УДК 004.056

Ю. В. ЛЫКОВ, канд. техн. наук

РЕЗУЛЬТАТЫ ЭКСПЕРИМЕНТАЛЬНОГО ИССЛЕДОВАНИЯ ТЕЛЕФОННЫХ РАДИОЗАКЛАДНЫХ УСТРОЙСТВ МЕТОДОМ НЕЛИНЕЙНОЙ ЛОКАЦИИ

Введение

Среди всего многообразия способов несанкционированного перехвата информации особое место занимает прослушивание телефонных переговоров, поскольку телефонная линия – самый удобный и при этом самый незащищенный источник связи между абонентами в реальном масштабе времени. На начальном этапе развития телефонной связи никто особо не задумывался о защите линий от прослушивания, и электрические сигналы распространялись по проводам в открытом виде. В наше время прослушивание телефонной линии можно осуществлять, не заходя в помещение, при минимальных затратах и минимальном риске. Нужно просто подключить к телефонной линии (ТЛ) объекта специальное приемопередающее или регистрирующее устройство.

С точки зрения безопасности телефонная связь имеет еще один недостаток: возможность перехвата речевой (акустической) информации из помещений, по которым проходит ТЛ и где подключен телефонный аппарат. Это осуществимо даже тогда, когда не ведутся телефонные переговоры (так называемый микрофонный эффект телефона и метод высокочастотного навязывания). Для такого перехвата существует специальное оборудование, которое подключается к ТЛ внутри контролируемого помещения или даже за его пределами.

На данный момент разработано большое количество методов и средств защиты ТЛ, которые при их комплексном использовании позволяют достаточно эффективно закрыть данный канал утечки информации. Однако зачастую более целесообразно не защищать линию связи, а выявить сам факт несанкционированного доступа к ней, с последующим разоблачением злоумышленника, что позволит полностью исключить применение им других более совершенных методов (средств) съема информации. Для этих случаев разработаны различные средства контроля ТЛ, среди которых самыми эффективными являются рефлектометры и нелинейные локаторы.

Преимущества нелинейного локатора следуют из его способности обнаруживать:

- неработающие в данный момент закладные устройства (ЗУ);
- ЗУ с дистанционным управлением, находящиеся в режиме ожидания;
- ЗУ со специальными технологиями передачи информации, служащими повышению скрытности их работы (узкополосная модуляция, передача сигналов короткими сериями после их предварительного накопления в запоминающем устройстве, использование нескольких несущих частот, различные сложные виды модуляции и др.).

Постановка задачи

Известные публикации дают достаточно подробное изложение метода нелинейной локации (НЛ) при облучении электромагнитной волной полупроводниковых элементов, описание принципов работы устройств, реализующих этот метод, при этом практически отсутствует информация о средствах реализующих данный метод для поиска закладных устройств (ЗУ) именно в телефонных (проводных) линиях связи, которые имеют свою специфику применения.

Цель работы – рассмотрение метода нелинейной локации и экспериментальное исследование его возможностей для поиска радиозакладных устройств в телефонных линиях (ТЛ). Данная статья является продолжением работы [1], в которой изложены результаты моделирования метода НЛ в САПР OrCad 9.2.

Экспериментальное исследование нелинейных свойств ЗУ в ТЛ методом НЛ

В основе экспериментальной установки использовался персональный компьютер с ПО *Spectra Plus*. В качестве генератора гармонического сигнала применялась внешняя звуковая карта *Creative Sound Blaster Live 5.1 USB*. Сигнал отклика, снимаемый с резистора номиналом 51 *Ом*, подключенного последовательно в ТЛ, подавался на линейный вход звуковой карты. Линия передач состоит из двух участков (15 и 20 *м*) провода марки ТРП (диаметр токопроводящей жилы 0.5 *мм*) разъединённых ЗУ. В качестве ЗУ применялись различные физические модели (диоды, диодный мост, микросхемы) и малогабаритное подслушивающее устройство с питанием от ТЛ, смонтированное в одной из розеток для подключения телефонного аппарата. Второй конец ТЛ (ближний к АТС) при параллельном подключения к ней ЗУ размыкался, при последовательном – закорачивался. Функциональная схема экспериментальной установки показана на рис. 1

