ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

М. Тынышбаев атындағы
ҚАЗАҚ КӨЛІК ЖӘНЕ КОММУНИКАЦИЯЛАР АКАДЕМИЯСЫ

КАЗАХСКАЯ АКАДЕМИЯ ТРАНСПОРТА И КОММУНИКАЦИЙ
имени М. Тынышпаева

QazATK
since 1931

МАГИСТРАНТТАРДЫҢ ҒЫЛЫМИ ЕҢБЕКТЕРІНІҢ ЖИНАҒЫ

СБОРНИК НАУЧНЫХ ТРУДОВ МАГИСТРАНТОВ

Алматы - 2018

СЕКЦИЯ №5. ИННОВАЦИОННЫЕ ПОДХОДЫ В ОРГАНИЗАЦИИ ПЕРЕВОЗОЧНОГО ПРОЦЕССА

СЕКЦИЯ №6. ЛОГИСТИЧЕСКИЕ СИСТЕМЫ И ТЕХНОЛОГИИ ПЕРЕВОЗОЧНОГО ПРОЦЕССА НА ТРАНСПОРТЕ

приложению перед его установкой, не позволяют оценить возможные риски персональным данным и последствия потенциальных злоумышленных действий. Современные средства защиты (антивирусы, снифферы) могут помочь предотвратить определенный спектр угроз, но их применение не позволит решить проблему безопасности комплексно. В связи с этим, возникает задача разработки комплексной методики по оцениванию угроз информационной безопасности в приложениях для мобильных систем, а также методики анализа приложений на предмет их соответствия требованиям информационной безопасности.

ЛИТЕРАТУРА

[1] Аналитический центр InfoWatch. Глобальное исследование утечек корпоративной информации и конфиденциальных данных, 2018. URL: https://www.infowatch.ru/report2018 (дата обращения 01.12.2018).

[2] Михайлов Д. М. Исследование уязвимости мобильных устройств систем Apple и Google / Д.М. Михайлов, А.В. Зуйков, И. Ю. Жуков и др. // Спецтехника и связь, 2011, № 6. С. 38-40. URL: http://cyberleninka.ru/article/n/issledovanie-uyazvimosti- mobilnyh-ustroystv-sistem-apple-i-google#ixzz4hjVQGz9w.

[3] Цыганенко Н. П. Статический анализ кода мобильных приложений как средства выявления его уязвимостей / Н. П. Цыганенко // Тр. БГТУ. Сер. 6: Физико-математические науки и информатика, 2015, № 6. С. 200-203. URL: http:// cyberleninka.ru/article/n/staticheskiy-analiz-koda-mobilnyh- prilozheniy-kak-sredstvo-vyyavleniya-ego-uyazvimostey.

[4] Android: A visual history [Электронный ресурс]. – URL: http://www.webcitation.org/6DpDvrrwH (дата обращения: 28.12.2018).

[5] Whitwam R. Google Rolling Out Android 4.4.4 Update (KTU84P) With A Security Fix, Factory Images/Binaries Up For Nexus Devices [Электронный ресурс]. – URL: http://www.androidpolice.com/2014/06/19/google-rolling-out-android-4-4-4-update-ktu84p-with-a-security-fix-factory-images- binaries-up-for-nexus-devices/ (дата обращения: 28.12.2018).

[6] When Malware Goes Mobile [Электронный ресурс]. – URL: https://www.sophos.com/en-us/security-news-trends/security-trends/malware- goes-mobile.aspx (дата обращения: 28.12.2018).

УДК 004.451.6

А.Н. Нургулжанова[1,a], Е. Омирзакулы[2,a]

[1]Казахская академия транспорта и коммуникаций им. М.Тынышпаева, г. Алматы, Казахстан

[2]Алматинский технологический университет

[a]a.nurgulzhanova@kazatk.kz

АНАЛИЗ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ПО КАНАЛАМ СОТОВОЙ СВЯЗИ

Аннотация. В статье приведены анализ защищенности информации по каналам сотовой связи. Предлагаемое в данной статье устройство построено по гибридному принципу с уровнем защиты, обеспечивающее временную стойкость. Для проверки достоверности работы модели схемы защиты речевой информации, имеющий аналоговый вид, разработана модель на пакете программ SystemView. Она позволяет оценить результаты эксперимента и дает визуальную информацию форм сигналов данного устройства.

