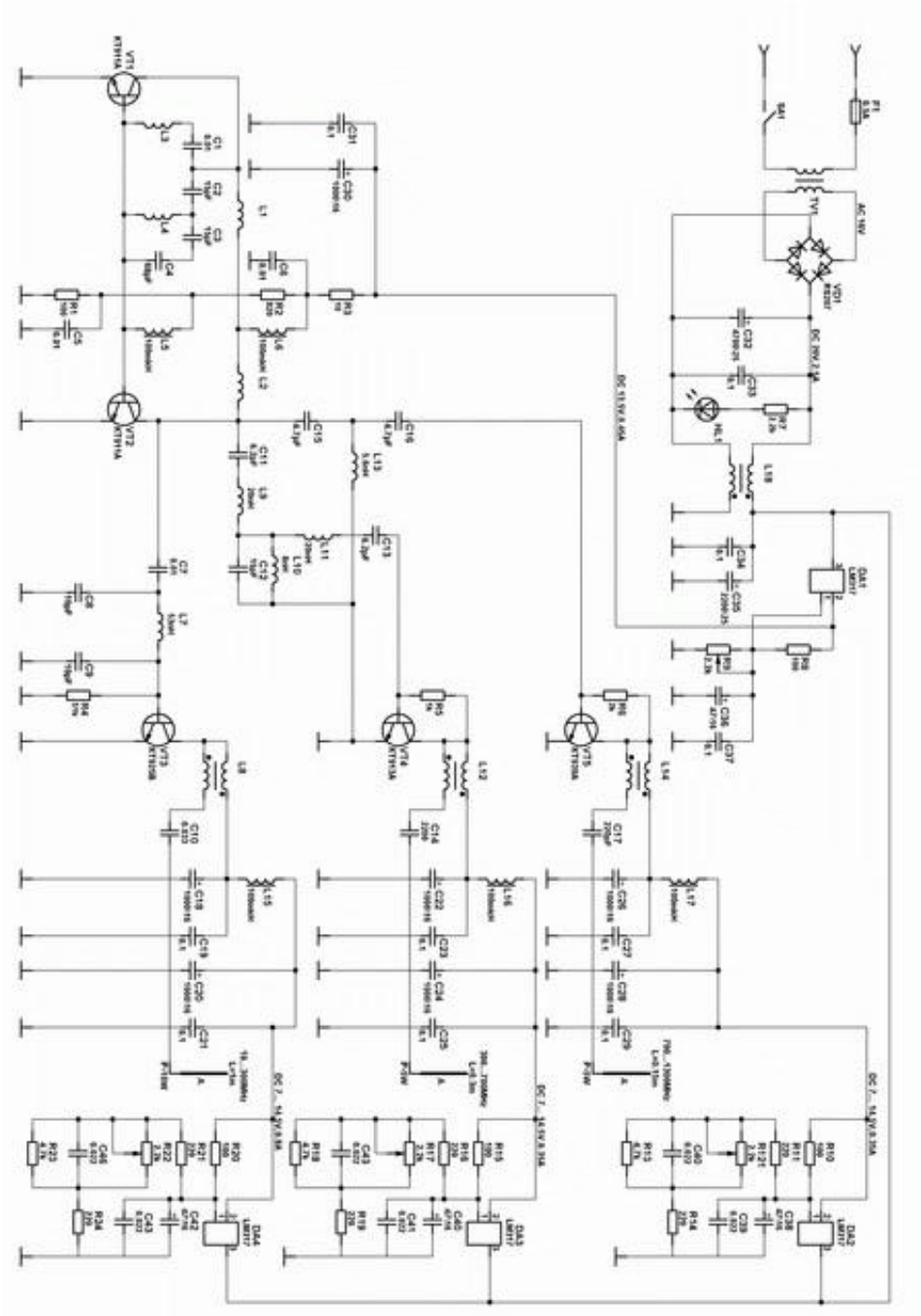


Рисунок 1 - Схема Генератора SEL SP-21 "Баррикада"

Технические характеристики:

- Потребляемая мощность (макс.) – 40Вт.
- Диапазон частот – 20….1300МГц.
- Максимальная выходная мощность – 20Вт.

В данной работе был произведен анализ существующих на рынке широкополосных генераторов шумов, а так же была выбрана схема для его самостоятельной реализации.

Список использованной литературы:

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. Технические средства и методы защиты информации: Учебник для вузов. М.: ООО «Издательство Машиностроение», 2009.

2. Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Гайнулин Т.Р.; Методы и средства инженерно-технической защиты информации: учебное пособие / М.: «ФЛИНТА», 2011

3. Торокин А.А. Основы инженерно-технической защиты информации.— М.: Издательство «Ось-89», 1998 г.

4. Бюро научно-технической информации [Электронный ресурс]. Режим доступа: http://www.bnti.ru/index.asp?tbl=04.03.04.01.

5. Very Reasonable Techological Pages [Электронный ресурс]. Режим доступа: http://vrtp.ru/index.php?act=categories&CODE=article&article=1797

ЗАЩИТА ИНФОРМАЦИИ СРЕДСТВАМИ ПОТОЧНОГО ШИФРОВАНИЯ

Левицкая Ю.С.-студент
Воронежский государственный университет (г. Воронеж)

В настоящее время потоковое шифрование является наиболее близким к идеальным криптосистемам по структуре и принципам построения, обеспечивающие, с высокой скоростью, защиту огромных массивов данных, а также, практически в режиме реального времени, шифрование или расшифрование информации. К преимуществам потокового шифрования относятся: отсутствие размножения ошибок; простота реализации; высокая скорость шифрования; защита от вставок и изъятия части шифрованного текста из потока данных, так как эти действия приведут к нарушению синхронизации[3].

В основе криптосхемы потокового шифрования лежит генератор псевдослучайной последовательности (ПСП), строящийся на базе регистров сдвига, который позволяет увеличить мощность ключевой системы, за счет использования секретного алгоритма шифрования [2, 3], и даже увеличить скорость шифрования при условии адаптации регистра сдвига к архитектуре вычислительного устройства. Например, используя непозиционные специализированные вычислительные системы для осуществления криптографических преобразований в конечных полях [4].

Предлагаемый алгоритм относится к классу алгоритмов, обеспечивающих работу синхронных потоковых шифров, но отличается от известных [3] возможностью выбора структуры регистра сдвига и использования не только посимвольного сложения по модулю p (p>2) открытого текста и элементов псевдослучайной последовательности, но и реализации множества других линейных и нелинейных криптографических преобразований, что не только увеличивает криптостойкость системы шифрования, но и разрушает возможность наиболее опасной криптографической атаки на основе известного или специально подобранного открытого текста и соответствующего ему шифрованного текста.

Рассмотрим характеристический многочлен: □^{6}+□ □^{5}+1. Этот многочлен является примитивным, и порядок этого многочлена равен: $N=2^6-1$.

В силу этих свойств генератор формирует ПСП чисел максимальной длины N=63 при любом (кроме нулевого) начальном заполнении линий задержек.

Для выбранного примитивного многочлена структурная схема регистра сдвига с обратной связью будет иметь вид, представленный на рис.1:

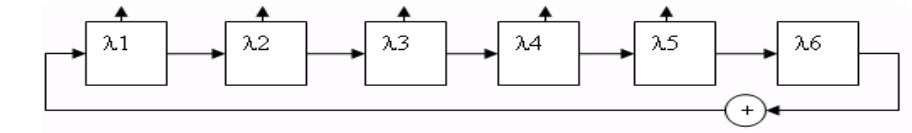


Рис. 1. Структурная схема линейного регистра сдвига

Двоичные числа снимаются с 1, 2, 3, 4 и 5 разряда регистра сдвига (блоки □1, □2, □3, □4, □5) и на каждом такте работы регистра сдвига с набором <□1, □2, □3, □4, □5> сопоставляется двоичный вектор (число) x:=2^4*□5+2^3*□4+2^2*□ □3+2*□ □2+□ □1; последовательность двоичных чисел в процессе работы регистра рассматриваем как последовательность x чисел (символов). Аналогично получаем последовательность чисел y :=2^4*□1+2^3*□2+2^2*□4+2*□5+□6;

Сформированные ПСП символов конечного поля x и y в виде двоичных векторов преобразуют поступающий поток данных в зашифрованное сообщение в соответствии с выбранным криптографическим преобразованием в конечном поле F_{31}.

Обозначим α – поток открытого текста; β – соответствующий поток шифрованного текста; p=31 – характеристика простого конечного поля F_p; $\gamma = 7$ – число, взаимно простое с функцией Эйлера $\varphi(p)$, используемое в качестве дополнительного секретного ключа γ; x и y – ПСП в формате поля F_p, формируемые при съеме информации с определенных отводов линейного регистра сдвига; $x^* = p - x$ и $y^* = p - y$ – сопряженные ПСП (т.е.обратные для конечного поля); $\varphi(p-1)$ – функция Эйлера числа $(p-1)$, тогда шифрование / расшифрование осуществляется одним из след. способов:

1) $\beta = (\alpha \cdot x + y) \bmod p$;

$[(\beta + y^*) \cdot x^{-1}] \bmod p = \alpha$;

$x^{-1} = x^{p-2} \bmod p$;

2) $\beta = (\alpha^{\gamma} + x) \bmod p$;

$[(\beta + x^*) \wedge \gamma^{-1}] \bmod p = \alpha$;

$\gamma^{-1} = \gamma^{\varphi(p-1)-1} \bmod (\varphi(p))$;

$(\gamma, (p-1)) = 1$;

$\wedge$ – операция возведения в степень;

Второй способ реализует возможность использования принципов асимметричной криптографии при поточном шифровании информации. Здесь, за счет секретности алгоритма и дополнительного ключа γ, криптоаналитику потребуется решение трудновычислимой задачи дискретного логарифмирования даже при известной паре: открытый текст – шифрованный текст.

Так, например, при □1=0, □2=0, □3=0, □4=1, □5=1, □6=1 получим следующие ПСП: x={24 16 30 1 2 4 8 16 1 3}; y={7 3 1 16 8 30 4 2 17 24}.

Тогда для 1-ого способа преобразования получится β={6 23 23 25 26 4 14 22 26 20}.Вычислив необходимую для расшифрования последовательность x^{-1}={22 2 30 1 16 8 4 2 1 21} и сопряженную ПСП y*={24 28 30 15 23 1 27 29 14 7}, мы можем получить первоначальный поток открытого текста α={9 9 9 9 9 9 9 9 9 9}.

Для второго способа преобразования шифрованный текст выглядит след. образом: β ={3 26 9 11 12 14 18 26 11 13}. Для расшифрования вычисляем x*={7 15 1 30 29 27 23 15 30 28} и $\gamma^{-1}(\varphi(p))$=13. Так же, вычислив, получаем поток открытого текста α ={9 9 9 9 9 9 9 9 9 9}.

На практике был реализован способ, отличающийся тем, что символы одной из формируемых псевдослучайных последовательностей конечного поля используют как порождающие элементы для формирования дополнительной псевдослучайной последовательности символов, которые на каждом такте работы сдвига определяют как порожденные элементы конечного поля F_p

Список использованной литературы:

1. Шеннон К. Э. Работы по теории информации и кибернетике / К. Э. Шеннон. − М.: Издательство иностранной литературы, 1963. − 694 с.

2. Молдовян А. А. Криптография / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов − Серия «Учебники для вузов. Специальная литература». − СПб.: Издательство «Лань», 2000. − 224 с.

3. Баричев С. Г. Основы современной криптографии / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. − М.: Горячая линия – Телеком, 2001. − 120 с.

4. Ирхин В. П. Проектирование непозиционных специализированных процессоров. − Воронеж: Издательство ВГУ, 1999. − 136 с.

РАЗРАБОТКА АППАРАТНОГО КОМПЛЕКСА И УЧЕБНО-МЕТОДИЧЕСКИХ МАТЕРИАЛОВ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНАМ "ЭЛЕКТРОТЕХНИКА И СХЕМОТЕХНИКА" И "МИКРОПРОЦЕССОРНАЯ ТЕХНИКА"

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

АлтГТУ им. И.И. Ползунова осуществляет подготовку кадров по направлению «Информационная безопасность» (квалификация (степень) «бакалавр») с сентября 2011 года. Направление является новым, в связи с чем актуальной задачей является разработка современных обучающих материалов по приоритетным дисциплинам.

Выполнение учащимися лабораторных работ [1] является важным средством более глубокого усвоения и изучения учебного материала. Но получение обучаемым практического опыта невозможно без применения средств, на которых можно было бы отрабатывать навыки программирования и наблюдать за ходом выполнения учебных программных кодов. С этой целью принято решение разработать лабораторный стенд на современной элементной базе [2].

Лабораторные стенды выпускаются на базе различных микроконтроллеров и имеют широкий спектр конфигураций. В состав периферии учебного стенда могут входить светодиодные и жидкокристаллические индикаторы, кнопки, клавиатура, имитаторы сигналов, излучатели звука, шаговые двигатели, датчики температуры и влажности, преобразователи интерфейсов, модули ППЗУ, разъёмы для подключения к ПК и дополнительным внешним устройствам. Но у всех фирменных плат (так называемых development boards и training boards) есть ряд недостатков [3].

Основными недостатками таких плат являются высокая стоимость и то что такие платы ориентированы на опытных пользователей, что не позволяет использовать их для обучения "с нуля". К тому же лабораторные стенды представляют собой конструктивно законченные устройства и обладают более высокой надёжностью по сравнению с фирменными платами, вследствие ограничения физического доступа к жизненно–важным узлам стенда.

Современный лабораторный стенд на микроконтроллере должен иметь широкий спектр конфигураций. Для того, чтобы не отставать от своих конкурентов и иметь широкой функциональный спектр возможностей не только для обучения студентов, но и для выполнения дипломный, курсовых и научных работ, лабораторный стенд включает в себя следующие компоненты: цифровой дисплей, графический дисплей, аналоговый вход, цифровой выход, клавиатура, кнопки с фиксатором, кнопки без фиксатора, светодиоды (одноцветные и двухцветные), COM интерфейс, USB интерфейс, динамик, элементы питания для электродвигателя. Управление стендом осуществляется посредством микроконтроллера Atmega 8535. Взаимодействие с персональным компьютером и программирование стенда осуществляется с помощью USB программатора и переключателя расположенного на лицевой панели стенда (работа / программирование). Так как микроконтроллер имеет ограниченное количество циклов перезаписи, в стенде реализована возможность его быстрой замены.

Разрабатываемый стенд можно разбить на 4 блока, каждый из которых является функциональной единицей. Перечень блоков: 1) Блок управления дисплеями; 2) ЦАП, АЦП

и силовой ключ; 3) COM порт и USB программатор; 4) Кнопки, клавиатура, звуковая и световая индикация. Все 4 блока подключены и непосредственно взаимодействуют между собой с помощью микроконтроллера.

В результате проделанной работы был получен прибор, который по функциональным возможностям не уступает аналогам, представленным на рынке, и имеет относительно дешевую стоимость. Лабораторный стенд является универсальным и может применяться для обучения в любых учебных заведениях для подготовки квалифицированных кадров широкого и узкого профиля. Широкая функциональность стенда позволит решать большинство учебных задач.

Список использованной литературы:

1. Бойт К. Цифровая электроника. -М: Техносфера, 2007.

2. Амосов В.В. Схемотехника и средства проектирования цифровых устройств. -СП: БХВ-Петербург, 2007.

3. Учебное оборудование, учебные лабораторные стенды [Электронный ресурс]: Режим доступа: http://www.labfor.ru/

ПРОБЛЕМЫ ЗАЩИТЫ ИСПДн В ВУЗах

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

В силу своей специфики в ВУЗе хранится и обрабатывается огромное количество информации, связанной с обеспечением учебного процесса, внеучебной деятельности, научных разработок, международного сотрудничества, служебная, коммерческая и иная конфиденциальная информация, в том числе персональные данные (ПДн) студентов, сотрудников, посетителей, абитуриентов, и других категорий субъектов ПДн. ПДн это важная и ценная информация о человеке, и государство требует от операторов, обрабатывающих ПДн, выполнение требований законодательства. ВУЗы являются операторами ПДн, и соответственно, на них распространяется действие закона о 152-ФЗ «О персональных данных».

Выполнив анализ существующей в данный момент нормативно-правовой базы, стандартов, требований и методических рекомендаций, а также сложившегося практического опыта в области информационной безопасности становится очевидным, что разработать эффективную систему защиты информационных систем можно только в соответствии с действующими требованиями руководящих документов и рекомендаций.

Поэтому ВУЗы, как правило, обращаются к коммерческим организациям, оказывающим услуги в области защиты информации. Это увеличивает расходы на защиту ПДн, но гарантирует более качественную работу и отлаженную систему защиты информации с полным пакетом документации.

Основными проблемами, с которыми сталкиваются при организации защиты ПДн в ВУЗе, являются: территориальная рассредоточенность ресурсов информационных систем, большое количество серверов, к которым привязаны ИСПДн, порой с разными уровнями защищенности, выход многих ИСПДн в глобальные инфо-телекоммуникационные сети и сети общего пользования. Поэтому самым разумным подходом будет являться рассмотрение каждой ИСПДн отдельно, а уже затем рассматривать их в совокупности.

В соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», требования по защите персональных данных в ИСПДн зависят от уровня защищенности ИСПДн.

Все ИСПДн по категориям обрабатываемых данных делятся на:

- обрабатывающие специальные категории персональных данных (ИСПДн-С);
- обрабатывающие биометрические категории персональных данных (ИСПДн-Б);

- обрабатывающие иные персональных данных (ИСПДн-И).