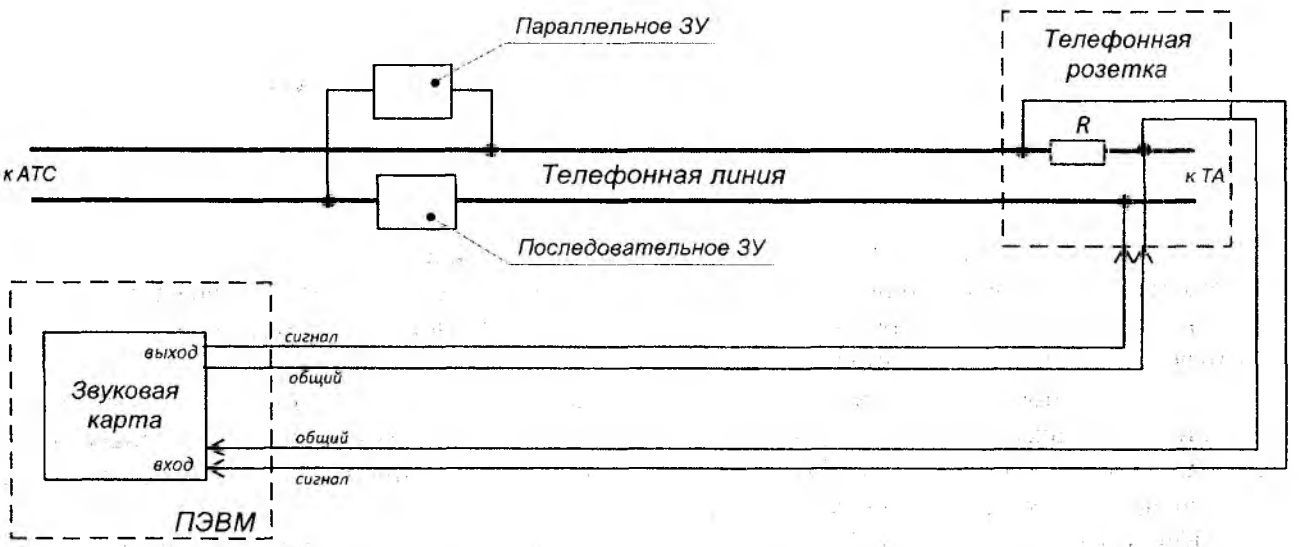

Рис. 1. Функциональная схема экспериментальной установки

До начала поиска ЗУ проведено исследование уровня шума в линии при отключенной АТС. Результаты показаны на рис. 2.

