Если в качестве примера взять систему, имеющую 1000 абонентов, каждый из которых передает в сутки один сигнал с длительностью t_c =0,1с, то вероятность совпадения можно вычислить по формуле

$$p_c = p_n^2 q^{998} C_{1000}^2 \text{, где } C_{1000}^2 = \frac{1000!}{2!\cdot(1000-2)!}. \quad (5)$$

После подстановки значений в выражение (5) и вычислений получим численное значение p_c порядка 10^{-6}.

Широко используемый способ повышения надежности СПИ (в нашей задаче – повышения вероятности правильного приема сообщения на ПЦО) – это дублирование (неоднократный повтор) сообщения. При этом целесообразно использовать не просто повтор сообщения через определенный интервал времени, а повтор со случайным временным сдвигом. Тогда вероятность полного совпадения двух сигналов будет практически равна нулю. Чтобы полностью подавить сигнал в этом случае необходимо, чтобы каждый из сигналов пачки совпадал с разными сигналами взаимных помех.

Приведенная выше методика расчета соответствуют первому случаю (равномерному распределению $p_1(t)$). Для второго примера допущение, сделанное выше, становится некорректным. В этом случае необходимо либо оценивать плотность распределения вероятности $p_2(t)$ и вероятность попадания в интервалы времени Δt максимальной загрузки канала, а также аппарат теории массового обслуживания.

Литература: 1. В. В. Волхонский. Системы охранной сигнализации. Экополис и культура. СПб., 2000, 160 с. 2. Варакин Л. Е. Системы связи с шумоподобными сигналами. –М., Радио и связь, 1985, 384 с. 3. Защита от радиопомех. – М., под ред. Максимова М. В., Сов. радио, 1976, 496 с. 4. В. В. Волхонский Оценка помехоустойчивости нелинейных алгоритмов обработки сигналов. Радиоэлектроника". Известия МВ и ССО СССР, т. 30, № 4, 1987.

УДК 621.96

ПРОБЛЕМНЫЕ АСПЕКТЫ РЕАЛИЗАЦИИ ПРОСТРАНСТВЕННОГО И ЛИНЕЙНОГО ЗАШУМЛЕНИЯ В СИСТЕМАХ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Сергей Емельянов, Николай Логвиненко, Виталий Носов, Владимир Писаревский
Национальный университет внутренних дел, г. Харьков

Аннотация: **Обоснована необходимость разработки генераторов шума, реализующих пространственное и линейное зашумление опасных сигналов в электромагнитном и электрическом каналах утечки информации. Приведены результаты экспериментальных исследований макетов разработанных генераторов шума, оценена эффективность их применения.**

Summary: **Necessity of creation of generators of noise is proved. Generators create a radio noise in space and in an electric network. Results of experiments are given. Efficiency of application of the developed generators is appreciated.**

Ключевые слова: **Генератор шума, радио закладка , сетевая закладка.**

I Введение

Одним из путей реализации угроз конфиденциальности информации, обрабатываемой средствами электронно-вычислительной техники (ЭВТ), являются технические каналы утечки информации (КУИ) [1–3]. Среди технических КУИ большую опасность для компьютерной информации представляют электромагнитный и электрический каналы. Первый из них может быть образован побочными электромагнитными излучениями (ПЭМИ) средств ЭВТ, а также за счет скрытно установленных закладных устройств с передачей информации по радиоканалу – радио закладка (РЗ). Источниками опасных сигналов во втором канале могут быть наводки ПЭМИ на цепи электропитания, просачивающиеся в них информационные сигналы средств ЭВТ, а также закладные устройства с передачей информации по электросети – сетевая закладка (СЗ) [2, 3].

Для блокировки указанных КУИ в системах активной защиты информации используют методы

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

пространственного и линейного зашумления, реализуемые с помощью генераторов шума (ГШ). Однако существующие сертифицированные ГШ радиодиапазона ("Волна", "Гамма", "Смог", "Гром" и др.) и сетевые ГШ (NG-201, "Соперник", SP-41G, "Соната-С", "Цикада-С" и др.) характеризуются недостаточно широким диапазоном защищаемых частот, значительными массогабаритными показателями, относительно высокой стоимостью, ограниченной мобильностью и др.

В этих условиях актуальной задачей является разработка недорогих отечественных ГШ, лишенных отмеченных недостатков.

II Результаты исследований ГШ

В рамках решения указанной задачи на кафедре "Защиты информации и спецтехники" Национального УниВД были разработаны и исследованы макеты ГШ радиодиапазона (рис. 1) и сетевого ГШ (рис. 2). Характеристики и результаты исследований ГШ радиодиапазона были приведены в [4]. Здесь отметим только, что ГШ (рис. 1) содержит два независимых антенных выхода: - высокочастотный (ВЧ) – 1 и низкочастотный (НЧ) – 2. Наличие двух выходов позволяет использовать различные типы антенных систем, близких к оптимальным в этих диапазонах, например, штыревую телескопическую – 3 и проволочную Г-образную – 4 антенны.

Достигнутое расширение границ диапазона защищаемых частот до 1500 МГц позволяет маскировать ПЭМИ до 3-й гармоники тактовой частоты $F_{такт}$ = 500 МГц, что актуально для современных средств ЭВТ [5]. По другим техническим характеристикам (выходная и потребляемая мощность, коэффициент качества помехи и др.) разработанное устройство аналогично переносному ГШ SP-21B1 ("Баррикада", Россия) [7].

Одним из проблемных аспектов в реализации метода пространственного зашумления является декларируемая некоторыми разработчиками ГШ возможность их эффективного применения для подавления акустических РЗ [2, 7]. Оценка возможностей подавления существующих РЗ с помощью серийно выпускаемых ГШ может проводиться на основе энергетического критерия, который требует знания технических характеристик и параметров подавляемых средств [8].

Выходная мощность ГШ, подводимая к его слабонаправленной антенне, составляет $P_{ш}$ = (2…10) Вт. Помеха имеет относительно равномерный спектр, характерный для “белого” шума, и перекрывает диапазон частот $\Delta F_{ш}$ = 5 кГц...1000 МГц. Тогда спектральная плотность мощности ГШ составляет величину $N_{ш} = P_{ш}/\Delta F_{ш} \approx$ (2…10) мкВт/кГц, что достаточно для маскировки ПЭМИ средств ЭВТ [2, 4].

Типовые РЗ содержат, как правило, собственно микрофон, определяющий зону акустической чувствительности закладки, радиопередатчик, выносную слабонаправленную антенну и источник питания (ИП) [2, 3]. Выходная мощность радиопередатчика лежит в пределах $P_{РЗ}$ = (1…500) мВт и напрямую связана с дальностью передачи РЗ и временем непрерывной работы ИП. Диапазон рабочих частот РЗ лежит в пределах $\Delta F_{раб}$ = (100…1000) МГц (VHF/UHF) и перекрывается рабочим диапазоном ГШ. В радиопередатчике используется, как правило, узкополосная (NFM) или широкополосная (WFM) частотная модуляция. Ширина спектра информационных сигналов РЗ на основных гармониках излучения составляет $\Delta F_{РЗN}$ = (6…12) кГц и $\Delta F_{РЗW}$ = (120…180) кГц и более. Тогда спектральная плотность мощности РЗ для указанных вида и параметров модуляции равна, соответственно, $N_{РЗN} = P_{РЗ}/\Delta F_{РЗN} \approx$ (0.1…100) мВт/кГц и $N_{РЗW} = P_{РЗ}/\Delta F_{РЗW} \approx$ (0.01…5) мВт/кГц. Очевидно, что $N_{ш} < N_{РЗW}$ и $N_{ш} << N_{РЗN}$, то есть условие маскировки информационных сигналов РЗ не выполняется.

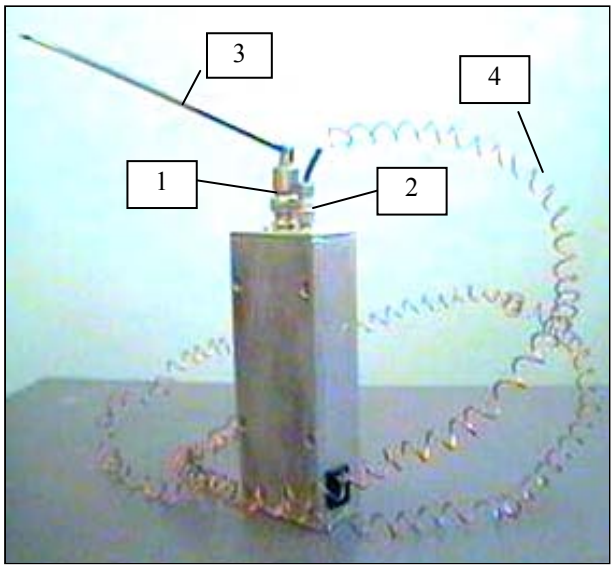

Рисунок 1 – Внешний вид ГШ радиодиапазона

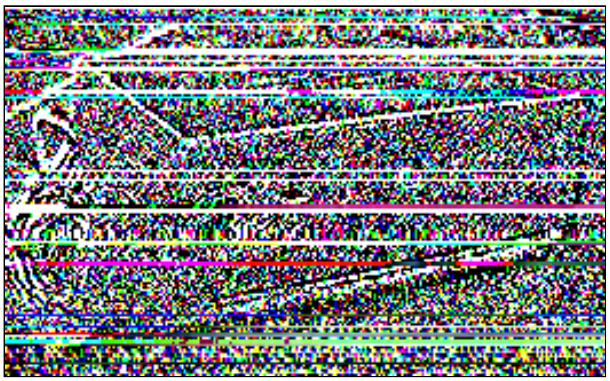

Рисунок 2 – Внешний вид сетевого ГШ

ISBN 966-622-022-9

Сказанное проиллюстрировано на рис. 3. Здесь приведены частотные панорамы (псевдоспектры) исследуемых сигналов в координатах “Уровень (дБ)-частота (МГц)” в диапазоне 200…500 МГц, полученные с помощью сканирующего приемника AR-3000A и персонального компьютера (ПК) Notebook с программной оболочкой SEDIF PLUS. Полутоном показаны сигналы радио эфира в выделенном помещении, тоном – ПЭМИ от работающего ПК типа PC 486 и гармоники сигналов РЗ1 типа РМК-120, жирной линией – огибающая спектра маскирующей помехи разработанного ГШ.

В этих условиях положительный эффект от применения ГШ заключается в упрощении (удешевлении) поиска излучающих РЗ. Он может быть проведен с помощью простых индикаторов (детекторов) поля типа D0006, ИП-4М, Interceptor R-10 и др. [2, 3, 7]. Порог срабатывания индикатора следует установить по среднему уровню шумовой помехи ГШ, превышающему на 10…15 дБ сигналы радио эфира, и перевести индикатор в "сторожевой" режим. В результате срабатывание индикатора произойдет только по сигналу РЗ1, превысившему порог.

Однако, в ряде встречающихся на практике частных случаев, обусловленных типом РЗ и условиями ведения технической разведки (ТР), применение ГШ может позволить решить задачи подавления РЗ. Рассмотрим их более детально.

1. Обычные РЗ с непрерывным излучением имеют малую продолжительность работы, ограниченную ресурсом ИП, и относительно невысокую скрытность. Одним из способов преодоления указанных недостатков является применение канала дистанционного управления (ДУ) РЗ [2, 3]. Он позволяет переводить закладку в режим излучения только по кодированному радиосигналу управления ("инициации") от передатчика, который может быть удален от РЗ на расстояние $Д_с$ = (100…500) м. Канал ДУ работает на частотах 140…170 МГц, ширина спектра сигнала управления составляет $\Delta F_{сДУ}$ = (800…1000) Гц при выходной мощности передатчика ДУ $P_{сДУ}$ = (10…50) мВт. Такие характеристики реализованы, например, в РЗ типа РК-570S, GTG 4215 и др. [2]. Следует учесть, что ГШ и РЗ с приемником ДУ находятся в одном помещении, так что дальность подавления $Д_п$ приемного устройства канала ДУ составляет единицы метров, т. е. $Д_п << Д_с$.