- обрабатывающие общедоступные персональные данные (ИСПДн-О).

Отдельно выделены информационные системы, обрабатывающие персональные данные только сотрудников оператора.

В постановлении приведены три типа актуальных угроз.

- 1 тип. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении (операционная система)

- 2 тип. Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении (программы обработки ПДн)

- 3 тип. Угрозы, не связанные с наличием недокументированных (недекларированных) возможностей

При этом в документе не дается указаний на способы выявления недекларированных возможностей программного обеспечения. Это привело к наличию различных точек зрения на этот вопрос.

Если программное обеспечение лицензионное, выпущено серийно и имеет широкое распространение, то с большой долей вероятности можно сказать, что недекларированные возможности в нем отсутствуют. В противном случае есть высокая вероятность наличия недокументированных функций, способных нанести вред.

Таблица 1. Уровни защищенности ИСПДн

Тип ИСПДн	Сотрудники оператора	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн-С	Нет	> 100 000	УЗ-1	УЗ-1	УЗ-2
	Нет	< 100 000	УЗ-1	УЗ-2	УЗ-3
	Да				
ИСПДн-Б			УЗ-1	УЗ-2	УЗ-3
ИСПДн-И	Нет	> 100 000	УЗ-1	УЗ-2	УЗ-3
	Нет	< 100 000	УЗ-2	УЗ-3	УЗ-4
	Да				
ИСПДн-О	Нет	> 100 000	УЗ-2	УЗ-2	УЗ-4
	Нет	< 100 000	УЗ-2	УЗ-3	
	Да				

АРМ пользователей одной ИСПДн находятся в разных зданиях, у пользователей, как правило, различные права доступа к обрабатываемой информации в зависимости от цели обработки. Подключение к сети Интернет осуществляется по выделенной линии. Межсетевое экранирование от сети Интернет осуществляется не сертифицированными межсетевыми экранами. В зданиях ВУЗа введен пропускной режим, что не допускает несанкционированный доступ в помещения университета. В помещениях установлены системы пожарной сигнализации, охранной сигнализации, двери помещений в нерабочее время закрываются на замок.

Типичная ситуация для ВУЗа это обработка специальных ПДн субъектов которые могут являться или не являться сотрудниками оператора в количестве до 100 000, актуальные угрозы третьего типа (для АС). Модель угроз строится на основе «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработанной ФСТЭК России в 2008 году. То есть, большая часть ИСПДн будет отнесена к 3 уровню защищенности, однако встречаются ИСПДн с другим уровнем защищенности.

Разногласия между заказчиком (ВУЗом) и исполнителем возникают в основном в части устанавливаемого ПО и оборудования - денежных средств не всегда хватает для проведения полного объема мероприятий. Приказ 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" предусматривает наличие компенсирующих мер при невозможности выполнения обязательных, но и этого не всегда достаточно и прибегают к понижению уровня защищённости. Если в ИСПДн обрабатывается биометрическая информация вместе с иными ПДн, то ищут пути убрать её из процесса обработки. Пример – фото сотрудника на пропуск хранится в ИСПДн, для неё характерны угрозы 3 типа, следовательно, ИСПДн можно отнести к 3 УЗ, но если фото на пропуск вклеивает сам сотрудник, а из ИСПДн фото удаляется, то уровень защищенности может понизиться до 4. Это значит, что большинство требований перестают быть обязательными для выполнения, можно сократить расходы на техническую и программную составляющую системы защиты и обойтись только организационными мерами защиты.

В реальном ВУЗе, который брался за основу разработки, ИСПДн имеют 3 УЗ, соответственно для выполнения большинства требований на АРМ и серверах оказалось достаточно установить антивирус, СЗИ НСД с токеном и персональный межсетевой экран соответствующих классов и сертифицированных ФСБ и ФСТЭК России. При выборе данных средств защиты руководствовались как эффективностью, так и экономической целесообразностью. Все СЗИ имеют централизованное управление и управляются администратором безопасности или штатным специалистом по защите информации.

На данный момент в учебном заведении уже установлена и настроена данная система защиты персональных данных. Все СЗИ настроены в соответствии с матрицей доступа. Так же были разработаны инструкции для операторов ИСПДн и администраторов безопасности. Система успешно функционирует, сообщений об ошибках и сбоях не поступало.

ВУЗ, как оператор ПДн, успешно прошел проверку государственных регуляторов на предмет выполнения требований закона №152-ФЗ «О персональных данных».

В силу ряда особенностей операторам ПДн сложно самостоятельно разработать, установить и настроить эффективную, отвечающую всем требованиям законодательства систему защиты, поэтому в нашем регионе они чаще всего прибегают к услугам коммерческих предприятий, занимающихся информационной безопасностью. Они предлагают ВУЗу индивидуальные проекты, которые согласовываются на всех этапах построения и, при наличии жестких рамок, не позволяющих реализовать ни один из предложенных проектов, ищут альтернативные пути защиты или ухода от защиты.

Список использованной литературы:

1. О персональных данных: Федеральный закон от 27 июля 2006 № 152-ФЗ (ред. от 23.07.2013 N 205-ФЗ): [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: http//www.consultant.ru.

2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 № 149-ФЗ (ред. от 02.07.2013): [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: http//www.consultant.ru.

3. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119: [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: http//www.consultant.ru.

4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных

системах персональных данных: Приказ ФСТЭК России от 18.02.2013 № 21: [Электронный ресурс] – электронные данные. – Программа информационной поддержки российской науки и образования // справочные правовые системы Консультант Плюс: Высшая школа. – 2013. – Режим доступа: http//www.consultant.ru.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ТЕХНОЛОГИЙ ДЛЯ ПРОЕКТИРОВАНИЯ ФИЗИЧЕСКОЙ АРХИТЕКТУРЫ СЕТИ ПРОВАЙДЕРА

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

Растущая конкуренция на рынке телекоммуникаций заставляет операторов искать новые решения, которые позволят расширить спектр предлагаемых услуг, снизить расходы на сопровождение сети, повысить прибыльность и привлечь новых клиентов. Такие решения также должны обеспечивать хорошую масштабируемость и быть рассчитаны на быстрый рост клиентской базы и внедрение новых приложений, требующих поддержки функций качества обслуживания и значительной полосы пропускания.

Построение современной сети городского оператора связи представляет собой нетривиальную задачу, при решении которой надо учитывать множество факторов. На выбор топологии и оборудования влияют доступность и пропускная способность каналов связи, плотность и распределение абонентов в черте города, спектр имеющихся и планируемых услуг.

Городские телекоммуникационные сети строятся на базе разных технологий, каждая из которых имеет как преимущества, так и недостатки. Рассмотрим некоторые технологии для проектирования физической архитектуры сети провайдера, такие как Synchronous Digital Hierarchy (SDH), Frame Relay (FR), Multiprotocol label switching (MPLS), Metro Ethernet (ME).

Обычно в составе городских сетей выделяют три иерархических уровня — уровень доступа, уровень агрегации и уровень ядра. Каждый из них выполняет определенные функции, что влияет на выбор технических решений.

Технология SDH строится по типу сетевой топологии кольцо и дает массу преимуществ, как операторам связи, так и их клиентам. Она обеспечивает высокую пропускную способность. Протоколы SDH предоставляют большую гибкость при упаковке различного рода полезной нагрузки. Это очень важно, поскольку многие приложения нуждаются в довольно узкой полосе пропускания, надо собирать в единый поток разные типы трафика - будь то ATM, IP или классический телефонный. Будучи иерархическими по своей структуре, системы SDH имеют возможность "объединять" низкоскоростные потоки в широкие "трубы" на магистрали сети.

Одно из главных преимуществ SDH - это высокая отказоустойчивость. Даже в случае обрыва оптоволокна пользователи могут быть уверены, что коммуникационный сервис восстановится практически мгновенно благодаря встроенному в системы SDH 50-мс механизму переключения.

Недостатком сетей SDH является то, что изначально спроектированные для передачи телефонного трафика (в режиме TDM), они не оптимизированы для IP-приложений. Построение кольцевых инфраструктур SDH занимает довольно много времени, а внесение каких-либо изменений, модернизация кольца или добавление нового могут оказаться очень сложными задачами. И достаточно важную роль в выборе данной технологии является высокая стоимость оборудования SDH, особенно по сравнению с технологией Ethernet.

Технология Frame Relay в основном используется для маршрутизации протоколов локальных сетей через общие (публичные) коммуникационные сети. Frame Relay обеспечивает передачу данных с коммутацией пакетов через интерфейс между оконечными устройствами пользователя Data terminal equipment (DTE) (маршрутизаторами, мостами, ПК)

и оконечным оборудованием канала передачи данных Data circuit-terminating equipment (DCE).

Коммутаторы Frame Relay используют технологию сквозной коммутации, т.е. кадры передаются с коммутатора на коммутатор сразу после прочтения адреса назначения, что обеспечивает высокую скорость передачи данных. В сетях Frame Relay применяются высококачественные каналы передачи, поэтому возможна передача трафика чувствительного к задержкам (голосовых и мультимедийных данных). В магистральных каналах сети Frame Relay используются волоконно-оптические кабели, а в каналах доступа может применяться высококачественная витая пара.

К достоинствам сети Frame Relay можно отнести высокую надежность работы сети и обеспечение передачи трафика, чувствительного к временным задержкам (голос, видеоизображение).

Недостатки сети Frame Relay – это, прежде всего, высокая стоимость качественных каналов связи и отсутствие механизмов, обеспечения достоверности доставки кадров.

Технология MPLS является масштабируемым и независимым от каких-либо протоколов механизмом передачи данных. В сети, основанной на MPLS, пакетам данных присваиваются метки. Решение о дальнейшей передаче пакета данных другому узлу сети осуществляется только на основании значения присвоенной метки без необходимости изучения самого пакета данных. За счет этого возможно создание сквозного виртуального канала, независимого от среды передачи и использующего любой протокол передачи данных. MPLS позволяет достаточно легко создавать виртуальные каналы между узлами сети. Технология позволяет инкапсулировать различные протоколы передачи данных.

Основным преимуществом MPLS является независимость от особенностей технологий канального уровня, таких как Frame Relay, SONET/SDH или Ethernet, и отсутствия необходимости поддержания нескольких сетей второго уровня, необходимых для передачи различного рода трафика. По виду коммутации MPLS относится к сетям с коммутацией пакетов, что тоже является преимуществом.

Одним из главных недостатков протокола MPLS является прерывание обслуживания при сбое, а так же высокая стоимость оборудования MPLS.

Metro Ethernet, как среда реализации коммуникационных сервисов представляет собой технологическую базу для доставки услуг. Это понятие охватывает оптические и другие сети Ethernet в масштабе города. Решения Metro Ethernet все больше становятся основной сервисной архитектурой в городах и все более привлекают городских операторов, поскольку при эквивалентной пропускной способности они обходятся в два-три раза дешевле других технологий.

Выбор технологии Metro Ethernet как серьезной альтернативы другим вариантам сетей городского масштаба обусловлено ростом требований к полосе пропускания в связи с появлением новых типов приложений, высокой концентрацией абонентов в офисных и жилых зданиях, низкой стоимостью первоначальных затрат и затрат на поддержку, большим количеством специалистов, имеющих опыт работы с Ethernet.

Решение Metro Ethernet обеспечивает мультисервисность и высокую надежность инфраструктуры, низкую стоимость развертывания сети, отличную масштабируемость по количеству портов, производительности узлов и скорости каналов, единую технологию, механизмы сигнализации и управления для всей сети, и максимальную автоматизацию управления сетью и активации услуг, поддержку средств самообслуживания клиентов.

Рост требований к емкости городских сетей и успех существующих операторов Metro Ethernet ясно показывают, что данная модель предоставления телекоммуникационных услуг на базе Ethernet в городских сетях конкурентоспособна, востребована и прибыльна для операторов связи. И так же позволяет обеспечить основу для value-added сервисов, таких как Voice over Internet Protocol (VoIP) и IPTV, хранение информации.

Архитектура сети Metro Ethernet разработана с учетом масштабируемости, высокой производительности, надежности и доступности, управляемости, безопасности, а также возможности быстрого внедрения новых услуг.

Многие Интернет-провайдеры такие как «Ростелеком», «Дианет», «ЭР-Телеком», строят свою сеть по этой технологии. Metro Ethernet является оптимальной технологией для развертывания надежной, производительной архитектуры сети провайдера. Так же в условиях жесткой конкуренции провайдеры стремятся быстро развернуть сеть в микрорайонах города и подключить большее количество абонентов к сети, а данная технология позволяет снизить затраты на подключение конечного пользователя.

Список использованных источников:

1.Олифер, В.Г.,Олифер, Н.А. Компьютерные сети. Принципы, технологии, протоколы, 4-е издание. – СПб.: Питер, 2010. – 944 с.:ил.

2.Магистральный участок городских сетей [Электронный ресурс] / Режим доступа: http://www.linkc.ru/article.php?id=245, свободный.

3.MetroEthernet. Что такое MetroEthernet? [Электронный ресурс] / Режим доступа: http://qwerty.ru/services/net/qwerty_net/metroethernet/ , свободный.

БЕЗОПАСНОСТЬ МОБИЛЬНОЙ СВЯЗИ: ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ЕЕ ОБЕСПЕЧЕНИЯ

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

Современные технологии прочно вошли в нашу жизнь. Но, несмотря на очевидные преимущества, которые дал нам прогресс, такое стремительное развитие техники сопряжено с рядом проблем, в том числе и проблемой безопасности. Теперь, чтобы получить конфиденциальную информацию, злоумышленнику возможно даже не понадобится выходить из дома. Принимая во внимание то, что информация сейчас является наиболее ценным «товаром», игнорирование вопроса ее защиты – это как минимум беспечность.

К сожалению, многие считают, что защита информации касается только государственных или коммерческих структур, а нарушитель непременно должен устанавливать жучки, микрофоны, скрытые камеры и т.д. Тем не менее, это не так. Номера карт, паспортные данные, код от замка – каждый из нас хотя бы раз передавал по мобильному телефону информацию, которую бы хотел скрыть от других. И не задумывался о том, что его могут прослушивать.

Актуальность данной работы в том, что в настоящее время мобильная связь распространена повсеместно, однако сохраняются проблемы, связанные с безопасностью телефонных переговоров.

Цель работы: исследование проблем безопасности мобильной связи, а также способы обеспечения защиты информации во время телефонных переговоров.

Для достижения цели были выбраны следующие *задачи*:

1. Оценка современного состояния организации защиты информации, передаваемой по мобильной связи.
2. Выявление проблем, связанных с обеспечением безопасности мобильной связи.
3. Исследование альтернативных способов защиты мобильной связи, а также оценка перспективы усовершенствования существующих стандартов связи.

Предмет исследования – обеспечение безопасности мобильной связи. В качестве *объекта исследования* выбран стандарт цифровой мобильной связи GSM.

Методологической базой при выполнении работы послужили законодательные и нормативные акты в сфере информационной безопасности, научные статьи, а также некоторые статистические данные.

В соответствии со ст.23 п.2 Конституции РФ «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения». Тем не менее, как утверждают специалисты, 4 млрд. абонентов сотовой связи по всему миру стали уязвимы для нелегального прослушивания телефонов. Стандарту GSM (Global System for Mobile communications) принадлежит 80% мирового рынка цифровой мобильной связи. В России эта цифра достигает порядка 100% [3,5].

По своему замыслу, цифровая система мобильной связи GSM вполне могла бы быть чрезвычайно защищенной. Ведь в создании схемы безопасности активное участие приняли спецслужбы стран НАТО. Основу системы безопасности GSM составляют три секретных алгоритма (официально не раскрытые и поныне): алгоритм аутентификации (для защиты от клонирования); алгоритм генерации криптоключа, алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров А5. В GSM используются две основные разновидности алгоритма: A5/1 - "сильная" версия шифра для избранных стран и A5/2 - ослабленная для всех остальных (для России) [5,6].

Вся эта архитектура при надлежащем исполнении и качественных алгоритмах призвана гарантировать надежную защиту абонентов. Однако спецслужбы должны не только защищать правительственные коммуникации, но и перехватывать их (коммуникации) в разведывательных целях. А5 реализует поточный шифр на основе трех линейных регистров сдвига с неравномерным движением, однако, длины регистров выбраны очень короткими – в сумме дает 64-битный сеансовый ключ шифрования в GSM. Алгоритм этот был разработан более 20 лет назад и не претерпевал изменений до сегодняшнего дня. И это несмотря на то, что уже на практике проверена атака, которая позволяет вскрыть ключ примерно за 2 секунды, а еще в 1998 г. группа компьютерных экспертов из Калифорнии продемонстрировала, что ей удалось клонировать мобильный телефон стандарта GSM. Шифр A5/2 создавался для облегчения вскрываемости, но в официальных результатах анализа сказано, что никаких криптографических дефектов алгоритма не найдено [4,6,7].

Один из членов Smartcard Developer Association подвел промежуточный итог своим изысканиям в области соотношения декларируемой и истинной безопасности системы GSM:

- в 64-битном ключе последние 10 бит обнулены, защита ослабляется примерно в 1000 раз;
- уязвимости системы аутентификации и алгоритма генерации секретного ключа позволяют клонировать телефоны и вычислять секретные ключи абонентов в ходе сеанса связи;
- в 64-битном ключе имеются многочисленные дефекты – стойкость понижена в 1000000 раз;
- всегда имеется возможность подключиться непосредственно к базовым станциям, где уже нет никакого шифрования. Единственной причиной для тотального ослабления криптозащиты оказывается "нелегальный доступ" без каких либо ордеров и санкций [1,2].

