МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра “Кибербезопасность, обработка и хранения информации”

Мерекебаев Санжар Мұратұлы

Устройство для защиты акустической информации по телефонному каналу связи

ДИПЛОМНАЯ РАБОТА

специальность 5В100200 – Системы информационной безопасности

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра “Кибербезопасность, обработка и хранения информации”

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой
Кибербезопасность, обработка и хранение информации
канд.техн.наук, ассист. профессор
_____ Сейлова Н.А.
"_13_" _____05_____2019 г

ДИПЛОМНАЯ РАБОТА

На тему: «Устройство для защиты акустической информации по телефонному каналу связи»

по специальности 5В100200 - Системы информационной безопасности

Выполнил Мерекебаев С.М.

Рецензент
канд. полит. наук, доцент
зав.кафедрой «Системы информационной безопасности» АУЭиС
_____ Бердибаев Р.Ш.
«_06_» _____05_____2019 г.

Научный руководитель
д.т.н., ассоц. профессор
_____ Джурунтаев Д.З.
«_13_» _____05_____2019 г.

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра “Кибербезопасность, обработка и хранения информации”

5В100200 - Системы информационной безопасности

УТВЕРЖДАЮ
Заведующий кафедрой
Кибербезопасность, обработка и хранение информации
канд.техн.наук, ассист. профессор
_____ Сейлова Н.А.
"_13_" _05_____2019 г.

ЗАДАНИЕ
на выполнение дипломной работы

Обучающемуся *Мерекебаеву Санжару Мұратұлы*
Тема: *Устройство для защиты акустической информации по телефонному каналу связи*
Утверждена *приказом руководителя университета №1162-б от «16» октября 2018г.*
Срок сдачи законченного проекта: *«___» _____ 2019 г.*
Исходные данные к дипломному проекту: *Заданная схема скремблера.*
Перечень подлежащих разработке в дипломном проекте вопросов: *а) технические средства прослушивания телефонных каналов связи; б) технические средства защиты информации от утечки по телефонным каналам связи; в) скремблирование.*
Перечень графического материала (с точным указанием обязательных чертежей): *16 графических слайдов*
Рекомендуемая основная литература*: 1. Ярочник В. И.Технические каналы утечки информации, Москва, ИПКИР 2010. 2. Киселев А. Е. Коммерческая безопасность. Москва, ИнфоАрт 2003. Рудаметов Е.А., Рудаметов Б.Е. Электроника и шпионские страсти. – СПб.: Пергамент, 2008.- 253с.3. Транзисторы: Справочник/Под ред. Григорьева О.П. и др.- М.: Радио и связь, 2010.- 387с.4. Вынин С. А., Шустов Л. Н. Основы радиопротиводействия радиотехнической разведки. Москва, Советское радио, 2010.5. Хорев П.Б.*

ГРАФИК

подготовки дипломного проекта

Наименования разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Технические средства прослушивания телефонных каналов связи	08.01.2019 - 14.01	
Технические средства защиты информации от утечки по телефонным каналам связи	15.02.2019. - 10.03	
Скремблирование	10.03-15.05.2019.	

Подписи

консультантов и нормоконтролера на законченный дипломный проект с указанием относящихся к ним разделов проекта

Наименования разделов	Консультанты, И.О.Ф. (уч. степень, звание)	Дата подписания	Подпись
Нормоконтролер	А.А Зиро	15.05.2019	

Научный руководитель _____ Д.З.Джурунтаев

Задание принял к исполнению обучающийся _____ С.М.Мерекебаев

Дата «13» 05 2019 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

ОТЗЫВ

НАУЧНОГО РУКОВОДИТЕЛЯ

на _____Дипломную работу_____
(наименование вида работы)

Мерекебаев Санжар Мұратұлы
(Ф.И.О. обучающегося)

5В100200 «Системы информационной безопасности»
(шифр и наименование специальности)
Тема: «Устройство для защиты акустической информации по телефонному каналу связи»

Одним из основных каналов утечки информации является телефонный аппарат и линия связи, соединяющая его с АТС. В условиях рыночной экономики ценность информации, возможность её прослушивания, в частности, путем её съема с телефонной линии связи, вызывает особое беспокойство у ряда коммерческих организаций, работников госсектора, политиков и бизнесменов за сохранения конфиденциальности своих переговоров. В этом аспекте актуальной является разработка электрической схемы устройства, анализирующего состояния телефонной линии для защиты информации от утечки. Решению указанной проблемы посвящена тема данного дипломного проекта. В нем рассмотрены различные схемы специальных электронных средств, предназначенных как для нелегального съема чужой информации, так и для её защиты от утечки и дано качественное их сравнение.

Наибольший интерес представляет разработанная автором дипломного проекта принципиальная электрическая схема устройства, названного скремблером, которое осуществляет преобразование аналоговых речевых сигналов и цифровое шифрование.

Особенностью разработанной схемы скремблера является то, что она принимает сигналы, поступающие с микрофона, шифрует их и затем отправляет телефонному каналу связи. Данное устройство может быть выполнено полностью на интегральных микросхемах, что обеспечивает простоту конструкции, компактность, сравнительно хорошие функциональные возможности и относительно низкую стоимость. Все это повышает практическую ценность выполненного проекта.

В заключении считаю, что дипломный проект выполнен качественно и технически грамотно, а его автор в ходе выполнения проекта показал высокую теоретическую подготовку, трудолюбие и инженерные навыки решения технических задач. Поэтому дипломный проект может быть допущен к защите.

Научный руководитель,
д. т. н., ассоциированный профессор
кафедры «КОиХИ» _____ Д.З. Джурунтаев
«13» 05 2019 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

РЕЦЕНЗИЯ

на _____Дипломную работу (проект) _____
(наименование вида работы)

Мерекебаева С.М
(Ф.И.О. обучающегося)

5В100200 «Системы информационной безопасности»
(шифр и наименование специальности)

На тему: Устройство для защиты акустической информации по телефонному каналу связи

Выполнено:
а) графическая часть на 27 листах
б) пояснительная записка на 7 страницах

ЗАМЕЧАНИЯ К РАБОТЕ

Нелегальный съем информации, в том числе подслушивание телефонных разговоров в условиях рыночной экономики получило заметное распространение как в бизнесе, так и в быту. Поэтому задача предотвращения утечки конфиденциальной информации по телефонным линиям связи является одной из наиболее важных для подразделений и служб безопасности частных, коммерческих и государственных учреждений. В этом аспекте актуальна тема дипломной работы, в которой студентом выявлена и решена задача разработки устройства со световой индикацией, которое не только анализирует состояние телефонной линии и обнаруживает несанкционированное подключение подслушивающего устройства, но и осуществляет блокировку радиоретранслирующего устройства и прибора регистрации телефонной информации. Для достижения цели, поставленной в дипломной работе ее автором рассмотрены различные схемы и способы нелегального съема телефонной информации и обнаружения каналов её утечки и дано качественное их сравнение.

Важной особенностью дипломного проекта является то, что в нем рассматривается вопрос разработки устройства, которое осуществляет преобразование аналоговых речевых сигналов и цифровое шифрование, т. е. принимает сигналы, поступающие с микрофона, шифрует их и затем отправляет телефонному каналу связи. Выполнение данного устройства на основе электрических микросхемах делает его более экономичным с точки зрения потребления энергии, простым в изготовлении, надежным, конструктивно малогабаритным и удобным в эксплуатации.

Дипломантом также рассмотрены основные блоки и их назначение схемы скремблера, разработана схема генератора псевдослучайных битовых

последовательностей (последовательность 2^M-1 бит), а также основные методы маскировки речи и особенности.

Все это повышает практическую ценность дипломной работы, которая выполнена качественно и технически грамотно.

Пояснительная записка к дипломной работе, состоящая из страниц, и графические материалы выполнены в соответствии с требованиями ГОСТа.

Оценка работы

Считаю, что студент Мерекебаев С., выполнивший данную дипломную работу на высоком инженерно-техническом уровне, заслуживает оценки 90 и присвоения ему степени Бакалавра военного дела и безопасности по специальности «Системы информационной безопасности».

Рецензент:
канд.полит.наук, доцент
заведующий кафедрой СИБ, АУиЭС Бердибаев Р.Ш

«06» «05» 2019 г.

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Мерекебаев Санжар

Название: Устройство для защиты акустической информации от утечки по телефонному каналу связи

Координатор: Джолдас Джурунтаев

Коэффициент подобия 1:0

Коэффициент подобия 2:0

Тревога:4

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

☐ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;
☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

..... в работе заимствования не обнаружено .....
.....
.....
.....

....

Дата 13.05.19г *Подпись заведующего кафедрой*

начальника структурного подразделения

Окончательное решение в отношении допуска к защите, включая обоснование:

допущен к защите!

Дата 13.05.19г

Подпись заведующего кафедрой /

начальника структурного подразделения

ВВЕДЕНИЕ

Развитие и использование достижений современной электроники привело к появлению новых радиоэлементов и устройств на их основе с новыми (частью уникальными) параметрами и потребительскими свойствами. Широкое внедрение данных элементов и устройств, особенно в быту, привело к коренному преобразованию условий жизни. Появились высокочувствительные малогабаритные радиоприемники, радиопередатчики и другие электронные устройства, выполненные в основном на интегральных микросхемах. Средства связи опутали весь мир. Это сопровождается значительными расширениями коммуникационных услуг. Однако чудеса электроники могут вызвать не только восторг.

Радиоприемники как средство связи расширяют возможности не только наши и наших друзей, коллег, партнеров. А у ряда потребителей изделий современной микроэлектроники некоторые цели и методы их достижения могут быть не только честными и благородными. И смотрят иногда не только в экран телевизора, компьютера и так далее, но к сожалению и в замочные скважины. И слушают не только свой телефон, а чужой и не из праздного любопытства, вызванного недостатком такта или культуры. И ущерб от этого может быть не только нравственный, но и экономический. Такие действия носят название промышленного, точнее экономического шпионажа, осуществляемого как правило, с использованием всех достижений современной микроэлектроники: усилителей, приемников, передатчиков, ретрансляторов, магнитофонов, компьютеров и тому подобное. Прослушивают, подсматривают, перехватывают сообщения. Могут быть проконтролированы все используемые каналы передачи информации: звук, телефон, радио и так далее.

Таким образом, в настоящее время информация приобретает ценность и становится товаром. И как товар ее похищают, копируют и перепродают без разрешения законного собственника, нарушая его права и нанося ему экономический ущерб.

Ценность информации передаваемой по телефонным линиям, а так же бытующее убеждение о массовом характере такого прослушивания вызывает небольшое беспокойство у организаций и частных лиц за сохранение конфиденциальности своих переговоров именно по телефонным каналам. Для защиты своих секретов необходимо знать методы и средства (в том числе технические), с помощью которых могут быть осуществлены операции по перехвату.

В связи с этим актуальной является разработка электрической схемы устройства защиты информации от утечки по телефонным линиям. Решению указанной проблемы посвящена тема данного дипломного проекта. В проекте рассматривается особенности электрических схем скремблера , который не только анализирует состояние телефонной линии и

обнаруживает несанкционированное подключение подслушиваемого устройства, но и осуществляет блокировку радиоретрансляционного устройства и прибора регистрации телефонной информации.

В настоящее время известно много специальных электронных средств, предназначенных как для несанкционированного доступа к чужой информации, так и для обнаружения и блокировки подслушивающего и регистрирующего устройства. Эти устройства отличаются широкими функциональными возможностями и улучшенными характеристиками, однако они, как правило, весьма дорогие. Поэтому в дипломном проекте данная проблема успешно решается с помощью более простого электронного устройства на базе высококачественных элементов (интегральных микросхем) и современных схемотехнических решений.

Отличительной особенностью разработанного устройства защиты информации – анализатора телефонной линии является простота конструкции, комплектность, относительно хорошие функциональные возможности и низкая стоимость.

В дипломном проекте рассматривается принцип работы основных блоков, узлов устройства защиты информации от утечки по телефонным линиям связи.

1. Технические средства прослушивания телефонных каналов связи

К одной из основных угроз безопасности информации ограниченного доступа относится утечка информации по техническим каналам, под которой понимается неконтролируемое распространение информативного сигнала от его источника через физическую среду до технического средства, осуществляющего прием информации.

Перехватом информации называется неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов.

В результате перехвата информации возможно неправомерное ознакомление с информацией или неправомерная запись информации на носитель.

Особенности технических каналов утечки информации определяются физической природой информационных сигналов и характеристиками среды их распространения.

Общая классификация технических каналов утечки информации включает следующие виды каналов:

- каналы утечки, обрабатываемой техническими средствами приема, обработки, хранения и передачи информации (ТСПИ);
- каналы утечки речевой информации;
- утечка информации при ее передаче по каналам связи;
- технические каналы утечки видовой информации.

Защита речевой (акустической) информации является одной из важнейших задач в общем комплексе мероприятий по обеспечению информационной безопасности объекта технической защиты информации (ЗИ). Это связано с тем, что в процессе обсуждения служебных вопросов может озвучиваться конфиденциальная информация (информация ограниченного доступа). Перехват этой информации может происходить максимально оперативно в момент ее первого озвучивания. Объектами технической защиты речевой (акустической) информации (ТЗРИ) являются учреждения системы государственного управления, военные и военно-промышленные объекты, научно-исследовательские учреждения и так далее. При этом на объектах ТЗРИ защищаются:

- специально предназначенные для обмена речевой информацией ограниченного доступа (звукозаписи, звуковоспроизведения такой информации) помещения;
- помещения, специально не предназначенные, но используемые для такого рода деятельности в силу обстоятельств;
- открытые площадки.

Нормативную базу, которой руководствуются при решении задач ТЗРИ, составляют нормативно-методические документы Государственной технической комиссии при Президенте Российской Федерации и другие ведомственные документы, разработанные на их основе. Органы

технической разведки различной принадлежности (иностранных государств, экстремистских и террористических организаций, конкурирующих фирм и других соперничающих организаций) могут использовать для перехвата широкий арсенал портативных средств акустической речевой разведки (АРР), позволяющих перехватывать речевую информацию по прямому акустическому, виброакустическому, оптико-электронному и другим каналам. К основным средствам АРР относятся:

- портативная аппаратура звукозаписи (малогабаритные диктофоны, магнитофоны и устройства записи на основе цифровой схемотехники);
- направленные микрофоны;
- электронные стетоскопы;
- электронные устройства перехвата речевой информации (закладные устройства) с датчиками микрофонного типа;
- оптико-электронные (лазерные) средства дистанционного прослушивания и так далее.

Проблемы ЗИ от АРР решаются в направлении совершенствования активных и пассивных способов защиты информации. Широко применяются технические меры, основанные на использовании специальных материалов и средств, технических и конструкторских решений. Для скрытия речевого сигнала применяются:

- специальные строительные и отделочные материалы, гильзы, коробы, прокладки, глушители, вязкоупругие заполнители, специальные вставки в разрывы труб системы теплоснабжения и воздуховодов, акустические фильтры, глушители звука и так далее, обеспечивающие звукоизоляцию выделенных помещений;
- системы активной акустической и виброакустической маскировки, создающие в разведопасных направлениях помехи, снижающие разборчивость перехваченных сообщений;
- средства электромагнитного и ультразвукового подавления диктофонов в режиме записи.

