3 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації

УДК 004.73.004

К ВОПРОСУ ОБ АКТИВНОЙ ЗАЩИТЕ КАНАЛОВ ТЕЛЕФОННОЙ СВЯЗИ

Александр Провозин, Максим Олейник, Александр Сытник*, Виталий Василевский*, Николай Ковинченко*, Вячеслав Абрамов*, Ульян Пейков*
ОАО «НИИ электромеханических приборов»
**НИЦ «ТЕЗИС» НТУУ «КПИ»*

Аннотация: **Рассматривается вопрос создания устройств активной защиты каналов телефонной связи.**
Sammary: **Is regarded an issue creations of devices of fissile protection of telephone channels**
Ключевые слова: **Активные методы защиты, генератор шума.**

I Введение

Активные методы защиты основаны на создании преднамеренных помех, маскирующих информативные речевые сигналы, при этом уровень преднамеренной помехи в δ-раз должен превышать уровень маскируемого сигнала. Уровень преднамеренных помех ограничивается соответствующими нормами (например, «Нормы 9-72» «Устройство проводной связи», ГОСТ 23511 или дополнительными условиями электромагнитной совместимости (ЭМС) РЭС на объекте установки при размещении РЭС в составе комплекса).

Дальнейшее повышение эффективности преднамеренных помех без увеличения их уровней возможно при учете свойств маскируемых сигналов и помех.

Максимальная эффективность достигается в том случае, когда помеха и маскируемый сигнал имеют подобные статистические характеристики при их взаимной независимости.

II Постановка задачи

Основным условием создания устройства активной защиты каналов телефонной связи является разработка эффективного генератора шума (ГШ) для маскирования полезной информации, усилителя и оконечных устройств подачи шумов в каналы утечки информации.

III Направление разработки устройств активной защиты каналов телефонной связи

Устройства активной защиты можно разделить на 3 функциональные части. Прежде всего необходим ГШ, создающий случайный процесс со статистическими характеристиками, близкими к защищаемой информации и, таким образом, способный маскировать последнюю. Далее необходима аппаратура, которая моделирует преобразования сигнала при прохождении его от информационного тракта до канала утечки (фильтрация, модуляция и т. п.) и, наконец, последнее звено необходимо для переноса сформированного сигнала в конкретный канал утечки (эффективной «накачкой» его шумом). Применительно к защите каналов телефонной связи устройства защиты могут иметь блок-схему, представленную на рис. 1.

Рассмотрим основные принципы, на которые нужно ориентироваться при проектировании генераторов шума для защиты аппаратуры передачи речевой информации в каналах связи.

Сформулируем основные требования, предъявляемые к генераторам шума, а затем рассмотрим способы генерации необходимых сигналов. Из определения функционального назначения ясно, что основным свойством, которое мы ожидаем от шума, должно быть свойство наилучшим образом маскировать информативный речевой сигнал.

Так как АЧХ оптимального приемника априорно устанавливается в соответствие со спектром ожидаемой информации (речи), то для минимизации соотношения сигнал/шум на детекторе приемника необходимо, чтобы энергетический спектр шума был подобен спектру речи. Во-вторых, два шумовых процесса одинаковой спектральной и суммарной мощности, но с разными законами распределения амплитуд, по разному будут маскировать сигнал, т.к. количество информации, определяемое энтропийной мощностью у

них различно. Известно [1], что наибольшей энтропийной мощностью при прочих равных условиях обладает нормальный шумовой процесс, поэтому необходимо стремиться, чтобы закон распределения генерируемого шума был близок к нормальному.

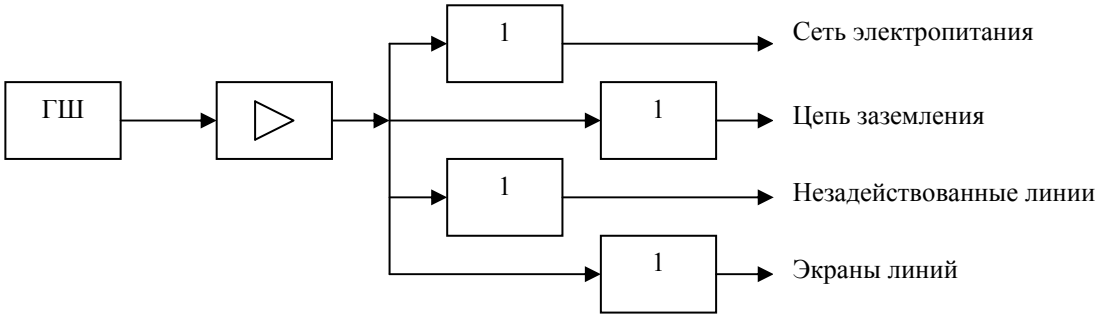

Рисунок 1

Для моделирования спектра речи обычно используют АЧХ передачи RC-цепи, образующей фильтр нижних частот первого порядка с частотой среза ~500 Гц. Если пропустить через такой фильтр широкополосный белый шум, то получим, так называемый «розовый» шум.

В дальнейшем мы также будем пользоваться этим термином, хотя он и не совпадает с общетехническим определением «розового» шума (как шума с равными энергиями в равных относительных частотных полосах). В связи с введением понятия «розового» шума отметим, что такой шум предпочтительно применять в устройствах защиты, и даже установлено соотношение сигнал/шум, гарантирующее маскирование сигнала.

Отметим еще одно необходимое свойство шума – за пределами частотной полосы речи мощность шумов должна быть минимальной. Это требование вытекает из того, что, во-первых, эта часть шумов не принося никакой пользы только перегружает последующие каскады аппаратуры зашумления и, во-вторых, взаимодействуя с высокочастотными сигналами преобразуется по частоте в полосу речи и увеличивает шумы фонограммы.

Таким образом, для зашумления каналов утечки речевой аппаратуры необходим генератор шума, формирующий нормальный шумовой процесс со спектром, равномерным до 500 Гц со спадом 6 дБ/октава до частот 10 – 15 кГц.

За пределами этого диапазона мощность шума должна быть минимальной. Для активной защиты каналов, в которых характерна утечка огибающей речевого сигнала, необходим шум с равномерным спектром от 0,1 – 2 Гц до 100 Гц и далее со спадом 6 дБ/октава до частот 10 – 15 кГц.

Рассмотрим возможные методы получения шумовых сигналов и, соответственно, способы построения ГШ.

Наиболее просто воспользоваться газоразрядными или полупроводниковыми шумовыми диодами, например, типа 2Г401, которые характеризуются весьма высокой спектральной плотностью шумового напряжения (~10 мкВ/Гц ½) или стабилитронами. Однако ГШ, собранные на основе диодов, обладают существенными недостатками. ТУ на диод 2Г401 гарантирует неравномерность спектра в 3 дБ только для диапазона частот от 200 кГц до 1 МГц, хотя имеются данные, что генерируются шумы и в районе 20 Гц.

Шум диапазона огибающей нельзя получить фильтрацией широкополосного шума, а амплитуду «розового» шума необходимо увеличить по крайней мере на величину неравномерности спектральной характеристики диода в речевом диапазоне. Если учесть, что указанная неравномерность неизвестна, а увеличение мощности шума может привести к уменьшению динамического диапазона в тракте основного сигнала, то использование таких источников шума весьма нежелательно.

Следует также добавить, что получаемое от диодного ГШ напряжение шума имеет температурную нестабильность 2 % /°С, а при замене диода может существенно изменяться (например, для 2Г401Б от 3 до 35 мкВ/Гц ½). Наиболее подходящим и стабильным по параметрам является диод 2Г401В.

Шумовые диоды широко применяются для генерации шумов, особенно в простейших устройствах с невысокими метрологическими характеристиками. Уменьшить указанные недостатки удается применением различных схемных методов построения ГШ на диоде. Так для получения низкочастотных шумов можно воспользоваться методом переноса спектра по частоте с помощью дополнительного гетеродина или амплитудного ограничителя [2], при котором спектральные составляющие из области высоких частот

переносятся вниз вплоть до нулевых частот. Получить шумы низких частот можно также путем амплитудного детектирования узкополосного шума. Однако в данном случае получается шум с релеевским распределением амплитуд.

Схема генератора шума на р-п переходе транзистора представлена на рис. 2, а. В рассматриваемом примере она реализована на транзисторной сборке типа КР158НТ1, однако для транзисторов сборки не нормируется спектральная плотность шумового напряжения.