Однако, есть решения для этой ситуации, хотя и весьма недешевые. Есть два типа устройств, предназначенных для полного шифрования трафика: аналоговые скремблеры и цифровые шифраторы. Использование подобных устройств позволяет защитить переговоры от прослушивания на любом участке передачи (разумеется, кроме непосредственного прослушивания микрофонами). По принципу работы различают 2 вида скремблеров: аддитивные и самосинхронизирующиеся.

Основной частью самосинхронизирующегося скремблера (СС) является генератор псевдослучайной последовательности (ПСП) в виде линейного n-каскадного регистра с обратными связями, формирующий последовательность максимальной длины $2^n - 1$. СС скремблер управляется последовательностью, которая передается в канал, поэтому при данном виде скремблирования не требуется специальной установки состояний скремблера и дескремблера: скремблированная последовательность записывается в регистры сдвига скремблера и дескремблера, устанавливая их в идентичное состояние. К недостаткам СС

скремблеров-дескремблеров относится свойство размножения ошибок. Данный недостаток ограничивает число обратных связей в регистре сдвига (не больше 2). Второй недостаток СС скремблера – возможность появления на его выходе т.н. «критических ситуаций» (выходная последовательность приобретает периодический характер с периодом, меньшим длины ПСП). При аддитивном скремблировании требуется предварительная идентичная установка состояний регистров скремблера и дескремблера. В скремблере с установкой производится суммирование входного сигнала и ПСП, но результирующий сигнал не поступает на вход регистра. В дескремблере скремблированный сигнал также не проходит через регистр сдвига, поэтому размножения ошибок не происходит. Суммируемые в скремблере последовательности независимы, поэтому их период всегда равен наименьшему общему кратному величин периодов входной последовательности и ПСП и критическое состояние отсутствует. Отсутствие эффекта размножения ошибок и необходимости в специальной логике защиты от нежелательных ситуаций делают способ аддитивного скремблирования предпочтительнее, если не учитывать затрат на решение задачи синхронизации скремблера и дескремблера [5,6,8].

В основном такие устройства распространяются иностранными фирмами, а их цена зависит от надежности и оригинальности алгоритма. Отечественные разработки тоже имеются, при этом стоят на порядок дешевле. Хотя и этот вариант не выход для рядовых абонентов. Если компании и организации могут защитить свои телефоны с помощью специализированных средств защиты, то рядовым пользователям можно только посоветовать не сообщать важную информацию по телефону, следить за телефонными счетами и использовать PIN защиту. Т.к. усиление безопасности алгоритмов не выгодно самим создателям стандарта связи GSM и в ближайшее время вряд ли они начнут предпринимать попытки по ликвидации уязвимостей.

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

3. Конституция Российской Федерации [Текст]: офиц. текст. - М.: Маркетинг, 2001. - 39, [1] с.

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

5. Скремблер – защита телефонных переговоров [Электронный ресурс]. Режим доступа: http://www.skrembler.ru/

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

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

8. Скремблер – Википедия [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D1%80%D0%B5%D0%BC%D0%B1%D0%BB%D0%B5%D1%80#.D0.A1.D0.B0.D0.BC.D0.BE.D1.81.D0.B8.D0.BD.D1.85.D1.80.D0.BE.D0.BD.D0.B8.D0.B7.D0.B8.D1.80.D1.83.D1.8E.D1.89.D0.B8.D0.B5.D1.81.D1.8F_.D1.81.D0.BA.D1.80.D0.B5.D0.BC.D0.B1.D0.BB.D0.B5.D1.80.D1.8B

РАСПРЕДЕЛЕННАЯ СИСТЕМА КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ С WEB-ИНТЕРФЕЙСОМ

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

В последнее время широкое распространение получили системы контроля и управления доступом (СКУД). Такие системы представляют собой совокупность программно-технических средств, имеющих целью обеспечение безопасности предприятия путем ограничения и/или регистрации входа-выхода объектов (людей, транспорта) на заданной территории через двери, ворота, проходные (т. н. «точки прохода»). Примеры объектов, на которые ставятся СКУД:

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

Целью работы является создание программно-аппаратного комплекса для контроля доступа, отличающегося от известных расширением круга управляющих доступом лиц за счет применения для управления доступом web - интерфейса. Данный комплекс может быть использован для всех вышеперечисленных объектов, для которых может потребоваться распределение полномочий по управлению доступом между несколькими лицами и ограниченный по времени пребывания доступ в которые нужно предоставлять не работающим на этих объектах посетителям или клиентам.

При использовании разработанной СКУД работающий на объекте персонал, обладающий соответствующими полномочиями, может сам управлять режимом доступа к себе посетителей (например, клиентов организации, представителей оказывающей аутсорсинговые услуги фирмы, временных работников, посещающих предприятие непродолжительное время в рамках выполнения работ по договорам подряда или иным гражданско-правовым договорам). Этим лицам для доступа предоставляется пароль, который будет необходимо ввести для попадания на объект на цифровой панели. Возможна также реализация доступа по RFID - карточкам (карточки радиочастотной идентификации), либо по цифровым ключам Touch Memory фирмы Dallas, широко применяемым в домофонах. При этом персонал может указывать интервал времени, в течение которого клиент или иной посетитель может находиться в зоне ограниченного доступа. В предлагаемой СКУД предусмотрен также отдельный администратор базы данных, который может добавлять как посетителей, так и персонал, а также просматривать лог событий (кто и когда добавил, удалил или изменил список гостей, когда пришел и ушел тот или иной посетитель). У персонала и у администратора есть логин и пароль, с помощью которого они могут заходить в систему с любого компьютера или мобильного устройства, имеющего выход в Интернет. Персонал может только добавлять, изменять и удалять своих гостей, а администратор может редактировать любые записи. Структура базы данных приведена на рис. 1.

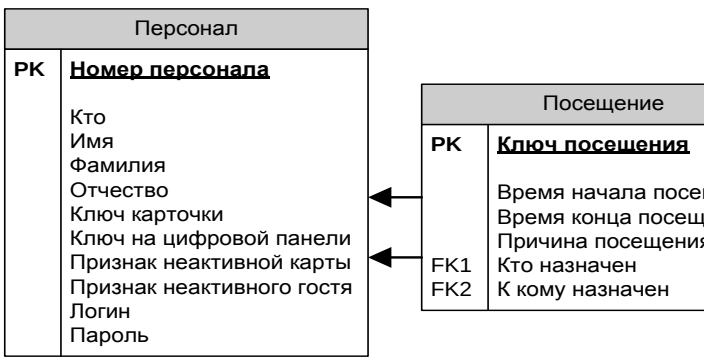


Рис. 1 – структура базы данных.

Программное обеспечение для СКУД написано на языке PHP. В качестве системы управления базами данных используется MySql. Также используется объектно-ориентированный подход,

который достигается с применением фреймворка Propel ORM, который генерирует PHP классы. В качестве WEB сервера можно использовать Apache. Все четыре компонента системы (PHP, Apache, MySql и Propel ORM) являются свободно распространяемыми программными продуктами. Сервер может быть установлен на Linux Ubuntu, которая также является свободной распроняемым продуктом.

Данный комплекс позволяет отказаться от бюро пропусков на предприятии, сделав процесс добавления, изменения и удаления посетителей более удобным, так как при его использовании персонал сможет сам управлять этим процессам в рамках выделенных ему прав. Однако следует понимать, что применение данной СКУД невозможно без принятия соответствующих организационных мер безопасности, поскольку любой сотрудник, имеющий право на допуск к себе посетителей, должен брать на себя ответственность за то время, пока эти ипосетители находятся на территории охраняемой зоны.

Уже реализован прототип такой системы, ориентированной на ее применение в рамках Алтайского государственного технического университета, но можно сделать и универсальный конструктор, который позволит добавлять группы пользователей предприятия при установке программы и генерировать соответствующие для работы СКУД PHP-файлы и код. Также можно будет назначать, какие группы пользователей имеют логин и пароль, то есть могут добавлять гостей, а какие - нет. Тогда данное приложение станет универсальным и сможет применяться на любом предприятии.

ПРОГРАММНО-ТЕХНИЧЕСКИЙ КОМПЛЕКС ДЛЯ РЕГИСТРАЦИИ ДВИГАТЕЛЬНОЙ АКТИВНОСТИ

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

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

В настоящее время на рынке представлены различные устройства, использующие МЭМС акселерометры и гироскопы для обнаружения и регистрации движений. Среди них можно выделить узкоспециализированные например, шагомеры, предназначенные для регистрации двигательной активности спортсменов (они обладают ограниченным функционалом и способны обрабатывать и распознавать только простые движения) и отладочные платы общего назначения (примером такого устройства является MOD-MMA7260 компании OLIMEX ltd.[1]), которые оснащены USB интерфейсом для подключения к ПК и позволяют получать и просматривать данные только в режиме реального времени. Поскольку существующие системы не позволяют проводить эксперименты, во время которых будет происходить запись в энергонезависимую память для дальнейшего анализа данных и разработки алгоритмов, а также не позволяют выполнить одновременное подключение нескольких сенсоров, возникает необходимость разработки собственного устройства.

Целью работы является создание устройства, позволяющего выполнять прием данных, поступающих с одного или нескольких МЭМС акселерометров и гоироскопов, и выполнять их запись для дальнейшего анализа. Устройство должно предоставлять разработчику возможность просматривать данные в режиме реального времени в ходе эксперимента на

экране персонального компьютера, поводить эксперименты без подключения к ПК и хранить записываемые данные. В дальнейшем разрабатываемое устройство может быть использовано в качестве модуля в системе Холтеровского мониторинга, технического контроля либо в системах инерционной навигации.

В разрабатываемом устройстве используется микроконтроллер компании Atmel, который принимает данные с датчика MPU-6050 и в зависимости от режима работы передает их на персональный компьютер или производит запись. Данный датчик является акселерометром и гироскопом, выполненными в одном корпусе, и имеет широкий диапазон измерений (±2*g*/±4*g*/±8*g*/±16*g* для акселерометра и ±250/±500/±2000 °/с для гироскопа[2]), низкое энергопотребление, а также оснащен цифровым интерфейсом I^2C, что упрощает работу с ним. Кроме того, возможно использовать программируемые прерывания от датчика при готовности данных для обнаружения свободного падения или движения. Данный датчик имеет ряд преимуществ по сравнению с другими, например, датчик LIS3LV02DQ имеет схожие характеристики акселерометра, но в нем отсутствует гироскоп. Одновременное использование акселерометра и гироскопа обусловлено тем, что акселерометр регистрирует на все ускорения, а значит, может передать одинаковые результаты, как при повороте, так и при ускоренном движении в одной плоскости. Использование раздельного акселерометра и гироскопа может увеличить как сложность изготовления изделия, так и его стоимость. Еще одним преимуществом является наличие цифрового интереса, в некоторые датчики, например, LSM320HAY30, оснащены аналоговым выходом, что требует использование дополнительных ресурсов микроконтроллера при получении и обработке данных.

Подключение к персональному компьютеру для обмена данных осуществляется с помощью интерфейса USB, поскольку данным интерфейсом оснащены все современные ПК, нет необходимости использовать переходники и преобразователи интерфейсов. Запись данных при автономной работе осуществляется на карту памяти SD. Разрабатываемое программное обеспечение позволяет отображать данные об угловой скорости и ускорении в виде таблиц и графиков, а также сохранять их для дальнейшего анализа.

Также стоит отметить невысокую стоимость компонентов разрабатываемого устройства, составляющую около 700р.

Список использованных источников:

1. MOD-MMA7260 [Электронный рессурс] // Режим доступа: https://www.olimex.com/Products/Modules/Sensors/MOD-MMA7260/

2. MPU-6000/6050 Six-Axis (Gyro + Accelerometer) MEMS MotionTracking™ Devices [Электронный ресурс] // Режим доступа: http://invensense.com/mems/gyro/mpu6050.html

РАЗРАБОТКА СИСТЕМЫ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ ПРОЦЕССОМ ПОДЪЕМА КОЛЕБЛЮЩЕЙСЯ ПОВЕРХНОСТИ МАЯТНИКОВОГО ДЕФОРМАТОРА

Перминов Т.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.

Установка «Лабораторный маятниковый деформатор» [3] - инновационная технология в области переработки зерна. Она предназначена для деформации зерна на стадии его подготовки к размолу. Деформатор разворачивает зерно, отделяя оболочку. После вымола дробленного таким образом зерна на вальцовых станках выход муки высшего качества повышается на 3,5...5% по отношению к традиционным способам помола. Энергозатраты на

помол в целом снижаются на 5...10%. Конструкция деформатора создана на основе патента №2263544 "Способ формирования зерновых продуктов размола" [1].

На текущий момент установка полностью механическая. Для автоматизации управления деформатором необходимо реализовать связку «механика – электроника – микроконтроллер – программа для ПК».

1) Механическая часть [5] будет состоять из трех основных частей: каретки, захватывающего устройства и направляющей. Последняя будет крепиться к нижней опоре деформатора и иметь форму изогнутой трубки с продольным разрезом. По направляющей будет ходить каретка с прикрепленным на ней захватывающим устройством, которое будет иметь форму пассатижей и удерживать маятник силой двух пружин.

Предложенная система удовлетворяет всем предъявляемым требованиям:

- стоимость необходимых элементов мала, основная сумма уйдет на приобретение шагового двигателя
- возможность поднять маятник с нейтрального положения, что очень важно, это сделает систему полностью автоматической;
- невысокое энергопотребление – на удержание маятника в верхнем положении не требуется никаких затрат электроэнергии;
- безопасность для оператора деформатора;
- надежность – деталей не много, они не представляют собой сложных или высокоточных механизмов.

К тому же реализация этого способа не повлечет каких-либо серьезных изменений всей конструкции. Поэтому он выбран наиболее совершенным из всех предложенных ранее, и было принято решение сделать чертежи для механических частей, необходимых для создания этого способа.

2) Электромеханическая часть будет состоять из шагового электродвигателя [2] и толкающего соленоида. Шаговый двигатель с помощью прикрепленного на вал троса будет управлять кареткой и, соответственно, углом наклона маятника. Толкающий соленоид будет в нужный момент размыкать захватывающее устройства для спуска маятника.

Был выбран шаговый двигатель Dunazun 4SHG-023A 39S. Этот двигатель имеет не только оптимальные технические (момент вращения, рабочие напряжение и ток), но также и физические характеристики (небольшие габариты и масса).

3) Электрическая часть будет состоять из микроконтроллера семейства AVR и нескольких драйверов (для управления двигателем, соленоидом).

В качестве драйвера шагового двигателя была взята связка микросхем «L298N+L297». L297 – непосредственно сама микросхема управления шаговым двигателем. Позволяет вращать вал двигателя как по, так и против часовой стрелки, задавать скорость вращения, выбрать режим (шаг/полушаг). Имеется возможность синхронизации нескольких таких микросхем. L298N – мостовой драйвер двигателей. Обеспечивает максимальную нагрузку до 4А.

В качестве драйвера соленоида была взята связка «биполярный транзистор BDW93C + оптопара PC817». Такое решение позволяет физически развязать цепь управления от силовой цепи, не подвергая основной контроллер опасности выйти из строя из-за больших токов.

В качестве основного контроллера был выбран микроконтроллер AT32UC3A1512AU семейства AVR. Для решения поставленной задачи он подходит идеально: имеется аппаратный USB 2.0, 8-канальный АЦП, 512 кбайт Flash-памяти, рабочая частота до 66 МГц, 69 портов ввода-вывода. Такое большое количество портов необходимо для дальнейшего развития автоматизированной системы управления деформатором. Добавятся несколько драйверов и других устройств, которые также будут управляться контроллером.

Электронную часть было решено разделить на несколько блоков: основная (управляющая) микросхема и драйверы устройств будут реализованы в виде разных плат, соединенных шлейфами.

Такой способ построения электронной части дает ряд преимуществ:

1 Простота реализации и сборки – при проектировании системы на одной плате ее пришлось бы делать многослойной, в данном же случае получится набор простых однослойных плат, соединенных шлейфами;

2 Отсутствие сложностей при дальнейшем совершенствовании системы – достаточно лишь подключить новые устройства к управляющей плате;

3 Простота в определении и устранении неисправностей – при выходе из строя одной из плат достаточно заменить лишь ее.

4) Программная часть. В качестве языка программирования был выбран C#. Для него есть готовые библиотеки для работы с интерфейсом USB, а также множество других открытых библиотек, которые позволят сделать удобную многофункциональную программу автоматизированного управления маятниковым деформатором.

На данный момент детально проработана механическая часть: проведены все расчеты, выполнены чертежи необходимых элементов. Разработаны и реализованы драйверы шагового двигателя и соленоида. Разработана управляющая плата.

Следующий этап – реализация механической части, установка всех частей на деформатор и написание управляющей программы [4].

Список использованной литературы:

1) Злочевский В. Л. Способ размола зерновых и зернистых материалов: пат. 2407590. – Российская Федерация. – 2009. – 7 с.

2) Кенио Т. Шаговые двигатели и их микропроцессорные системы управления: Пер. с англ. – М.: Энергоатомиздат, 1987. – 200 с.: ил.

3) Лабораторный маятниковый измельчитель [Электронный ресурс]: Центр Научно-Технического Развития Зерноперерабатывающей Промышленности. – Электрон. текст. дан. – Барнаул, 2013. – Режим доступа: http://intensifikachia.ucoz.com/index/majatnikovyj_izmelchitel/0-5

4) Тарасов, В. П. Технологическое оборудование зерноперерабатывающих предприятий. Учебное пособие / В. П. Тарасов; Алт. гос. техн. ун-т им. И. И. Ползунова. – Барнаул : Изд-во АлтГТУ, 2002. – 232 с.