Снятие информации, передаваемой по телефонной линии является одним из простейших, самых распространенных и результативных и наиболее дешёвых способов. Прослушивание разговора на телефонной линии осуществляется в коммерческих или других целях. По американским данным вероятность утечки информации по телефонным каналам составляет от 5% до 20%. В настоящее время известны следующие способы несанкционированного получения необходимой информации и перехвата телефонных сообщений:

- непосредственное подключение подслушивающего устройства к телефонной линии;
- подключение устройства с использованием индукционных датчиков (датчиков Холла и пр.);
- использование телефонного радиотранслятора;
- перехват сообщений сотовой связи;

- перехват пейджеговых сообщений;
- перехват факсимильных сообщений и.т.д.

Самым простым и часто применяемым способом съема телефонной информации является простое параллельное подключение к вашему телефону другого телефонного аппарата либо устройства заменяющего его функции. Подключение может произойти на любом участке телефонной линии вплоть до АТС. Данный способ подключения обнаружить его легко, так как такое подключение сопровождается понижением напряжения в сети, что может быть обнаружено несложными индикаторами. Чтобы устройство съема не приносило изменения в электрические параметры прослушиваемой линии, его подключают через какой-либо высокоомный каскад. В данном случае выявить подключение практически невозможно, и единственным действенным способом борьбы с “прослушиванием” является скремблирование (шифрование) данных.

Если абоненты хотят произвести закрытый сеанс связи, скремблеры должны устанавливаться с обеих сторон телефонной линии. Алгоритм кодирования и декодирования определяется только двумя скремблерами, которые перед началом закрытого сеанса связи обмениваются паролями. В зависимости от технических характеристик скремблеров, алгоритм кодирования и съема паролей могут отличаться по сложности. Скремблеры работают со спектром шифруемого сигнала. Если голосовое сообщение сначала преобразуется в цифровой вид, а затем шифруется, то такие устройства называются вокодерами.

1.1 Схема телефонной линии связи

Схема телефонной линии связи в общем виде представлена на рисунке 1.1, где показаны зоны возможного прослушивания телефонных переговоров. Зона1 является зоной телефонного аппарата (ТА). Зона 2 представляет собой двухпроводную линию (шлейф) от ТА, включая распределительную коробку. Зона 3, называемая кабельной (магистральной), включает участок телефонной линии связи от АТС до распределительной коробки. Остальные зоны: 4, 5 и 6 являются зонами АТС, многоканального кабеля и радиоканала, соответственно.

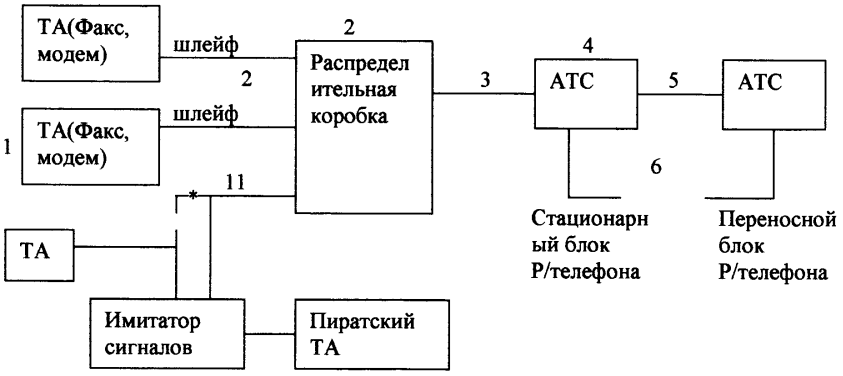


Рисунок 1.1. Схема телефонной линии связи

Прослушивание разговора на телефонной линии, обычно осуществляется на первых трех зонах. В этих зонах легче всего подключится к телефонной линии. Чаще всего прослушивание осуществляется номером параллельного аппарата (ТА). Подключение в 3-ей зоне менее распространено, так как, необходимо проникать в систему телефонных коммуникаций, состоящую из труб с проложенными внутри них кабелями, а также разобраться в этой системе и определить нужную пару среди сотни других. Однако эту задачу не следует считать невыполнимой. В качестве примера можно привести американскую систему «Крот». С помощью специального индуктивного датчика, охватывающего кабель, снимается передаваемая по нему информация. Подключение к телефонным линиям осуществляется не только гальванически (прямым соединением), но и с помощью индукционных или ёмкостных датчиков. Съем информации с телефонной линии при индукционном способе основан в следующем. Так как по телефонной линии протекает электрический ток, то она может наводить электродвижущую силу (сигнал) в катушке, которой в данном случае является зонд устройства съема телефонной информации. При индукционном способе съем информации производится без повреждения информации и является полностью пассивным устройством. То есть выявить подключение к телефонной линии становится практически невозможным и единственным способом борьбы в этом случае является скремблер.

Отдельное место занимают устройства, которые предназначены не для прослушивания телефонных переговоров, а для использования телефонных линий при прослушивании контролируемых помещений, где установлены телефонные аппараты или проложены провода телефонных линий.

Примером такого устройства может служить «телефонное ухо», которое представляет собой небольшое устройство, подключенное параллельно к телефонной линии или розетке в любом удобном месте контролируемого помещения. Для прослушивания помещения необходимо набрать номер абонента, в помещении которого стоит «телефонное ухо». Первые два гудка «проглатываются», то есть телефон не звонит. После этого необходимо положить трубку и через определенное время позвонить снова. Только после этого система включится в режим прослушивания.

В случае обычного звонка «телефонное ухо» пропускает все звонки после первого, выполняя роль обычной телефонной розетки и не мешая разговору.

1.2 . Прослушивание через микрофон телефонного аппарата

На рисунке 1.2 приведена схема прослушивания помещения способом, называемым высокочастотным навязыванием.

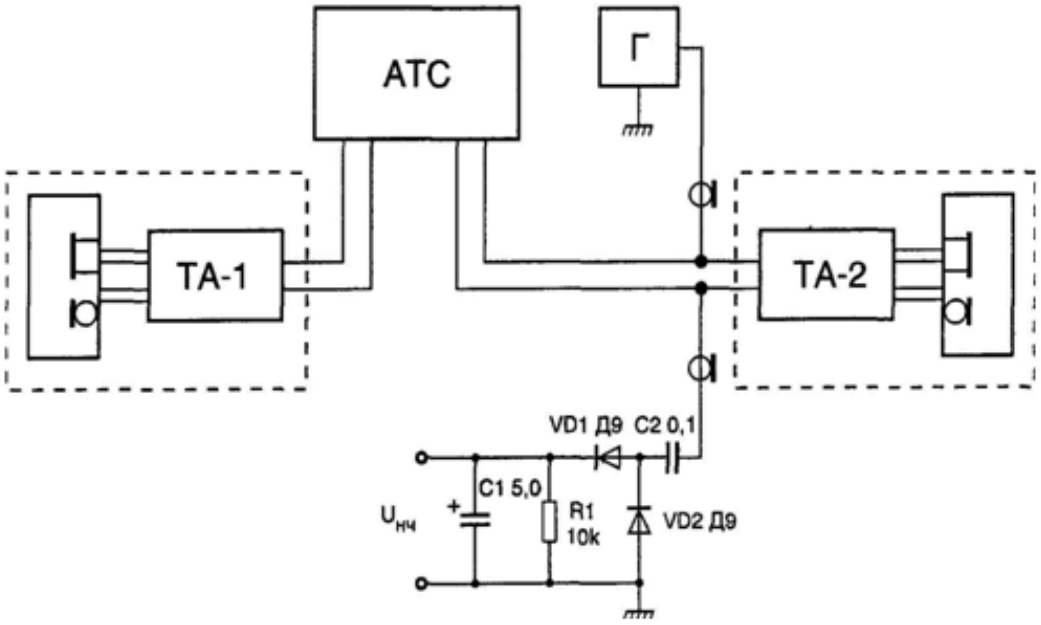


Рисунок 1.2. Прослушивание через микрофон телефонного аппарата

Этот способ состоит в следующем. На один из проводов телефонной линии, идущий от АТС к телефонному аппарату ТА-2, подаются колебания частотой 150 кГц и выше от генератора высокочастотных колебаний, Г. К другому проводу линии подключается амплитудный детектор с усилителем, выполненный на элементах Cl, C2, VD1, VD2 и R1. Корпус передатчика (генератор Г) и приемника (детектор) соединены между собой или с общей землей, например с водопроводной трубой.

Высокочастотные колебания через элементы схемы телефонного аппарата ТА-2 поступают на микрофон и модулируются модулируются речью (акустическими сигналами) прослушиваемого помещения. Детектор приемника выделяет речевую информацию, которая усиливается до необходимого уровня и обрабатывается. Другими словами, модулированный высокочастотный сигнал демодулируется амплитудным детектором и после усиления прослушивается или записывается. Вследствие существенного затухания ВЧ сигнала в двухпроводной линии, дальность съема информации таким методом не превышает нескольких десятков метров.

Для защиты телефонного аппарата от снятия информации таким способом достаточно параллельно микрофону подключить конденсатор емкостью 0,01 – 0,05 мкФ. При этом последний будет шунтировать микрофон по высокой частоте и глубина модуляции ВЧ колебаний уменьшится более чем в 10 000 раз, что делает дальнейшую демодуляцию сигнала практически невозможной.

Рассмотрим некоторые способы прослушивания телефонных линий.

Более скрытым методом является установка в аппарат устройства, активизируемого специальным кодом через любой внешний телефон. В

упрощенном варианте в схему телефонного аппарата вводят небольшое резонансное реле, настроенное на определенную частоту. Подслушивающий набирает номер контролируемого аппарата с любого другого телефона, в том числе и междугородного, и подносит к своей трубке портативный звукоизлучатель (бипер), тональный сигнал которого соответствует частоте срабатывания реле. Реле быстро отключает звонок аппарата и переводит трубку во включенное состояние, позволяя звонившему прослушивать все разговоры в комнате. Устройство работает независимо от самого телефона и, как правило, требует дополнительной телефонной линии. Такие устройства широко продаются на Западе для домашнего мониторинга.

Описанная схема имеет несколько модификаций, в частности, усложненный код (чтобы затруднить случайное обнаружение факта перехвата), использование специального усилителя и микрофона (для улучшения качества сигнала).

Следует подчеркнуть, что иногда звонок может кратковременно сработать до того, как резонансное реле его отключит. Такой сокращенный звонок может стать возможным признаком того, что телефон используется для подслушивания. Дополнительным настораживающим моментом является занятость рабочей линии в те периоды времени, когда она должна быть свободной.

«Атаки» на компьютеризованные телефонные системы

В последнее время объектом повышенного внимания злоумышленников стали компьютеризованные телефонные системы (АТС и офисные мини-АТС, управляемые компьютером). В таких системах все телефонные соединения осуществляются компьютером в соответствии с заложенной в него программой. В общем виде «атака» на такую телефонную систему состоит в том, что злоумышленники, используя хорошо отработанные способы, дистанционно проникают в локальную компьютерную систему или в сам управляющий компьютер и изменяют программу, по которой он выполняет телефонные соединения или предоставляет доступ абонентов в систему. В результате они получают возможность перехватывать со своего телефона все виды информационного обмена, ведущегося в контролируемой системе. При этом обнаружить факт такого перехвата чрезвычайно сложно.

2. Технические средства защиты информации от утечки по телефонным каналам связи

Самым распространенным средством прослушивания телефонных разговоров является радиоретранслятор. Телефонные радиоретрансляторы подключаются параллельно или последовательно в любом месте телефонной линии и имеют больший срок службы, так как питаются от телефонной сети.

Радиоретранслятор автоматически включается при поднятии телефонной трубки и передают разговор по радиоканалу на приемник пункта перехвата, где он может быть прослушан и записан. Радиоретрансляторы используют микрофон телефонного аппарата (ТА) и не имеют своего источника питания, поэтому их размеры могут быть очень не большие. В качестве антенны используется телефонная линия. Для маскировки радиоретрансляторы выпускаются в виде реле, конденсатора, фильтров и других стандартных элементов, входящих в состав ТА.

Ниже будут рассмотрены радиоретрансляторы, подключаемые к телефонной линии и предоставляющие возможность прослушивать телефонные разговоры с помощью АМ или ЧМ-радиоприемников. В зависимости от типа используемой модуляции эти радиоретрансляторы разделяются на АМ- и ЧМ-ретрансляторы.

2.1 Схема Телефонного АМ-ретранслятора

Телефонный АМ-ретранслятор с кварцевым резонатором обеспечивает прослушивание телефонных разговоров на радиоприемник, работающий в диапазоне частот 27 – 28 Мгц с амплитудной модуляцией. Принципиальная схема этого телефонного ретранслятора представлена на рисунке 2.1.

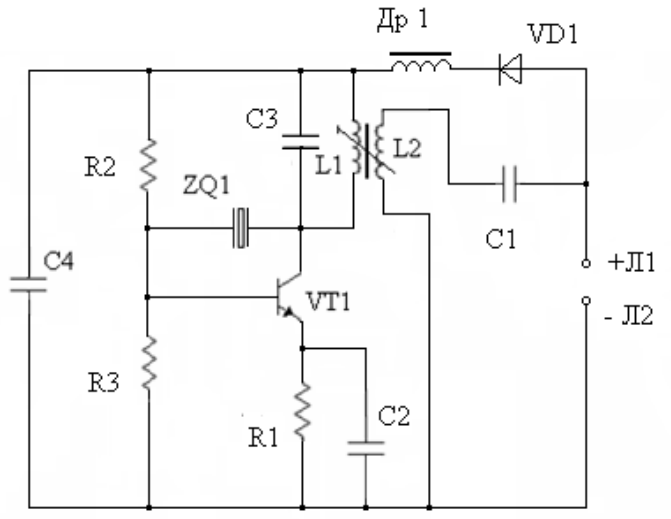


Рисунок 2.1. Схема однотранзисторного устройства - телефонного АМ-ретранслятора с кварцевым резонатором.

Данный телефонный ретранслятор пр. собой маломощный однокаскадный передатчик с амплитудной модуляцией и кварцевой стабилизацией несущей частоты.

Задающий генератор выполнен по традиционной схеме на транзисторе VT1. Режим работы транзистора по постоянному току задается подбором сопротивлений резисторов R2 и R3. Кварцевый резонатор ZQ1 включен между коллектором и базой транзистора VT1. Колебательный контур, состоящий из катушки связи L2 и конденсатора C3, настроен на частоту кварцевого резонатора. С катушки связи L1 сигнал поступает в антенну, в качестве которой используются телефонные провода. Дроссель Др1 служит для разделения высокочастотного и низкочастотного сигналов. Диод VD1 предохраняет устройство от выхода из строя в случае неправильного подключения.

