разработке данного инструмента за прототип был взят вышеупомянутый CoDeSys, как один из наиболее известных универсальных инструментов программирования ПЛК и промышленных компьютеров [1].

В качестве примера реализации управляющей программы в среде SoftPLC рассмотрим револьверную головку Baruffaldi TAN 265/4HS имеющую следующие характеристики:

Револьверная головка относится к виду систем автоматической смены инструментов. В данном случае возможна установка одновременно не более четырех инструментов.

Таблица 1. Характеристики револьверной головки Baruffaldi TAN 265/4HS

Характеристика	Размерность	TAN 265/4HS
Количество инструментов	шт	4
Момент инерции масс	кгм ^{2}	8
Максимальный крутящий момент	Нм	3600
Время разблокировки	сек	0,5
Время одного оборота	сек	5

На приведенной, на рис.2 циклограмме показана последовательность операций, которым необходимо следовать для управления револьверной головкой в рабочем режиме.

С момента старта тормоз обесточен и размагничен. После 50 мс паузы двигатель начинает вращение против часовой стрелки. После поступления сигнала от переключателя (соответствует нужному положению) двигатель блокируется (начинает вращаться в обратную сторону). Через некоторое время срабатывает переключатель блокировки, наступает момент первой паузы t1=350 мс. В конце этой паузы тормоз должен быть включен. Далее следует вторая пауза t2=150 мс, необходимая для блокировки всех кинематических частей, после чего двигатель останавливается. Тормоз должен быть включен, пока ищется новая нужная позиция.

Программа управления револьверной головкой Baruffaldi TAN 265/4HS реализована на языке функциональных блоков (FBD).

Стартом является команда M06 (команда смены инструмента), по которой запускается таймер Timer1 на размагничивание. После срабатывания Timer1 запускается Timer2, после отсчета 50мс запускается вращение двигателя. Вращение осуществляется по тех пор, пока в результате сравнения элемента Tool (Tool – номер искомого инструмента) с каждым из I0.0, I0.1, I0.2, I0.3 сигналов датчиков на выходе не будет получена 1 означающая, что нужная позиция найдена. Далее через RS-триггер прекращается вращение двигателя. Запускается таймер для переключателя, и таймер для блокировки, а также на размагничивание.

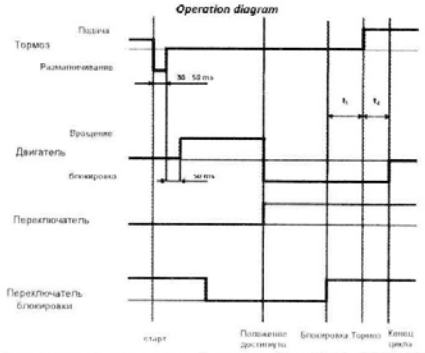

Рис.2 Циклограмма револьверной головки Baruffaldi TAN 265/4HS

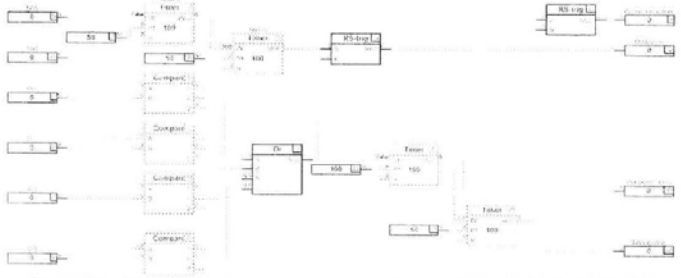

Рис. 3 Код программы управления револьверной головкой Baruffaldi TAN 265/4HS

В ходе работы была реализована программа управления револьверной головкой Baruffaldi TAN 265/4HS на базе программно-реализованного контроллера. Данная технология получила в последние годы заслуженную популярность и позволяет получить ряд преимуществ, среди которых: упрощение общего программного обеспечения, уменьшение ошибок системного программирования, возможность отладки управляющих программ электроавтоматики в рамках самой системы ЧПУ, гибкость конфигурирования электроавтоматики, возможность использования различных коммерческих библиотек.