Ключевые слова: аналоговые сигналы, гибридные сигналы, полосовые фильтры, защита информации, скрэмблеры, биквадратный фильтр.

Андатпа. Мақалада ұялы байланыс арналары бойынша ақпараттың қорғалуына талдау келтірілген. Ұсынылған мақалада құрылғы уақытша төзімділікті қамтамасыз ететін қорғаныс деңгейі бар гибрид принципі бойынша салынған. Аналогты түрі бар, сөйлеу ақпаратын қорғау схемасының моделі жұмысының дұрыстығын тексеру үшін SystemView бағдарлама пакетінде жасалған. Эксперимент нәтижелерін бағалауға және осы құрылғының сигнал формаларының визуалды ақпаратын көрсетуге мүмкіндік береді.

Түйінді сөздер: аналогтық сигналдар, гибридтік сигналдар, жолақтық сүзгілер, ақпаратты қорғау, скремблерлер, биквадратдық сүзгі.

Abstract. The article provides an analysis of the security of information via cellular communication channels. The proposed, in this article, the device is built on a hybrid principle with a level of protection that provides temporary resistance. To verify the validity of the model of the voice information protection scheme, which has an analog form, a model has been developed on the SystemView software package. It allows you to evaluate the results of the experiment and provides visual information about the waveforms of this device.

Key words: analog signals, hybrid signals, bandpass filters, information protection, scramblers, bi-square filter.

Проблема защиты речевой информации от подслушивания стала актуальной задачей. Перехват разговоров может служить основанием для экономических преступлений, шантажа, имитации абонентов и т.д.

Устройства защиты речевой информации классифицируются по способу обработки сигналов на:

-аналоговые;

-цифровые;

-гибридные.

Аналоговые устройства не практичны из-за их громоздкости и ограниченных возможностей. К достоинствам аналоговых систем можно отнести простоту схемной реализации и дешевизну конструкции. Но за достоинствами идут недостатки и самый главный – низкий уровень секретности, что на данном этапе развития телекоммуникации не является приемлемым.

Цифровые системы требуют специальных сигнальных процессоров, которые осуществляют различные математические алгоритмы закрытия речи. Цифровые системы создают более высокий уровень секретности документа и дают возможность сохранности (от несанкционированного доступа) в течение длительного периода времени. Из-за сложности алгоритмов шифрования цифровые системы должны иметь в своем составе высокоскоростные скремблеры и дескремблеры, аналого-цифровые и цифро-аналоговые преобразователи, а также вокодеры исключающие избыточность речи построенные по принципу линейного предсказания. Все перечисленные компоненты делают цифровые устройства сложными с точки зрения схемной реализации и дорогостоящими, что делает их малоприменимыми к мобильным системам связи, но дающими высокую степень секретности, занимая при этом широкую полосу частот при передачи. Вследствие всего вышесказанного цифровые системы также редко применимы в средствах стационарной телефонной сети общего пользования.

Наиболее широкое распространение находят гибридные устройства защиты речевой информации, основная идея которых заключается в том, что входные и выходные сигналы у них являются аналоговыми, а весь процесс закрытия информации происходит в цифровом виде. Наличие аналогового сигнала позволяет использовать такие устройства на любых речевых трактах, будь то аналоговые или цифровые, в первом случае устройство просто монтируется после микрофона, осуществляя необходимые преобразования, в остальных случаях (цифровых каналах) выходной сигнал в цифровой форме передавался в линию связи. Использование цифровых методов кодировки позволяет применять практически любые математические алгоритмы закрытия речи. Рассмотрев все достоинства и недостатки устройств защиты, приходим к выводу, что наиболее эффективными и малогабаритными являются устройства, построенные по гибридному принципу обработки данных. Этот принцип мы и будем использовать при дальнейшей разработке.