Передатчик подключается параллельно телефонной трубке. Когда трубка положена на рычаг, разговорный узел отключен от линии. Подключена к линии в этот момент только цепь вызывного устройства. Таким образом, до тех пор пока трубка не снята, напряжение питания на передатчик не поступает. Как только трубку снимают, к линии подключается разговорная часть. Во время разговора ток через разговорную часть меняется синхронно с речью, соответственно изменяется и напряжение в точках +Л1 и –Л2. Изменение напряжения питания приводит к соответствующему изменению амплитуды генерируемых высокочастотных колебаний, то есть имеет место амплитудная модуляция высокочастотного колебания. В результате разговор может слушать на расстоянии до 50 м на приемник, работающий в диапазоне частот 27 – 28 МГц на прием АМ сигнала. Настройка устройства осуществляется путем настройки колебательного контура L2 и C3 на несущую частоту. При подключении следует учитывать полярность напряжения линии.

2.2 Схема телефонного ретранслятора УКВ диапазона с ЧМ

Телефонный ретранслятор УКВ диапазона с ЧМ . Данный телефонный ретранслятор имеет сходство с предыдущим ретранслятором по способу подсоединения к телефонной линии. Устройство представляет собой маломощный передатчик, работающий в диапазоне УКВ ЧМ с использованием частотной модуляции.

Дальность действия передатчика около 100 м. Особенность схемы состоит в том, что передатчик, на транзисторе VT1, питается от телефонной линии, используя её в качестве антенны, а частотная модуляция

осуществляется путем изменения ёмкостей переходов этого транзистора при изменении питающего напряжения.

Простейшими устройствами обнаружения наличия подслушивающих устройств и несанкционированного подключения в телефонных линиях являются индикаторы состояния телефонных линий.

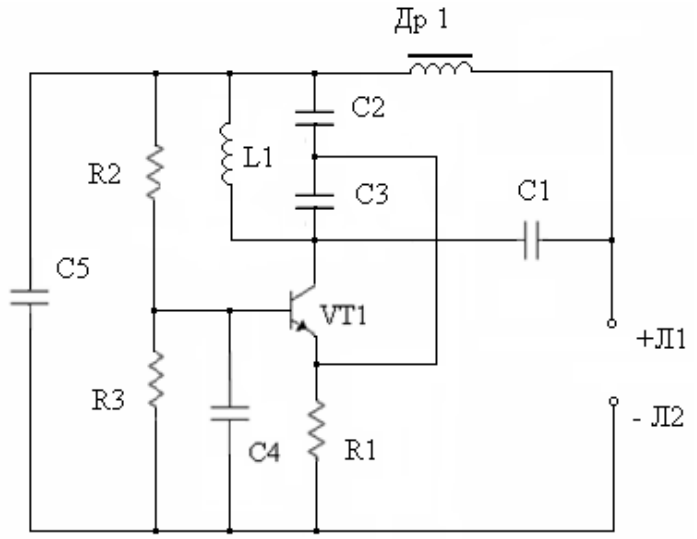


Рисунок 2.2. Принципиальная схема телефонного ретранслятора с ЧМ.

Задающий генератор выполнен на транзисторе VT1 по схеме с общей базой. Напряжение обратной связи поступает на его эмиттер с делителя, состоящего из конденсаторов С2 и С3. Частоту задающего генератора определяют конденсаторы С2 и С3, катушка L1 и межэлектродные ёмкости транзистора VT1. С коллектора транзистора VT1 сигнал через конденсатор С1 поступает в линию, провод которой используется в качестве антенны. Дроссель Др1 служит для разделения ВЧ и НЧ составляющих сигналов.

Подключение данного устройства к линии аналогично подключению устройства, рассмотренного выше в данном разделе. Настройка передатчика заключается в подборе сопротивления резисторов R2 и R3 для получения максимального излучения. Колебательный контур передатчика настраивают растяжением или сжатием витков катушки L1 на свободный участок УКВ ЧМ диапазона. Мощность (и дальность) телефонных УКВ ЧМ-ретрансляторов может быть увеличена за счет введения в схему дополнительных ВЧ-каскадов - усилителей мощности.

Рассмотрим устройство – индикатор, который позволяет обнаруживать нелегальное подключение подслушивающих устройств. Данное устройство является простейшим индикатором наличия подслушивающих устройств. Оно устанавливается на предварительно проверенной телефонной линии. Питание осуществляется от телефонной линии. При наличии любых несанкционированных подключений различных устройств, питающихся от телефонной линии, выдается сигнал тревоги (включается красный
светодиод). Схема такого устройства приведена на рисунке2.3.

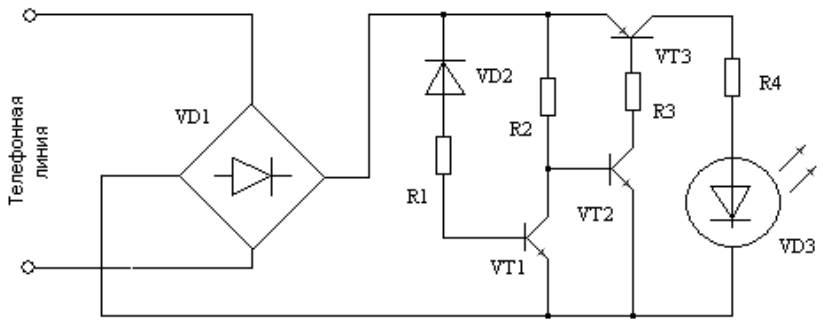


Рисунок 2.3. Простейший индикатор состояния телефонной линии.

К выходу усилителя через ограничительный резистор R_4 подключен светодиод VD_3 типа АЛ307. Выпрямительный мост VD_1 типа КЦ407 обеспечивает требуемую полярность питания устройства независимо от подключения его к телефонной сети. При свободной линии постоянное напряжение в ней около 60 В. Стабилитрон VD_2 открывается, и в базу транзистора VT_1 подается через ограничительный резистор R_1 управляющий ток. Открытый и насыщенный транзистор VT_1 шунтирует вход каскада на транзисторе VT_2, поэтому усилитель тока закрыт и светодиод VD_3 погашен. При подключении в линию посторонних устройств напряжение в линии падает и ток, протекающий через стабилитрон VD_2, уменьшается (вплоть до закрытия последнего). Транзистор VT_1 закрывается, а в базу транзистора VT_2 через резистор R_2 подается управляющий ток. Усилитель открывается и светодиод VD_3 включается.

Рассмотрим схему и принцип работы индикатора состояния телефонной линии (анализатора телефонных линий). Принципиальная схема индикатора приведена на рисунке 2.4. Индикатор устанавливается в корпус телефонного аппарата и питается от телефонной линии. Он индицирует любое несанкционированное подключение к линии в момент ведения разговора, т. е. когда трубка снята с рычага телефона. Основу схемы составляет операционный усилитель DA1 типа КР1407 УД2, включенный по схеме компаратора напряжений. При снятии телефонной трубки напряжение с линии подается на рассматриваемое устройство через диод VD4 типа КД522, образующий со стабилитроном VD3 типа КС156 параметрический стабилизатор напряжения. Одновременно напряжение поступает через резистор R1 на не инвертирующий вход компаратора DA1. На инвертирующий вход последнего подается опорное напряжение, снимаемое с движка подстроичного резистора R3.

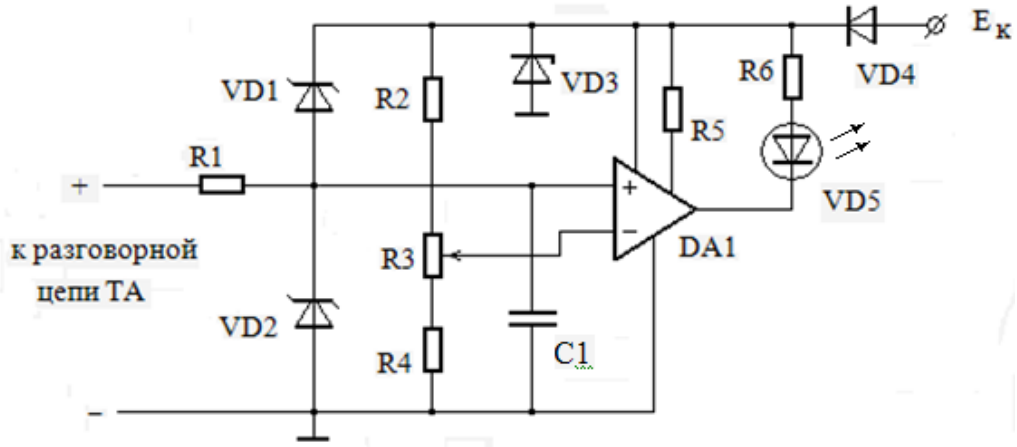


Рисунок 2.4. Анализатор состояния телефонных линий

При снижении входного напряжения до уровня, меньшего чем опорное напряжение, на выходе компаратора DA1 появляется уровень логического нуля, что вызывает включение светодиода VD5 типа АЛЗО7. Диоды VD1 и VU2 совместно с резистором R1 ограничивают напряжение на не инвертирующем входе DA1 на уровнях, выходящих за пределы питающих напряжений - не более, чем на 0,7 В (на величину прямого падения напряжения на диодах VD1, VD2). Конденсатор С1 защищает схему от высокочастотных наводок в линии. Резистор R5 устанавливает режим работы микросхемы DA1. В устройстве использованы резисторы типа МЛТ-О,125 . Диоды VD1, VD2, VD4 - любые кремниевые. Стабилитрон VD3 - любой на напряжение стабилизации 4,7-7,0 В. Микросхему DA1 можно заменить на КР140 УД1208, а также на любой операционный усилитель с током потребления не более 5 мА.

3. Скремблирование

Скремблер - это устройство, которое шифрует речь, передаваемую по каналам связи. Речь идет не о криптографии, используемой в сотовых сетях, а о надежной защите. Скремблер подключается напрямую к телефону и не работает при его выключении. Но стоит владельцу устройства включить его, так как он сразу начинает принимать сигналы, поступающие с микрофона, шифровать их и затем отправлять. Расшифровка речи происходит в обратном порядке. Сигналы от антенны поступают на скремблер, а оттуда на динамик.

Мерой по предотвращению прослушивания телефонных разговоров считается внедрение криптографических методов защиты информации. В настоящее время для защиты телефонных сообщений используются два метода: преобразование аналоговых речевых характеристик и цифровое шифрование. Устройства, использующие эти методы, называются скремблерами. При аналоговом скремблировании описание исходного аудио сигнала изменяется, так что результирующий сигнал становится неразборчивым, но занимает ту же частоту. Это дает еще одну возможность без проблем передавать его по обычным каналам связи. При использовании этого метода сигнал может подвергаться следующим преобразованиям: инверсия частоты; перестановка; временное перемещение. Во втором способе закрытия передаваемого сообщения непрерывный аналоговый сигнал преобразуется в цифровую форму. Впоследствии шифрование сигнала происходит, как правило, с помощью сложного оборудования, часто с использованием персональных компьютеров. Ниже приведено описание скремблера с использованием метода инверсии частоты. Этот метод давно и успешно используется зарубежными государственными службами и гарантирует достойную защиту радио и телефонных разговоров от несанкционированного прослушивания Частотно-инвертированный сигнал выделяется из нижней боковой полосы диапазона преобразования сбалансированного звукового сигнала выше звукового носителя. Два последовательных обращения восстанавливают исходный сигнал. Устройство работает как кодер и декодер одновременно.

Синхронизации двух скремблеров не требуется. Схема такого скремблера приведена на рис.8.

Это прибор состоит из таких элементов:

— тактового генератора на микросхеме DD2 типа К561ЛА7, вырабатывающего сигнал частотой 7 кГц;

— делителя-формирователя несущей 3,5 кГц на микросхеме DD3.1 типа К561ТМ2;

— аналогового коммутатора;

— балансного модулятора на микросхеме DD4 типа К561КТ3;

— входного полосового фильтра с полосой пропускания 300—3000 Гц на микросхеме DA1.1 типа К574УД2;

— сумматора балансного модулятора с фильтром низкой частоты на микросхеме DA1.2.

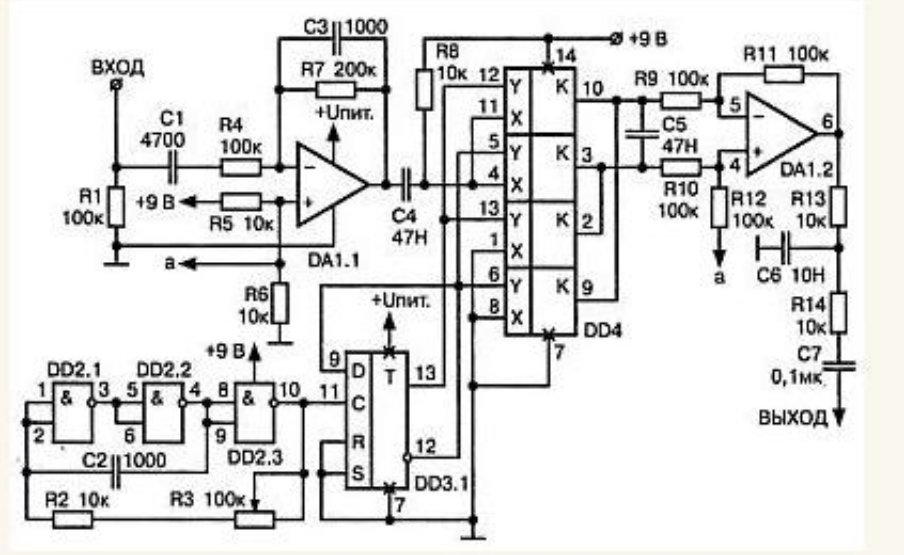


Рисунок 3.1. Схема Скремблера

Регулировка частоты синхроимпульсов и, следовательно, несущей частоты, производится многооборотным резистором R3. В диапазоне частот 300-3000 Гц разборчивость речи после двух преобразований составляет не менее 65%.

Методы маскировки речи

Источник. При защите телефонных разговоров на уровне энергии электронные устройства перехвата информации подавляются с использованием активных методов и средств.

К основным методам относятся:

— «синфазной» низкочастотной маскирующей помехи;

— высокочастотной маскирующей помехи;

— «ультразвуковой» маскирующей помехи;

— низкочастотной маскирующей помехи;

— повышения напряжения;

— понижения напряжения;

— компенсационный;

— «выжигания».

Метод «синфазной» маскирующей низкочастотной помехи

Способ заключается в отправке во время вызова на каждый провод телефонной линии скачка и фазы, скоординированных относительно нейтрального провода электрической сети 220 В, маскирующего мешающие сигналы спектра речевой частоты (маскирующего низкочастотный шум).

Из-за согласования амплитуды и фазы в телефонной системе, подключенной параллельно с телефонной линией, эти мешающие сигналы

компенсируют друг друга и не ухудшают требуемый сигнал, то есть не ухудшают качество связи.