5) Чигарев, А. В. Курс теоретической механики: учеб. пособие / А. В. Чигарев, Ю. В. Чигарев. – Минск: Новое знание, 2010. – 399 с.: ил.

СИСТЕМА МНОГОТОЧЕЧНОГО КЛИМАТИЧЕСКОГО МОНИТОРИНГА

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

В настоящее время информационные технологии играют важную роль во всех сферах жизни и деятельности человека. Особое место в многообразии информационных технологий занимают автоматизированные информационно-измерительные системы (АИИС), основное назначение которых — автоматизация деятельности, связанной со сбором, хранением, накоплением, поиском, передачей, обработкой и визуализацией информации.

На принципах автоматизированных систем сбора данных строятся крупные системы в промышленности и энергетике, в системах транспортного обеспечения и в государственных структурах. Особое место среди них занимают автоматизированные системы метеомониторинга.

Климатический мониторинг лежит в основе работы метеослужб, которые предоставляют так необходимые практически любой отрасли информацию о прогнозе погоды. Они нужны и предприятиям агропромышленного комплекса, и туристическим организациям, и образовательным учреждениям, а своевременные и точные данные метеомониторинга.

Нужны также исследовательским институтам, занимающимся вопросами пргонозирования погоды и изучения климата.

На сегодняшний день многие компании готовы предоставить системы для точечного мониторинга окружающей среды. Примером может быть термогигрометр с каналом измерения давления ИВА-6Н-КП-Д, представленный компанией «Техноком»[1]. Такие устройства обычно оснащаются USB интерфейсом для подключения к персональному компьютеру (ПК), картой памяти, резервным источником питания, а также жидкокристаллическим дисплеем. Однако, практически все системы не предназначены для централизованного сбора информации, имеют закрытый исходный код и протоколы обмена.

Целью работы является создание программно-технического комплекса, осуществляющего сбор информации, передачу данных на сервер обработки и отображение информации для конечного пользователя. В нем предусматривается возможность работы собственно системы сбора данных (ССД) от резервного источника питания (аккумуляторной батареи) во время отсутствия питания от ПК, а также наличие энергонезависимой памяти для сохранения данных, полученных в автономном режиме работы. Программное обеспечение, предназначенное для приема данных с устройства и для передачи на сервер, является кроссплатформенным, чтобы ССД можно было подключать к ПК, или даже к смартфону с любой установленной на нем ОС. Визуализация данных для конечного пользователя осуществляется через web – интерфейс, для чего все передаваемые со всех узлов системы данные консолидируются в единую базу, размещенную на web - сервере. В дальнейшем предполагается, что разрабатываемый программно-технический комплекс может быть использован и как часть системы «умный» дом, если наряду с метеоданными он будет собирать информацию о работе различных систем жизнеобеспечения дома.

В разработанном ССД используется микроконтроллер AT90USB162[2] компании Atmel. Микроконтроллер имеет аппаратную поддержку USB интерфейса — самого распространенного в современное время. Для измерения температуры использован высокоточный цифровой программируемый датчик DS18B20 фирмы Dallas Semiconductors[3]. В качестве датчика влажности — DHT22[4]. Эти датчики подключаются к микроконтроллеру по интерфейсу 1-wire, разработанному компанией Dallas Semiconductros. Для измерения давления используется BMP085 компании BOSCH. Для сопоставления результатов измерения временным интервалам используются часы реального времени в виде цифровой микросхемы DS1307[5], подключающейся к МК по интерфейсу I2C. Выбор составляющих устройства основывается как на технических характеристиках, нацеленных на точность измерения и низкое потребление тока, так и на диапазоне рабочих температур, в которых должно функционировать устройство, который составляет от -30 до 60 С°.

Программное обеспечение для ПК было разработано в кроссплатформенной среде QtSDK, позволяющей использовать устройство на всех популярных операционных системах, таких как Windows, Linux, MacOS. Отображение обработанных на сервере данных не требует от пользователя специальных программных пакетов кроме браузера.

Помимо прочего, стоит также отметить невысокую суммарную стоимость компонентов разрабатываемого устройства, составляющую 1700 рублей.

Список использованной литературы:

1. НПО «Техноком» [Электронный ресурс] // Режим доступа: http://www.tehno.com/

2. AT90USB162 [Электронный ресурс] // Режим доступа: http://www.atmel.com/ru/ru/devices/AT90USB162.aspx

3. DS18B20 Programmable Resolution 1-Wire Digital Thermometer [Электронный ресурс] // Режим доступа: http://www.maximintegrated.com/datasheet/index.mvp/id/2812

4. Humidity and Temperature Sensor — RHT03 [Электронный ресурс] // Режим доступа: https://www.sparkfun.com/products/10167

5. DS1307 64x8, Serial, I^2C Real-Time Clock [Электронный ресурс] // Режим доступа: http://www.maximintegrated.com/datasheet/index.mvp/id/2688

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ, СВЯЗАННЫЕ С НЕСАНКЦИОНИРОВАННЫМ ДОСТУПОМ К ИНФОРМАЦИИ

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

Проблема обеспечения информационной безопасности актуальна с тех пор, как люди стали накапливать, хранить и передавать информацию. Во все времена возникала необходимость надежного сохранения наиболее важных достижений человечества с целью передачи их потомкам. Аналогично возникала необходимость обмена конфиденциальной информацией и надежной ее защиты. Предотвращение компьютерных атак, связанных с несанкционированным доступом (НСД) к информации со стороны злоумышленников, выявление возможных уязвимостей программного обеспечения – первоочередная задача для специалистов, работающих в сфере информационных технологий.

Раскрываемость компьютерных преступлений данного типа находится в настоящее время на низком уровне ввиду того, что очень часто деяния злоумышленников остаются незамеченными, а их жертвы иногда по каким-либо причинам боятся, либо считают нецелесообразным обращаться в правоохранительные органы. По статистике «American Internet Crime Complaint Center» («Центра жалоб по компьютерным преступлениям - IC3»), число жалоб в центр значительно превышает количество обращений, переданных на рассмотрение в правоохранительные органы в случаях возникновения инцидентов компьютерных преступлений.

Данная статистика публикуется ежегодно и служит для выявления необнаруженных инцидентов преступлений в отношении компьютерной информации. Приведенные на рисунках 1-2 диаграммы лишь подтверждают точку зрения о высокой латентности компьютерных преступлений, что является одной из главных причин их низкой раскрываемости. Проанализировав эти данные, можно сделать вывод о том, что порядка 58% преступлений проходят «мимо» поля зрения правоохранительных органов. Обнаруживаются же преступления, как правило, в случаях, приведенных на диаграмме рисунке 3.

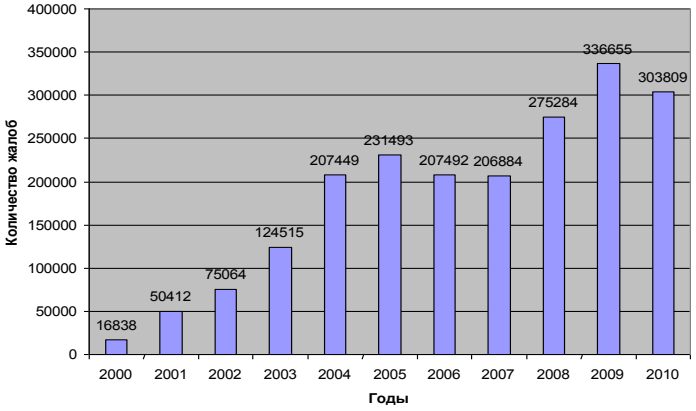


Рисунок 1 - Количество жалоб в IC3 по случаям возникновения инцидентов компьютерных преступлений

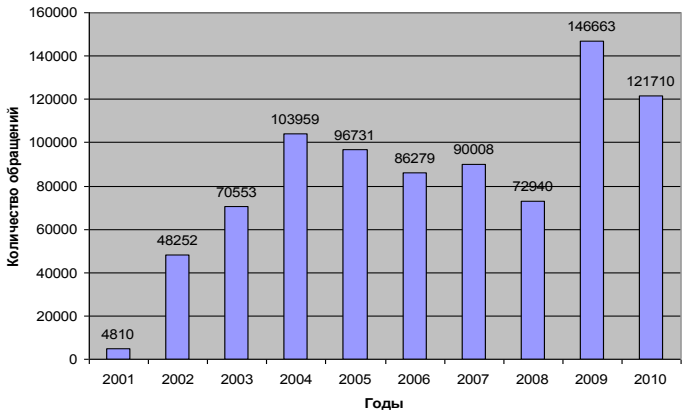


Рисунок 2 - Количество переданных на рассмотрение дел по случаям возникновения инцидентов компьютерных преступлений

Рисунок 3 - Соотношение причин обнаружения случаев компьютерных преступлений при отсутствии соответствующего обращения в правоохранительные органы

На данной диаграмме мы можем наблюдать что, наиболее часто компьютерные преступления обнаруживаются именно проверками службы безопасности.

Для осуществления преступного посягательства злоумышленники чаще всего применяют пять способов, которые приведены ниже:

1) Использование чужих IP-адресов в ЛВС с выходом в Интернет. Следы могут быть представлены в виде IP и MAC-адресов.

2) Использование беспроводного соединения Wi-Fi. Сервер провайдера содержит настройки и некоторые данные злоумышленника.

3) Использование чужого телефонного номера. Следы также можно обнаружить на сервере провайдера.

4) Использование чужого компьютера. Целесообразно воспользоваться файлами регистрации и аудита системных событий. Однако грамотные взломщики такие следы тщательно скрывают.

5) Пользование услугами провайдера, не хранящего данные о своих пользователях. Следов не остается.

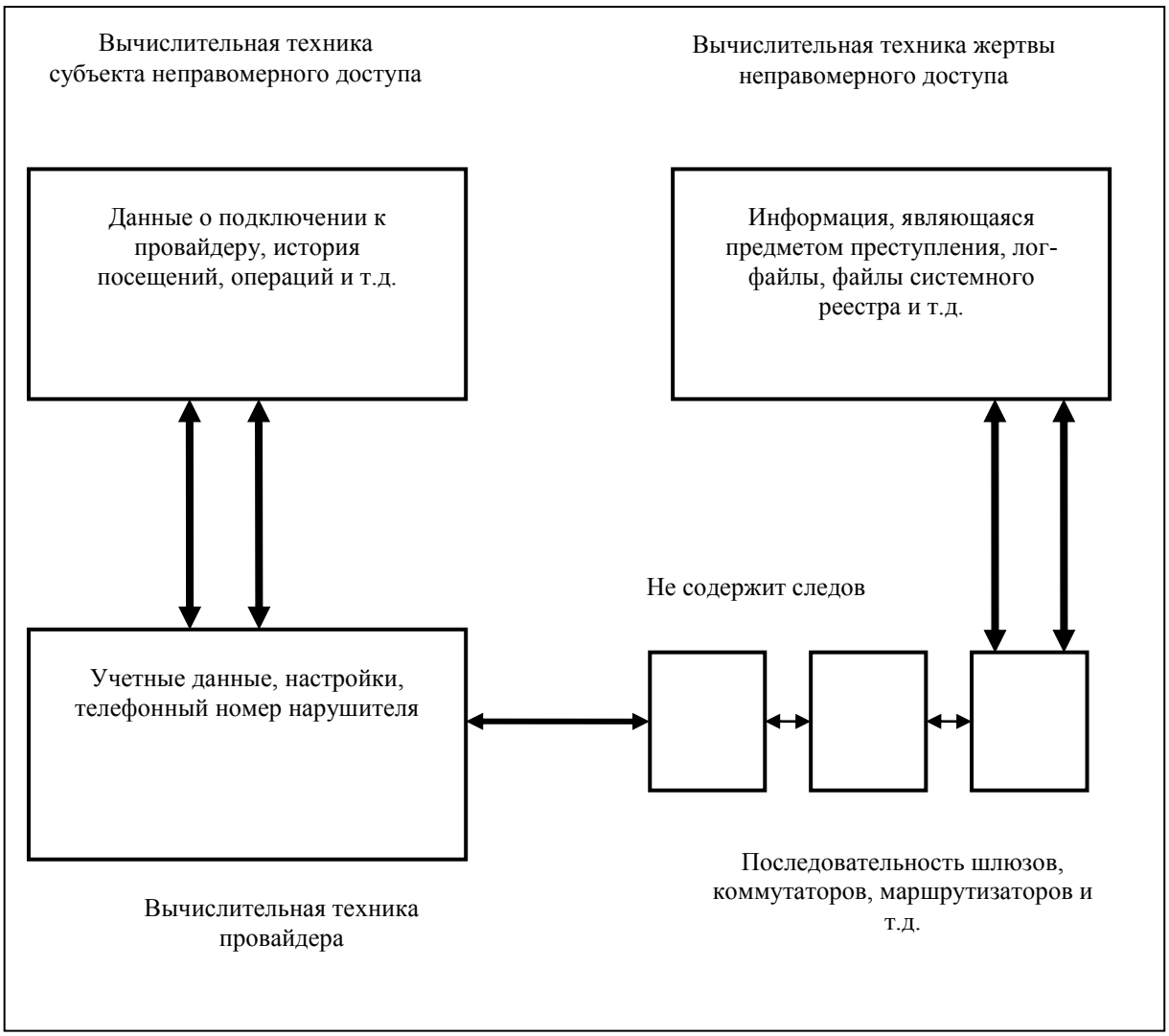


Рисунок 4 - Обобщенная схема удаленного неправомерного доступа к компьютерной информации с перечнем следов преступления

Необходимо выделить ряд методов, а также средств, которые позволят специалистам по информационной безопасности предотвратить атаки со стороны злоумышленников, связанные с НСД к компьютерной информации. Методы и средства обеспечения безопасности информации приведены на рисунке 5.

Рисунок 5 – Методы и средства обеспечения безопасности информации

Раскроем основное содержание представленных методов защиты информации, составляющих основу механизмов защиты.

1) Препятствия – методы физического преграждения пути злоумышленника к защищаемой информации (ЗИ).

2) Управление доступом – метод защиты, предполагающий регулирование использования всех ресурсов компьютерной системы.

3) Маскировка – метод ЗИ посредством криптографического закрытия информации.

4) Регламентация – метод защиты, заключающийся в создании определенных условий автоматизированной обработки, хранения и передачи ЗИ, при которых возможности НСД сводились бы к минимуму.

5) Принуждение – метод защиты, при котором пользователи системы вынуждены соблюдать правила обработки, передачи и использования ЗИ под угрозой материальной, административной или уголовной ответственности.

6) Побуждение – метод, побуждающий пользователя системы не нарушать установленный порядок за счет соблюдения сложившихся моральных и этических норм.

Таким образом в статье были рассмотрены «две стороны одной медали», а именно, компьютерных преступлений, связанных с НСД к информации. Сначала были приведены основные способы, применяющиеся злоумышленники при осуществлении преступлений данного типа. Затем были рассмотрены методы предотвращения компьютерных атак, которые в своей работе могут использовать специалисты по защите информации.

Литература:

Белевский Р.А. Методика расследования преступлений, связанных с неправомерным доступом к компьютерной информации в сетях ЭВМ: дис. канд. юрид. наук: 12.00.09. / Белевский Роман Александрович. - Санкт-Петербург, 2006.

Борисов В.И. Оценка рисков информационно-телекоммуникационных систем, подвергающихся НСД-атакам. / В.И. Борисов, Н.М. Радько, И.О. Скобелев, Ю.С. Науменко // Информация и безопасность: Регион. Науч.-тех. журнал. - Воронеж. 2010.

Батурин Ю.М. Компьютерное преступление - что за этим понятием? / Ю.М. Батурин. «Интерфейс», 1990

РАЗРАБОТКА МОБИЛЬНОГО ПРИЛОЖЕНИЯ ДЛЯ ИДЕНТИФИКАЦИИ ДВИГАТЕЛЬНОЙ АКТИВНОСТИ ПАЦИЕНТА

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

Необходимость разработки данного мобильного приложения объясняется следующим: на базе кафедры ВСИБ ведется разработка системы холтер-мониторинга, но помимо информации, получаемой от обследуемого органа, а именно – битрейт сердца, очень важно знать при каких условиях происходит запись кардиологических данных. К таким условиям относятся – информация о погоде (атмосферное давление, температура, влажность и т. д.), информация о местоположении пациента (геолокация) и информация о его двигательной активности. Для того, чтобы получать необходимые данные, разработчикам приходится утяжелять и без того достаточно громоздкие устройства, усложняя их схему и прикрепляя дополнительные модули.

Лучшим решением проблемы получения данных об условиях, в которых на данный момент находится пациент – использование современных мобильных устройств, многие из которых имеют всевозможные датчики и модули, способные решить описанную выше проблему. И если получение данных о метеоусловиях и геолокации доступны без применения каких-либо алгоритмов и не требуют обработки, то данные для идентификации двигательной активности (с акселерометра и гироскопа) напротив – не представляют информацию в «чистом» виде. Кроме того, большинство современных мобильных устройств

имеют интерфейсы для подключения переферии, что говорит нам о возможности подключения холтер-монитора или каких-либо других устройств.

Для разработки данного мобильного приложения была выбрана платформа iOS, в связи с тем, что имеется соответствующий опыт разработки под данную платформу, оборудование и сертифицированный аккаунт разработчика. Стоит также сказать, что разработка ведется в операционной системе OS X, среде программирования XCode.