Библиографический список:

1.Сосонкин В.Л., Мартинов Г.М. Системы числового программного управления: Учеб пособие. – М. Логос, 2005. – 296 с. ISBN 5-98704-012-4

2.Нежметдинов Р.А. Расширение функциональных возможностей систем ЧПУ для управления механо-лазерной обработкой / Нежметдинов Р.А., Соколов С.В., Обухов А.И., Григорьев А.С. // Автоматизация в промышленности. - 2011. - № 5. - С. 49-51

БЕЗОПАСНЫЙ МОБИЛЬНЫЙ КАНАЛ СВЯЗИ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ АНДРОИД

Захаров А.А.
Научный руководитель: к.т.н., проф. Кабак И.С.

Кафедра «Компьютерные системы управления» ФГБОУ ВПО МГТУ «СТАНКИН»

Тенденция развития современных технологий характеризуется постоянным

повышением значения информации. Производственные процессы имеют в своём составе материальную и нематериальную составляющие. Первая - это необходимое для производства оборудование, материалы и энергия в нужной форме. Вторая составляющая - технология производства. В последнее столетие появилось много таких отраслей производства, которые почти на 100% состоят из одной информации, например, дизайн, создание программного обеспечения, реклама и другие. Соответственно, и себестоимость товара складывается из стоимости материала, энергии и рабочей силы с одной стороны и стоимости технологии, с другой. Кроме производственных процессов информация играет большую роль, а иногда и является основой деятельности Управленческих организаций, страховых обществ, банков, организаций социальной сферы и т.д. Во многих из перечисленных случаях информация представляет большой интерес для криминальных элементов. Все преступления начинаются с утечки информации.

Сегодня у руководства большинства организаций, предприятий и банков не остается сомнений в необходимости серьезно заботиться об информационной безопасности.

Именно поэтому вырос интерес к вопросам защиты информации. Это связано с тем, что стали более широко использоваться вычислительные сети, что приводит к тому, что появляются большие возможности для несанкционированного доступа к передаваемой информации.

В литературе выделяют различные способы защиты информации среди них выделим:

-физические (препятствие)

-законодательные

-управление доступом

-криптографическое закрытие.

В данном докладе будут рассматриваться криптографические способы защиты информации. Так как целью работы является обеспечение безопасного (шифрованного) канала связи.

Криптография - наука о методах обеспечения конфиденциальности

(невозможности прочтения информации посторонним). Заключается в том, что последовательность символов (открытый текст) подвергается некоторому преобразованию (в котором используется ключ) и в результате получается закрытый текст, непонятный тому, кто не знает алгоритма шифрования и, конечно, ключа.Для преобразования (шифрования) обычно используется некоторый алгоритм или устройство, реализующее заданный алгоритм, которые могут быть известны широкому кругу лиц. Управление процессом шифрования осуществляется с помощью периодически меняющегося кода ключа, обеспечивающего каждый раз оригинальное представление информации при использовании одного и того же алгоритма или устройства. Знание ключа позволяет просто и надёжно расшифровать текст. Однако без знания ключа эта процедура может быть практически невыполнима даже при известном алгоритме шифрования.[1]

Рассмотрим основные современные методы защиты информации.

Скремблер — это устройство, которое осуществляет шифрование передаваемой по каналам связи речи. При скремблировании возможно преобразование речевого сигнала по следующим параметрам: амплитуде, частоте и времени. В системах подвижной радиосвязи практическое применение нашли в основном частотные, временные преобразования сигнала или их комбинация. Помехи в радиоканале существенно затрудняют точное восстановление амплитуды речевого сигнала, поэтому

амплитудные преобразования при скремблировании практически не применяются. Достоинство скремблеров: защита осуществляется на всем протяжении линии связи, то есть в открытом виде информация передается только от скремблера к телефону, это расстояние ограничено длиной провода или радиусом действия Bluetooth. Недостатки скремблера: необходимость использования совместимого оборудования всеми абонентами, с которыми предполагается вести защищенные переговоры и потеря времени необходимая для синхронизации аппаратуры при установке безопасного соединения.