В любых устройствах, подключенных к одному телефонному проводу, мешающий сигнал не компенсируется и «накладывается» на полезный сигнал. А поскольку его уровень значительно превышает полезный сигнал, перехват передаваемой информации становится невозможным. В качестве маскирующего помехового сигнала, как правило, используются дискретные сигналы (псевдослучайные последовательности М-импульсов) в диапазоне частот от 100 до 10000 Гц. Метод высокочастотных маскирующих помех заключается в подаче маскирующего помехового сигнала в высокочастотный диапазон звукового диапазона (маскирующий высокочастотный шум) во время вызова на телефонную линию. Частоты маскирующих помеховых сигналов выбираются таким образом, чтобы после прохождения низкочастотного усилителя или селективных цепей модулятора закладок телефона их уровень был достаточным для подавления полезного сигнала (речевого сигнала в телефонной линии), но в то же время чтобы они не ухудшали качество связи. В качестве маскирующего шума используются широкополосные аналоговые сигналы типа «белый шум» или дискретные сигналы псевдослучайной последовательности импульсов с шириной спектра не менее 3-4 кГц. Этот метод будет использоваться для подавления буквально всех типов электронных устройств для сбора речевой информации, которые подключены к телефонной линии как последовательно, так и параллельно.

Однако эффективность подавления захвата информации при последовательном подключении к линии (особенно с помощью индукционных датчиков) значительно ниже, чем при использовании метода «синфазного» маскирования низкочастотных помех.

Метод «ультразвуковой» маскировки шума в основном аналогичен рассмотренному выше. Разница заключается в том, что частота мешающего сигнала находится в диапазоне от 20-30 кГц до 50-100 кГц, что значительно упрощает схему подавляющего устройства, но в то же время эффективность этого метода ухудшается по сравнению с методом высокочастотной маскировки шума.

Метод низкочастотной маскировки помех. При применении этого метода маскирующий низкочастотный шумовой сигнал подается на линию, когда телефонная линия размещена. Этот метод используется для включения записи диктофонов, подключенных к телефонной линии, с использованием адаптеров или индукционных датчиков, что приводит к заполнению памяти в режиме записи шума, то есть при отсутствии полезного сигнала.

Метод увеличения напряжения заключается в повышении напряжения в телефонной линии во время разговора и используется для снижения качества использования телефонных закладок путем переключения их передатчиков в нелинейный режим. Увеличение напряжения в линии до 25–

35 В приводит к появлению телефонных закладок с последовательным подключением и параметрической стабилизации частоты передатчика, потере несущей частоты и ухудшению разборчивости речи. В телефонных закладках с последовательным соединением и кварцевой стабилизацией частоты передатчика наблюдается уменьшение отношения сигнал / шум на 3-10 дБ. Передатчики телефонных закладок с параллельным подключением к линии при таких напряжениях в некоторых случаях просто отключаются. Способ понижения напряжения предусматривает подачу питания во время разговора по линии постоянного напряжения, соответствующего напряжению в линии при поднятой трубке, но обратной полярности. Этот метод используется для нарушения работы всех типов электронных устройств перехвата с контактным (как последовательно, так и параллельно) подключением к линии, используя его в качестве источника питания.

Способы, рассмотренные выше, обеспечивают подавление устройств поиска информации, подключенных к линии только от защищенного телефона к УАТС. Для защиты телефонных линий используются устройства, которые одновременно реализуют несколько методов подавления. Метод компенсации используется для краткой маскировки голосовых сообщений, передаваемых абонентом по телефонной линии. Этот метод обладает высокой эффективностью подавления всех способов незаконного удаления данных, подключенных к линии, по всей телефонной линии от одного абонента к другому. Суть метода заключается в следующем: перед началом передачи скрытого сообщения генератор шума включается на принимающей стороне по команде пользователя. Он подает в телефонную линию маскирующие шумовые помехи речевого диапазона частот, которые в линии смешиваются с передаваемым сообщением. В то же время один и тот же шумовой сигнал подается на один из входов двухканального адаптивного фильтра. На другой вход этого фильтра поступает аддитивная смесь принятого речевого сигнала и маскирующего шума. Аддитивный фильтр компенсирует шумовую составляющую и излучает скрытый речевой сигнал. Наличие таких устройств защиты для обоих абонентов позволяет организовать полудуплексный закрытый канал связи.

Метод «выгорания» реализуется путем подачи высоковольтных (более 1500 В) импульсов на линию мощностью 15–50 ВА. Это приводит к электрическому «выгоранию» входных каскадов электронных устройств перехвата информации и их блоков питания, которые гальванически связаны с телефонной линией . Импульсы высокого напряжения подаются, когда телефон отключен от линии. В то же время, для разрушения параллельно соединенных устройств, импульсы высокого напряжения подаются, когда устройства разомкнуты, и последовательно соединенные, когда телефонная линия «замкнута» (обычно в телефонной будке или коммутаторе).

Скремблирование – это шифрация потока данных, в результате которой он выглядит как поток случайных битов. Последовательности битов в исходном массиве данных, как регулярные, так и нерегулярные, обратимо разрушаются, так что вероятности появления логической единицы и логического нуля в каждой последующей битовой позиции потока одинаковы и не зависят от предыстории. Применительно к телекоммуникационным системам скремблирование повышает надежность синхронизации устройств, подключенных к противоположным сторонам линии связи и уменьшает уровень помех, изучаемых на соседние линии многожильного кабеля. Есть и иная область применения скремблеров – защита передаваемой информации от несанкционированного доступа. В данной работе приведены схемы классических и модернизированных скремблеров и дескремблеров, описаны преимущества, связанные с их применением, рассмотрены меры защиты систем передачи скремблированных данных от злонамеренного пользователя.

3.1 Генераторы псевдослучайных битовых последовательностей

Скремблеры и дескремблеры (шифраторы и дешифраторы особого класса) обычно построены на основе генераторов псевдослучайных последовательностей битов. Генераторы чаще всего выполняются с использованием M-разрядных сдвиговых регистров RG с цепями обратной связи (рисунок 3.2 и 3.3).

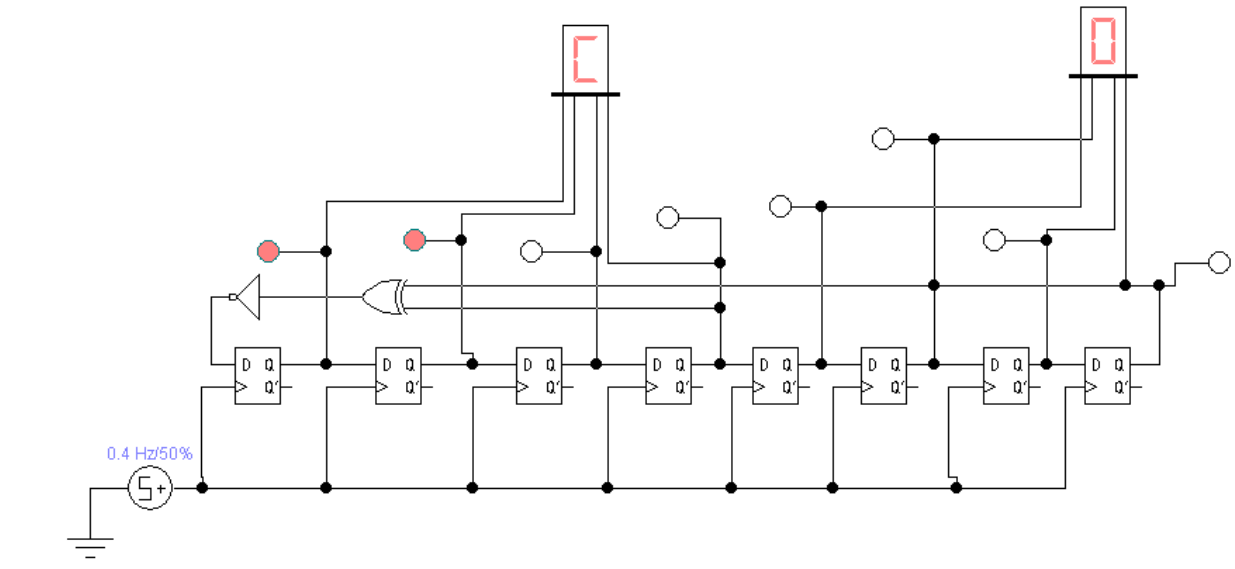


Рисунок 3.2. Генератор псевдослучайных битовых последовательностей (последовательность 2^M-1 бит)

В общем случае при использовании M-разрядного регистра цепь обратной связи подключаются к разрядам с номерами M и N (M > N). Для того чтобы на выходе генератора формировалась псевдослучайная последовательность битов с периодом повторения, равным 2^M-1, следует выбирать точки подключения цепи обратной связи в соответствии с таблицей.

В полном цикле (2^M-1 тактов) число логических единиц, формируемых на выходе генератора, на единицу больше, чем число логического нуля. Добавочная логическая единица появляется за счет исключения состояния, при котором в регистре присутствовал бы нулевой код. Это можно интерпретировать так, что вероятности появления логического нуля и логической единицы на выходе генератора практически одинаковы.

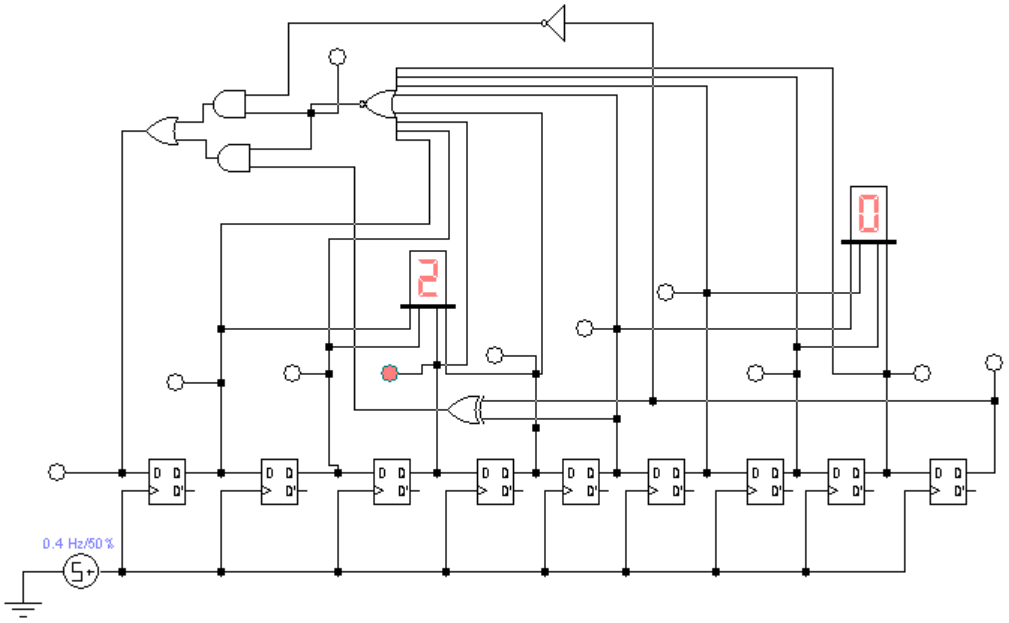


Рисунок 3.3. Генератор псевдослучайных битовых последовательностей (последовательность 2^M бит)

M	3	4	6	7	9	10	11	15	17	18	20	21	22	23	25	28	29	31	35
N	2	3	3	5	6	7	9	14	14	11	17	19	21	18	22	25	27	28	20

Рисунок 3.4. Таблица для выбора промежуточной точки N подключения цепи обратной связи

Приведенные схемы различаются длинами периодов генерируемых последовательностей битов. В схеме, показанной на рисунке 3.2, регистр

RG исходно установлен в некоторое ненулевое состояние (цепь начальной установки не показана). Под действием положительных фронтов синхросигнала CLK хранимый в регистре код непрерывно циркулирует в нем и одновременно видоизменяется благодаря преобразованию битов логическим элементом Исключающее ИЛИ (XOR). Генерируемая последовательность битов снимается с выхода любого разряда регистра. Направление сдвига данных в регистре показано стрелкой. В полном цикле работы генератора в регистре однократно формируется все возможные M-разрядные коды, за исключением нулевого. Циклы следуют один за другим без пауз.

Приведенной на рисунке 3.4 таблица, которая описывает ряд генераторов различной разрядности.

Псевдослучайная последовательность битов с периодом повторения, равным 2^m-1, обладает следующими свойствами.

В полном цикле (2^M-1 тактов) половина серий из последовательных логической единицы имеет длину 1, одна четвёртая серий - длину 2, одна восьмая- длину 3 и так далее. Такими же свойствами обладают и серий из логической единицы с учетом пропущенного логического нуля. Это говорит о том, что вероятности появления «орлов» и «решек» не зависят от исходов предыдущих «подбрасываний». Поэтому вероятность того, что серия из последовательных логической единицы или логического нуля закончится при следующем подбрасывании, равна S.

Если последовательность полного цикла (2^M-1 тактов) сравнивать с этой же последовательностью, но циклически сдвинутой на любое число тактов W(W не является нулем или числом, кратным 2^M -1), то число несовпадений будет на единицу больше, чем число совпадений.

Улучшенная схема (рисунок 3.3) формирует псевдослучайную последовательность битов с периодом повторения, равным 2^M. К этой схеме также применима таблица, приведенная на рисунке 3.4. В регистре в определенном порядке формируется все возможные коды, включая нулевой. Схема дополнительно содержит элемент ИЛИ-НЕ, инвертор и мультиплексор. Сигнал Z на выходе элемента ИЛИ-НЕ задает направление передачи данных через мультиплексор. При Z = 0 на выход мультиплексора транслируется сигнал с выхода элемента Исключающее ИЛИ, а при Z=1 – сигнал с выхода инвертора.

До тех пор пока на входах элемента ИЛИ-НЕ присутствует хотя бы одна логическая единица, на его выходе сформирован сигнал Z = 0. В этом случае мультиплексор в каждом такте передает в освободившийся (нижний) разряд сдвигового регистра бит с выхода элемента Исключающее ИЛИ так же, как и в схеме, показанной на рисунке 3.2.

В некотором такте i в регистре фиксируется код, содержащий единственную логическую единицу, размещенную в разряде M – 1. Так как в разрядах M и N присутствуют логическая ноль, то на выходе элемента исключающее ИЛИ сформирован сигнал логического нуля, который к началу такта i+1 поступает на вход регистра. В начале такта i+1 логическая

единица перемещается из разряда М – 1 в разряд М, на входах элемента ИЛИ – НЕ формируется нулевой код. Сигнал Z= 1 переводит мультиплексор в состояние, при котором на вход нижнего разряда сдвигового регистра поступает бит с выхода инвертора. В данном случае этот бит равен нуля, поэтому в такте i + 2 в регистре фиксируется нулевой код.

К началу такта i + 3 на вход сдвигового регистра с выхода инвертора поступает логическая единица, поэтому по положительному фронту синхросигнала CLK в регистре фиксируется код, содержащий логическую ноль во всех разрядах, кроме первого. Сигнал Z вновь принимает нулевое значение, мультиплексор переключается в состояние передачи сигнала с выхода элемента Исключающее ИЛИ и так далее. Таким образом, регистр проходит через все состояния, включая нулевое. Возможны и иные варианты построения генераторов с числом состояний, равным 2^M .