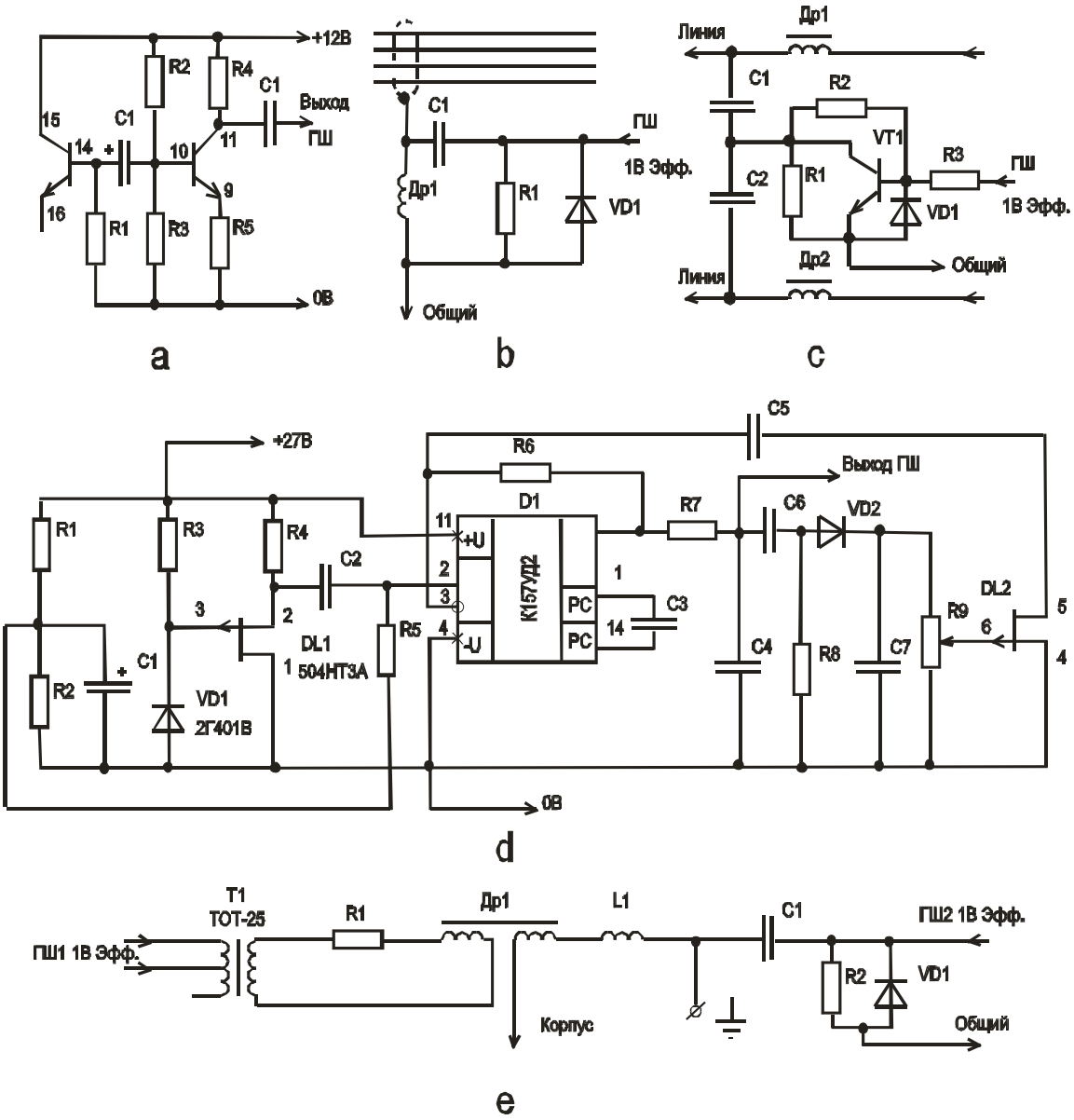

Рисунок 2 – Схемы электрические: a) ГШ на транзисторе; b) подключение ГШ к экранам линий; c) подключение ГШ к линии; d) ГШ на диоде; подключение ГШ к корпусу

Описанные способы требуют довольно сложной аппаратурной реализации, трудоемки в настройке, не позволяют получить стабильные уровни шумов.