Средства защиты различают системы с преобразованием речи во временной или в частотной области, при этом используется маска и криптографические преобразования.

Согласно алгоритмам преобразования во временной области, форматы речи или цифровые отсчеты переставляют местами во времени. Устройства такого типа широко распространены и часто называются скремблерами. Скремблеры в настоящее время находят широкое применение в средствах телекоммуникации за счет своей простоты и гарантийной стойкости от взлома. Скремблеры в свою очередь также делятся на группы. Так, при частотном преобразовании речь разделяется на форматы, затем подвергаются линейным преобразованиям по определенному закону. Данный алгоритм не является на сегодняшний день универсальным, вследствие низкого уровня защиты.

Предлагаемое в данной статье устройство построено по гибридному принципу с уровнем защиты, обеспечивающего временную стойкость. Как уже было сказано выше, входные и выходные сигналы здесь аналоговые, а весь процесс закрытия информации происходит в цифровом виде внутри передатчика и приемника. Структурная схема данного устройства предложена на рисунке 1.

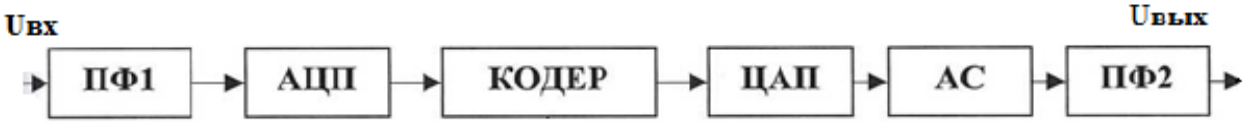

Рисунок 1 - Структурная схема устройства защиты речевой информации

Рассмотрим основное назначение каждого блока. Аналоговый сигнал поступает на вход полосового фильтра ПФ1, который ограничивает речевой спектр до стандартного значения 0,3 - 3,4 кГц. Фильтр является активным, т.е. собран с использованием операционных усилителей ОУ, но т.к. высокий коэффициент усиления обуславливает возникновение искажений необходимо его снижение, что и сделано включением в цепь отрицательной обратной связи ООС других операционных усилителей. Далее сигнал поступает на аналого-цифровой преобразователь АЦП, который переводит аналоговый сигнал в восьмиразрядный цифровой код, над которым впоследствии будет проходить процедура шифрования. После АЦП цифровой сигнал поступает на КОДЕР, который осуществляет процесс закрытия речи. Далее, уже закрытый речевой сигнал поступает на цифроаналоговый преобразователь ЦАП, который переводит цифровой восьми разрядный код в аналоговый сигнал. Следующим после ЦАП элементом является аналоговый скремблер АС, который в свою очередь стробирует определенную длительность аналогового сигнала и делает временную перестановку, увеличивая тем самым степень защиты. Завершает структурную схему полосовой фильтр ПФ2, который устраняет побочные продукты преобразования, приводя сигнал к стандартному значению 0,3-3,4 кГц. Следует также отметить, что данный полосовой фильтр снижает избыточность зашифрованного речевого сигнала, он также является активным – т.е. собран на операционных усилителях.

Разработка принципиальной схемы. Полосовые фильтры. В данной схеме целесообразно использовать активные фильтры, собранные на операционных усилителях ОУ, т.к. они помимо фильтрации осуществляют функцию усиления.

Активные фильтры можно использовать для реализации ФНЧ, ФВЧ, ПФ, ППФ. Известны различные конструкции активных фильтров, каждые из которых зависят от аппроксимации передаточной характеристики по функциям Баттерворта, Чебышева или другим. Некоторые свойства желательные для активного фильтра таковы:

- малое число элементов, как активных, так и пассивных;
- легкость регулировки;
- малое влияние разброса параметров элементов по характеристике фильтра, в особенности значений емкостей конденсаторов;
- отсутствие жестких требований к применяемому ОУ;

- возможность создания высокодобротных фильтров;
- нечувствительность характеристик фильтра по отношению к параметрам элементов и коэффициенту усиления ОУ.