Основной функцией приложения является идентификация двигательной активности в реальном времени, кроме того, требуется осуществлять запись и отправку полученных данных на электронную почту пользователя или врача, чтобы при сверке и анализе данных, полученных с холтер-монитора, увеличить количество информации о состоянии пациента.

Для того чтобы стало понятно, что подразумевается под двигательной активностью, было определено несколько ключевых состояний пациента, а именно:

- Пациент стоит
- Пациент сидит
- Пациент упал
- Пациент идет
- Пациент бежит

Одним из самых важных моментов, которому уделялось особое внимание при проектировании и разработке приложения, была идентификация пользователя, и самое главное – персонализация его активности. Каждый пациент обладает уникальными биометрическими характеристиками и особенностями организма, а не только идентификаторами в виде фамилии, имени и отчества. В связи с этим, было решено реализовать обучение программы для каждого из пациентов, предложив пользователю побывать в каждом из описанных выше состояний (рисунок 1) Во время обучения каждому из состояний создается выборка, которая после обработки будет сравниваться с данными, поступающими в реальном времени с акселерометра и гироскопа.

Рисунок 1 – алгоритм обработки данных при обучении программы.

На скетчах ниже (рисунок 2) представлены экраны, с которыми пользователь встречается при первом запуске приложения.

Обработка данных, получаемых с акселерометра и гироскопа ведется с помощью фреймворка Core Motion (позволяет разработчику использовать данные, полученные с аппаратной части устройства и обрабатывать их), предоставленным компанией Apple, стоит также отметить, что данный фреймворк имеет множество аналогов для других платформ, а это говорит нам о том, что при портации на другие мобильные операционные системы, например Android, проблем не будет.

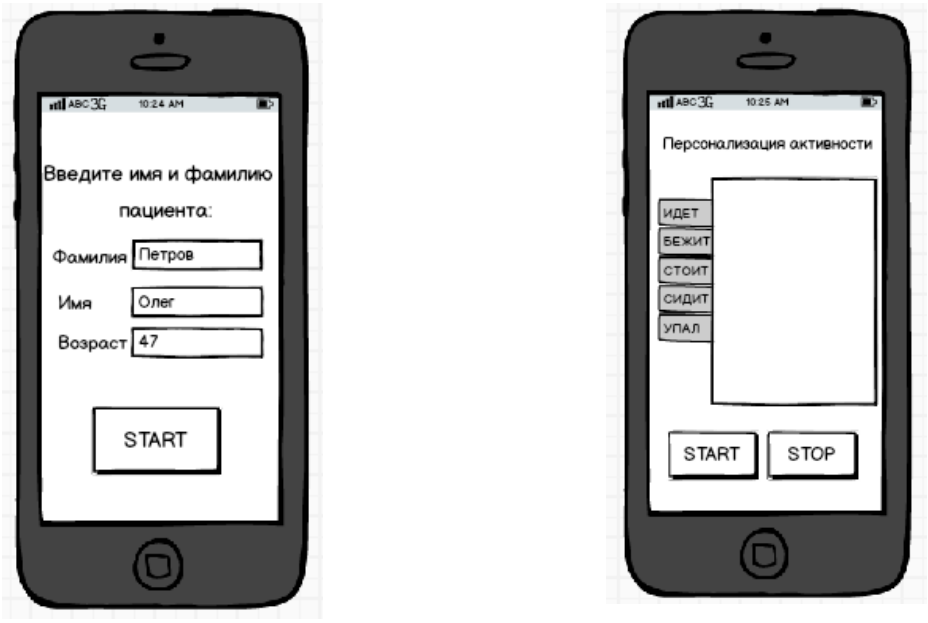


Рисунок 2 – скетчи экранов идентификации и персонализации активности пациента

На данный момент, в разрабатываемом приложении реализовано определение состояний для каждого пользователя и ведется работа по улучшению алгоритма обработки данных для более точной идентификации при обучении программы, и при смене состояний двигательной активности.

В перспективе планируется добавить в это приложение опредение других условий, в которых находится пациент, такие как геолокация и информация о погоде.

РАЗРАБОТКА МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ПОМЕЩЕНИЙ ОТ УТЕЧКИ ИНФОРМАЦИИ ПО АКУСТИЧЕСКОМУ КАНАЛУ

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

Несмотря на широчайшее внедрение автоматизированных и компьютеризованных систем обработки информации, человеческая речь остается одним из важнейших путей информационного взаимодействия, исходя из этого акустическая информация, циркулирующая в пределах защищаемого помещения, требует обеспечения конфиденциальности.

Защита информации (ЗИ) необходима по следующим причинам:

– Развитие методов и средств несанкционированного получения информации.

– Создание технической базы для изготовления средств нелегального добывания информации.

– Наличие в помещениях аппаратуры, физические процессы в которой способствуют утечки информации из помещения.

Для решения задач защиты предусматривается применение системного подхода для создания модели изучаемого объекта (ЗП) в совокупности с взаимосвязанными объектами и процессами, использующими защищаемую информацию. Решение предполагает совокупность сил и средств с учетом внутренних и внешних влияющих факторов, и должно обеспечивать:

– Надежность ЗИ.

– Непрерывность ЗИ.

– Скрытность ЗИ.

– Рациональность и гибкость ЗИ.

– Экономичность ЗИ.

Разработка мероприятий представляет собой последовательность действий, направленных на изучение ЗП, определение каналов утечки и мер защиты.

Для определения угроз ЗИ необходимо рассмотреть структурную и пространственную модели помещения. Структурная модель описывает состав основных элементов ЗП, влияющих на безопасность информации в нем (двери, окна, толщина стен, радио- и электронные устройства, телефонные и другие линии связи, кабели электропитания). Пространственная модель характеризует расположение ЗП в коридоре, этаже, ориентацию окон относительно внешних возможных мест расположения технических средств злоумышленника.

Основная часть информации, характерной для утечек по акустическому каналу, передается посредством человеческой речи. Кроме того, источниками речи могут быть люди, чья речь предварительно записана и воспроизводится с помощью технических средств.

Акустический канал утечки информации состоит из трех составляющих: источник опасного сигнала, физической среды его распространения (воздух, вода, земля, строительные и другие конструкции) и технического средства его приема, определяющих физический путь, по которому злоумышленник обеспечивает ее несанкционированное получение. Возникновение акустического канала утечки информации может быть обусловлено физическими полями, сопровождающими работу объекта или специально созданными злоумышленником (за счет использования технических устройств, преобразующих конфиденциальную информацию к условиям оптимальной ее передачи с объекта).

В качестве основных угроз безопасности информации выступают:

– Непосредственное подслушивание и подслушивание при помощи технических средств.

– Перехват электромагнитных излучений при работе звукозаписывающих устройств и электроприборов.

– Перехват структурных сигналов, распространяющихся по строительным конструкциям здания (двери, окна, стены, пол, потолок, батареи центрального отопления, трубопроводы, вентиляция).

Меры защиты должны обеспечивать защиту от угроз утечки информации и создание условий, при которых невозможна реализация данных угроз. Данные меры реализуются с применением организационных и технических мер.

Организационные меры [1] должны исключать возможность реализации угрозы утечки ЗИ. В качестве основных организационных мер рекомендуется:

– Проверка помещения перед проведением мероприятий, связанных с использованием защищаемой информации.

– Управление допуском участников мероприятия в помещение.

– Организация наблюдения за входом в ЗП и окружающей обстановкой (смежные помещения) в ходе проведения мероприятий.

Технические меры должны обеспечивать [2]:

– Обнаружение, локализация и изъятие закладных устройств (ЗУ).

– Подавление опасных сигналов с речевой информации.

– Повышение звукоизоляции помещения.

Целесообразно применять в совокупности активные (использование различных генераторов помех и средств поиска ЗУ) и пассивные (звукоизоляция и экранирование) технические меры защиты.

Проверить ЗП на утечки и определить места уязвимости можно при использовании радиозакладочного устройства, учитывая, что оно является наиболее распространенным способом несанкционированного получения конфиденциальной информации. ЗУ состоит (рисунок 1):

– Микрофон, определяющий зону акустической чувствительности ЗУ.

– Радиопередатчик, определяющий дальность ее действия и скрытость работы.
– Источник питания, от которого зависит продолжительность ее работы.

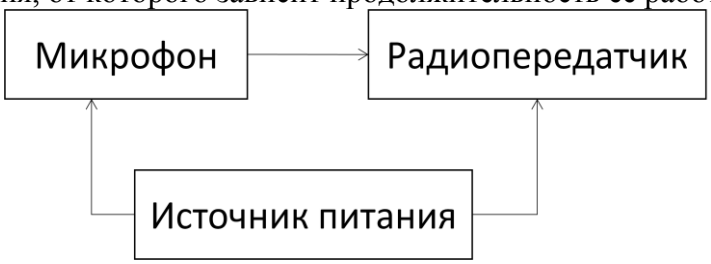


Рисунок 1 – Общая схема радиозакладки

Для проведения проверки необходимо поместить в ЗП ЗУ и реализовать канал утечки с применением радиозакладочного устройства и приемника сигнала (рисунок 2). ЗУ необходимо поместить в ЗП в месте, где его обнаружение минимально и обеспечить его маскировку для создания ситуации, близкой к действительности.

Рисунок 2 – Канал утечки информации

Для получения объективного результата ЗУ должно обладать средними параметрами, исходя из размеров, потребляемой мощности, дальности передачи, стабильности и времени работы и частоты сигнала. Также ЗУ должно предполагать маскировку. В результате, была подобрана схема, отличающаяся дальностью передачи, широким диапазоном питания о 3 до 9 В и малыми размерами, позволяющими произвести маскировку (рисунок 3) [3].

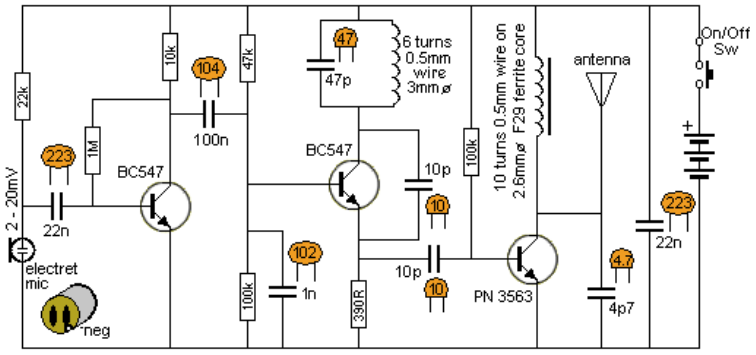


Рисунок 3 – Схема радиозакладки

Данная схема имеет микрофонный усилитель, позволяющий увеличить чувствительность закладки.

Съем передаваемого сигнала необходимо производить в различных местах, чтобы оценить влияние элементов конструкции на передачу. Степень защиты помещения определяется стабильностью и разборчивостью полученного сигнала за пределами помещения. Если получаемый сигнал не информативен, то угроза применения радиопередающего устройства минимальна.

На основании проведенной работы можно сделать следующие выводы:

– Для решения задач защиты помещения предусматривается применение системного подхода для создания модели изучаемого объекта.

– Разработка мероприятий реализуется в поэтапном изучении ЗП

– Для эффективной защиты необходимо применением в совокупности организационных и технических мер.

– Принимаемые меры должны обеспечивать защиту от угроз утечки информации и создание условий, при которых невозможна реализация данных угроз.

– Степень защиты помещения и поиск уязвимых мест реализации угрозы определяется при использовании непосредственно средства для несанкционированного получения информации.

Список использованной литературы:

1. Торокин А.А. «Инженерно-техническая защита информации». Москва, «Гелиос АРВ», 2005.

2. Хорев А.А. «Защита информации от утечек по техническим каналам».

3. Лекции по инженерно-технической защите информации.

ЗАЩИТА ИНФОРМАЦИОННЫХ РЕСУРСОВ ГЕТЕРОГЕННЫХ СЕТЕЙ, ИСПОЛЬЗУЮЩИЕ КАНАЛЫ СВЯЗИ МОБИЛЬНЫХ ТЕХНОЛОГИЙ

Присада С.К. - студент, Шарлаев Е.В. – к.т.н., доцент

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

С ростом популярности мобильных технологий мобильные устройства уже стали неотъемлемой частью нашей повседневной жизни, выполняя широкий спектр функций [1]. В настоящее время такие устройства находят все более широкое применение, будь то: сотовые телефоны, ноутбуки, нетбуки, планшеты и другое.

По политике безопасности использование мобильных устройств на рабочем месте запрещено, ввиду того что они наиболее подвержены уязвимостям. Но не смотря на это, согласно исследованиям IDC, 55 процентов сотрудников в России и 75 процентов в Западной Европе используют свои устройства на работе, 75 процентов организаций в России используют элементы BYOD (Bring Your Own Device – «принеси свое устройство») [3]. В связи с этим необходимо обеспечить должным образом безопасность мобильных устройств на ряду с персональными компьютерами, разработать и внедрить политику безопасности.

При использовании мобильных устройств необходимо следовать следующим правилам:

1. Установка MDM/MAM ПО (mobile device management и mobile application management).
2. Подключение через VPN.
3. Надежные пароли на устройствах.
4. Шифрование данных на устройствах.
5. Установка антивирусного ПО.
6. Внедрение листов контроля доступом и брандмауэров.
7. Оповещения о подозрительной деятельности.
8. Ограничение на скачивание и установку программ со сторонних источников [4].

предварительные исследования ресурсов Internet [1-4] свидетельствуют, что 90 процентов прорывов безопасности можно было бы избежать, при условии обеспечения базовых мер, таких как надежные пароли (у большинства пользователей отсутствует пароль вообще) и антивирусное ПО, не говоря об использовании технологии VPN и брандмауэров. Так же персоналу необходимо менее халатно относится к данным к которым он имеет допуск, ведь на сегодняшний момент в тройке атак до сих пор находится «социальная инженерия» (метод несанкционированного доступа к информационным ресурсам основанный на особенностях психологии человека).

В настоящее время для решения рассмотренной проблемы ведутся исследования применимости технологии VPN совместно с различным антивирусным ПО, а также возможность реализации удаленного управления мобильными устройствами.

Список использованной литературы:

1. Безопасное использование мобильных устройств в корпоративной среде [Электронный ресурс]. – Электрон. текст. дан. – Режим доступа: http://www.aladdin-rd.ru/company/pressroom/articles/37692/ - Загл. с экрана.

2. Защита информации на мобильных устройствах и MobilEcho 4.5 [Электронный ресурс]. – Электрон. текст. дан. – Режим доступа: http://habrahabr.ru/company/acronis/blog/195756/ - Загл. с экрана.

3. Корпоративная мобильность (Bring Your Own Device - BYOD) [Электронные ресурс]. – Электрон. текст. дан. – Режим доступа: http://www.tadviser.ru/index.php/Статьи:Корпоративная_мобильность_(Bring_Your_Own_Device_-_BYOD) – Загл. с экрана.

4. Маршоллек, Б., Мейер, У., Эгнерс, А. Хакеры в вашем кармане: исследование безопасности разных платформ смартфонов [Электронный ресурс]. – Электрон. текст. дан. – Режим доступа: http://stealthphone.ru/article_157.html - Загл. с экрана.

РАЗРАБОТКА УЧЕБНО-МЕТОДИЧЕСКИХ МАТЕРИАЛОВ ДЛЯ ПРОВЕДЕНИЯ ЛАБОРАТОРНЫХ РАБОТ ПО ДИСЦИПЛИНЕ "ЗАЩИТА ИНФОРМАЦИИ" ОПП 230100

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

На современном этапе развития общества все более интенсивно используются компьютерная техника, новые информационные технологии, системы телекоммуникаций. Информация является важнейшим стратегическим ресурсом общества и занимает ключевое место в экономике, образовании и культуре, социальной сфере. Обеспечение безопасности информации является одной из важных задач, решаемых на уровне государства.

Для обеспечения информационной безопасности бакалавры направления подготовки ИВТ должны иметь знания в данной области. При подготовке таких специалистов особую роль занимает практическая часть обучения. Знания, полученные, в ходе изучения теоретического материала является основой для закрепления практических умений и навыков в области информационной безопасности и защиты информации, овладение компетенциями по квалифицированному применению на практике профессиональной терминологии, по классификации защищаемой информации средств и систем её защиты, проведению целенаправленного поиска в различных источниках информации по основам информационной безопасности и защиты информации, в том числе в глобальных компьютерных системах.

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

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

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

На данный момент по дисциплине «Защита информации» для направления подготовки бакалавров «Информатика и вычислительная техника» существует 4 лабораторные работы, которые охватывают следующие темы:

– работа с программами сокрытия файлов и папок, взлом паролей и расшифровка текста из изображений;

– работа с антивирусным программным обеспечением;

– создание частной виртуальной сети на примере подключения ноутбуков по локальной сети;

– настройка и обеспечение информационной безопасности с помощью средств шифрования.

Для полного изучения всех вопросов обеспечения информационной безопасности количества существующих лабораторных работ не достаточно. С этой целью необходимо разработать ещё 4 лабораторные работы, по следующим темам:

– межсетевые экраны;

– электронная цифровая подпись;

– программные продукты для управления рисками информационной безопасности;

– системы обнаружения вторжений.

Выполнение лабораторных заданий осуществляется в программном обеспечении Comodo Firewall, Outpost Firewall, AVS Firewall, КРИПТОН-Подпись, Crypton ArcMail, Блокхост-ЭЦП, КриптоАРМ, Microsoft Baseline Security Analyzer, РискМенеджер, vsRisk, Snort. Дистрибутивы всех программ можно легко найти и скачать с сайта производителя. Программы являются бесплатными и автоматически обновляются при подключении к сети Интернет. Весь курс состоит из 8 лабораторных работ, которые выполняются индивидуально или по группам, а так же распределяются по вариантам.