При частотных преобразованиях сигнала[2] в средствах подвижной радиосвязи чаще всего используются следующие виды скремблирования:

•.частотная инверсия сигнала (преобразование спектра сигнала с помощью гетеродина и фильтра);

•.разбиение полосы частот речевого сигнала на несколько поддиапазонов и частотная инверсия спектра в каждом относительно средней частоты поддиапазона.

•.разбиение полосы частоты речевого сигнала на несколько поддиапазонов и их частотные перестановки.

При временных преобразованиях производится разбиение сигнала на речевые сегменты и их перестановки во времени

•.инверсия по времени сегментов речи;

•.временные перестановки сегментов речевого сигнала.

Комбинированные методы преобразования сигнала используют одновременно частотные и временные преобразования.

Скремблер присоединяется к телефону(по проводу или Bluetooth) и в выключенном состоянии никак себя не проявляет. Как только владелец аппарата включает его, как он тут же начинает принимать все сигналы, идущие с микрофона, шифровать их и только после этого отсылать на выход. Декодирование речи происходит в обратном порядке. Сигналы с антенны подаются в скремблер, а уже оттуда — на динамик. Таким образом, скремблер шифрует передаваемую речь и дешифрует принятый сигнал.

Криптофон — сравнительно новое устройство защиты телефонных разговоров. Криптофон представляет собой тот же смартфон, но на нем установлено специальное программное обеспечение. Принцип работы криптофона схож с со скремблером: сигнал с микрофона оцифровывается, затем кодируется и передается абоненту. Отличие состоит в способе шифрования. Для этого используют способы криптографической защиты.[3] Современные криптофоны используют следующие алгоритмы шифрования: AES, Twofish и др.

Недостатки криптофонов:

•.Необходимость у обоих абонентов таких устройств;

•.Неприятности, связанные с задержкой голоса (могут достигать нескольких секунд);

•.Наличие эха во время разговора.

Таким образом на данный момент на рынке существует определенный набор средств защиты связи, но все они имеют один важный недостаток, им требуется специальная аппаратура. Отсюда высокая стоимость данных решений.

Я предлагаю подойти к проблеме защиты связи по-другому. В настоящее время большинство абонентов сотовой связи используют смартфоны, в частности под системой Андроид. На мой взгляд целесообразнее разработать специализированное ПО позволяющее производить конфиденциальные телефонные переговоры по каналу данных CSD в сетях сотовой связи, обеспечивая эффективную двустороннюю защиту от прослушивания разговоров. Для его использования потребуется только соответствующие смартфоны и установленное ПО.

Принцип действия ПО заключается в передачи в момент соединения на аппарат собеседника закрытого ключа для блочного шифрования[5].В процессе общения происходит шифрование разговора, в данном случае блочным способом[4].

Библиографический список

1. Герасименко В. А., Малюк А.А. Основы защиты информации М.,1994г. 540с.

2.Овчинников А. М. Методы защиты информации в системах конвенциональной радиосвязи

3.Д. В. Скляров Искусство защиты и взлома информации

4.Патент на изобретение 2481715 Российская Федерация МПК 7 H04L9/00 Способ блочного шифрования сообщений и передачи 2013.05.10шифрованных данных с закрытым ключом [Текст]/ Позднеев Б. М., Кабак И.С. , Суханова Н. В.: заявитель и патентообладатель Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Московский государственный технологический университет "СТАНКИН" (ФГБОУ ВПО МГТУ "СТАНКИН").-№ 2011148733 ; заявл. 30.11.2011; опубл. 10.05.2013, Бюл. № 13- 13 с.: ил.

5.Патент на изобретение 2459367 Российская Федерация МПК 7 H04L9/00 Способ формирования переменного ключа для блочного шифрования и передачи шифрованных данных [Текст]/ Кабак И.С. , Суханова Н. В., Позднеев Б. М.: заявитель и патентообладатель Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Московский государственный технологический университет "СТАНКИН" (ФГБОУ ВПО МГТУ "СТАНКИН").-№ 2010129310 ; заявл. 16.07.2010; опубл. 20.08.2012, Бюл. № 23- 11 с.: ил.