По многим причинам последнее свойство является одним из наиболее важных. Фильтр, который требует соблюдения высокой точности значения параметров элементов, трудно настраивать, и по мере старения элементов настройка теряется; кроме того дополнительной неприятностью является требование использовать элементы с малым допуском значений параметров. В данном устройстве используется полосовой фильтр ПФ т.к. он должен пропускать лишь узкий диапазон тональной частоты 0,3 - 3,4 кГц. Существуют два основных метода, по которым строятся ПФ:

- метод переменных состояний;
- фильтры на ИНУН (источник напряжения управляемый напряжением).

Схема фильтра на ИНУН обязана широкой популярностью в основном своей простоте и малому числу деталей, но эта схема страдает недостатком, а именно, высокой чувствительностью к изменениям значения параметров элементов.

Фильтр, построенный на основе метода переменных состояний, куда более сложен по сравнению с фильтрами на ИНУН, и он широко применяется благодаря повышенной устойчивости и легкости регулировки. Наиболее близким к фильтру, на основе метода переменных состояний, примыкает так называемый биквадратный фильтр, представленный на рисунке 2.

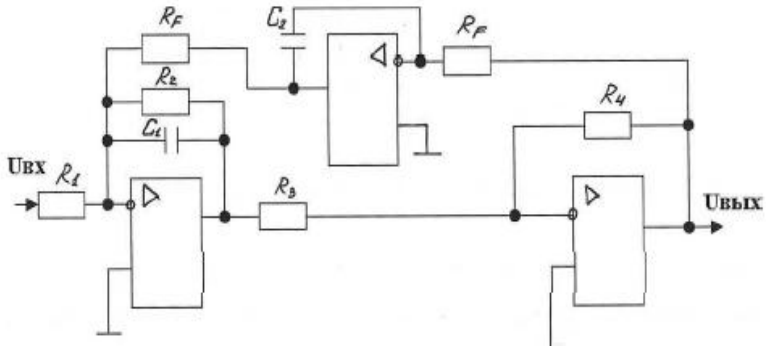

Рисунок 2 - Биквадратный фильтр

Данный фильтр обеспечивает 10 дБ коэффициента усиления и полосы пропускания - ПП 0,3 - 3,4 кГц. В этой схеме используются три ОУ, можно сконструировать на основе метода переменных состояний. Замечательным свойством такого фильтра является возможность регулировки его частоты (с помощью RF) при сохранении постоянной ширины полосы пропускания ПП.

Рассмотрим и другие модификации биквадратных фильтров.

Активный полосовой фильтр LM 358 (КР1040УД1), сдвоенный с внутренней частотной коррекцией см. рисунок 3.3. Данный фильтр обеспечивает 2дБ коэффициента усиления и ПП 0,3 - 3,4 кГц.

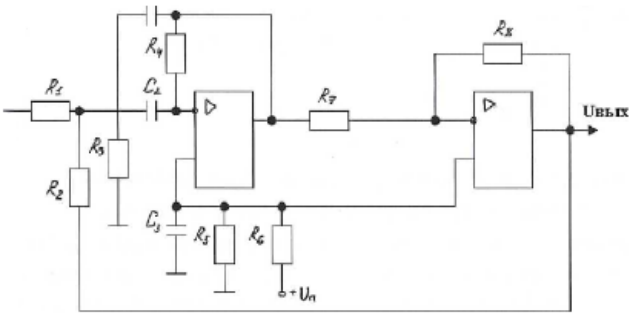

Рисунок 3 - Сдвоенный ПФ с внутренней частотной коррекцией

Активный биквадратный полосовой RC - фильтр LM124 (К1401УД2) - счетверенный ОУ с внутренней частотной коррекцией, но используется лишь три ОУ. Предложенный фильтр обеспечивает коэффициент усиления, равный 40дБ на ПП 0,8 - 2,8 кГц.