3.2 Скремблеры и дескремблеры (шифраторы и дешифраторы особого класса

Наиболее распространены два вида систем «скремблер - дескремблер»: с неизолированными и изолированными (от линии связи) генераторами псевдослучайных последовательностей битов (рисунок 3.5).

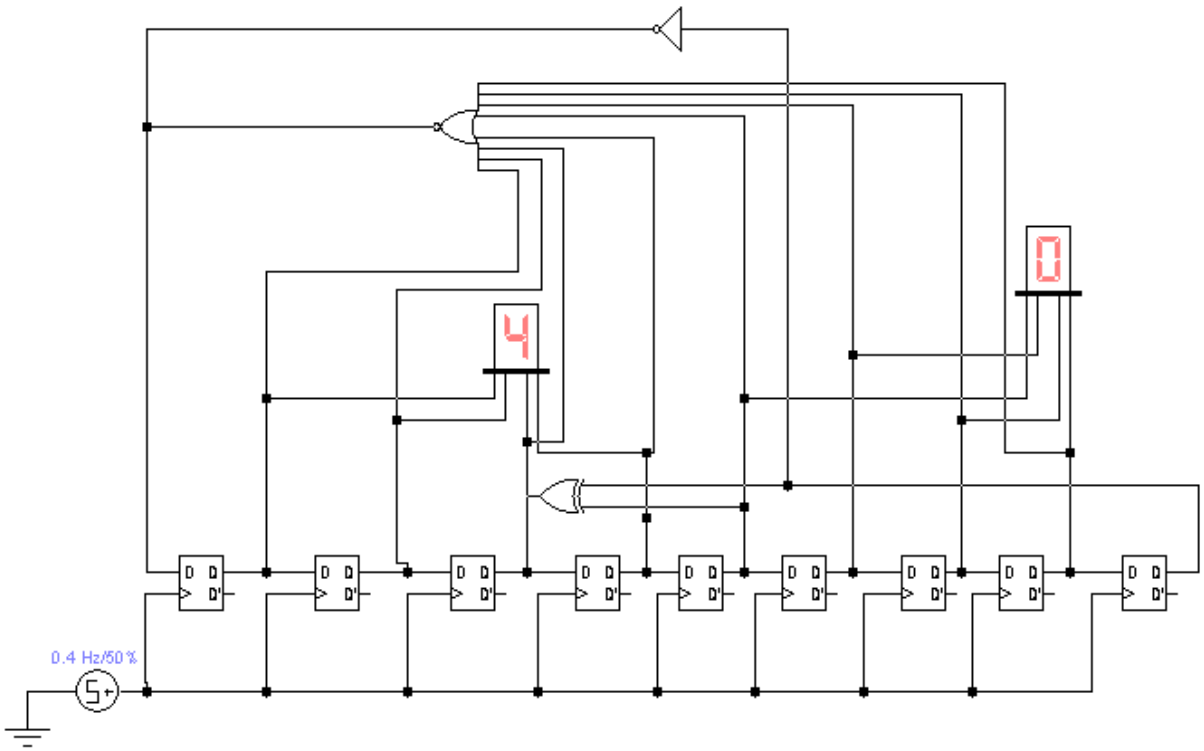


Рисунок 3.5. Система «скремблер - дескремблер» с генераторами псевдослучайных последовательностей битов.

В системе, показанной на рисунке 3.5, скремблер и дескремблер содержат фрагменты рассмотренного ранее генератора (рисунок 3.2) псевдослучайных последовательностей битов. В скремблере цепь обратной связи генератора на основе сдвигового регистра 1 дополнительно содержит элемент Исключающее ИЛИ. В дескремблере применен аналогичный генератор на основе сдвигового регистра 2 с разомкнутой цепью обратной связи.

Все процессы, протекающие в системе, синхронизируется от тактового генератора, размещенного в источнике данных (возможно также его размещение в скремблере). Тактовый генератор формирует сигнал CLK – непрерывную последовательность тактовых импульсов со скважностью, равной двум. В каждом такте по положительному фронту сигнала CLK на вход скремблера подается «новый» бит передаваемых данных, а код в его сдвиговом регистре 1 продвигается на один разряд вправо, причем в этот же момент в освободившийся разряд заносится «старый» бит данных, просуммированный по модулю два со «старым» битом с выхода элемента ИЛИ.

Строго говоря, на границах между битовыми интервалами на выходе элемента ИЛИ могут формироваться короткие ложные импульсы в результате неодновременного формирования «новых» сигналов на его входах. Для устранения ложных импульсов можно ввести в цепь сигнала SCRD D-триггер, синхронизируемый отрицательным фронтом сигнала CLK (триггер на рисунке не показан). Короткими ложными импульсами пока пренебрегаем для упрощения изложения основных идей построения систем «скремблер - дескремблер».

Если источник данных посылает в скремблер длинную последовательность сигналов логического нуля (DATA=0), то элемент XOR2 можно рассматривать как повторитель сигнала Y1. Тогда регистр 1 фактически оказывается замкнутым в кольцо и генерирует точно такую же псевдослучайную последовательность битов, как и в рассмотренной ранее схеме генератора, приведенной на рисунке 3.2. Отметим, что в этой ситуации при неблагоприятном стечении обстоятельств есть опасность потери работоспособности скремблера, если в регистре 1 к началу передачи последовательности сигналов логического нуля зафиксирован нулевой код.

Если от источника данных поступает произвольная битовая последовательность, то она взаимодействует с последовательностью битов с выхода элемента XOR1. В результате формируется новая (скремблированная) последовательность битов данных SCRD, по структуре близкая случайной. Эта последовательность, в свою очередь, продвигается по регистру 1, формирует поток битов Y1 на выходе элемента ИЛИ и так далее.

Скремблированная последовательность битов SCRD проходит через передающий усилитель и по линии связи поступает в дескремблер , где проходит через приемный усилитель. Линия связи может быть выполнена, например, в виде витой пары проводов многожильного кабеля городской

телефонной сети. С помощью генератора PLL (Phase Locked Loop) с фазовой автоподстройкой частоты из входного сигнала SCRD* выделяется тактовый сигнал CLK*, который передается на синхронизирующие входы регистра 2 и приемника данных.

Генератор PLL с фазовой автоподстройкой частоты может быть построен по одной из известных схем. Он предназначен для формирования высокостабильного синхросигнала CLK* но основе непрерывного слежения за входным сигналом SCRD*. В данном случае отрицательный фронт сигнала CLK* привязан к моментам изменения сигнала SCRD* (0 – 1 или 1 - 0), так что положительный фронт сигнала CLK* формируется в середине битового интервала сигнала SCRD*, что соответствует его установившемуся значению. Сдвиг данных в регистре 2 и прием очередного бита SCRD* в его освободившийся в разряд происходят по положительному фронту сигнала CLK*. Дескремблированные данные DATA* поступают в приемник данных и фиксируется в нем по положительным фронтам сигнала CLK*. Благодаря достаточной инерционности генератора PLL сигнал CLK* практически нечувствителен к «дрожанию фазы» сигнала SCRD* и иным его кратковременным искажениям вызванным помехами в линии связи.

Потоки данных DATA и DATA* совпадают с точностью до задержки передачи. Действительно в установившемся режиме в сдвиговых регистрах 1 и 2 присутствуют одинаковые коды, так как на входы D этих регистров поданы одни и те же данные SCRD = SCRD* (с учетом задержки передачи), а тактовая частота одна и та же. Поэтому Y2 = Y1 и с учетом этого

$$DATA^* = SCRD^* \oplus Y2 = SCRD \oplus Y2 = (DATA \oplus Y1) \oplus Y2 =$$
$$= DATA \oplus Y1 \oplus Y1 = DATA \oplus 0 = DATA.$$

Единственное преимущество данного способа скремблирования является то что, синхронизация достигается автоматически после заполнения регистров одинаковыми данными.

К сожалению, есть и существенные недостатки. О первом из них уже всклюзь упоминалось – это плохая устойчивость по отношению к некоторыми неблагоприятным кодовым ситуациям, которые могут возникнуть как при нормальной работе системы, так и в результате злого умысла пользователя.

Второй недостаток состоит в размножении ошибок. При появлении одиночной ошибки в линии связи идентичность содержимого регистров 1 и 2 временно нарушается, но затем автоматически восстанавливается, как только правильные данные вновь заполнят регистр 2. Однако в процессе продвижения ошибочного бита по сдвиговому регистру 2, а именно, в периоды его попадания сначала на один, а затем на другой вход элемента ИЛИ сигнал Y2 дважды принимает неправильное значение. Это приводит к размножению одиночной ошибки – она впервые появляется в сигнале DATA* в момент поступления из линии и затем возникает еще два раза при последующем двукратном искажении сигнала Y2.

Генерация случайных чисел имеет широкое применение — от игр (например, «Тетрис») до криптографии (криптографические протоколы, генерация сеансовых ключей). В пример можно привести шифр блокнота: система с таким шифром абсолютно надёжна, пока собеседники используют ключ один раз. Чем дольше он используется, тем менее надёжным он становится. Вместо того, чтобы использовать общий секретный ключ, которые знают оба собеседника, можно генерировать с его помощью «сеансовый» ключ и периодически его менять. Чтобы сгенерировать надёжный сеансовый ключ, который злоумышленник не может предсказать, нужен генератор случайных чисел. Генератор случайных чисел — это алгоритм (или физический процесс), который воспроизводит случайные числа. Этот процесс стараются сделать качественным, быстрым и дешёвым. Под качеством понимают способность алгоритма генерировать случайные числа с одинаковой вероятностью. Можно сказать, что если генератор случайных чисел является источником случайной величины X, то энтропия этой случайной величины должна быть максимальна, а это возможно, только если значения каждого события равновероятны. Выполнение требования по скорости означает, что в секунду выдается достаточное количество событий, чтобы зашифровать нужный поток данных. Например, если речь идёт о шифровании гигабита данных в секунду, то генератор случайных чисел должен давать миллиарды случайных событий в секунду. Никакая механическая машина, подбрасывающая монеты и записывающая результаты, не подходит для такой цели. Можно предложить другие способы генерации истинно случайных событий. Например, в качестве случайного процесса можно взять шум, записываемый со входа микрофона. Тепловой шум тоже можно рассматривать как случайный процесс. Но эти процессы дают слишком малое количество данных. Если же попробовать использовать радиоактивный распад, то это даст порядка десяти событий в секунду (если использовать миллионы, то находиться рядом с таким генератором будет опасно). Также для вышеперечисленных способов не будет выполняться правило дешевизны. В настоящее время для целей криптографии пока что нет дешёвого, быстрого и качественного генератора. Поэтому приходится использовать так называемые псевдослучайные генераторы (генераторы псевдослучайной последовательности). Они отличаются от генератора случайной последовательности тем, что являются алгоритмом, то есть можно записать математический закон получения следующего случайного числа на основании предыдущего случайного числа и некоторого состояния вычислительного комплекса. Все существующие алгоритмы генерации псевдослучайных последовательностей можно реализовать на машине Тьюринга, то есть это полноценные алгоритмы. Они детерминированы, то есть ничего случайного в этих алгоритмах нет. Тем не менее выход этих алгоритмов обладает свойствами случайной последовательности:

1. Примерное совпадение количества сгенерированных чисел разных типов (нулей и единиц).

2. Наличие конечного числа состояний. Любой алгоритм использует определенный набор памяти. В этом объёме памяти находится его состояние. Количество состояний конечно, потому что объём используемой памяти конечен. Если он будет бесконечен, то это будет плохой алгоритм, потому что его нельзя будет использовать в постоянном режиме.

3. Наличие периода, что следует из принципа ящиков Дирихле, суть которого состоит в следующем: если имеется набор из 9-ти ящиков, и там сидят 10 кроликов, то хотя бы в одном ящике сидят 2 кролика. Значит, если внутреннее состояние состоит из 20-ти бит, то в это внутреннее состояние можно поместить максимум 2^{20} бит.

2. Линейный конгруэтный генератор

Это генератор, который описывается следующей формулой:

$$X_{n+1}=(aX_n+b) \bmod m_1,$$

где, X_n — состояние генератора. При этом в качестве выхода генератора можно использовать как число X, так и какой-то набор битов этого числа. Оказывается, что это довольно хороший со статистической точки зрения генератор. Этот генератор используется в большом количестве приложений. Период этого генератора можно сделать максимальным, а именно $2^m - 1$. Для этого необходимо выполнить следующие правила:

1. Число b должно быть взаимно простым с m.

2. Число a должно быть кратным всем простым делителям числа m.

3. $(a - 1)$ должно быть кратно четырём, если $(m - 1)$ кратно четырём.

В качестве числа m можно взять 2 в некоторой степени, например, 2^{32} или 2^{64}. И, таким образом, вообще избавиться от операции взятия по модулю. Вместо этого будет выполняться умножение с отбрасыванием переполнения и сложение с отбрасыванием переполнения.

Линейный конгруэтный генератор используется во многих языках программирования: как в старых, так и в недавних (например, Java, C/C++). Иногда используются генераторы с разными коэффициентами.

Этот генератор довольно хорош для целого спектра приложений, но не для криптографии. По четырём числам, т. е. по четырём выходам, этого генератора можно восстановить все коэффициенты: a, b и m.

3. Статистические свойства генераторов

Выше рассматривалось свойство алгоритмов генерировать числа с одинаковой вероятностью. Если брать в качестве выхода нули и единицы, то количество этих нулей и единиц должно быть примерно одинаково.

Есть и куда более сложные характеристики, например: будет ли хорошим генератор, указанный ниже?

0101010101…

Число нулей и единиц у него одинаково. Но очевидно, что никакой случайности данный генератор не несёт.

Заключение

Разработаны электрические схемы устройства защиты информации-индикатора состояния телефонной линии связи, который не только обнаруживает несанкционированное подключение к телефонной линии связи, но и также нейтрализует автоматическую запись телефонных переговоров.

Рассмотрены особенности построения и даны сравнительные характеристики наиболее распространенных схем автоколебательных и заторможенных генераторов прямоугольных импульсов, которые входят в состав схемы блокировки и нейтрализации автоматического записывающего устройства.

Список использованной литературы

1. Блинов А.М. Информационная безопасность: Учебное пособие. Часть 1. – СПб.: Изд-во СПбГУЭФ, 2010

2. Ланцов А. Л. и др. Цифровые устройства на комплементарных МДП интегральных микросхемах. Москва, Радио и связь, 2010.

3. Калниболотский Ю. М. И др. Расчет и конструирование микросхем. Киев, Высшая школа, 2009

4. СТ РК 34.026-2006. Защита информации. Термины и определения ГОСТ Р 50922-96 Защита информации. Основные термины и определения, MOD

5. Вынин С. А., Шустов Л. Н. Основы радиопротиводействия радиотехнической разведки. Москва, Советское радио, 2010.

6. Ярочник В. И.Технические каналы утечки информации, Москва, ИПКИР 2010

7. Киселев А. Е. Коммерческая безопасность. Москва, ИнфоАрт 2003. Рудаметов Е.А., Рудаметов Б.Е. Электроника и шпионские страсти. – СПб.: Пергамент, 2008.- 253с.

