УДК 621.39:621.39.82

ОЦЕНКА УСТОЙЧИВОСТИ ШИРОКОПОЛОСНЫХ СИГНАЛОВ К ИМИТАЦИОННЫМ ПОМЕХАМ

А. В. Черноусов[1], А. В. Кузовников[1], В. Г. Сомов[2]

[1]ОАО «Информационные спутниковые системы» имени академика М. Ф. Решетнева»
Российская Федерация, 662972, г. Железногорск Красноярского края, ул. Ленина, 52
E-mail: chernousovalexey@gmail.com
[2]Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Российская Федерация, 660014, Красноярск, просп. им. газ. «Красноярский рабочий», 31

Оценивается устойчивость сигналов к имитационным помехам. Рассчитывается вероятность навязывания сигналов и безопасное время работы систем радиосвязи. Предложено три алгоритма формирования сигналов в системах радиосвязи. Сделан вывод о целесообразности использования вейвлет-модулированных широкополосных сигналов в системах радиосвязи с целью борьбы с имитационными помехами.

Ключевые слова: вейвлет, широкополосный сигнал, модуляция, безопасное время работы, вероятность навязывания, имитационная помеха.

THE ASSESSMENT OF BROADBAND SIGNALS IMMUNITY AGAINST SIMULATION ECHOES

A. V. Chernousov[1], A. V. Kuzovnikov[1], V. G. Somov[2]

[1] JSC “Information satellite system” named after academician M. F. Reshetnev”
52, Lenin str., Jeleznogorsk, 662971, Russian Federation. E-mail: chernousovalexey@gmail.com
[2]Siberian State Aerospace University named after academician M. F. Reshetnev
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660014, Russian Federation

Broadband signals immunity against simulation echoes is assessed. Probability of signals intrusion and safety running time for communication systems are calculated. Three algorithms of signals forming in communications systems are provided. The conclusion that it is reasonable to use the wavelet modulated broadband signals in communication systems for the purpose of simulated echoes suppression is made.

Keywords: wavelet, broadband signal, modulation, safety running time, probability of intrusion simulated echo.

Системы радиосвязи подвержены негативному воздействию со стороны различного типа помех, в то же время существуют способы обнаружения каналов связи и методы несанкционированного доступа для добывания информации или навязывания имитационных помех с целью их радиоподавления. В связи с этим актуальной является проблема организации безопасной связи, обеспечивающей конфиденциальность и имитостойкость.

Задачи обеспечения конфиденциальности решаются применением современных способов криптографии. В настоящее время активно развивается направление обеспечения имитостойкости радиоканалов. Возможности воздействия имитопомех (имитонападения) значительно расширились. Процесс воздействия значительно изменился на канальном, сервисном и аппаратном уровнях.

В статье [1] приводится следующее определение имитационной помехи и имитационной стойкости: «Согласно принятому определению, под имитационной помехой понимают активное воздействие радиоэлектронных средств, регистрируемое средством радиосвязи как полезный сигнал. Более полно сущность и возможности имитационных помех раскрыты в определении имитостойкости, под которой понимают способность системы связи противостоять вводу ложной информации, несанкционированному доступу к передаваемой или принимаемой информации и навязыванию ложных режимов средствам связи». Исходя из этого определения, выделяют два типа имитационных помех для воздействия на автоматизированный радиоканал:

– первый тип – имитопомехи, воздействующие на радиоканалы дежурного приема;

– второй тип – имитопомехи, воздействующие в момент передачи сообщения (во время сеанса связи).

Возможность применения имитопомех того или иного типа определяется длительностью передачи сигнала и инерционностью систем радионаблюдения (РН) и радиоэлектронного воздействия (РЭВ).

В связи с этим выделяют понятие «имитационная стойкость системы связи». Система является стойкой к воздействию имитационных помех, если задача подбора имитационной помехи требует больше времени, чем продолжительность передачи сигнала в канале связи.

Проблема имитостойкости радиоканалов частично решается применением методов (средств) повышения скрытности работы СРС, направленных на затруднение обнаружения радиосигналов подсистемой радио-

разведки и, следовательно, на затруднение создания помех [2]. Одним из таких методов является применение в системах радиосвязи широкополосных сигналов.