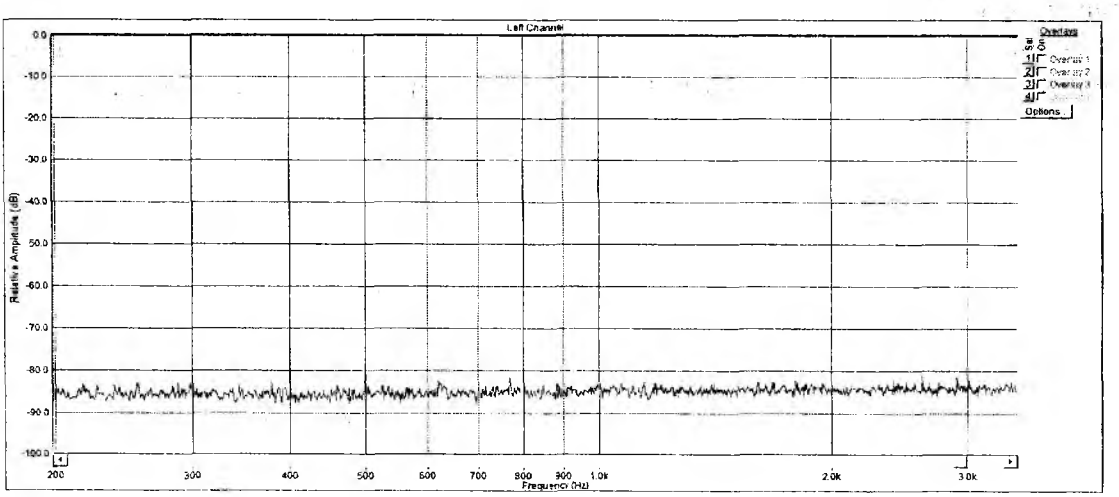

Рис. 2. Спектр шума в ТЛ

Как видно из рис. 2, уровень шума в исследуемой ТЛ не превышает 80 *дБ*.

Получен спектр отклика сигнала от НЛ в ТЛ подключенной к АТС (микроАТС К16010) результат показан на рис. 3.

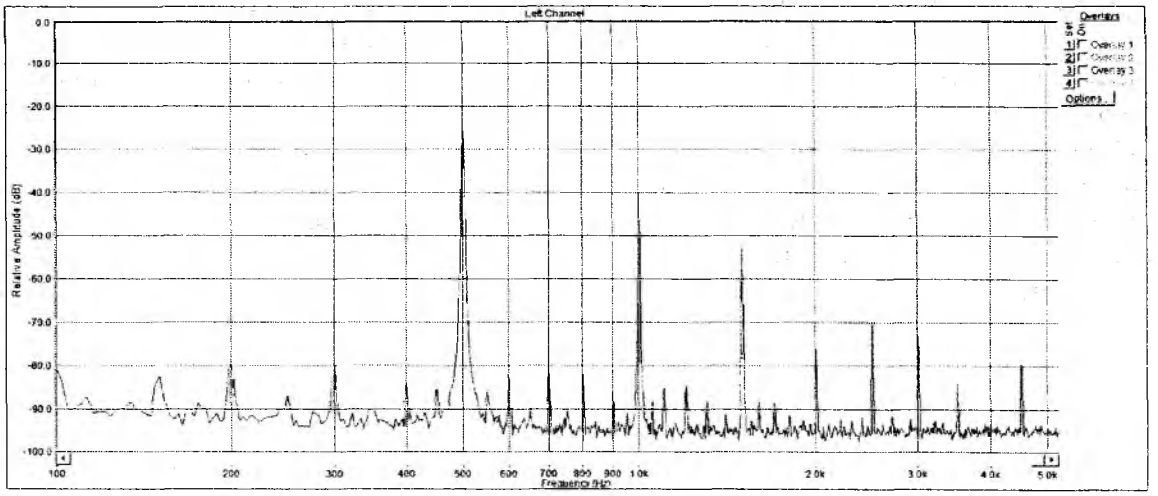

Рис. 3. Спектр сигнала в ТЛ при подключенной АТС

Проведенный эксперимент (рис. 3) показывает, что исследуемая на наличие закладны устройств линия обязательно должна быть отключена от АТС, которая вызывает значитель ные нелинейные искажения. Это подтверждает необходимость отключения всех известны нагрузок и источников питания от линии.

В работе проанализированы нелинейные свойства некоторых диодов как простейши моделей ЗУ, спектр отклика от диода Д2 показан на рис. 4. Для оценки нелинейных свойст выбран параметр *THD (Total Harmonic Distortion)* – коэффициент гармоник. Данный пара метр вычисляется автоматически программой *Spectra Plus*.

Как правило, на входе ЗУ находится диодный мост, упрощающий злоумышленник подключение к ТЛ, поэтому было уделено внимание исследованию диодного моста как воз можной модели ЗУ. Кроме того, исследованы нелинейные свойства микросхем, которы могут применяться в ЗУ, в частности стабилизаторы напряжения 7805с и LM7905C.