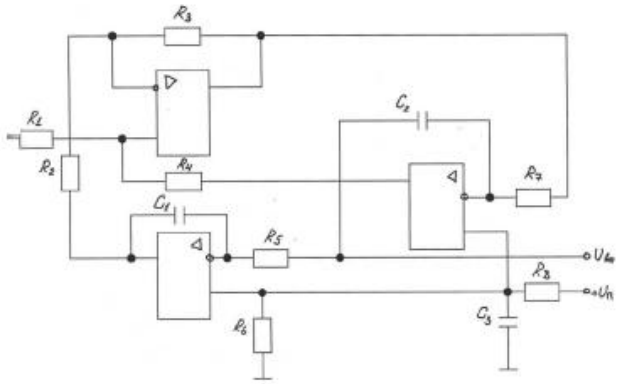

Рисунок 4 - Полосовой RC - фильтр с внутренней частотной коррекцией

В предложенном устройстве выберем фильтр LM358 (КР1040УД1) т.к. он обладает более широкой полосой пропускания 0,3 - 3,4 кГц и невысоким коэффициентом усиления 2дБ, что полностью удовлетворяет нашим требованиям. Данный фильтр полностью перекрывает наш диапазон 0,3 - 3,4 кГц, а малый коэффициент усиления, не приводит к искажениям.

Для проверки достоверности работы модели схемы защиты речевой информации, имеющий аналоговый вид, разработана модель на пакете программ SystemView. Она позволяет оценить результаты эксперимента и дает визуальную информацию форм сигналов данного устройства. Разработанная модель представлена на рисунке 5.

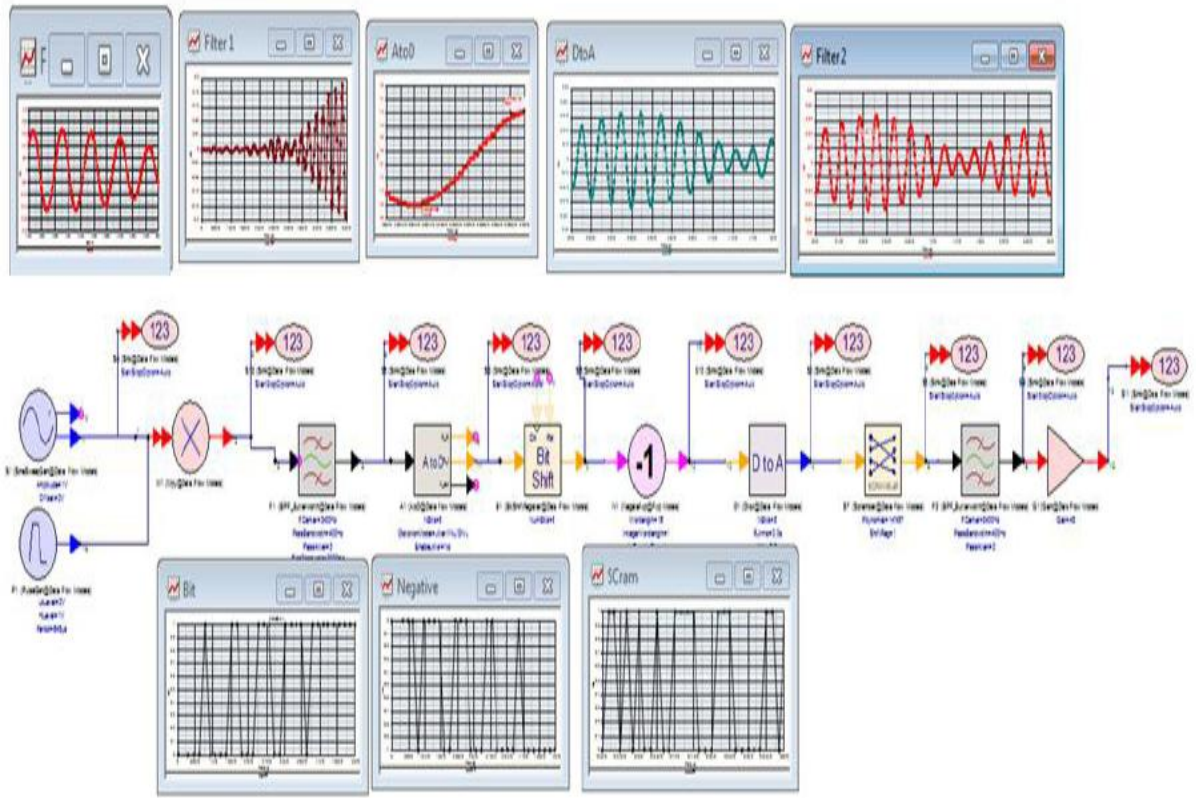

Рисунок 5 - Модель схемы в пакете SystemView

На рисунке 6 представлены исходный и результирующий сигналы модели системы защиты информации.

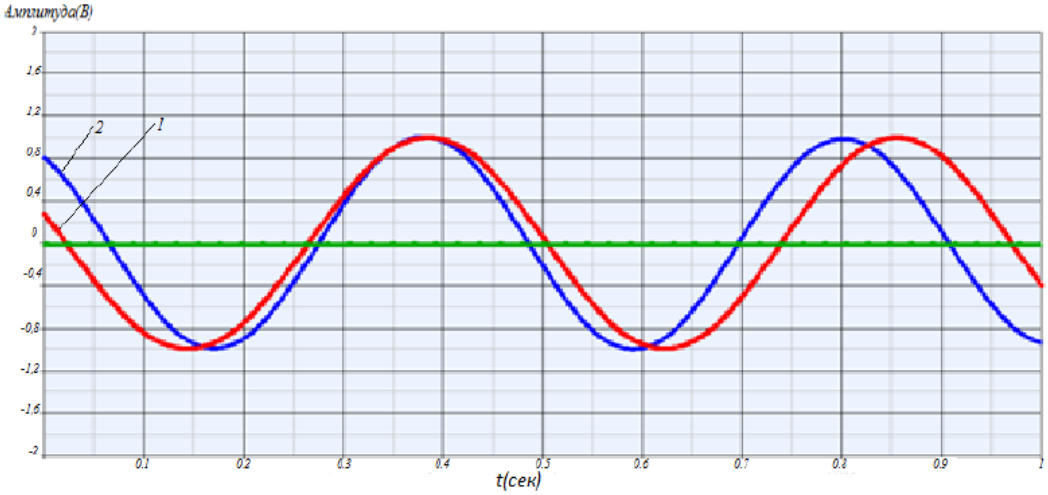

Рисунок 6 – Исходный и результирующий сигналы смоделированной системы

Из рисунка видно, что сигнал на выходе отличается по фазе.

Как видно из приведенных рисунков зашифрованный файл претерпел значительные изменения. Анализ остаточной разборчивости показал, что в зашифрованном файле нельзя разобрать ни одного слова, следовательно, остаточная разборчивость равна нулю, что подтверждает эффективность предлагаемого метода защиты информации.

ЛИТЕРАТУРА

[1] Ризви А. Оптимизация сети GSM / А. Ризви // Мобильные системы. М —2001. № 3. -С.21-23.

[2] Громаков Ю.А. Стандарты и системы подвижной радиосвязи. — М.: Эко-Трендз, 2000. 240 с.

[3] Карташевский В.Г., Семенов С.Н. Сети подвижной связи. М.: Эко- Трендз, 2001.-299 с.

[4] GPRS технология пакетной передачи данных в сетях GSM / М.А. Кузнецов, П.С. Абатуров, И.Ю. Никодимов, и др. - СПб: Судостроение,2002.-125 с.

[5] Малахов В.Б. Комплексное решение CBOSS компании "СофтПро" для автоматизации работы предприятия связи / В.Б. Малахов // Мобильные системы. Спецвыпуск по биллинговым системам М.-1999.-С. 4-8.

[6] Треногин Н.Г. Методика размещения данных при проектировании биллинговых систем / Н.Г. Треногин, В.И. Терехов // Мобильные системы. -М.-2002.-№3.-С. 32-34.