Широкополосными (сложными, шумоподобными) сигналами (ШПС) являются такие сигналы, у которых произведение ширины спектра F на длительность T много больше единицы. Это произведение называется базой сигнала B. Для ШПС

$$B = F \times T >> 1 . \quad (1)$$

В системах связи с ШПС ширина спектра излучаемого сигнала F всегда много больше ширины спектра информационного сообщения.

Одними из основных преимуществ, за счет которых ШПС получили применение в широкополосных системах связи (ШПСС), являются:

– обеспечение высокой помехоустойчивости связи;

– создание системы связи с повышенной скрытностью;

– обеспечение электромагнитной совместимости ШПСС с узкополосными системами радиосвязи и радиовещания, системами телевизионного вещания.

В случае формирования сигналов в системах связи при помощи вейвлет-модуляции и применения псевдослучайных последовательностей задача формирования имитационной помехи сводится к двум подзадачам:

1) обнаружение передаваемого сигнала;

2) формирование имитационной помехи с использованием информации, полученной при обнаружении передаваемого сигнала.

В рамках данной статьи произведена оценка устойчивости следующих сигналов к имитационным помехам:

– узкополосный, фазомодулированный сигнал;

– широкополосный фазомодулированный сигнал;

– широкополосный вейвлет-модулированный сигнал с фиксированными значениями формирующих параметров *Fb*, *Fc*,

Алгоритмы формирования сигналов, приведенных выше, отображены на рис. 1–3.

На рис. 1 представлен алгоритм формирования узкополосного фазомодулированного сигнала. Информационный сигнал поступает на вход модулятора, где умножается на сигнал с несущей частотой и передается абонентам.

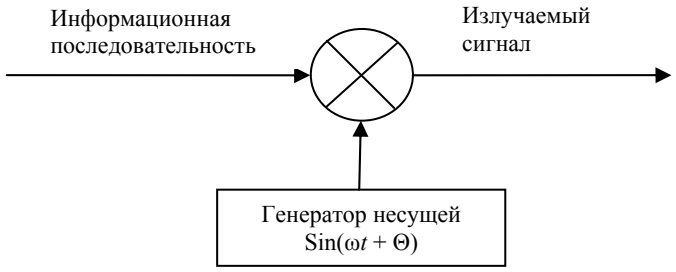

Рис. 1. Формирование узкополосного фазомодулированного сигнала.