Наиболее показательным является поиск реального ЗУ, которое последовательно под ключено к телефонной линии в месте соединения ТЛ с контактной розеткой и спрятан в ней. Данное ЗУ питается от ТЛ, его рабочая частота составляет 433 *МГц*, в схеме использу ется фильтр на ПАВ. Спектр отклика от данного закладного устройства показан на рис. 5.

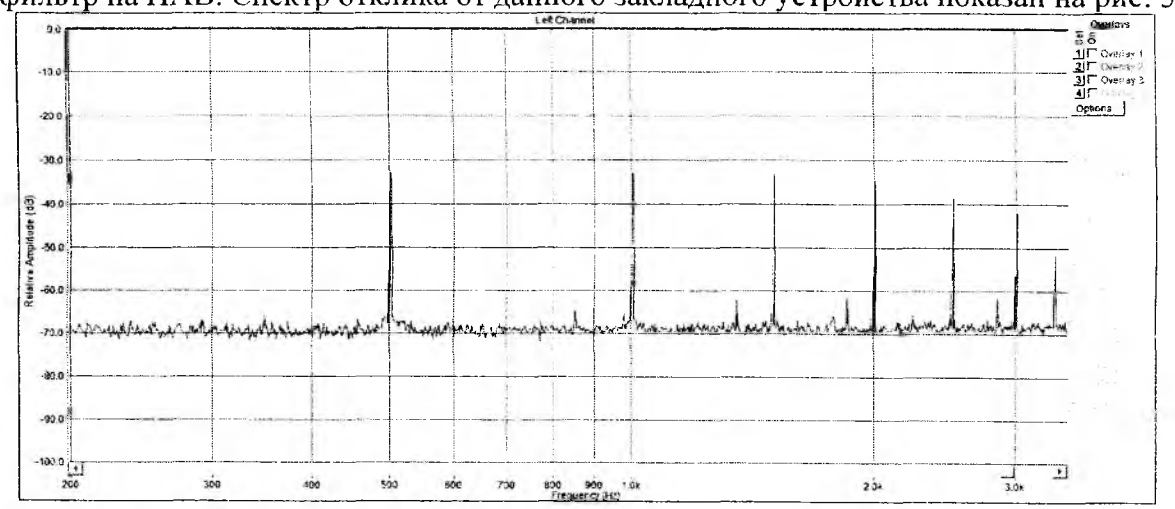

Рис. 4. Спектр отклика от диода Д2

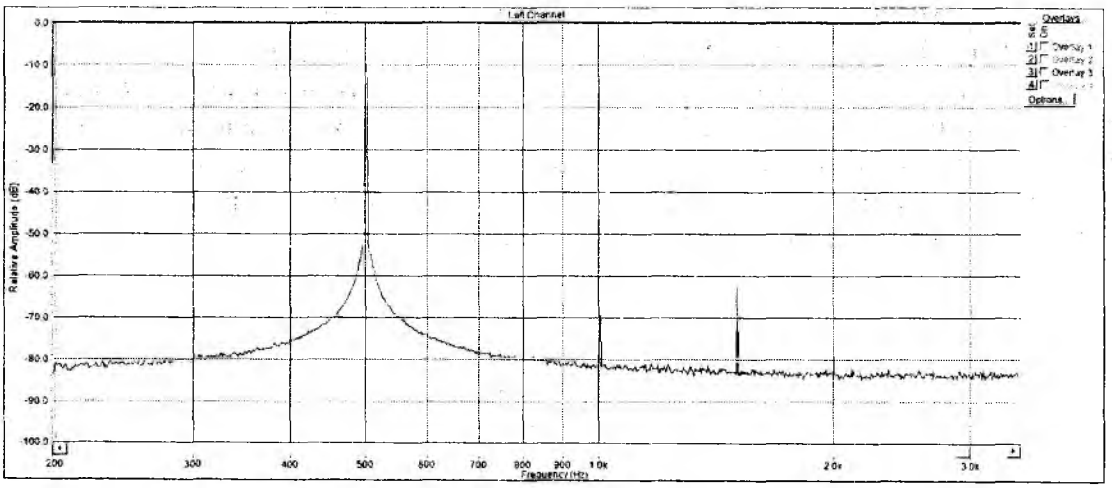

Рис. 5. Спектр отклика от ЗУ

Как видно из рис. 5, первая гармоника на 60 *дБ* превышает вторую и на 50 *дБ* – третью, коэффициент нелинейных искажений равен 0,22 %. Несмотря на незначительное значение коэффициента гармоник, по полученной спектрограмме можно достаточно точно идентифицировать наличие нелинейного элемента. Значения параметра нелинейных искажений для каждого исследуемого объекта сведены в таблицу:

Объект исследования	Коэффициент гармоник
Диод Д2	1,41
Диод Д9	1,52
Диод Д226	1,60
Диодный мост КЦ406	0,73
Микросхема 7805с	1,28
Микросхема LM7905C	0,54
Телефонное закладное устройство №1	0,01
Телефонное закладное устройство №2	0,32

В результате экспериментального исследования, а также моделирования [1] были обнаружены все используемые в работе телефонные ЗУ и их простые физические и математические модели.

Возможности метода НЛ наглядно продемонстрированы на рис. 6. Максимально неуязвимыми для устройств контроля ТЛ, в том числе и для НЛ, являются ЗУ с индуктивным подключением, которое в свою очередь может быть реализовано через трансформатор или магнитную рамку. При использовании достаточно высоких напряжений (для кабеля ТРП,ТРВ, испытательное напряжение в течение 1 *мин* составляет 1000 *В* [3]) зондирующего сигнала возникает потенциальная возможность и по обнаружению ЗУ с индуктивным подключением к ТЛ.

Кроме того, методом НЛ возможно обнаруживать устройства съема акустической информации в помещении, реализующие метод ВЧ-навязывания.

Разработка требований к нелинейному локатору

Основными параметрами нелинейного локатора являются: частота зондирующего (выходного) сигнала; выходное напряжение; коэффициент гармоник выходного сигнала; динамический диапазон измеряемых уровней сигнала на частотах гармоник.

В качестве частоты зондирующего сигнала нелинейного локатора целесообразно выбирать частоты менее 20 *кГц*, так как при этом обеспечивается максимальное отношение сигнал/шум. Кроме того, для минимизации влияния помех от сети питания 220 *В* необходимо чтобы частоты гармоник были не кратны частоте 50 *Гц*. Для повышения достоверности получаемых результатов необходимо предусмотреть возможность перестройки нелинейного локатора по частоте. С другой стороны, для повышения скрытности проведения поисковых работ частота зондирующего сигнала должна быть выше 16 *кГц*.

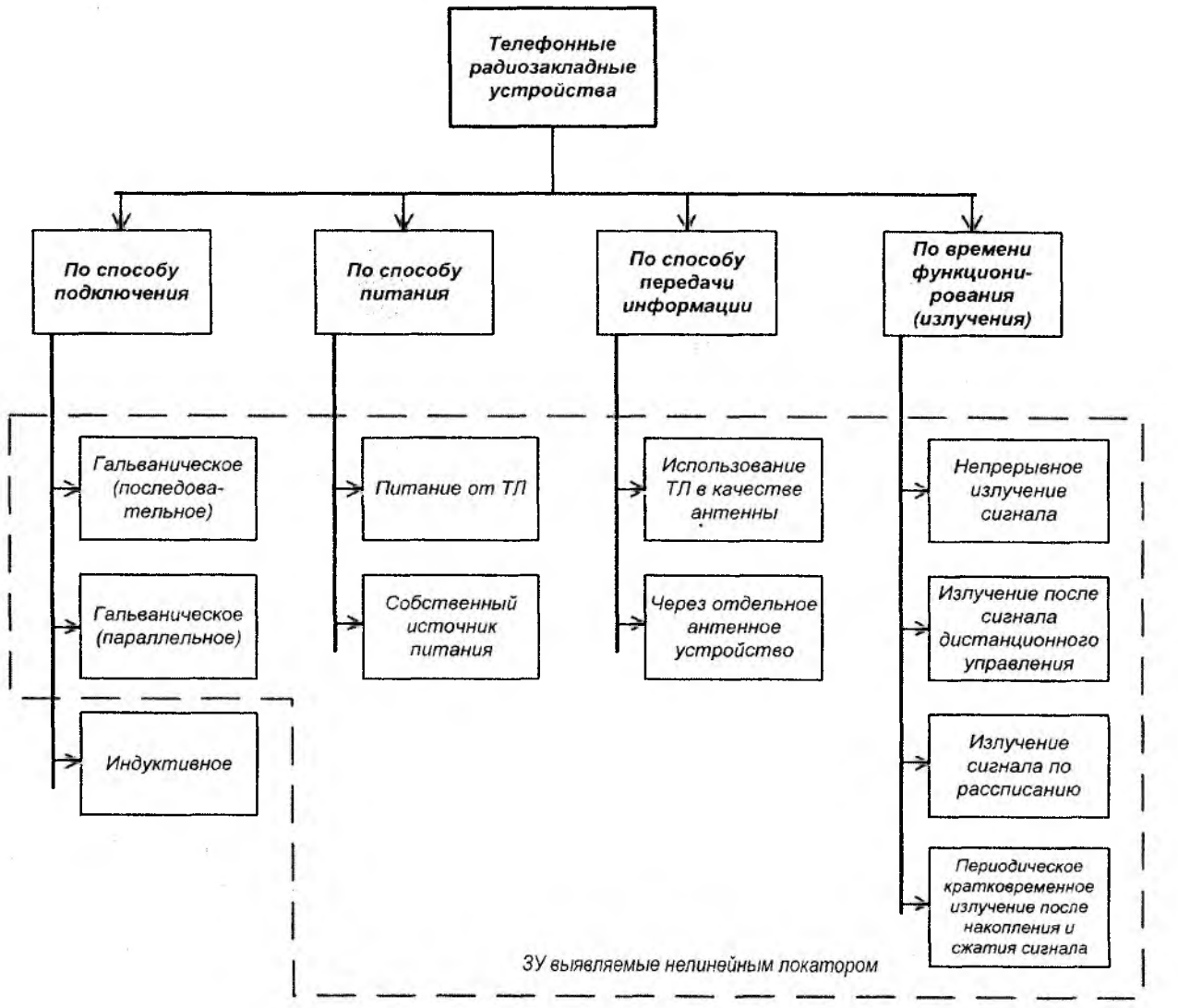

Рис. 6. Классификация телефонных радиозакладных устройств

Исходя из значений рабочего затухания абонентской линии телефонной сети на частоте 1000 *Гц*, которое согласно [4] должно быть не более 5,0 *дБ* и уровнем тепловых шумов в линии -90 *дБВ* (для линии длиной 500 *м*, полосы частот 20 *кГц*, комнатой температуры), а также возможного дополнительного затухания (1 – 5 *дБ*), вызванного подключенным ЗУ, для обеспечения динамического диапазона измерения 70 *дБ* (рис. 5) необходимо максимальное значение выходного напряжения нелинейного локатора порядка 1 – 10 *В*.

Коэффициент гармоник зондирующих сигналов согласно данным эксперимента и моделирования должен быть менее 0,1 %. Для его уменьшения, например при использовании некачественной внутренней звуковой карты ПЭВМ, можно использовать режекторные фильтры, настроенные на частоты второй и третьей гармоник.

Для активации некоторых ЗУ и введение их в рабочий режим в схеме должен быть предусмотрен источник постоянного напряжения на 10 – 15 *В*. В результате обобщённая функциональная схема нелинейного локатора показана на рис. 7.

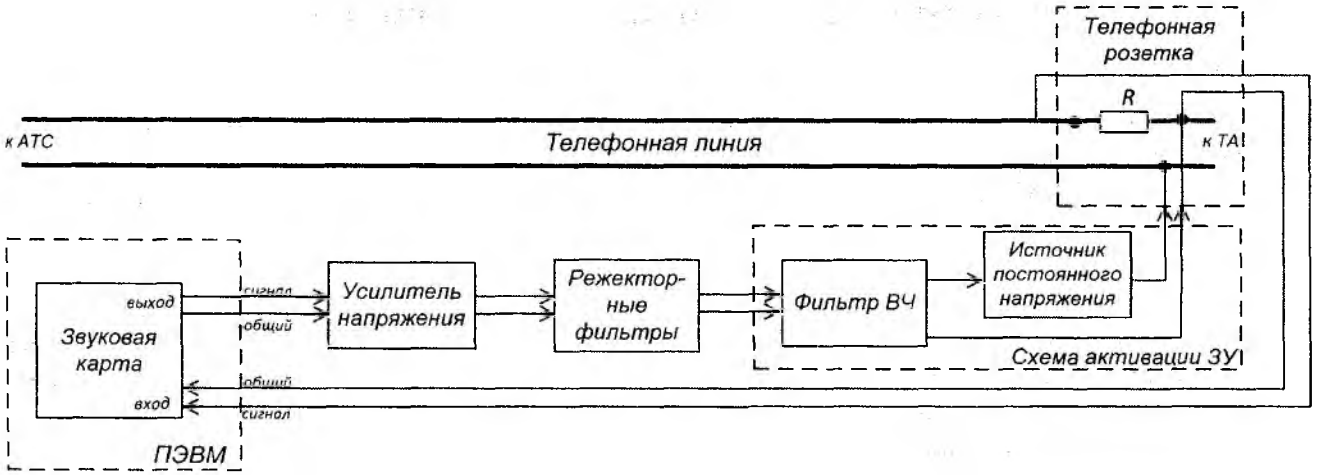

Рис. 7. Обобщённая функциональная схема нелинейного локатора

Выводы

В работе исследован метод нелинейной локации применительно к поиску радиозакладных устройств в проводных телефонных линиях связи. В результате натурных испытаний получено следующее:

- диапазон коэффициентов гармоник для физических моделей ЗУ и реальных ЗУ лежит в пределах от 0,01 до 1,5;

- при небольших протяженностях линии связи и малом уровне помех в качестве аппаратной реализации нелинейного локатора может использоваться ноутбук с качественной звуковой картой, что значительно доступнее, чем применение специализированных нелинейных локаторов. При исследовании протяженных ТЛ или/и высоком уровне помех может потребоваться внешний усилитель на выходное напряжение 10 *В*;

- применение метода нелинейной локации телефонной линии позволяет обнаружить подключение большинства используемых злоумышленниками типов телефонных закладных устройств.

Список литературы: 1. *Лыков, Ю.В.* Поиск радиозакладных устройств в телефонной линии методом нелинейной локации / *Ю.В. Лыков* // Восточно-Европейский журнал передовых технологий. – Харьков : Технологический центр, 2012. – №6/9 (60). – С.56-72. 2. *Вернигоров, Н.С.* Принцип обнаружения объектов нелинейным локатором // Защита информации. Конфидент. – 1998. – №4. –С. 65-70. 3. *ГОСТ* Р 51311-99. Кабели телефонные с полиэтиленовой изоляцией в пластмассовой оболочке. Технические условия. – Введ. 2000-07-01. – М. : Изд-во стандартов, 2000. – 27 с. 4. *ОСТ 45.83-96* Сеть телефонная. Линий абонентские кабельные с металлическими жилами. Нормы эксплуатационные. – Введ. 1997-22-12. – М. : Изд-во стандартов, 1997. – 15 с.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 13.09.2012