8. Балахничев И.Н., Дрик А.В.,Крупа А.И. Борьба с телефонным пиратством.- Минск: Омо “Наш город”, 2009.- 121с.

9. Транзисторы: Справочник/Под ред. Григорьева О.П. и др.- М.: Радио и связь, 2010.- 387с.

10. Аверченков В.И. Организационная защита информации: учеб. Пособие для вузов / В.И. Аверченков, М.Ю. Рытов. – Брянск: БГТУ, 2005

11. Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей. – М.: Горячая линия – Телеком, 2008

12. Оценка эффективности методов защиты речевой информации. Общесистемные вопросы защиты информации / под ред. Е. М. Сухарева. - М.: Радиотехника, 2003

13. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учебное пособие для вузов. – М: Издательский центр «Академия», - 2005

Приложение 1

Схема телефонной линии связи в общем виде представлена на рисунке 1.1, где показаны зоны возможного прослушивания телефонных переговоров. Зона1 является зоной телефонного аппарата (ТА). Зона 2 представляет собой двухпроводную линию (шлейф) от ТА, включая распределительную коробку. Зона 3, называемая кабельной (магистральной), включает участок телефонной линии связи от АТС до распределительной коробки. Остальные зоны: 4, 5 и 6 являются зонами АТС, многоканального кабеля и радиоканала, соответственно.

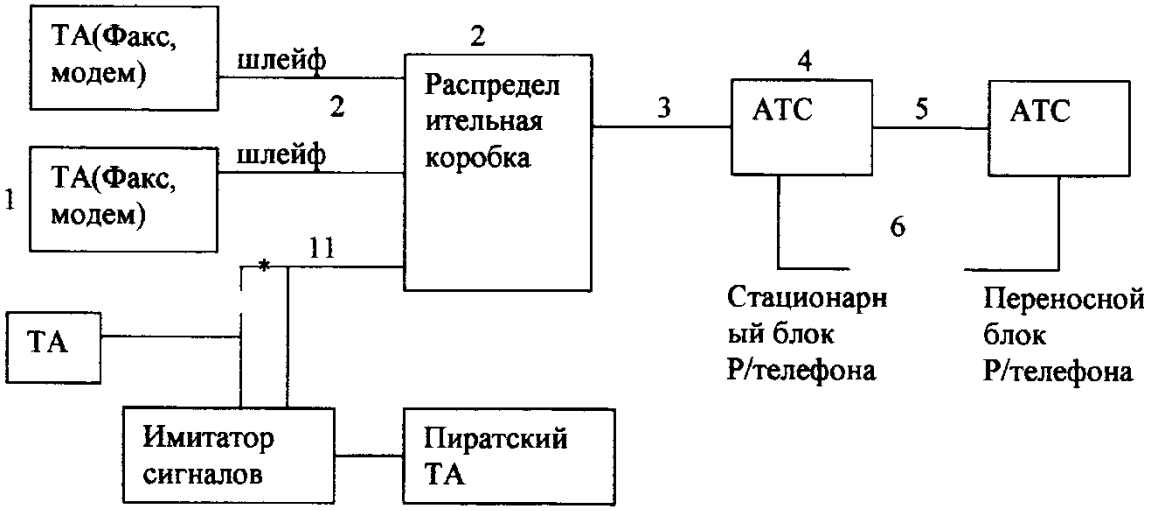


Рисунок 1.1. Схема телефонной линии связи

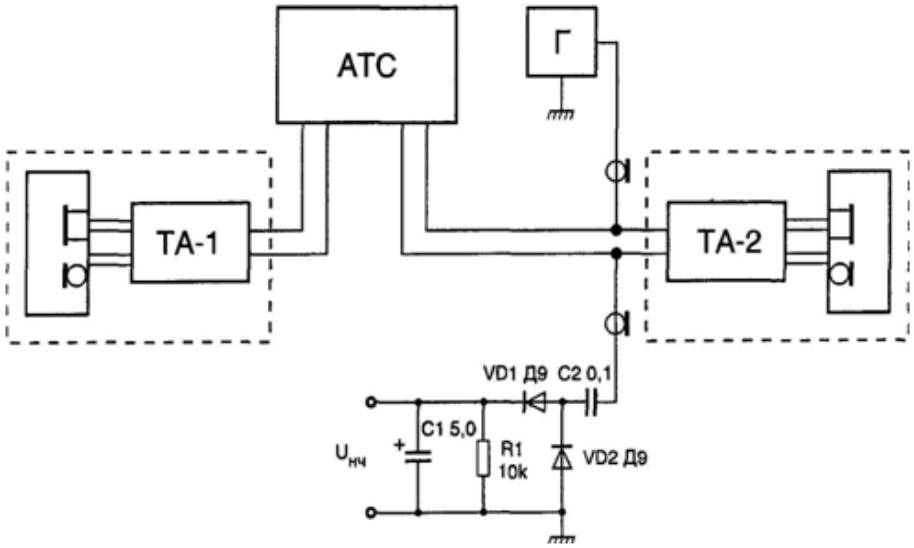
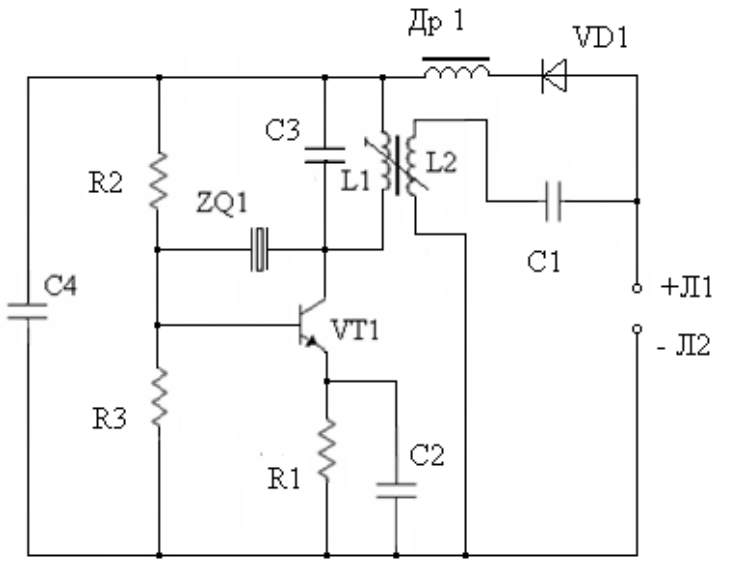


Рисунок 1.2. Прослушивание через микрофон телефонного аппарата

Этот способ состоит в следующем. На один из проводов телефонной линии, идущий от АТС к телефонному аппарату ТА-2, подаются колебания частотой 150 кГц и выше от генератора высокочастотных колебаний, Г. К другому проводу линии подключается амплитудный детектор с усилителем, выполненный на элементах Cl, C2, VD1, VD2 и R1. Корпус передатчика (генератор Г) и приемника (детектор) соединены между собой или с общей землей, например, с водопроводной трубой.

Высокочастотные колебания через элементы схемы телефонного аппарата ТА-2 поступают на микрофон и модулируются модулируются речью (акустическими сигналами) прослушиваемого помещения. Детектор приемника выделяет речевую информацию, которая усиливается до необходимого уровня и обрабатывается. Другими словами, модулированный высокочастотный сигнал демодулируется амплитудным детектором и после усиления прослушивается или записывается. Вследствие существенного затухания ВЧ сигнала в двухпроводной линии, дальность съема информации таким методом не превышает нескольких десятков метров.



Телефонный АМ-ретранслятор с кварцевым резонатором обеспечивает прослушивание телефонных разговоров на радиоприемник, работающий в диапазоне частот 27 – 28 Мгц с амплитудной модуляцией. Принципиальная схема этого телефонного ретранслятора представлена на рисунке 1. Данный телефонный ретранслятор пр. собой маломощный однокаскадный передатчик с амплитудной модуляцией и кварцевой стабилизацией несущей частоты. Телефонный ретранслятор УКВ диапазона с ЧМ (4). Данный телефонный ретранслятор имеет сходство с предыдущим ретранслятором по способу подсоединения к телефонной линии. Устройство представляет

собой маломощный передатчик, работающий в диапазоне УКВ ЧМ с использованием частотной модуляции.

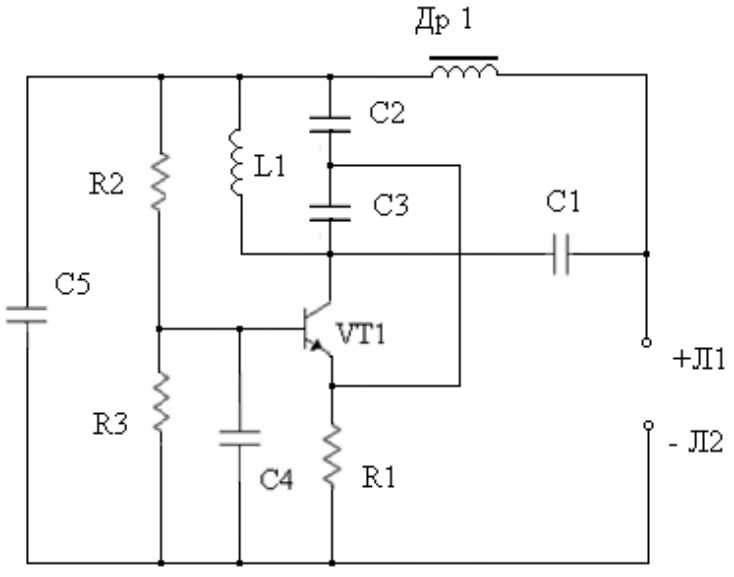


Рисунок 4. – Принципиальная схема телефонного ретранслятора с ЧМ.

Дальность действия передатчика около 100 м. Особенность схемы состоит в том, что передатчик, на транзисторе VT1, питается от телефонной линии, используя её в качестве антенны, а частотная модуляция осуществляется путем изменения ёмкостей переходов этого транзистора при изменении питающего напряжения.

Задающий генератор выполнен на транзисторе VT1 по схеме с общей базой. Напряжение обратной связи поступает на его эмиттер с делителя, состоящего из конденсаторов С2 и С3. Частоту задающего генератора определяют конденсаторы С2 и С3, катушка L1 и межэлектродные ёмкости транзистора VT1. С коллектора транзистора VT1 сигнал через конденсатор С1 поступает в линию, провод которой используется в качестве антенны. Дроссель Др1 служит для разделения ВЧ и НЧ составляющих сигналов.

Рассмотрим устройство – индикатор, который позволяет обнаруживать нелегальное подключение подслушивающих устройств. Данное устройство является простейшим индикатором наличия подслушивающих устройств. Оно устанавливается на предварительно проверенной телефонной линии. Питание осуществляется от телефонной линии. При наличии любых несанкционированных подключений различных устройств, питающихся от телефонной линии, выдается сигнал тревоги.

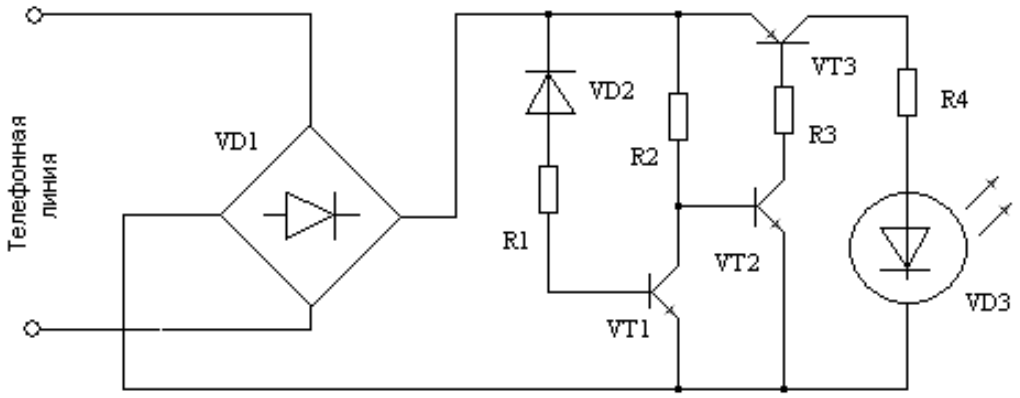


Рис. 5. Простейший индикатор состояния телефонной линии.

К выходу усилителя через ограничительный резистор R_4 подключен светодиод VD_3 типа АЛ307. Выпрямительный мост VD_1 типа КЦ407 обеспечивает требуемую полярность питания устройства независимо от подключения его к телефонной сети. При свободной линии постоянное напряжение в ней около 60 В. Стабилитрон VD_2 открывается, и в базу транзистора VT_1 подается через ограничительный резистор R_1 управляющий ток. Открытый и насыщенный транзистор VT_1 шунтирует вход каскада на транзисторе VT_2, поэтому усилитель тока закрыт и светодиод VD_3 погашен. При подключении в линию посторонних устройств напряжение в линии падает и ток, протекающий через стабилитрон VD_2, уменьшается (вплоть до закрытия последнего). Транзистор VT_1 закрывается, а в базу транзистора VT_2 через резистор R_2 подается управляющий ток. Усилитель открывается и светодиод VD_3 включается.