Для оценки требуемой мощности помехи воспользуемся уравнением противорадиосвязи, которое для случая ненаправленных антенн и подавления радиолинии шумовыми помехами в условиях свободного пространства (наихудших для подавления) имеет вид [8]

$$P_ш^{треб} \geq P_{сДУ} \left(\frac{Д_п}{Д_с} \right)^2 \frac{\Delta F_ш}{\Delta F_{сДУ}}. \qquad (1)$$

Для вышеприведенных характеристик ГШ и РЗ и условий их применения получаем из (1) $P_{ш}^{треб} \geq$ (0.2…10) Вт. Таким образом, условие подавления канала ДУ выполняется, так как $P_ш \geq P_{ш}^{треб}$.

Следует заметить, что кроме указанного существуют и другие способы увеличения времени работы закладки, например, системы VAS или VOX, автоматически включающие РЗ на излучение только при появлении в прослушиваемом помещении акустических сигналов [2, 3].

2. В некоторых случаях для повышения скрытности РЗ используется способ, заключающийся в выборе рабочей частоты закладки вблизи частоты мощного источника радио излучений с одновременным снижением излучаемой РЗ мощности [2]. В этом случае дальность действия РЗ существенно снижается. Однако гармоники его излучения маскируются сигналами и шумами радио эфира, что и затрудняет их обнаружение при радио мониторинге. Такая ситуация может иметь место, когда нарушитель находится внутри контролируемой зоны, но не имеет доступа в выделенное помещение. Снижение мощности излучения РЗ до значений сотен мВт позволяет успешно применять ГШ для их подавления. В качестве примера на рис. 3 показан сигнал маломощной РЗ2 типа РМК 0300, "спрятанный" под сигналами сотовой телефонии (СТЛФ) стандарта NMT-450.

Следует учесть, однако, что для повышения скрытности РЗ более вероятно применение кодирования сигналов и сложных видов их модуляции [2, 3].

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

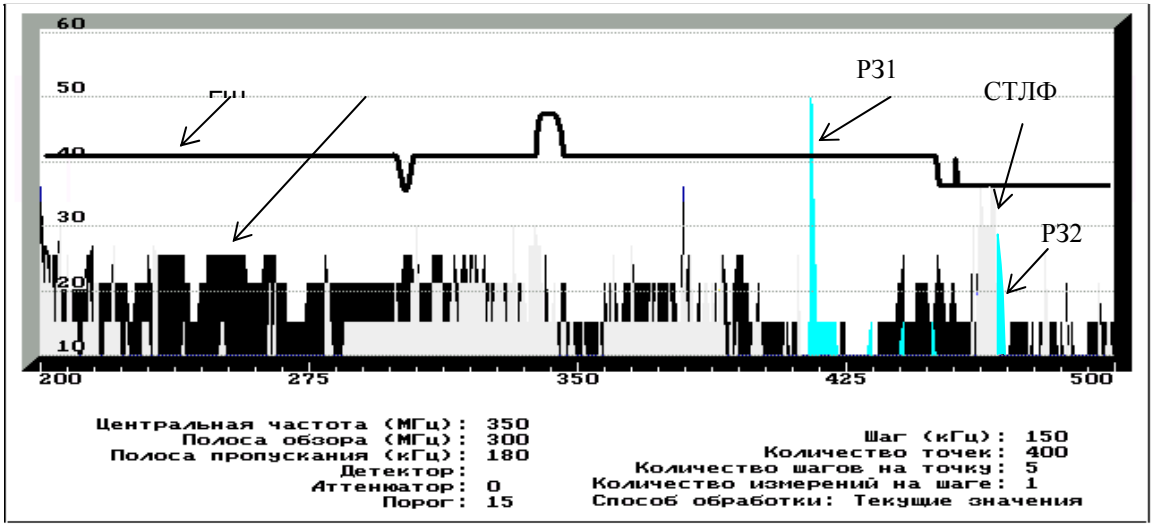

Рисунок 3 - Частотные панорамы исследуемых сигналов

3. В некоторых случаях вероятная зона ТР может быть предположительно известна. Применительно к защищаемым объектам это могут быть: стоянка автомобилей, близкорасположенные здания и автомобильные трассы, бюро пропусков и т. д. В таких ситуациях возможен вынос ГШ (или их антенных систем) в сторону зоны ТР. Вынос ГШ может привести к подавлению приемного устройства, осуществляющего съем информации с РЗ. Радиус зоны подавления приемника РЗ может быть найден из (1)

$$Д_п = Д_с \sqrt{\frac{P_ш \Delta F_{РЗ}}{P_{РЗ} \Delta F_ш}}. \qquad (2)$$

Графики зависимости (2) показаны на рис. 4 в логарифмическом масштабе для различных дальностей разведки $Д_с$ в случае применения в РЗ сигналов с узкополосной ($\Delta F_{РЗN} = 12$ кГц) и широкополосной ($\Delta F_{РЗW} = 120$ кГц) частотной модуляцией пунктирной и сплошной линией соответственно. Отсюда видно, что размещение переносных ГШ на расстоянии нескольких десятков метров от приемных устройств типовых РЗ может приводить к их подавлению.

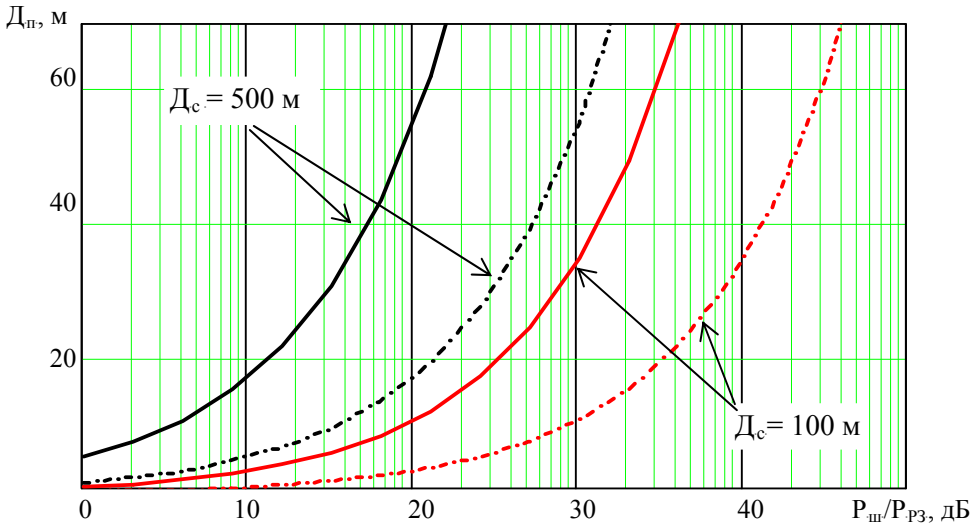

Рисунок 4 – Зависимости дальности подавления приемных устройств от энергетики ГШ и РЗ

ISBN 966-622-022-9

В разработке и применении сетевых генераторов шума (СГШ) одним из проблемных аспектов является обоснование необходимого диапазона защищаемых частот в электрическом КУИ, образованном с помощью СЗ.

Оптимальный рабочий диапазон частот СЗ составляет от 50 до 300 кГц [2]. Нижняя граница частотного диапазона обусловлена резким возрастанием уровня кондуктивных сетевых помех (помех проводимости) от включенных бытовых электроприборов на частотах ниже 50 кГц. Верхняя граница обусловлена, с одной стороны, увеличением затухания сигналов при распространении в электросети (ЭС) на частотах свыше 300 кГц, с другой - возрастанием интенсивности электромагнитного излучения в радио эфир сетевых проводов как пространственной антенны с распределенными параметрами. Указанные факторы могут привести к снижению, соответственно, дальности передачи информации и скрытности работы СЗ. Однако далеко не все передатчики в составе СЗ удовлетворяют требованиям на уровни внеполосных излучений. Кроме основной частоты их излучение может содержать несколько убывающих по амплитуде гармоник, на каждой из которых возможен прием по ЭС на определенных дальностях. Поэтому в некоторых случаях верхняя граница диапазона рабочих частот СЗ может отличаться от оптимальной и достигать 1…10 МГц [2].

Разработанный сетевой ГШ (рис. 2) имеет диапазон защищаемых частот от 100 кГц до 15 МГц и выходную мощность около 5 Вт, что позволяет маскировать информационные сигналы СЗ со спектральной плотностью мощности до единиц мВт/кГц. Сказанное иллюстрирует частотная панорама сканирования ЭС в диапазоне частот 0.1...5 МГц на рис. 5. Здесь полутоном показаны сигналы в ЭС в выделенном помещении, тоном – наводки на ЭС при включении ПК Pentium II и гармоники СЗ типа ССТ-700 из состава поискового комплекса СРМ-700 "Акула".

Однако, спектральная плотность мощности сигналов существующих серийных СЗ может быть на порядок выше указанной [2, 3, 9]. В этих условиях более предпочтительным является пассивный метод блокирования электрического КУИ, основанный на применении помехоподавляющих сетевых фильтров типа ФП, ФСП, "М" и др.

Следует заметить, что достижение требуемого коэффициента подавления в таких фильтрах ($К_п \geq 100$ дБ) существенно зависит от ширины диапазона защищаемых частот, способа подключения фильтра, вида ЭС, характеристик заземления и других факторов [6], которые далеко не всегда возможно учесть и реализовать на практике.

Поэтому целесообразным представляется объединение в одном устройстве сетевого фильтра, осуществляющего подавление мощных спектральных составляющих сигналов СЗ, и маломощного СГШ, зашумляющего неподавленные остатки опасных сигналов СЗ на выходе фильтра [9]. Последние могут быть обусловлены недостаточным значением $К_п$ на гармониках неизвестной априори частоты СЗ и наводками ПЭМИ на близко расположенную ЭС в смежном с выделенным помещении. Реализация такого комплексного метода блокирования электрического КУИ позволит смягчить требования к базовым характеристикам сетевого фильтра и СГШ и, как следствие, снизить их стоимость.

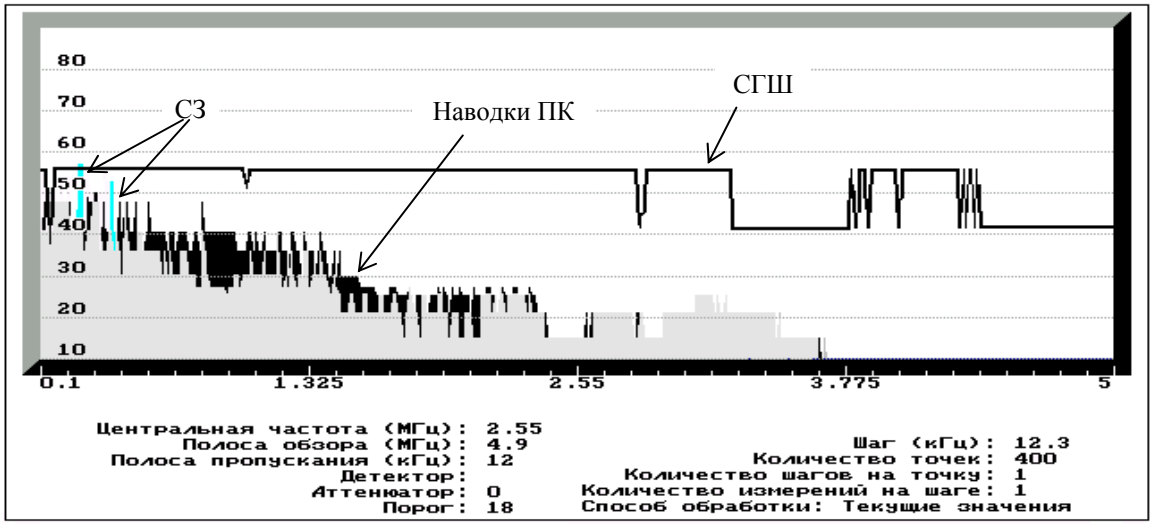

Рисунок 5 – Частотные панорамы исследуемых сигналов в ЭС

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

III Выводы

1. Актуальной задачей является разработка, производство и сертификация недорогих эффективных отечественных ГШ, реализующих пространственное и линейное зашумление опасных сигналов в электромагнитном и электрическом каналах утечки информации.
2. В рамках решения этой задачи в Национальном университете внутренних дел были разработаны и исследованы макеты ГШ радиодиапазона (0.05...1500 МГц) и СГШ (0.1...15 МГц).
3. Разработанные ГШ по базовым техническим характеристикам не уступают, а по ряду из них (диапазон защищаемых частот, массогабаритные показатели, цена) превосходят известные ГШ.
4. На основе энергетического критерия показано, что в общем случае ГШ радиодиапазона не обеспечивают подавление акустических радио закладок, но позволяют упростить (удешевить) процесс обнаружения мощных кварцованных РЗ.
5. Использование широкополосных ГШ радиодиапазона для активной защиты от РЗ дает положительный эффект только в ряде частных случаев:
   - наличия в составе РЗ радиоканала ДУ, приемное устройство которого будет подавлено маскирующей помехой ГШ;
   - пониженной до значений сотен мкВт…единиц мВт мощности излучений РЗ для повышения скрытности его работы;
   - наличия априорной информации о вероятной зоне технической разведки и выносе ГШ в сторону работающего с РЗ приемного устройства. Радиус зоны подавления может составлять от единиц до нескольких десятков метров.
6. В целях надежного блокирования электрического КУИ, образованного мощными кварцованными сетевыми закладными устройствами в условиях априорной неопределенности о диапазоне их работы и виде модуляции сигналов, целесообразно комплексирование активного и пассивного методов защиты. Оно может быть реализовано на основе сопряжения в едином устройстве сетевых фильтра и ГШ, требования к базовым характеристикам которых (коэффициенту подавления фильтра, спектральной плотности мощности шума) могут быть снижены.

Литература: 1. Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96. 2. Энциклопедия промышленного шпионажа / Под общ. ред. Е. В. Куренкова – С.-Петербург: ООО "Изд-во Полигон", 1999. – 512 с. 3. Хорев А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Уч. пособ. М.: ГТК России, 1998. – 320 с. 4. Емельянов С. Л., Логвиненко Н. Ф., Марков С. И., Носов В. В. Проблемные аспекты разработки, производства и применения отечественных генераторов шума в системах защиты информации // Сбірник матеріалів II НТК "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". Київ, 2000. С. 159 – 162. 5. Ю. Зиньковский, В. Клименко. Задачи электромагнитной технической защиты основных информационно-вычислительных средств // Там же. С. 87 – 92. 6. В. Первой, В. Швайченко. Эффективность помехоподавляющих защитных фильтров в двух и трёхпроводных однофазных электрических сетях // Там же. С. 184 – 187. 7. Каталог МАСКОМ. Специальная техника защиты информации, М., 1998. С. 9. 8. Вакин С. А., Шустов Л. Н. Основы радиопротиводействия и радиотехнической разведки. М.: Изд-во "Сов. Радио". 1968. - 448 с. 9. Емельянов С. Л., Логвиненко Н. Ф., Марков С. И., Носов В. В. Технические методы защиты каналов утечки информации по электросети // Бизнес и безопасность, № 2, 2000. С. 8 – 9.

УДК 004.056.5

ПРИМЕНЕНИЕ ФОРМАЛЬНЫХ МОДЕЛЕЙ БЕЗОПАСНОСТИ ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ СИСТЕМ ОТ НЕСАНКЦИОНИРОВАННОГО УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

Денис Кудин, Владислав Корольков
ООО «Центр информационной безопасности», Запорожский государственный