Избавиться от недостатков, присущих аналоговым методам генерации шумов можно, перейдя к цифровым методам [3], которые дают возможность реализовать более стабильные по времени и температуре процессы, спектр которых простирается вплоть до самых низких частот, однако электрические схемы цифровых ГШ получаются сложнее аналоговых.

Если не предъявляются жесткие требования по температурным и временным параметрам, то предпочтение отдают простым схемам ГШ на шумовых диодах. Схема ГШ на диоде 2Г401В представлена на рис. 2, d. Указанный генератор обладает равномерным спектром шумов в полосе частот 100 – 10000 Гц.

Для зашумления экранов линий связи разговорного тракта используется схема подключения ГШ, представленная на рис. 2, b, для зашумления корпуса аппаратуры используется схема подключения ГШ, представленная на рис. 2, e, а для зашумления незадействованных линий связи используется схема подключения ГШ, представленная на рис. 2, c.

IV Выводы

Для эффективной активной защиты каналов телефонной связи в качестве простейших устройств с невысокими метрологическими характеристиками может быть рекомендован аналоговый ГШ на шумовом диоде типа 2Г401В с зашумлением цепей экранов линий связи, корпуса аппаратуры, незадействованных линий связи и сети электропитания.

Литература: ***1.*** *«Справочник по теоретическим основам радиоэлектроники» под ред.Кривицкого Б. Х. в 2-х ч, т.1, т.2. – М.: «Энергия», 1977.* ***2.*** *Тетерич Н. М. «Генераторы шума и измерение шумовых характеристик». – М.: «Энергия», 1968.* ***3.*** *Алексеев А. И. «Теория применения псевдослучайных сигналов». – М.: Наука, 1969*

УДК 621.391:519.2

НЕЛИНЕЙНОЕ СЛУЧАЙНОЕ КОДИРОВАНИЕ В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ ПО КАНАЛУ СВЯЗИ С ОТВОДОМ

Антон Алексейчук, Сергей Гришаков
СФ СБ Украины в составе ВИТИ НТУУ "КПИ"

Аннотация: **Получены неасимптотические границы вероятности оптимального приема сообщений в отводном канале системы передачи информации со случайным кодированием, построенной на основе произвольной устойчивой функции над конечной абелевой группой. Описаны алгоритмы случайного кодирования и декодирования сообщений в основном канале с использованием нелинейных систематических кодов. Рассмотрен пример системы передачи со случайным кодированием, построенной на основе кодов Препараты.**

Summary: **Non-asymptotically bounds for the probability of optimal messages decoding in the wiretap channel of a information transmission system with random coding by a arbitrary resilient function over an Abelian group, are obtained. Algorithms of random messages coding and decoding in main channel which use non-linear systhematic codes, are described. An example of the information transmission system with random coding by Preparata codes is considered.**

Ключевые слова: **Криптографическая защита информации, случайное кодирование, отводной канал, устойчивая функция, нелинейный систематический код, код Препараты.**

I Введение

Концепция отводного канала, основанная на теоретико-информационной модели системы передачи дискретных сообщений по "каналу связи с подслушиванием" ("wire-tap channel") была впервые предложена в [1] и в дальнейшем получила развитие в [2 – 8] и ряде других работ. В настоящее время эта концепция охватывает широкий круг теоретических и прикладных задач в областях криптографии и стеганографии [6 – 10], позволяя строить унифицированные математические модели вероятностно-криптографических систем [11] и решать, в определенной степени, едиными общими методами различные по своей прикладной направленности криптографические задачи.

В рамках классической концепции отводного канала, в последние годы заметное развитие получило направление, имеющее своей задачей разработку математических основ теории кодовой защиты информации [5], включающей, в том числе, методы построения неасимптотических оценок стойкости и практически эффективных алгоритмов кодирования-декодирования сообщений в системах передачи информации по каналу связи с отводом [3, 4, 12 – 17]. Наиболее подробно изученный класс таких систем составляют системы передачи с линейным случайным кодированием в двоичном симметричном канале, являющиеся традиционным объектом исследования в теории кодовой защиты [1, 3 – 5].