Приложение 2

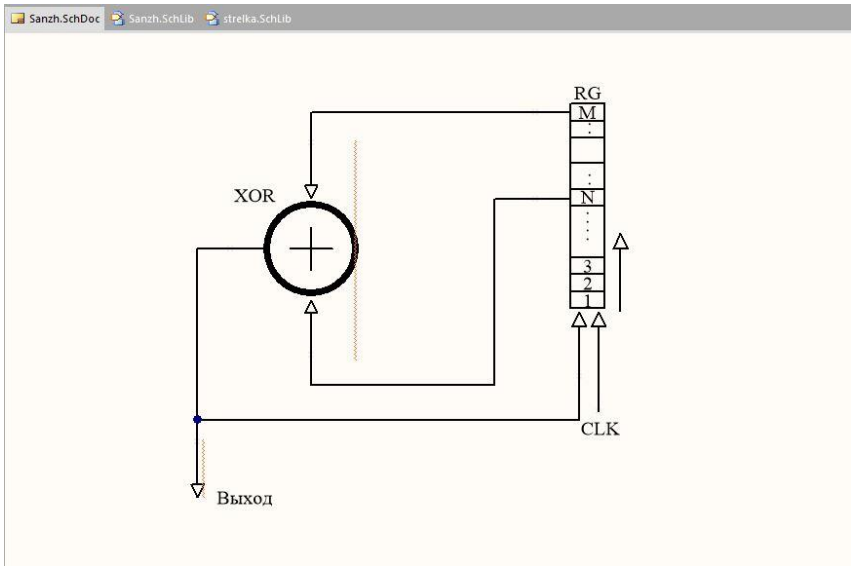


Рисунок 2.1. Генератор псевдослучайных битовых последовательностей (последовательность 2^M-1 бит)

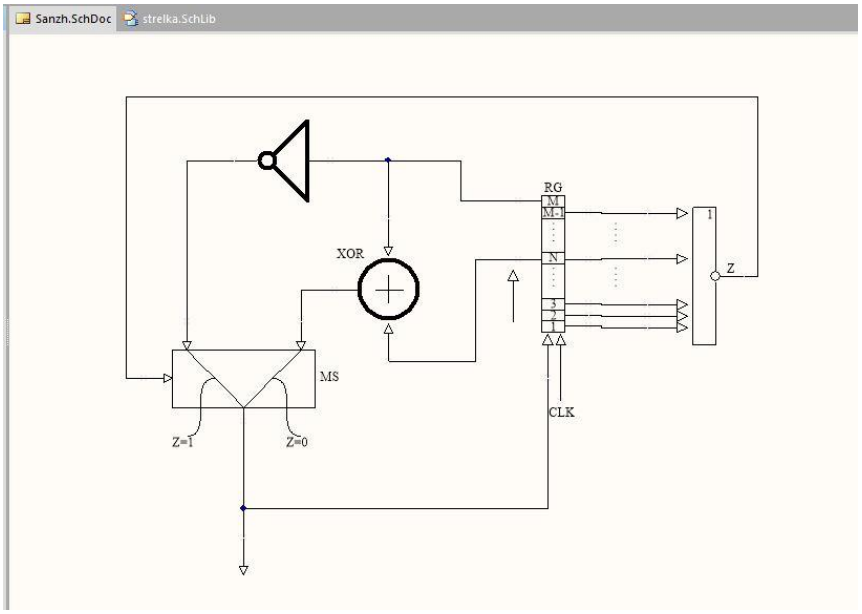


Рисунок 2.2. Генератор псевдослучайных битовых последовательностей (последовательность 2^M бит)

M	3	4	6	7	9	10	11	15	17	18	20	21	22	23	25	28	29	31	35
N	2	3	3	5	6	7	9	14	14	11	17	19	21	18	22	25	27	28	20

Рисунок 2.3. Таблица для выбора промежуточной точки N подключения цепи обратной связи

Приведенные схемы различаются длинами периодов генерируемых последовательностей битов. В схеме, показанной на рисунке 2.1, регистр RG исходно установлен в некоторое ненулевое состояние (цепь начальной установки не показана). Под действием положительных фронтов синхросигнала CLK хранимый в регистре код непрерывно циркулирует в нем и одновременно видоизменяется благодаря преобразованию битов логическим элементом Исключающее ИЛИ (XOR). Генерируемая последовательность битов снимается с выхода любого разряда регистра. Направление сдвига данных в регистре показано стрелкой. В полном цикле работы генератора в регистре однократно формируется все возможные M-разрядные коды, за исключением нулевого. Циклы следуют один за другим без пауз.

В общем случае при использовании M-разрядного регистра цепь обратной связи подключаются к разрядам с номерами M и N (M > N). Для того чтобы на выходе генератора формировалась псевдослучайная последовательность битов с периодом повторения, равным 2^M-1, следует выбирать точки подключения цепи обратной связи в соответствии с таблицей,

Приведенной на рисунке 2.3 таблица, которая описывает ряд генераторов различной разрядности.

Псевдослучайная последовательность битов с периодом повторения, равным 2^m-1, обладает следующими свойствами.

В полном цикле (2^M-1 тактов) число логических единиц, формируемых на выходе генератора, на единицу больше, чем число логического нуля. Добавочная логическая единица появляется за счет исключения состояния, при котором в регистре присутствовал бы нулевой код. Это можно интерпретировать так, что вероятности появления логического нуля и логической единицы на выходе генератора практически одинаковы.

В полном цикле (2^M-1 тактов) половина серий из последовательных логической единицы имеет длину 1, одна четвёртая серий - длину 2, одна восьмая- длину 3 и так далее. Такими же свойствами обладают и серий из логической единицы с учетом пропущенного логического нуля. Это говорит о том, что вероятности появления «орлов» и «решек» не зависят от исходов предыдущих «подбрасываний». Поэтому вероятность того, что серия из последовательных логической единицы или логического нуля закончится при следующем подбрасывании, равна S.

Если последовательность полного цикла (2^M-1 тактов) сравнивать с этой же последовательностью, но циклически сдвинутой на любое число тактов W(W не является нулем или числом, кратным 2^M -1), то число несовпадений будет на единицу больше, чем число совпадений.

Улучшенная схема (рисунок 2.2) формирует псевдослучайную последовательность битов с периодом повторения, равным 2^M. К этой схеме также применима таблица, приведенная на рисунке 2.3. В регистре в определенном порядке формируется все возможные коды, включая нулевой. Схема дополнительно содержит элемент ИЛИ-НЕ, инвертор и мультиплексор. Сигнал Z на выходе элемента ИЛИ-НЕ задает направление передачи данных через мультиплексор. При Z = 0 на выход мультиплексора транслируется сигнал с выхода элемента Исключающее ИЛИ, а при Z=1 – сигнал с выхода инвертора.

До тех пор пока на входах элемента ИЛИ-НЕ присутствует хотя бы одна логическая единица, на его выходе сформирован сигнал Z = 0. В этом случае мультиплексор в каждом такте передает в освободившийся (нижний) разряд сдвигового регистра бит с выхода элемента Исключающее ИЛИ так же, как и в схеме, показанной на рисунке 3.2.

В некотором такте i в регистре фиксируется код, содержащий единственную логическую единицу, размещенную в разряде M – 1. Так как в разрядах M и N присутствуют логическая ноль, то на выходе элемента исключающее ИЛИ сформирован сигнал логического нуля, который к началу такта i+1 поступает на вход регистра. В начале такта i+1 логическая единица перемещается из разряда M – 1 в разряд M, на входах элемента ИЛИ – НЕ формируется нулевой код. Сигнал Z= 1 переводит мультиплексор в состояние, при котором на вход нижнего разряда сдвигового регистра поступает бит с выхода инвертора. В данном случае этот бит равен нуля, поэтому в такте i + 2 в регистре фиксируется нулевой код.

К началу такта i + 3 на вход сдвигового регистра с выхода инвертора поступает логическая единица, поэтому по положительному фронту синхросигнала CLK в регистре фиксируется код, содержащий логическую ноль во всех разрядах, кроме первого. Сигнал Z вновь принимает нулевое значение, мультиплексор переключается в состояние передачи сигнала с выхода элемента Исключающее ИЛИ и так далее. Таким образом, регистр проходит через все состояния, включая нулевое. Возможны и иные варианты построения генераторов с числом состояний, равным 2^M .

Единственное преимущество данного способа скремблирования являлется то что, синхронизация достигается автоматически после заполнения регистров одинаковыми данными.

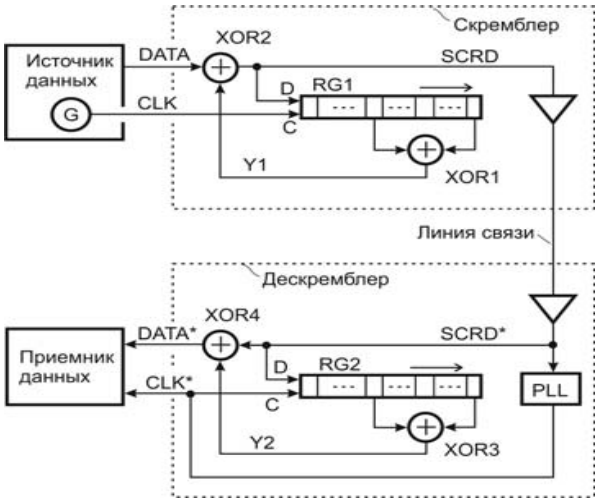


Рисунок 2.4. Система «скремблер - дескремблер» с генераторами псевдослучайных последовательностей битов.

В системе, показанной на рисунке 3.5, скремблер и дескремблер содержат фрагменты рассмотренного ранее генератора (рисунок 3.2) псевдослучайных последовательностей битов. В скремблере цепь обратной связи генератора на основе сдвигового регистра 1 дополнительно содержит элемент Исключающее ИЛИ. В дескремблере применен аналогичный генератор на основе сдвигового регистра 2 с разомкнутой цепью обратной связи.

Все процессы, протекающие в системе, синхронизируется от тактового генератора, размещенного в источнике данных (возможно также его размещение в скремблере). Тактовый генератор формирует сигнал CLK – непрерывную последовательность тактовых импульсов со скважностью, равной двум. В каждом такте по положительному фронту сигнала CLK на вход скремблера подается «новый» бит передаваемых данных, а код в его

сдвиговом регистре 1 продвигается на один разряд вправо, причем в этот же момент в освободившийся разряд заносится «старый» бит данных, просуммированный по модулю два со «старым» битом с выхода элемента ИЛИ.

Строго говоря, на границах между битовыми интервалами на выходе элемента ИЛИ могут формироваться короткие ложные импульсы в результате неодновременного формирования «новых» сигналов на его входах. Для устранения ложных импульсов можно ввести в цепь сигнала SCRD D-триггер, синхронизируемый отрицательным фронтом сигнала CLK (триггер на рисунке не показан). Короткими ложными импульсами пока пренебрегаем для упрощения изложения основных идей построения систем «скремблер - дескремблер».

Если источник данных посылает в скремблер длинную последовательность сигналов логического нуля (DATA=0), то элемент XOR2 можно рассматривать как повторитель сигнала Y1. Тогда регистр 1 фактически оказывается замкнутым в кольцо и генерирует точно такую же псевдослучайную последовательность битов, как и в рассмотренной ранее схеме генератора, приведенной на рисунке 3.2. Отметим, что в этой ситуации при неблагоприятном стечении обстоятельств есть опасность потери работоспособности скремблера, если в регистре 1 к началу передачи последовательности сигналов логического нуля зафиксирован нулевой код.

Если от источника данных поступает произвольная битовая последовательность, то она взаимодействует с последовательностью битов с выхода элемента XOR1. В результате формируется новая (скремблированная) последовательность битов данных SCRD, по структуре близкая случайной. Эта последовательность, в свою очередь, продвигается по регистру 1, формирует поток битов Y1 на выходе элемента ИЛИ и так далее.

Скремблированная последовательность битов SCRD проходит через передающий усилитель и по линии связи поступает в дескремблер , где проходит через приемный усилитель. Линия связи может быть выполнена, например, в виде витой пары проводов многожильного кабеля городской телефонной сети. С помощью генератора PLL (Phase Locked Loop) с фазовой автоподстройкой частоты из входного сигнала SCRD* выделяется тактовый сигнал CLK*, который передается на синхронизирующие входы регистра 2 и приемника данных.

Генератор PLL с фазовой автоподстройкой частоты может быть построен по одной из известных схем. Он предназначен для формирования

высокостабильного синхросигнала CLK* но основе непрерывного слежения за входным сигналом SCRD*. В данном случае отрицательный фронт сигнала CLK* привязан к моментам изменения сигнала SCRD* (0 – 1 или 1 - 0), так что положительный фронт сигнала CLK* формируется в середине битового интервала сигнала SCRD*, что соответствует его установившемуся значению. Сдвиг данных в регистре 2 и прием очередного бита SCRD* в его освободившийся в разряд происходят по положительному фронту сигнала CLK*. Дескремблированные данные DATA* поступают в приемник данных и фиксируется в нем по положительным фронтам сигнала CLK*. Благодаря достаточной инерционности генератора PLL сигнал CLK* практически нечувствителен к «дрожанию фазы» сигнала SCRD* и иным его кратковременным искажениям вызванным помехами в линии связи.

Потоки данных DATA и DATA* совпадают с точностью до задержки передачи. Действительно в установившемся режиме в сдвиговых регистрах 1 и 2 присутствуют одинаковые коды, так как на входы D этих регистров поданы одни и те же данные SCRD = SCRD* (с учетом задержки передачи), а тактовая частота одна и та же. Поэтому Y2 = Y1 и с учетом этого

$$DATA^* = SCRD^* \oplus Y2 = SCRD \oplus Y2 = (DATA \oplus Y1) \oplus Y2 =$$
$$= DATA \oplus Y1 \oplus Y1 = DATA \oplus 0 = DATA.$$

Приложение 3

Способы прослушивания телефонной линии связи

Непосредственное подключение к телефонной линии наиболее простой и надежный способ получения информации. В простейшем случае применяется трубка ремонтника - телефониста, подключаемая к линии распределительной коробке где производится разводка кабелей.). Необходимо помнить, что АТС переключает линию на разговор при шунтировании её сопротивлении около 1 кОм, применение аппаратуры подслушивания с низкоомным входом приводит к обнаружению прослушивания.

Прослушивание через электромагнитный звонок ТА. Телефонные аппараты, где в качестве вызывного устройства используется эл/м звонок пока ещё наиболее распространенны в нашей стране. Звонок обладает свойством дуальности, тесть если на эл/м звонок действуют звуковые волны, он начнёт вырабатывать соответствующим образом модулированный ток. Амплитуда его достаточна для дальнейшей обработки. Эксперименты показали, что амплитуда ЭДС наводимая в линии, для некоторым типов ТА может достигать нескольких милливольт (мВ). Корпус аппарата является дополнительным резонирующим устройством.

Прослушивание через микрофон телефонного аппарата.

На первый взгляд, когда трубка лежит на аппарате нет никакой возможности использовать микрофон для подключения к телефонной линии. Микрофон является частью электронной схемы телефонного аппарата(ТА);он либо соединен с линией (через отдельные элементы

схемы) при разговоре, либо отключен от линии, когда ТА находится в готовности к приёму вызова (трубка находится на аппарате в качестве источника съема информации). Но это только на первый взгляд.

Для понимания проблемы необходимо классифицировать методы съема информации с телефонной линии и методов противодействия, для облегчения понимания и краткости введём некоторые понятия и определения.

Кратковременное подключение: Характеризуется малым временем контакта пиратского ТА с линией в точке подключения. Как правило, наблюдаются единичные случаи использования различных телефонных аппаратов или линий с отсутствием или незначительной маскировкой мест подключения. Достаточно хорошо поддаются выявлению и предупреждению (в суммарном выражении не наносят значительного финансового ущерба).

Длительное подключение: Сам факт такого подключения говорит о том, что лица осуществившие подключение находятся где-то рядом (соседи, сослуживцы) либо показывают уязвимость данного абонентского комплекта для пиратского подключения.

Подключение без разрыва шлейфа (двухпроводная линия от АТС до телефонного аппарата). К такому виду подключений относятся параллельное подключение на абонентской линии, распределительной коробке, телефонном шкафу, в кабельной зоне АТС либо использование неисправного телефона жертвы. Для такого рода подключений характерно подзвякивание основного телефона, что заставляет пользоваться линией в отсутствие хозяев. Производится обычно разъёмами типа «крокодил» или иголками в открытых распределительных шкафах, колодцах, коробках после чего практически не остаётся следов подключения.

Подключение с разрывом шлейфа: Отличительной особенностью является высокой скрытностью проведения незаконных разговоров. Практически невозможно выявить факт подключения в момент его проведения (хозяину линии имитатором подаётся определённый сигнал не вызывающий подозрений типа «занято»).