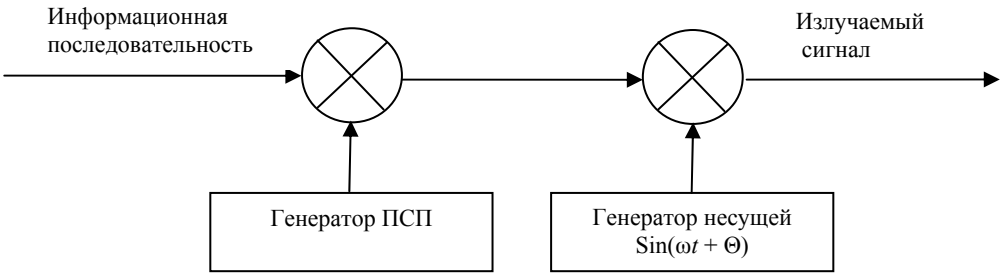

Рис. 2. Формирование широкополосного фазомодулированного сигнала

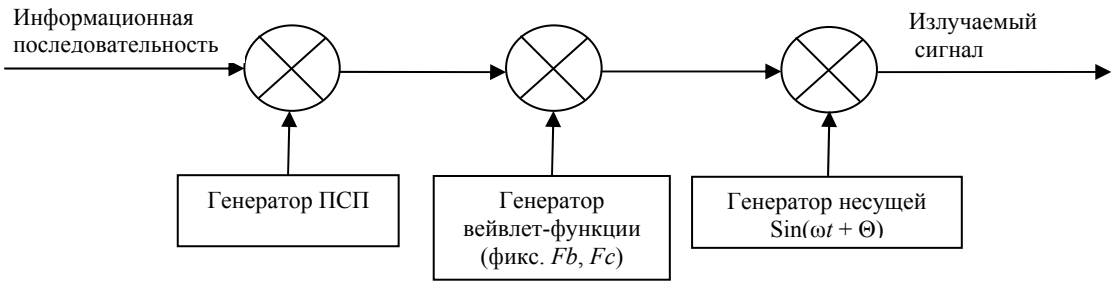

Рис. 3. Формирование вейвлет-модулированного широкополосного сигнала с фиксированными значениями параметров модулирующей функции

На рис. 2 представлен алгоритм формирования широкополосного фазомодулированного сигнала. Информационный сигнал расширяется при помощи псевдослучайной последовательности (ПСП). После чего сигнал поступает на вход модулятора, где умножается на сигнал с несущей частотой и передается абонентам.

На рис. 3 представлен алгоритм формирования вейвлет-модулированного широкополосного сигнала (W ШПС) с фиксированными значениями вейвлет-функции (*Fb*, *Fc*). Информационный сигнал расширяется при помощи псевдослучайной последовательности. После чего сигнал поступает на вход модулятора. При модуляции, полученной ПСП, каждый бит модулируется вейвлетом с фиксированным значением формирующих параметров. Затем сигнал, модулированный вейвлетом, умножается на сигнал с несущей частотой и передается абонентам.

Для сигналов, сформированных каждым приведенным алгоритмом, посчитана вероятность навязывания и безопасное время. Расчет был произведен согласно методике, отображенной в статье [3].

Для вычислений были определены следующие параметры:

1) $N_{псп}$ – количество ПСП (в зависимости от длины);

2) $K_в$ – количество вейвлетов;

3) m, n = 50 – число параметров *Fb* и *Fc*, используемых для формирования вейвлета.

Полученные результаты отображены в табл. 1, 2.

Для вычисления безопасного времени работы использовалась формула

$$T_б = \frac{1}{2} Z \cdot t_{опр}, \qquad (2)$$

где $T_б$ – математическое ожидание времени статистического опробования всевозможных вариантов навязывания противником сигнала с использованием всего пространства $\{Z\}$ сложных сигналов; $T_{опр}$ – время передачи имитационного сигнала.

$$T_{опр} = \frac{1}{R_п}, \qquad (3)$$

где $R_п$ – скорость имитационного воздействия противника.

Очевидно, что на скорость имитационного воздействия противника влияет множество параметров. Среди них:

– инерционность систем РН и РЭВ;

– время, затрачиваемое на обнаружение сигнала;

– время, затрачиваемое на передачу сигнала.

В данной статье для расчета безопасного времени во внимание принималось лишь время, затрачиваемое на передачу сигнала. Это позволило абстрагироваться от влияния параметров систем РН и РЭВ и сосредоточиться только на влиянии алгоритмов формирования сигналов на их способность противостоять имитационным помехам.

Проанализировав полученные данные, можно сделать вывод о том, что наибольшей имитостойкостью, а значит, наилучшей способностью противостоять имитационным помехам обладает вейвлет-модулированный широкополосный сигнал с фиксированными значениями параметров модулирующей функции. Например, применение данного алгоритма формирования сигнала позволяет увеличить безопасное время передачи информационной последовательности на 4,69 с для длинны ПСП 32 бита. Тогда как широкополосный фазомодулированный сигнал увеличивает безопасное время передачи всего лишь на 3,1E–4 с для аналогичной длины ПСП. А узкополосный фазомодулированный сигнал никак не влияет на изменение безопасного времени передачи, так как вероятность его навязывания 100 %.

Стоит отметить, что исходные данные носят приблизительный характер, и для их уточнения следует провести более детальные исследования. Например, по результатам исследований для формирования широкополосных сигналов наиболее предпочтительным является вейвлет Шеннона, следовательно, можно сократить априорное значение до 1. То же самое касается и других параметров.