Пятая лабораторная работа посвящена настройке межсетевых экранов и обеспечению безопасности с помощью данного программного обеспечения [3,4]. Пример настройки межсетевого экрана Comodo Firewall представлен на рисунке 1.

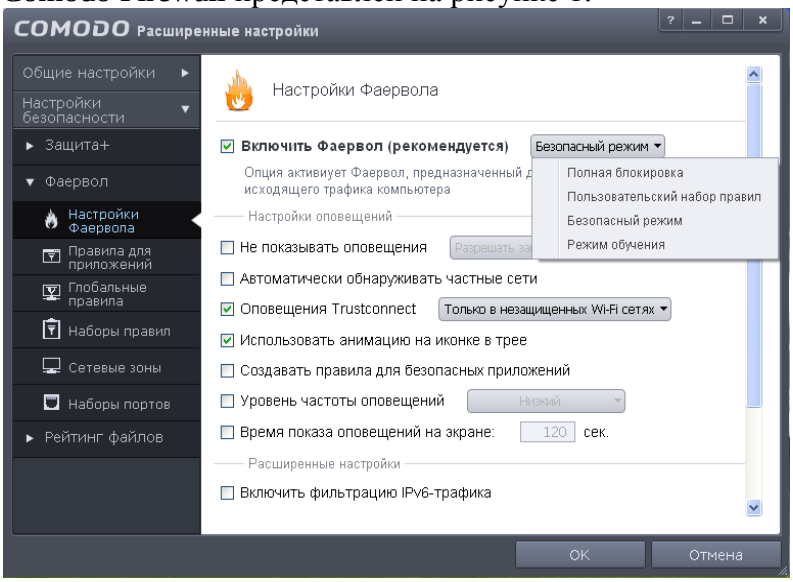


Рисунок 1 – Настройка режима безопасности в Comodo Firewall

Межсетевой экран (сетевой экран, файервол, брандмауэр) — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Контроль трафика состоит в его фильтрации, то есть выборочном пропускании через экран, а иногда и с выполнением специальных преобразований и формированием извещений для отправителя, если его данным в пропуске было отказано.

В лабораторной работе связанной с межсетевой защитой студенты научаться настраивать межсетевые экраны и осуществлять защиту информации с помощью данной программы.

Шестая лабораторная работа осуществляется с помощью программ для электронной цифровой подписи. Выполнения данной лабораторной работ осуществляется с помощью предложного программного обеспечения [5].

Электронная цифровая подпись (ЭЦП) — реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий установить отсутствие искажения информации в электронном документе с момента формирования подписи и проверить принадлежность подписи владельцу сертификата ключа подписи. Электронная подпись предназначена для идентификации лица, подписавшего электронный документ, и является полноценной заменой (аналогом) собственноручной подписи в случаях, предусмотренных законом.

В данной лабораторной работе студенты научатся подписывать электронные документы с помощью программ для электронной цифровой подписи. Ознакомятся со средствами создания электронной цифровой подписи, а так же смогут осуществлять настройку данных средств [6].

Седьмая лабораторная работа посвящена анализу информационных рисков. Выполнение лабораторной работы осуществляется с помощью программ для управления рисками информационной безопасности.

Анализ рисков - это то, с чего должно начинаться построение любой системы информационной безопасности. Он включает в себя мероприятия по обследованию безопасности информационной системы, целью которого является определение того какие ресурсы и от каких угроз надо защищать, а также в какой степени те или иные ресурсы нуждаются в защите. Определение набора адекватных контрмер осуществляется в ходе управления рисками.

В ходе выполнения лабораторной работы студент получит навыки по работе с программными продуктами для управления рисками информационной безопасности.

Восьмая лабораторная работа связанная с системами обнаружения вторжений. Выполнение данной лабораторной осуществляется с помощью предложенных систем обнаружения вторжений. Система обнаружения вторжений (СОВ) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей) [7].

В заключительной лабораторной работе студенты научатся обеспечивать информационную безопасность с помощью систем обнаружения вторжений.

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

Список использованной литературы:

1. СТО 13.62.1.1201 – 2012. Система качества АлтГТУ. Образовательный стандарт высшего профессионального образования АлтГТУ. Образовательный стандарт учебной дисциплины «Защита информации». – Введ. 2012-2-10. – Барнаул: АлтГТУ, 2012. – 28 с.

2. СТП 12700 – 2007. Система качества АлтГТУ. Образовательный стандарт высшего профессионального образования АлтГТУ. Занятия лабораторные. Общие требования к организации, проведению и методическому обеспечению. – Введ. 2007-09-01. – Барнаул: АлтГТУ, 2007. – 10 с.

3. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. : Форум, 2008. – 416с.
4. Олгтри Т.В. Практическое применение межсетевых экранов.: ДМК Пресс, 2001. – 400с.
5. Электронная цифровая подпись [Электронный ресурс]. – Режим доступа: http://www.ancud.ru/ecp - Загл. с экрана.
6. Астахов А.М. Искусство управления информационными рисками.: ДМК Пресс, 2010. – 312с.
7. Системы обнаружения вторжений [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/software/1258/ - Загл. с экрана.

СОПРЯЖЕНИЕ ОХРАННО-ПОЖАРНОГО ПРИБОРА С СОТОВЫМ ТЕЛЕФОНОМ

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

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.

Для более быстрого реагирования на нарушение безопасности объекта необходимо, чтобы информация об этом передавалась не только в правоохранительные органы, но и хозяину помещения. Стандартные средства охраны не позволяют передавать такие данные по средствам gsm, поэтому необходимо разработать такой модуль.

Разработанная приставка (рисунок 1) служит дополнением к прибору приемно-контрольному охранно-пожарному (ППКОП) "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 [1]. Она и позволяет автоматически передавать сигнал тревоги по сотовому телефону.

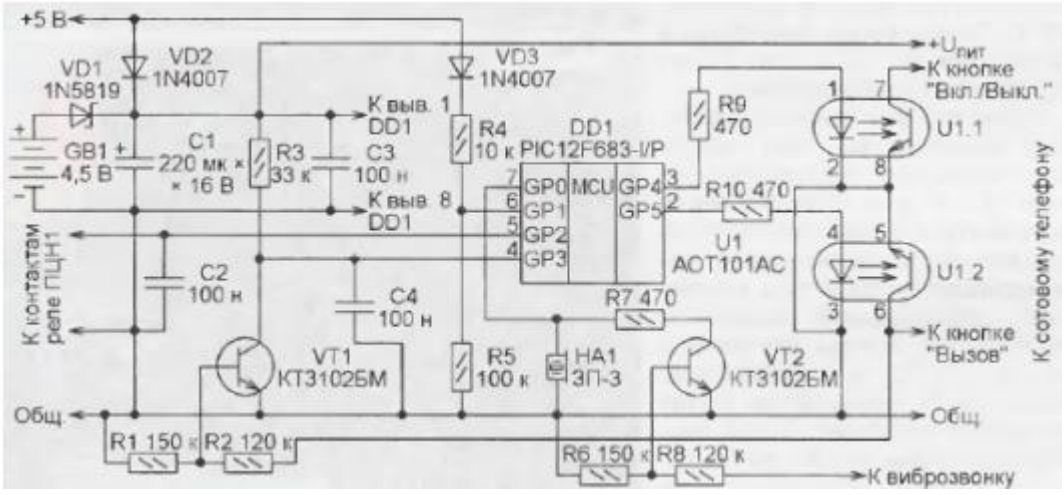


Рисунок 1 – Приставка к ППКОП «Кварц»

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 [2]. 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, была разработана приставка, позволяющая автоматически передавать сигнал тревоги по сотовому телефону в случае обнаружения нарушения безопасности здания: несанкционированного проникновения, возгорания и т.д.

Список использованной литературы:

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.

СТЕГАНОГРАФИЧЕСКОЕ СКРЫТИЕ ИНФОРМАЦИИ В СТАТИЧЕСКИХ ИЗОБРАЖЕНИЯХ

Ребро И.В. – студент, Ленюк С.В. – к.ф.-м.н., доцент
Алтайский государственный технический университет им. И.И. Ползунова (г. Барнаул)

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Уже в древнем мире выделилось два основных направления решения этой задачи, существующие и по сегодняшний день: криптография и стеганография. Целью криптографии является скрытие содержимого сообщений за счёт их

шифрования, в то время как задача стеганографии – сохранение в тайне самого факта передачи информации. Стеганография не заменяет, а дополняет криптографию. В настоящее время, когда объёмы обрабатываемой информации растут, соответственно растет и доля сведений, которые необходимо держать втайне от посторонних глаз. Применение компьютеров позволило усовершенствовать известные идеи скрытия информации и дало возможность более надёжно прятать информацию. При этом существует и необходимость определять эту скрытую информацию. Такие задачи позволяют решать методы стегоанализа. Широкое распространение имеют алгоритмы, позволяющие встраивать информацию в статические изображения [1,2].

Целью работы является исследование и реализация методов встраивания секретной информации в изображения, а так же их стегоанализа.

Наиболее простым и распространённым является метод замещения при встраивании в младшие биты. Суть этого метода заключается в замене последних значащих битов изображения на биты скрываемого сообщения, которое перед встраиванием преобразуется в вектор двоичных данных [3].

При извлечении биты сообщения находятся путём обратного считывания младших бит изображения.

Более новый метод встраивания заключается в том, что вместо операции замены младших бит, используется сложение или вычитание единицы:

$$\bar{x}_i = \begin{cases} x_i, & LSB(x_i) = m_i; \\ x_i + r_i, & LSB(x_i) \neq m_i,\ x_i \neq 0,\ x_i \neq 255; \\ x_i + 1, & LSB(x_i) \neq m_i,\ x_i = 0; \\ x_i - 1, & LSB(x_i) \neq m_i,\ x_i = 255; \end{cases}.$$

Эта модификация позволяет значительно повысит стойкость встраивания к обнаружению.

Главным недостатком последовательного встраивания является то, что оно вносит искажения в корреляцию, что является демаскирующим при проведении простейшего визуального стегоанализа младшего бита. Для его решения применяется рассеивание битов встраиваемого сообщения по контейнеру [2].

На рисунке 1 представлено изменением маски шума при последовательном и рассеянном выстраиваниях. В левом верхнем углу представлено исходное изображение, в левом нижнем углу – маска шума исходного изображения, в верхнем правом углу вносимые искажения при последовательном встраивании, в нижнем правом углу – рассеянное встраивание.

Несмотря на повышение стойкости стегосистемы при рассеянном встраивании, его всё равно можно обнаружить.

Младшие биты цифровых изображений не являются случайными, как может по срезу младшего бита. Между ними существуют корреляционные связи. Чтобы увидеть эти связи используются гистограммы яркости суммарные или разделённые по цветовым каналам [4].

При встраивании информации в биты изображения распределение яркости существенно изменяется (рисунок 2).

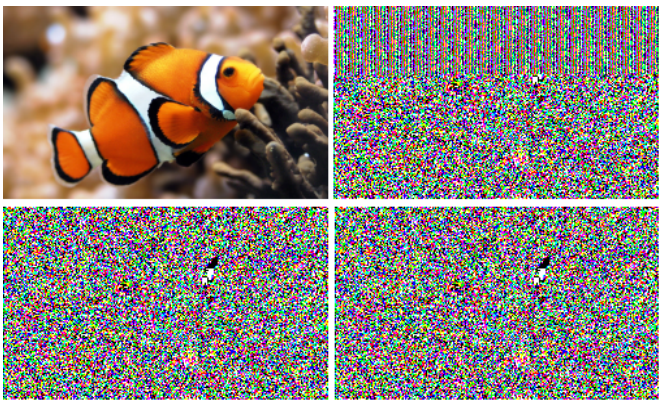


Рисунок 1 – Сравнение изменения маски шума при последовательном и рассеянном встраивании

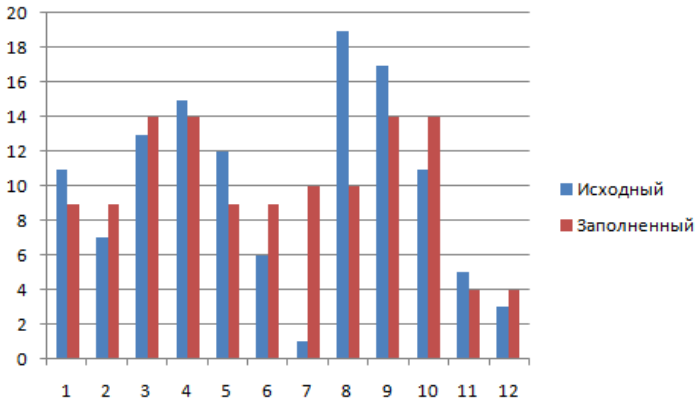


Рисунок 2 – Выравнивание соседних значений гистограммы яркости

Выявить такие изменения позволяет анализ пар величин. Суть данного метода заключается в анализе степени различия между вероятностными распределениями элементов естественных контейнеров и заполненных, которая может быть использована для оценки вероятности существования стегосообщения.

Данная вероятность определяется с помощью критерия согласия Хи-квадрат, который показывает насколько распределение исследуемой последовательности близко к характерному для стегограмм распределению.

В исследуемой последовательности подсчитывается, сколько раз её элементы принимали рассматриваемые значения. Для этого используется формула $\chi^2 = \sum_{i=1}^{N} \frac{(E_i - T_i)^2}{T_i}$, где N – количество элементов последовательности, E_i – экспериментальное значение выбранного элемента, а T_i – ожидаемое его значение, которое вычисляется для соответствующих пар пикселей $T_i = \frac{t_0 + t_1}{2}$.

Такой способ вычисления ожидаемого значения связан с предполагаемой гипотезой о том, что в стегоконтейнере вероятность появления 0 и 1 в младшем бите является одинаковой.

Для подтверждения или опровержения принадлежности изображения к стегоконтейнерам используется теоретическое значение статистики Хи-квадрата при заданном уровне значимости α и количестве степеней свободы $k-1$. Если неравенство $\chi^2 < \chi^2_\alpha(k-1)$ справедливо, то встраивание в проверяемую последовательность обнаружено.

Для количественной оценки вероятности наличия стего используется формула асимптотического распределения вероятности последовательности $p = 1 - \frac{1}{2^{\frac{k-1}{2}} \Gamma(\frac{k-1}{2})} \int_0^{\chi^2_{k-1}} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx$. [1]

На основании описанных алгоритмов было разработано программное обеспечение, позволяющее производить встраивание, извлечение информации в контейнер, а так же производить стегоанализ и оценку качества стегоконтейнеров.

Список использованной литературы:

1. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев – М.: «СОЛОН-ПРЕСС», 2009 – 272 с.

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

3. Рябко Б. Я. Основы современной криптографии и стеганографии / Б. Я. Рябко, А. Н. Фионов – М.: «Горячая Линия – Телеком», 2010. – 232 с.

4. Аграновский А. В. Стеганография, цифровые водяные знаки и стегоанализ / А. В. Аграновский – М.: «Вузовская книга», 2009. – 220 с.

РАЗРАБОТКА ПРОГРАММНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ КОНТРОЛЯ ПЕРЕМЕЩЕНИЯ ПЕРЕДВИЖНЫХ МОТОРИЗОВАННЫХ ГРУПП УВД Г. БАРНАУЛА

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

В последнее время широкую область применения получили системы GPS/ГЛОНАСС трекинга. Они устанавливаются в охранные системы, автомобили, разрабатываются в виде наручных часов и т. д. Область применения этой системы широко используется для слежения за людьми, например, за детьми или же работниками фирм [1].

В Российской Федерации было принято Постановление Правительства РФ от 25 августа 2008 г. N 641 "Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS"[6], в п.3 которого написано следующее: «Оснащению аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS подлежат технические средства и системы, образцы вооружения, военная и специальная техника, предназначенные для Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, в которых предусмотрена военная и приравненная к ней служба, а также транспортные средства, поставляемые и используемые для обеспечения органов, в которых предусмотрена военная и приравненная к ней служба».

Целью НИР является создание аппаратно-программного комплекса, который совмещал в себе и систему глобального позиционирования, и систему передачи данных о технических средствах на сервер, а также наблюдению за ними во время их работы. Поскольку Алтайский край является не самым богатым регионом в РФ, а автопарк в УВД г. Барнаула достигает порядка тысяч машин и похожие аналоги на рынке являются дорогостоящими, появилась необходимость разработать аппаратно-программный комплекс для УВД столицы Алтайского края г. Барнаула.

Аппаратно-программный комплекс построен на платформе Arduino, которая в свою очередь построена на микроконтроллерах Atmel[3]. К данной платформе подключен модуль GPS для определения местоположения, модуль GSM/GPRS, для отправки данных на сервер, и карта памяти SD в роли черного ящика для хранения последних отправленных данных. Стоимость готового аппаратно-программного комплекса не превышает 5000 рублей.

Логика работы аппаратно-программного комплекса представлена на блок-схеме.

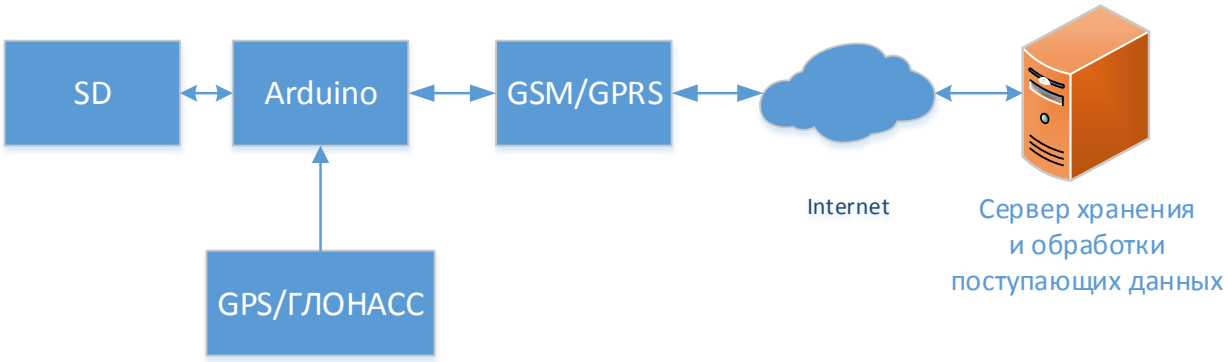
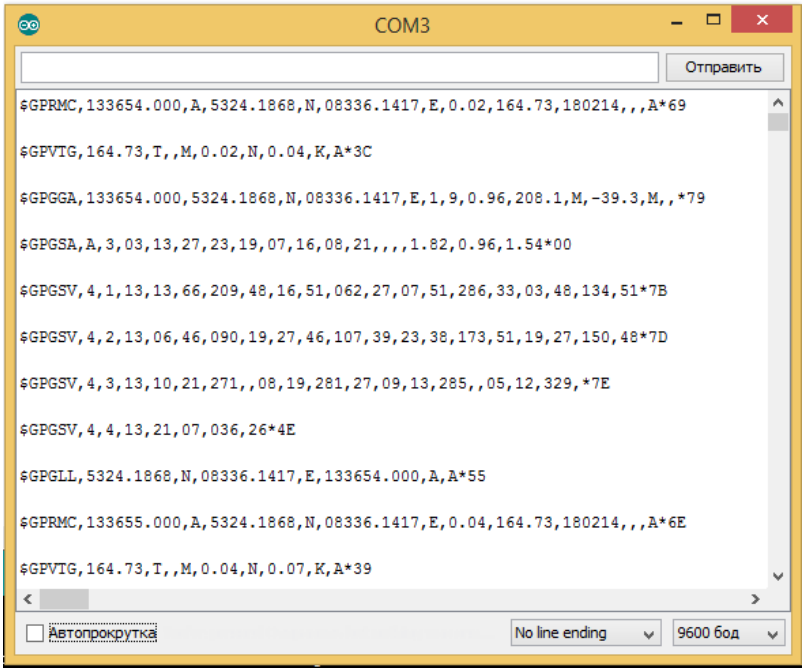


Рисунок 1 – Блок-схема аппаратно-программного комплекса

Устройство с ГЛОНАСС/GPS размещается в автомобиле и генерирует телематическую информацию о своем состояние относительно земли (географические координаты, скорость, направления движения и т.д.) и передаёт на сервер при помощи модуля GSM. К этим данным может быть добавлена информация о состоянии систем автомобиля. Попав на сервер информация, разбирается и записывается в базу данных. После чего с данными начинает работать различный софт. Если по каким-либо причинам связь с сервером пропала данные начинают записываться на карту памяти SD, а затем, как только связь с сервером восстанавливается данные с SD отправляются на сервер. Если сообщение логистическое (треки движения автомобилей в реальном времени), то оно отображается в веб-интерфейсе или в программе (рисунок 2).



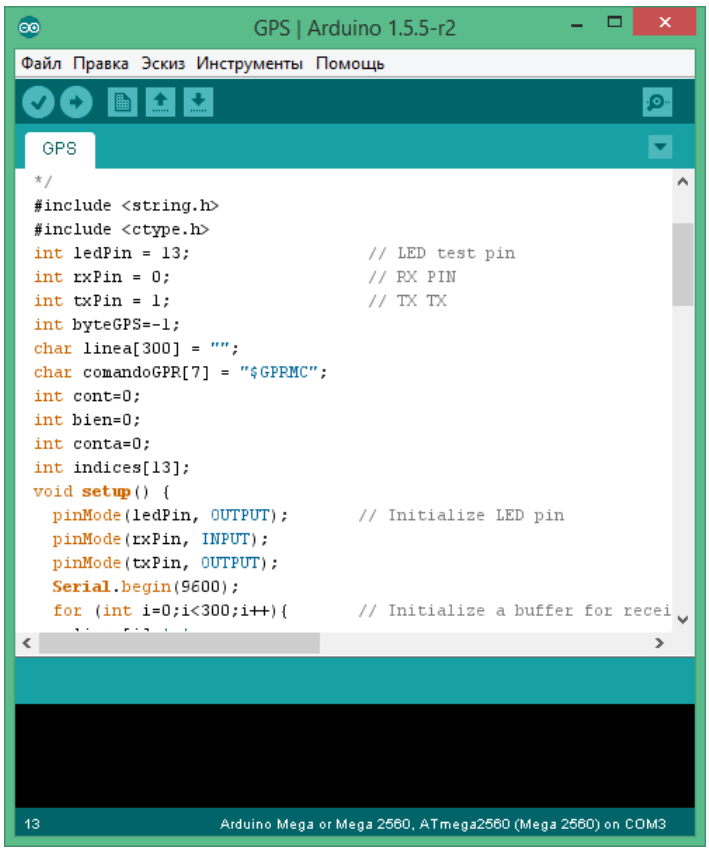


Рисунок 2 – Веб-интерфейс программы

В итоге был получен достаточно производительный аппаратно-программный комплекс, не уступающий аналогам и менее дорогой. Данный аппаратно-программный комплекс можно будет дополнять в зависимости от потребностей тех или иных служб.

Список литературы:

1. Шебшаевич В. С., Дмитриев П. П., Иванцев Н. В. и др. Сетевые спутниковые радионавигационные системы / Под ред. В. С. Шебшаевича. — 2-е изд., перераб. и доп. — М.: Радио и связь, 1993. — 408 с. — ISBN 5-256-00174-4

2. Гарант. Информационно-правовой портал [Электронный ресурс]: – Режим доступа: http://base.garant.ru/12162134/

3. Arduino [Электронный ресурс]: – Режим доступа: http://arduino.ru/About

ПОИСК ПРОСТЫХ ЧИСЕЛ

Стромов Л.В. – студент, Ленюк С.В. – к.ф.-м.н., доцент

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

Алгоритм RSA на сегодняшний день является одним из наиболее используемых алгоритмов ассиметричной криптографии [1]. Он удобен и для шифрования ключей и для цифровой подписи. Одним из основных моментов этого алгоритма является нахождение больших простых чисел. Причем, криптостойкость этого алгоритма на прямую зависит от длины простых чисел, которые в нем используются. В настоящее время используются числа, которые имеют порядка 100-150 знаков.

Поэтому поиск больших простых чисел является одной из актуальнейших задач криптографии на сегодняшний день. Существуют два принципиально разных подхода к поиску простых чисел.

1. С помощью детерминированных алгоритмов (строятся гарантированно простые числа).

Здесь используются такие алгоритмы, как: перебор делителей, теорема Вильсона, тест Миллера, тест Люка, тест AKS

2. С помощью вероятностных алгоритмов (строятся т.н. промышленно простые числа).

Здесь используются такие алгоритмы, как: тест Миллера – Рабина, тест Соловея – Штрассена, тест Ферма.

Вероятностные алгоритмы работают гораздо быстрее детерминированных и выдают вполне приемлемый для практических целей результат. Самым распространенным из них является тест Миллера-Рабина [2].

В разработанном программном обеспечении реализованы все перечисленные тесты. С помощью данной программы можно определить точно или с заданной вероятностью, является ли число простым или составным, при этом можно выбрать необходимый тест из заданных вариантов. Также программное обеспечение показывает ход проверки и выводит основные шаги своей работы.

Таким образом, можно не только проверять числа на простоту, но и изучать данные алгоритмы.

Также в данном программном обеспечении реализована возможность построения больших простых чисел по заданному простому числу меньшего размера. Данный алгоритм также является вероятностным, однако с его помощью имея достаточные вычислительные мощности можно строить простые числа, которые будут подходить для современных ассиметричных криптографических алгоритмов.

Таким образом, в результате проделанной работы было разработано программное обеспечение для поиска больших простых чисел и тестирования на простоту.

Список использованной литературы:

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2002. 2-е изд.
2. Василенко О.Н. Современные способы проверки простоты чисел. Обзор / Кибернетич. сборн. 1988. Вып. 25. С. 162—188.
3. Василенко О.Н. Об алгоритме Миллера—Рабина / Вестн. Моск. ун-та. Матем. Механ. 2000. №2. С. 41—42.
4. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. — М.: МЦНМО, 2003.—328 с.
5. Виноградов И.М. Основы теории чисел. М.: Наука, 1972.

РАЗРАБОТКА МИНИ-АТС И ЗАКЛАДОК ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНОГО ПРАКТИКУМА ПО ДИСЦИПЛИНЕ «ИЗМЕРИТЕЛЬНАЯ АППАРАТУРА АНАЛИЗА ЗАЩИЩЕННОСТИ ОБЪЕКТОВ И ЭЛЕКТРОРАДИОИЗМЕРЕНИЯ» ДЛЯ НАПРАВЛЕНИЯ ПОДГОТОВКИ БАКАЛАВРОВ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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

Человечество живет в век информационных технологий, для которых информация стала самым дорогим товаром. Чтобы получить необходимую информацию, люди применяют различную шпионскую технику, в частности подслушивающие устройства [1]. Теперь, чтобы установить шпионскую технику не нужно служить в разведке или правоохранительных органах – это может сделать каждый. Возможности таких устройств позволяют добыть ценную информацию. Телефонная сеть является одним из самых распространенных мест, куда злоумышленник может установить прослушивающее устройство (жучок).

Простейшие закладные устройства включают три основных узла, которые определяют их тактико-технические возможности. Это: микрофон, определяющий зону акустической чувствительности жучка, радиопередатчик, определяющий дальность его действия и

скрытность работы, источник электропитания, определяющий время непрерывной работы. Закладные устройства работают как обычный передатчик. Обнаружение жучков требует проведения специальных мероприятий.

Поиск жучков осуществляется при помощи следующих методов:

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

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

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

Большое внимание специалисту в области информационной безопасности стоит уделить практическому изучению современных приборов и аппаратных комплексов по защите телефонных переговоров. Для получения базовых и углубленных знаний в области электрорадиоизмерения и измерительной аппаратуры, студентам специальности 090900 «Информационная безопасность» предлагается изучение дисциплины «Измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения» [2].

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

В ходе учебного курса специальности 090900 «Информационная безопасность» студенты выполняют ряд лабораторных работ. Для выполнения данных лабораторных работ студентам необходим определенный набор технических устройств. Такими устройствами могут быть различные закладки, как акустические, так и аппаратные, и телефонная сеть для демонстрации работы данных жучков. В аудитории, где проходят лабораторные работы, нет возможности подключиться к телефонной линии. В связи с этим было решено приобрести офисную автоматическую телефонную станцию (мини-АТС), для выполнения лабораторных работ. В процессе анализа различных мини-АТС, которые предлагаются на рынке, выяснилось, что стоимость большинства из них неприемлема, также они имеют множество ненужных функций для выполнения данных лабораторных работ. Поэтому целью работы стало создание мини-АТС, которая удовлетворяла бы следующим требованиям: простота , низкая себестоимость, компактные размеры устройства, небольшая потребляемая мощность.

За основу будущей мини-АТС разработана схема, которая позволяет организовать связь между двумя абонентами посредством двух стандартных телефонных аппаратов (рисунок 1).

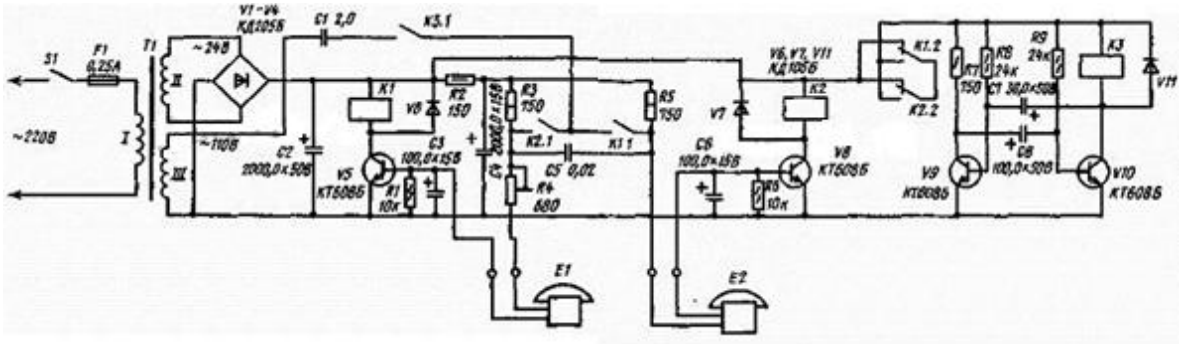


Рисунок 1 – Мини-АТС

Таким образом, разработанные переговорное устройство и закладки, а также полученные навыки работы с этим оборудованием будут иметь практическое применение,

как в рамках лабораторного практикума по дисциплине «Измерительная аппаратура анализа защищенности объектов и электрорадиоизмерения», так и в дальнейшей работе по обеспечению информационной безопасности.

Список используемых источников:

1. Цит. по ст. «Переговорное устройство с телефонными аппаратами» [Электронный ресурс] : Официальный сайт. – Режим доступа: http://guarda.ru/

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

ОХРАННО-ИНФОРМАЦИОННОЕ УСТРОЙСТВО НА ОСНОВЕ КОМПЬЮТЕРА

Шелковникова 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.

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 (рисунок 1).

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].

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].

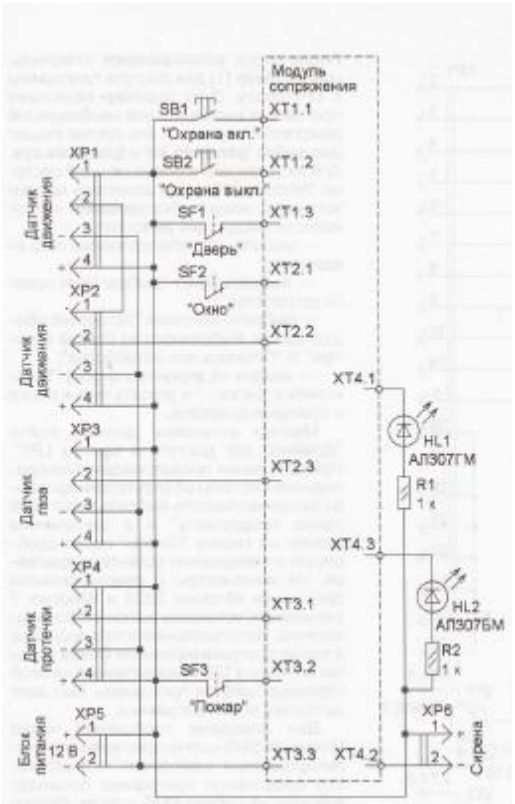


Рисунок 1 - Общая схема устройства

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 использованной литературы:

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 ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ НАУЧНО-ПРОИЗВОДСТВЕННОГО ПРЕДПРИЯТИЯ

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

В условиях рыночных отношений и острой конкуренции особенно возрастает роль информации, которая фактически становится средством производства. Для того, чтобы у предприятий, учреждений, организаций была возможность противостоять противникам в конкурентной борьбе, информационный ресурс предприятия должен быть достаточно хорошо защищен.

В настоящее время в Центре научно-технического развития зерноперерабатывающей промышленности, который располагается в 118 ПК, инновационные разработки никак не защищаются. То есть практически любой человек, имеющий доступ к помещению может получить информацию, которая впоследствии может стоить миллионы.

В данной работе предлагается обеспечить безопасность информации по основным каналам утечки информации, а именно:

- по виброакустическому каналу;
- по каналу побочных электромагнитных излучений и наводок;
- защитить электронные вычислительные машины от несанкционированного доступа;
- защитить информацию от разглашения.

На рисунке 1 представлен план защищаемого помещения.

Для обеспечения безопасности информации по виброакустическому каналу будет использоваться специальное техническое средство «Барон-S1» [1].

Генератор шума «ГШ-К-1800» предназначен для защиты информации от утечки за счёт побочных электромагнитных излучений и наводок, создаваемых средствами вычислительной техники, а «Гном-3» нужен для защиты от утечки информации по каналу побочных электромагнитных излучений и наводок средств офисной техники [2-3].

Для защиты интеллектуальной собственности в электронных вычислительных машин от несанкционированного доступа будет использоваться система защиты информации Secret Net 7, которая реализует мандатную политику безопасности для пользователей различных уровней конфиденциальности. Для обеспечения безопасности межсетевого взаимодействия будет использоваться ViPNet Office Firewall. Для защиты от вирусов – Kaspersky Anti-Virus 6.0 [4-5].

Чтобы защитить интеллектуальную собственность от разглашения предлагается ввести режим коммерческой тайны, который включает в себя следующие мероприятия:

- ознакомление под расписку работника, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты;
- ознакомление под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;
- создание работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны [6].

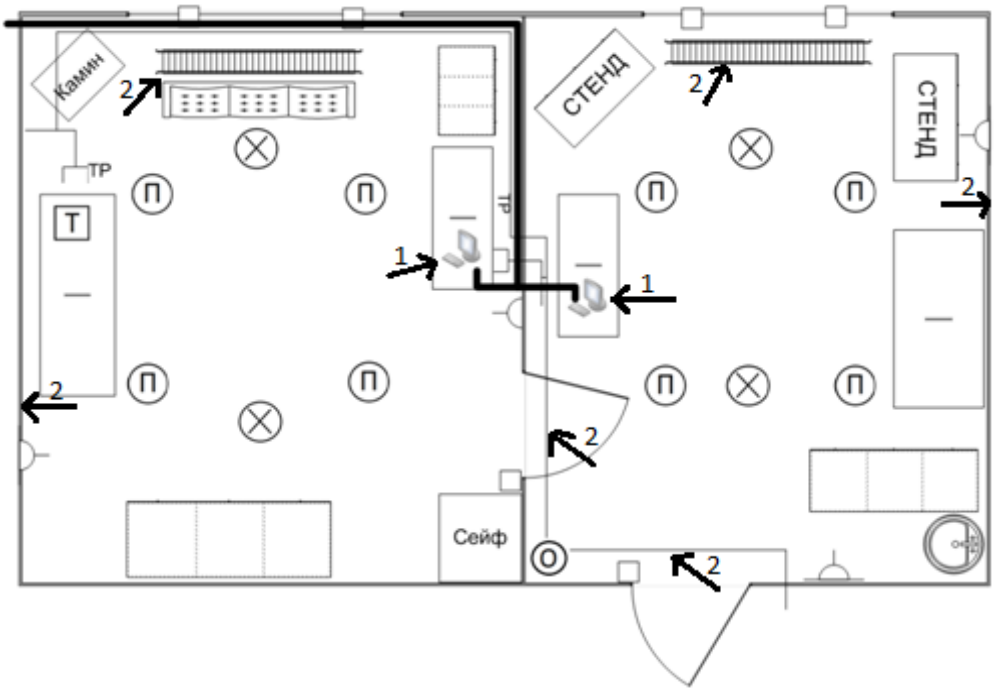


Рисунок 1 – План защищаемого помещения. 1 – побочные электромагнитные излучения и наводки; 2 – виброакустический канал.

Таким образом, предложенные мероприятия обеспечат безопасность инновационных разработок, а также удобный и защищенный доступ авторизованных пользователей.

Список использованной литературы:

1. Комплекс виброакустической защиты объектов информатизации "Барон-S1" [Электронный ресурс]. Режим доступа: http://www.t-ss.ru/baron_s1.htm - Загл. с экрана.

2. Генератор шума «Гном-3» [Электронный ресурс]. Режим доступа: http://www.t-ss.ru/gnom_3.htm - Загл. с экрана.

3. Генератор шума "ГШ-К-1800М" [Электронный ресурс]. Режим доступа: http://www.t-ss.ru/gshk_1800m.htm - Загл. с экрана.

4. Secret Net система защиты информации от несанкционированного доступа [Электронный ресурс]. Режим доступа: http://www.securitycode.ru/products/secret_net - Загл. с экрана.

5. ViPNet Office Firewall (сертифицированный) [Электронный ресурс]. Режим доступа: http://infotecs.ru/products/catalog.php?SECTION_ID=&ELEMENT_ID=171 - Загл. с экрана.

6. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 11.07.2011) "О коммерческой тайне".

АВТОМАТИЗАЦИЯ ПРОЦЕССА ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОРГАНИЗАЦИИ

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

Персональные данные в наше время становятся ценным и важным активом. Обеспечение безопасности персональных данных – необходимость, продиктованная современным миром. Его важность на сегодняшний день является неоспоримым фактом: это неотъемлемое требование к современному успешному бизнесу, закрепленное на законодательном уровне Российской Федерации [1].

Для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных требуется построение адекватной системы защиты.

Существует несколько способов решения данной задачи (рисунок 1), одним из них является обращение к специализированной организации, занимающейся вопросами защиты персональных данных. Этот способ, безусловно, имеет ряд преимуществ, таких как профессиональная помощь, гарантии качества, экономия времени сотрудников. Но данный способ достаточно дорогой.

Рисунок 1 – Способы решения задачи

Вторым способом является самостоятельная разработка требующихся документов. Данный способ не целесообразен, особенно в том случае, если в организации функционирует несколько информационных систем персональных данных, защиту которых требуется обеспечить.

Наиболее оптимальным способом по соотношению цены и качества является промежуточный вариант – самостоятельное использование программного обеспечения, позволяющего частично автоматизировать процесс проектирования системы защиты информационных систем персональных данных. Данный способ позволяет сэкономить деньги, при этом избежав ошибок из-за человеческого фактора.

После выявления данного способа решения задачи был проведен анализ рынка, в ходе которого не было обнаружено программных продуктов с требующимся функционалом, поэтому было принято решение разработать программное обеспечение, которое позволит решить данную проблему. В процессе разработки были выполнены следующие задачи:

– Разработан алгоритм работы программы на основании современных требований по защите информационных систем персональных данных.

– Разработаны подпрограммы, реализующие основные функции программы.

– Реализована подсистема формирования необходимых документов.

Разработанный программный продукт написан на языке программирования высокого уровня C# в среде разработки Microsoft Visual Studio 2013, подсистема формирования документов использует встроенную библиотеку Microsoft Office с наименованием «COM Interop».

Принцип работы программы заключается в полуавтоматическом сборе данных об информационной системе персональных данных за счет использования механизма выбора ответов пользователем программного обеспечения, анализе полученной информации, проведении пользователем с использованием программы экспертной оценки выявленных угроз безопасности персональных данных, комплексной обработке полученной информации по заданным правилам и выдаче отчетной документации.

Данный принцип работы позволяет автоматизировать расчеты и составление документации, повышая оперативность работ по проектированию систем защиты информационных систем персональных данных.

Работа с данным программным обеспечением не предполагает наличие знаний о требованиях законодательства в области защиты персональных данных у пользователя, необходимо лишь иметь полное представление о той информационной системе персональных данных, для которой необходимо проектирование системы защиты.

Пользователь отвечает на приведенные вопросы, отмечает необходимые параметры в ходе работы с программой. После того, как ответы пользователя об информационной системе персональных данных попадают в программу, вызывается подпрограмма анализа – определяется тип информационной системы персональных данных и соответствующие ему угрозы безопасности персональных данных, вычисляется исходной уровень защищенность информационной системы персональных данных. Сформированный общий перечень угроз безопасности персональных данных подлежит экспертной оценке – пользователь проводит анализ опасности и вероятности каждой угрозы. На основании полученных от пользователя данных, строится модель угроз, определяется тип актуальных угроз, а также требуемый уровень защищенности, формируются два документа – «Частная модель угроз» и «Состав и содержание требований к мерам по обеспечению безопасности персональных данных в информационной системе персональных данных».

Данное программное обеспечение имеет модульную структуру, что позволяет работать с требующейся частью функционала: есть два модуля в составе программы – «Модель угроз» и «Определение требуемого уровня защищенности». Можно работать как с каждым модулем по отдельности, так и с двумя сразу, в зависимости от требующихся функций (рисунок 2).

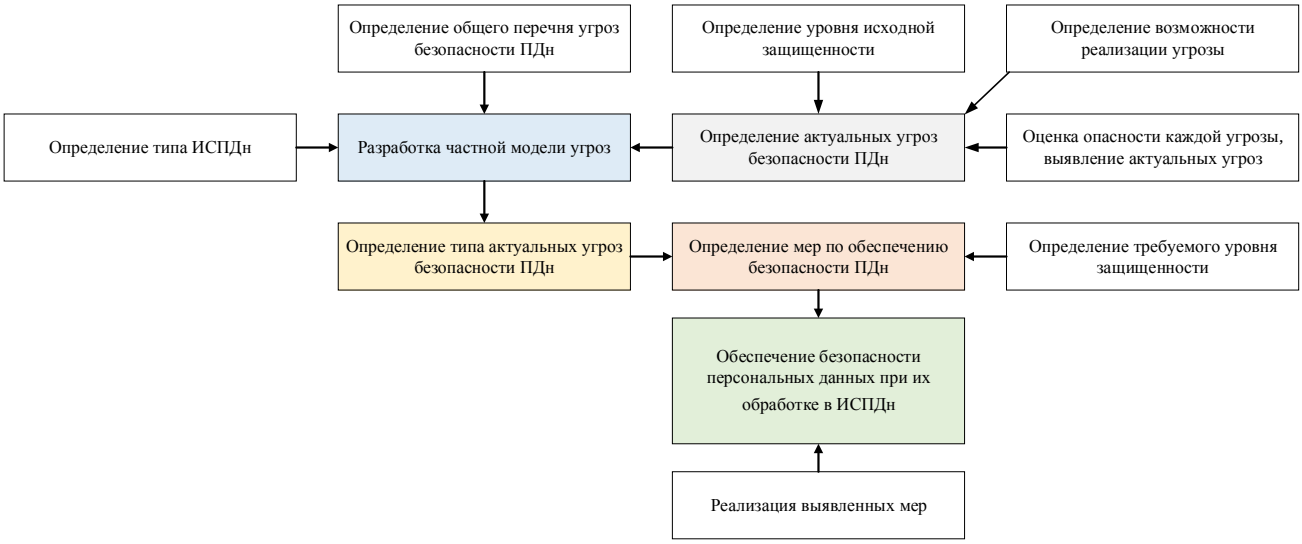


Рисунок 2 – Основные реализованные функции

К модулю «Модель угроз» относятся такие функции, как:

– определение типа ИСПДн на основе ответов пользователя [2];

– определение общего (предварительного) перечня угроз безопасности персональных данных на основе типа ИСПДн [2];

– определение актуальных угроз безопасности персональных данных, включающее в себя [3]:

а) определение уровня исходной защищенности на основе ответов пользователя;

б) определение возможности реализации угрозы;

в) оценка опасности каждой угрозы и выявление актуальных угроз;

– определение типа угроз безопасности персональных данных;

К модулю «Определение требуемого уровня защищенности» относятся такие функции, как:

– определение типа угроз безопасности персональных данных [4];

– определение требуемого уровня защищенности персональных данных [4];

– определение мер по обеспечению безопасности персональных данных [5].

В приложение также включены справочные материалы, такие как основные нормативно-методические документы, на которых базируется работа программы, а также инструкция по работе с приложением.

Таким образом, данное программное обеспечение позволяет сэкономить деньги организации, время специалистов компании, а также позволяет избежать ошибок в расчетах (которые возможны при ручной обработке данных). Данное программное обеспечение незаменимо в случае проектирования системы защиты информационных систем персональных данных собственными силами, также может использоваться организациями, предлагающими услуги по защите персональных данных, для упрощения и автоматизации своей деятельности.

В качестве развития планируется также создание веб-версии программы. Приложение будет предоставлено пользователям в качестве платного сервиса, который они могут использовать постоянно или единоразово в зависимости от своих потребностей. Разделение на коробочную и онлайн версии будет способствовать привлечению дополнительных клиентов. Также будут распространятся обновления – добавление функционала, внесение корректировок при незначительных изменениях в законодательстве (на данный момент учтены последние изменения в законодательстве в области защиты персональных данных, имеющиеся на первый квартал 2014 года).

Список использованной литературы:

1. Федеральный закон №152-ФЗ от 27.07.2006 «О персональных данных» [Электронный ресурс] / Режим доступа: http://www.consultant.ru/document/cons_doc_LAW _149747/, свободный - Загл. с экрана. – Яз. рус.

2. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс] / Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_99662/, свободный - Загл. с экрана. – Яз. рус.

3. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК РФ 14.02.2008) [Электронный ресурс] / Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_77814/, свободный - Загл. с экрана. – Яз. рус.

4. Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] / Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/, свободный - Загл. с экрана. – Яз. рус.

5. Приказ ФСТЭК №21 от 18.02.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс] / Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_146520/, свободный - Загл. с экрана. – Яз. рус.

РАЗРАБОТКА СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ В ИННОВАЦИОННУЮ ЛАБОРАТОРИЮ

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

Одним из главнейших видов деятельности Алтайского Государственного Технического Университета им. Ползунова является научная деятельность. Для того, чтобы научная деятельность приносила плоды, безусловно, необходимы специальные лаборатории с новейшим оборудованием, качественными приборами и техникой. Все это в наше время стоит недешево, и соответственно требует квалифицированного обращения и ухода. Так же

необходимо обеспечить, чтобы не произошло утечки информации о работе, проводимой в подобных лабораториях иначе, если она попадет в руки конкурентов, будет раскрыт секрет производства, что грозит полной или частичной потерей коммерческой ценности этой информации и как следствие – потере прибыли [1].

Поэтому доступ к помещениям такого рода необходимо ограничивать особенно тщательно. Чтобы допустить к работе в инновационных лабораториях только обученный персонал, необходимо наличие специальных систем контроля и управления доступом. Поэтому основной задачей является разработка и внедрение подобных систем.

В настоящее время на рынке существует масса продуктов систем разграничения доступа к помещениям различного рода. Для лабораторий самыми популярными решениями данной проблемы являются кодовые замки, которые устанавливаются на главную дверь. 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 оптимальным решением для разграничения доступа в лабораторию выбран радиоэлектронный замок. Перехват радиосигнала специальной аппаратурой практически невозможен, что обеспечивается небольшим радиусом действия модулируемых радиоволн, а так же расположением лаборатории в глубине университета, что не позволит злоумышленнику незаметно пронести аппаратуру для перехвата. В простейшем варианте система состоит из миниатюрного передатчика (ключа) и настроенного на его частоту приемника, а также исполнительного устройства с источником питания.

Принципиальная электрическая схема передатчика показана на рисунке 1.

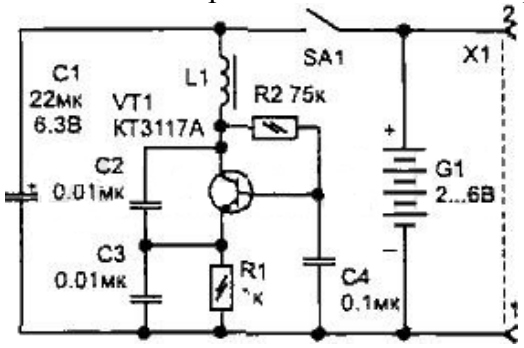


Рисунок 1 - Схема ключа-передатчика

Индуктивность L1 и конденсаторы C2, C3 обеспечивают работу автогенератора на частоте около 200 кГц. Для питания взяты четыре аккумуляторных таблетки типа Д-0,115. Потребляемый передатчиком ток не превышает 1,6 мА, и одной зарядки аккумуляторов хватает для непрерывной работы схемы в течение трех суток [3].

Схема приемника показана на рисунке 2.

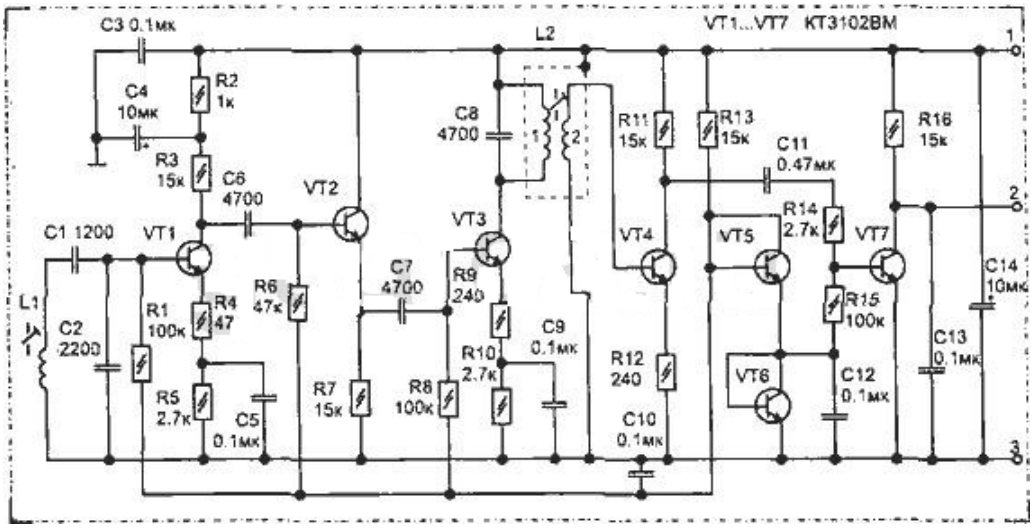


Рисунок 2 - Схема приемника

Наведенный в катушке L1 сигнал усиливают транзисторы VT1 VT3. Детектирование сигнала выполняет транзистор VT4 (активный детектор) На VT5 и VT6 (в диодном включении) обеспечивается стабилизация рабочей точки каскадов усиления. Два резонансных контура (L1-C1-C2 и L2-C8) настраиваются на частоту передатчика с помощью ферритовых сердечников. Этим обеспечивается узкополосное усиление приемника и срабатывание (появление нулевого напряжения на коллекторе транзистора VT7) только от передатчика с определенной частотой[3].

В ходе работы были изучены принципиальные электрические схемы приемника и передатчика, а так же изучен принцип действия системы контроля и управления доступом с беспроводным радиоключом, состоящей из передатчика, приемника и исполнительного устройства.

Список использованной литературы:

1. Системы контроля и управления доступом (СКУД) [Электронный ресурс]. – Электрон. текст. дан.- М., 2007.- Режим доступа: http://www.bezopasnost.ru/about/articles/40/ - 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. Бесконтактный ключ [Электронный ресурс]. – Электрон. текст. дан.- М., 2007.- Режим доступа: http://guarda.ru/guarda/data/code_lock/txt_23.php - Загл. с экрана.