Бесконтактное подключение: Проявляется в зоне радиоканала между стационарным и переносным блоком радиотелефона. Путем электронного сканирования распознается кодовая посылка сигнала снятия трубки, и далее, связь происходит обычным образом, только вместо переносного блока владельца линии используется пиратский аппарат, «прошитый» соответственным образом. Таким образом происходит мошенничество в области сотовых систем связи. Есть несколько методов, с помощью которых третья сторона может собрать данные об опознавательных (телефонных) номерах, последовательных электронных индексах абонентов сети и воссоздать копию-клон, реализующую возможности оригинала в

упрощенном варианте. Запущенные в сеть клоны опознавательного номера сотового телефона могут быть использованы для ведения за день телефонных разговоров (в том числе международных) на ощутимую сумму. Существуют также «телефоны вампиры», которые непрерывно «обнюхивают» эфир и вытягивают опознавательный номер и последовательный электронный индекс санкционированного пользователя для однократного разговора.

Существуют следующие способы подключения и сьема информации:

- простейшее контактное подключение к линии;
- применение телефонного “жучка”;
- индукционное подключение к линии;
- профессиональное подключение к линии (фильтрация внеполосных помех);
- емкостное подключение к линии;
- перехват радиотелефона в стандарте AMPS(DAMPS) [ ];
- перехват радиотелефона в стандарте NMT [ ];
- перехват радиотелефона в стандарте GSM [ ];
- перехват спутниковой телефонной связи (в ближней зоне).

Спектр угроз показывает нам, наибольшую опасность представляет собой контроль телефонных разговоров с помощью простейшего контактного подключения к линии. Примерно равную, но меньшую опасность представляет перехват телефонных разговоров с проводных линий с помощью “жучков”, ответчиков и бесконтактного съема информации. Существенно меньшую (почти на порядок) опасность представляют собой угрозы, связанные с перехватом сотовой телефонной связи, особенно в стандарте GSM. минимальная опасность прогнозируется для спутниковой телефонной связи.

Простейшее контактное подключение осуществляется обычным телефонным аппаратом или монтёрской трубкой непосредственно к абонентской проводке при помощи разъемов типа «крокодил» либо иголками. При этом порой невозможно определить место подключения, так как в данном случае практически не остаётся никаких следов подключения, а время самого подключения обычно не превышает продолжительности интересующего разговора.

Краткий обзор схем прослушивания телефонных переговоров и блокировки несанкционированного подключения к линии связи

Задача обнаружения и следовательно защиты при контактном подключении решается достаточно просто установкой несложного блокиратора телефонной линии аналогичного приведённому на рисунке 1.2 не требующего специализированной настройки и знаний радиотехники. Схемы таких устройств достаточно распространённы и собираются в домашних условиях из недорогих комплектующих достаточно быстро и с хорошим качеством.

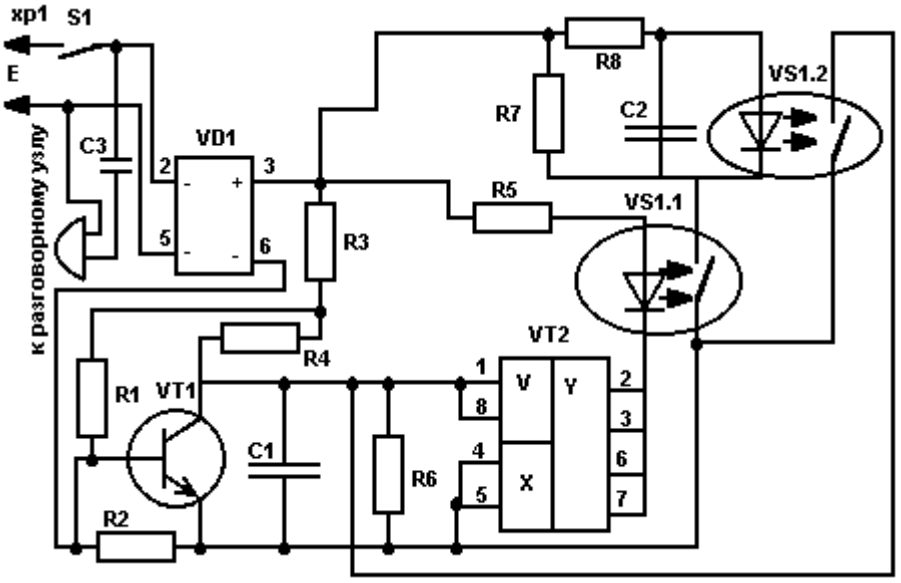


Рисунок 3.1. Блокиратор дополнительного аппарата

Данное устройство используется как блокиратор несанкционированного (пиратского) подключения к линии. Любой параллельный телефонный аппарат будет заблокирован (с него нельзя будет вести разговоры). Питание устройства осуществляется от телефонной линии. Режим работы линии не нарушается.

В основе работы схемы используется пороговое устройство на транзисторе VT1, который контролирует уровень напряжения в телефонной линии. Как известно, при поднятии трубки с аппарата, напряжение в линии падает с 60 до 5...15 В (зависит от сопротивления цепей ТА). Режим работы VT1 настраивается резистором R2 так, чтобы он при напряжении ниже +18 В запирался. При этом транзистор VT2 током через резисторы R3-R4 откроется, что приведет к срабатыванию оптронного ключа VS1.1. Резистор R7 закоротит телефонную линию, что воспрепятствует импульсному набору номера на время заряда С2. Как только С2 зарядится - сработает ключ VS1.2 и разрядит С1. Этот процесс периодически повторяется, что исключает фиксацию схемы в режиме закорачивания линии после однократного

срабатывания блокировки. Конденсатор С1 обеспечивает нечувствительность схемы к сигналу вызова в линии. Устройство подключается параллельно звонку (или схеме звукового сигнализатора) до разделительного конденсатора так, чтобы при поднятии трубки оно отключалось контактами, связанными с положением трубки (S1). В этом случае не потребуется отключать устройство от линии при использовании собственного телефонного аппарата, что удобно при эксплуатации. Схема не критична к выбору типов резисторов и конденсаторов. Вместо диодного моста VD1 можно использовать один диод, но в этом случае при подключении устройства к телефонной линии потребуется соблюдать необходимую для работы полярность.

Прослушивание с помощью радиомикрофона с питанием от телефонной линии (телефонного «жучка»)

Длительное подключение характеризуется применением особых устройств, высокой скрытностью, тщательностью подготовки и существенно меньшим влиянием на параметры линии, так как требует определённых знаний радиотехники, построения телефонных сетей и соответствующего уровня подготовки. В качестве примера можно привести следующую схему «радиожучка» (рисунок 3.2).

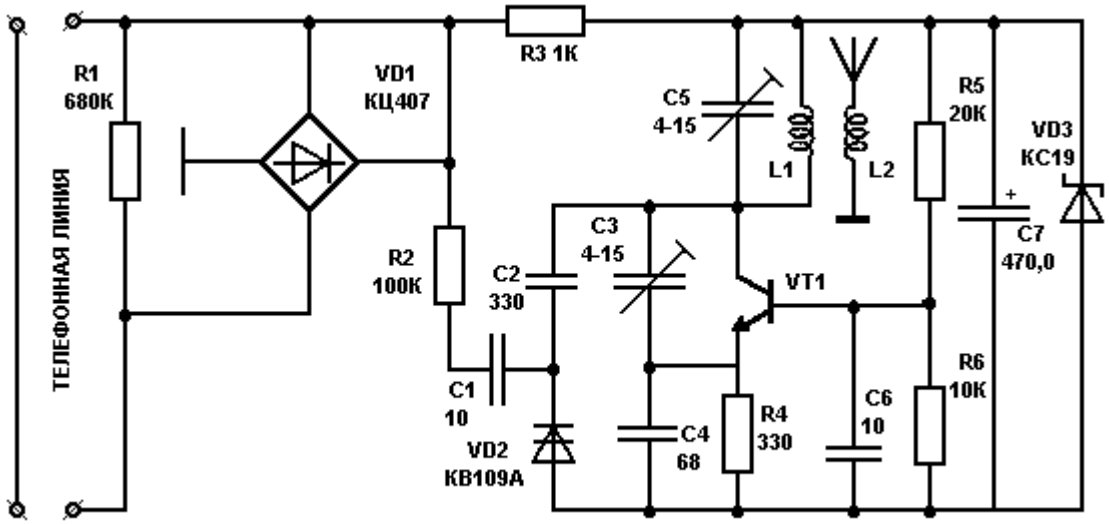


Рисунок 3.2. Телефонный ретранслятор средней дальности

Очевидно, что для обнаружения и нейтрализации подобного устройства требуется аппаратура так как при включении устройства хозяин

линии не догадывается о её незаконном использовании и что вся передаваемая им по телефону информация подвергается прослушиванию.

Для нейтрализации данного типа устройств можно использовать датчик нерезонансного подключения с индикацией зоны незаконного подключения (рисунок 3.3) к линии.

Принцип действия довольно прост. При включении в линию подслушивающего устройства на различных участках шлейфа на выходе датчика формируется соответственно, один из четырёх уровней напряжения E0 – U1 ,U2 ,U3 , U4 . Численные значения были выявлены в результате экспериментов на реальной телефонной линии с достаточно длинным шлейфом при включенным стандартном телефоне. В зависимости от зоны включения загораются светодиоды, в 4 зоне все 4, в 3 зоне 3 и т.д.

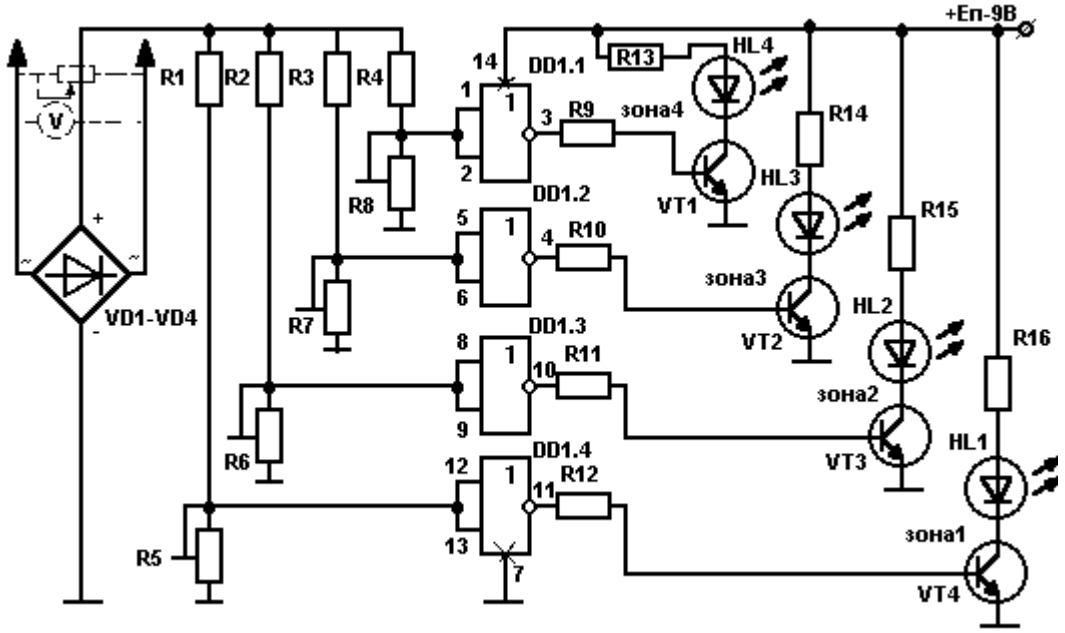


Рисунок 3.3 Датчик нерезонансного подключения с индикацией зоны.

На рисунке 3.4 приведена схема прослушивания с помощью радио-микрофона с питанием от телефонной линии.

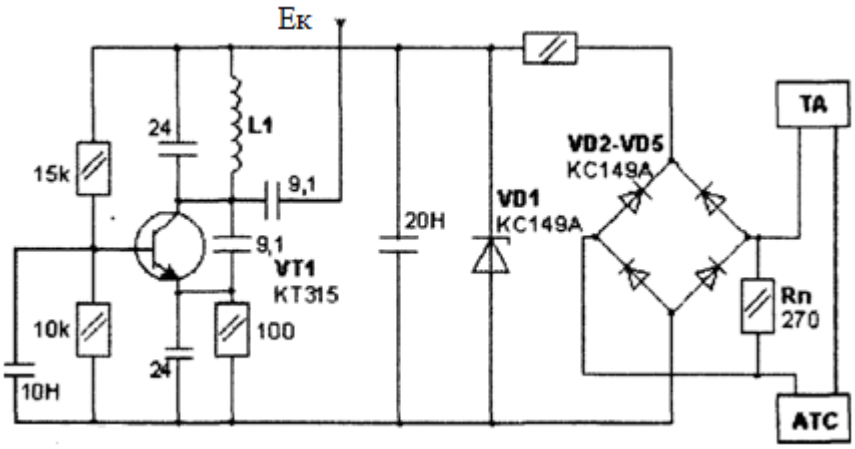


Рисунок 3.4 - Схема прослушивания телефонных линий

Устройство питается благодаря последовательному включению с телефоном в любом месте линии от аппарата до АТС. При снятии трубки и при вызове абонента на резисторе Rn происходит падение напряжения, которое используется для питания схемы передатчика. Таким образом можно получить питание 3-4 вольта, что вполне достаточно для маломощного передатчика. В принципе, подбирая резистор Rn можно получить и большее падение напряжения, но при этом уже будет ощутимое снижение громкости переговоров на этом ТА, что может привести к рассекречиванию прослушивающего устройства.

Прослушивание с помощью кодового микрофонного усилителя. Этот способ является, пожалуй, одним из самых сложных и требует специального устройства. Принципиальная схема такого устройства была опубликована в открытом журнале как схема прослушивания своей квартиры на расстоянии. Очевидно, что кто-то может поступить так и с Вашей квартирой, предварительно установив на линии (в квартире) этот прибор. Он собран на зарубежной элементной базе. Любой телефон, если в него встроить определенную приставку можно прослушать следующим образом: Вы звоните по этому телефону и сразу подносите к трубке портативный тональник.

Тональник звучит на определенной частоте, сигнал проходит по линии на телефон и обрабатывается схемой. Автоответчик, подключенный к проводам телефонной линии, реагирует на звонок и шунтирует линию сопротивлением 600 Ом. При этом телефонная станция переключает телефон на приём и передачу информации. Первыми к линии подключены три устройства: коммутатор питания схемы, цепь имитации поднятия трубки и цепь приема и передачи информации.

После прохождения вызова, коммутатор питания подает напряжение на все блоки и запускает таймер А. который в свою очередь включает имитатор поднятия трубки. По истечении времени таймер отключает телефон от линии в том случае, если Вы не подали тональный сигнал в линию если тональный вызов будет правильным, частотный детектор его опознает и запустит таймер В. Таймер В выполняет двойную функцию: включает питание на усилитель и блокирует таймер А, не давая ему отключаться. Ко входу подключен микрофон, воспринимающий все звуки в помещении и через усилитель и согласующий трансформатор передаёт их в линию. По окончании выдержки таймера в питание будет отключено, поэтому в линию необходимо подавать периодически сигнал тональника.