Таблица 1

Вероятность навязывания сигнала

Алгоритм формирования	Вероятность навязывания
Узкополосный фазомодулированный сигнал	1
широкополосный фазомодулированный сигнал	1,6E–1
W ШПС с фиксированными значениями параметров модулирующей функции	1,1E–5

Таблица 2

Безопасное время работы

Алгоритм формирования	Длина ПСП					
	32	64	128	256	512	1024
Узкополосный фазомодулированный сигнал	–	–	–	–	–	–
Широкополосный фазомодулированный сигнал	3,1E–4	6,3E–4	1,3E–3	2,5E–3	5E–3	1E–2
W ШПС с фиксированными значениями параметров модулирующей функции	4,69	9,53	1,92E+1	3,86E+1	7,73E+1	1,55E+2

Для определения влияния инерционности систем РН и РЭВ, времени, затрачиваемого на обнаружение сигнала, вероятности правильного априорного определения параметров формирующих функций необходимо более детальное исследование.

Библиографические ссылки

1. Орощук И. М. Основные направления применения имитационных помех в системах радиосвязи. Классификация способов ими [Электронный ресурс] // Центр информационной безопасности : портал. 2005. URL: http://www.bezpeka.com/ru/lib/spec/metr/art184.html.

2. Ширман Я. Д. Теоретические основы радиолокации. М. : Сов. радио, 1970. 561 с.

3. Воронов Д. Н. Критерии оценки имитостойкости командно-телеметрических радиолиний // Системи обробки інформації. 2007. № 4(62). С. 14–16.

References

1. Oroshchuk I. M. [Main pathways of simulated echoes application in communication systems. Classification of simulated echoes]. *Tsentr informatsionnoy bezopasnosti: portal.* 2005 (In Russ.) Available at: URL: http://www.bezpeka.com/ru/lib/spec/metr/art184.html.

2. Shirman Y. D. *Teoreticheskiye osnovy radiolokatsii* (Theoretical foundations of radiolocation). Moscow, Soviet radio, 1970, 561 p.

3. Voronov D. N. *Sistemi obrobki iniformatsii.* 2007, no. 4 (62), p. 14–16.

УДК 004.056

МЕТОДИКА ДИНАМИЧЕСКОГО АНАЛИЗА УЯЗВИМОСТЕЙ В БИНАРНОМ КОДЕ*

М. О. Шудрак, В. В. Золотарев, И. А. Лубкин

Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Российская Федерация, 660014, Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: mxmssh@gmail.com

Описывается методика и ее реализация в виде программного продукта, осуществляющая обнаружение уязвимостей в бинарном коде с использованием сочетания технологий динамической бинарной инструментации, анализа покрытия кода и так называемого фаззинга – технологии генерации потенциально ошибочных данных и мониторинга результата. В результате было разработано программное средство для поиска уязвимостей в сетевых и файловых приложениях, позволяющая значительно оптимизировать процесс динамического тестирования.

Ключевые слова: динамический анализ, уязвимость, фаззинг, бинарная инструментация.

THE TECHNIQUE FOR BINARY EXECUTABLES VULNERABILITIES DETECTION

M. O. Shudrak,V. V. Zolotarev, I. A. Lubkin

Siberian State Aerospace University named after academician M. F. Reshetnev
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660014, Russian Federation. E-mail: mxmssh@gmail.com

The article describes dynamic analysis techniques and cloud-based platform for software security and reliability testing. In the article the authors contribute to the dynamic execution analysis techniques. In the first part of the article the authors describe the technique of dynamic binary analysis which is referred to as fuzzing. The authors show basic architecture of the tool for security and reliability testing of application and vulnerabilities detection. Due to the use of the dynamic binary instrumentation this technique implementation is much faster than ones applied previously. The technique described in the article has been implemented as the software platform which includes web-interface, virtual machine dispatcher, dynamic instrumentation library, debugger, special dll, protocol description and fuzzing manager tool.

Keywords: dynamic analysis, vulnerability, fuzzing, binary instrumentation.

* Работа выполнена в рамках гранта по соглашению № 14.132.21.1365 от 22.10.2012 федеральной целевой программы «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы.