РАДИОТЕХНИКА И СВЯЗЬ

УДК 621.391
DOI: 10.22213/2413-1172-2023-3-75-81

Оценка влияния аддитивного белого гауссова шума на энергетическую скрытность сложных сигналов

Л. А. Сенаторов, аспирант, ИжГТУ имени М. Т. Калашникова, Ижевск, Россия
В. В. Хворенков, доктор технических наук, профессор, ИжГТУ имени М. Т. Калашникова, Ижевск, Россия
А. В. Савельев, доктор технических наук, профессор, АО «Сарапульский радиозавод», Сарапул, Россия

При проектировании систем радиосвязи специального назначения важно учитывать работу потенциальных противников или злоумышленников, обладающих средствами радиоэлектронной борьбы и радиоэлектронного подавления, задачей которых является нарушение работы радиосвязи или перехват передаваемых сообщений.

Сегодня известен ряд способов противодействия средствам радиоэлектронной борьбы, основные из них направлены на уход от деструктивных воздействий. В этой области перспективным является вопрос создания бескомпроматных радиопередающих устройств. Под термином «бескомпроматность» понимается такое радиопередающее устройство, которое способно передавать скрытный сигнал таким образом, чтобы средства радиоэлектронной борьбы и радиоэлектронного подавления противника не могли зафиксировать выход в эфир. Скрытность сигнала обеспечивается за счет комплекса технических и организационных мер. При исследовании вопросов скрытности наибольшее внимание уделяется энергетической скрытности, так как эта компонента зависит в основном от конструкторских решений на стадии проектирования.

Рассматривается проблема получения оценки влияния аддитивного белого гауссова шума на вероятность правильной передачи сигналов. Влияние шума и помех рассматривается в качестве важного элемента радиоэлектронной борьбы и противодействия радиоэлектронной борьбы противника. Целью статьи является изучение влияния шума на степень энергетической скрытности сигналов.

Проведена оценка влияния аддитивного белого гауссова шума и фазового шума для сигналов BPSK, QPSK, QAM-16 и линейной частотной модуляции. На основании результатов описаны некоторые закономерности, позволяющие оценить влияние аддитивного белого гауссова шума и фазового шума на помехоустойчивость этих сигналов.

Проведены исследования сигнала линейной частотной модуляции на степень энергетической скрытности под воздействием шумов. В результате исследования сделаны выводы о влиянии внешних шумов на степень энергетической скрытности сигналов, при этом сигнал линейной частотной модуляции признан потенциально годным для применения в специальных системах связи.

Ключевые слова: помехоустойчивость, Matlab, BPSK, QPSK, линейная частотная модуляция (ЛЧМ), квадратурные сигналы, энергетическая скрытность, бескомпроматность.

Введение

Системы радиосвязи являются важным элементом во многих структурах, они активно применяются как в военной сфере, так и в гражданских направлениях.

При передаче радиосигнала в городах основные проблемы связаны со средой распространения (переотражение радиосигналов от зданий при плотной застройке, увеличение пути передачи радиосигнала, наличию препятствий на пути распространения сигнала, и так далее), а также с частотным распределением каналов (вокруг много устройств разной величины, которые могут мешать друг другу). То есть при разработке гражданских систем радиопередачи необходимо учитывать, что окружающая обстановка в целом является благоприятной за счет наличия качественной инфраструктуры (базовых станций, антенн, ретрансляторов, практически повсеместного доступа к широкополосной связи), однако необходимо уделять внимание эффективности использования энергетического спектра.

В области военной радиосвязи дела обстоят совершенно иным образом. При работе в полевых условиях нет необходимости заботиться об

эффективности использования сети, так как радиоустройства распределены менее плотно, при этом связь будет осуществляться, как правило, в условиях непрямой видимости. Также необходимо учитывать присутствие противника, потенциально обладающего средствами радиоэлектронной борьбы (РЭБ) и подавления (РЭП). В городской среде помехи обычно непреднамеренные и обусловлены ошибками при проектировании и эксплуатации устройств, а также наличием рядом с точкой приема мощных источников электрических сигналов. В военной области помехи носят направленный характер. Системы РЭБ и РЭП используются для обнаружения, перехвата и расшифровки сообщений, подавления передаваемых сигналов, обнаружения примерного местоположения передатчика.

Воздействие систем РЭБ и РЭП определяет востребованность исследований вопросов обеспечения помехозащищенности и скрытности сигналов [1]. Наибольшее внимание уделяется вопросам обеспечения скрытности сигнала, так как независимо от степени помехозащищенности лучше всего применять в системе сигналы таким образом, чтобы их было труднее обнаружить.

Под скрытностью сигнала понимается способность передачи сигнала незаметно для стороннего наблюдателя, обеспечиваемая за счет комплекса технических и организационных мер. Принято выделять 5 компонентов скрытности: энергетическая, структурная, информационная, временная и пространственная [2].

Проблемы повышения скрытности радиосигналов рассматриваются во многих отечественных и зарубежных работах [3–7]. Перспективным направлением исследования является вопрос обеспечения бескомпроматности передаваемого радиосигнала [8–11]. Термин «бескомпроматность» не является общепринятым и не включен в российские и зарубежные стандарты (ГОСТ Р 50922–2006 Защита информации. Основные термины и определения; MIL-STD-188-141D Interoperability and performance standards for medium and high frequency radio systems (22 December 2017)), поэтому далее под бескомпроматным радиопередающим устройством будем понимать радиопередатчик, который способен передавать скрытный сигнал таким образом, чтобы средства РЭБ и РЭП противника не фиксировали выход в эфир.

Определение выхода радиостанции на связь фиксируется в результате наблюдения за уровнем сигналов в эфире (Ляхов А. В. Модели и методы оценки энергетической скрытности низкочастотных систем спутниковой связи : дис. … канд. техн. наук. Ставрополь, 2021. 343 с.). Если в эфире нет работающих станций, то уровень шума является постоянным. При передаче сигнала уровень излучений в полосе передачи заметно повышается, что свидетельствует об осуществлении передачи.

Логичным решением было бы использовать шумоподобные сигналы, а когда станция ничего не передает, заполнять эфир шумами того же уровня, чтобы у противника не возникало подозрений о том, что кто-то выходит в эфир. Однако у этого подхода есть существенный недостаток, который заключается в том, что в полевых условиях носимая радиостанция не сможет занимать шумами достаточно широкую полосу. Подобное решение также плохо отразится на размере станции и ее энергопотреблении.

В связи с этим можно выдвинуть гипотезу о том, что бескомпроматная передача возможна в случае маскирования сигнала под сигнал другой станции. То есть передача сигнала одновременно с передачей другой станции (идеально – станции противника).

Целью настоящей статьи является изучение влияния аддитивного белого гауссова шума (АБГШ) на степень энергетической скрытности сигналов.

Для этого были решены следующие задачи.

1. Разработаны модели формирования и передачи сигналов BPSK, QPSK, ЛЧМ и QAM-16.

2. Проведено сравнение вероятностей правильного приема под воздействием шума сигналов BPSK, QPSK, ЛЧМ и QAM-16.

3. Дана количественная оценка степени энергетической скрытности сигнала под воздействием АБГШ в канале связи.

Исследование влияния АБГШ и фазового шума на вероятность правильного приема сложных сигналов

В качестве исследуемых сигналов были выбраны сигналы с модуляцией BPSK, QPSK, ЛЧМ и QAM-16.

QPSK получила применение в системах массового обслуживания, предъявляющих повышенные требования к скорости и качеству передаваемой информации. Сюда относятся телевизионные, спутниковые и мобильные сети связи. В частности, QPSK применяется в стандарте 4G.

Сигнал BPSK редко применяется в современных системах связи. Сегодня его основная сфера применения – недорогие пассивные передатчики, например RFID.

Основная сфера применения ЛЧМ-сигналов – радиолокация. За счет сжатия сигнала в цепях

обработки приемника сигналы станции РЛС обладают хорошей разрешающей способностью и дальностью. Сигнал ЛЧМ также может использоваться для передачи малых объемов данных (не более нескольких килобайт), как это реализовано в стандарте LoRa.

QAM-16 широко применяется в цифровых телекоммуникационных системах, в частности в стандарте WiFi 802.11 и высокоскоростных системах с оптическим волокном. Данный тип модуляции может применяться и при разработке SDR-приемников, хотя данная практика не так распространена, как использование QAM-8.

Для изучения помехоустойчивости этих сигналов в программе Matlab R2021b были разработаны математические модели, имитирующие модуляцию цифрового информационного потока, передачу по каналу связи, а также дальнейшую демодуляцию на приемной стороне.

Модель состоит из источника информации, модулятора, канала связи, демодулятора и схемы сравнения.

Источник информации генерирует информационный поток необходимой разрядности (2 для BPSK и ЛЧМ, 4 для QPSK, 16 для QAM-16).

Модулятор преобразует полезную информацию и передает ее в канал связи, где на сигнал накладывается аддитивный белый гауссов шум (АБГШ).

Зашумленный сигнал поступает на демодулятор, который выделяет из смеси сигнала и шума полезную информацию.

Схема сравнения сравнивает исходный и принятый информационные потоки между собой и вычисляет вероятность ошибки.

В результате моделирования было установлено, что все рассматриваемые сигналы, кроме ЛЧМ, обладают достаточно низкой помехоустойчивостью при отношении сигнал/шум (ОСШ) 0 дБ и менее. При положительном ОСШ наихудшей помехоустойчивостью обладает сигнал BPSK, а наилучшей – QAM-16 и ЛЧМ. Полученные в результате моделирования данные согласуются с известными данными из справочников и работ других исследователей [12–17]. Полученные в результате моделирования данные представлены в таблице 1.

Скрытная передача под шумами предполагает передачу сигнала по каналу с ОСШ на уровне 0 дБ и менее с приемлемым качеством. Приемлемым качеством передачи будем считать передачу с вероятностью битовой ошибки 0,1 и менее. Таким образом, выбор осуществлялся среди сигналов QPSK, BPSK и ЛЧМ.

Таблица 1. **Сравнение вероятности битовой ошибки сигналов QPSK, BPSK, ЛЧМ и QAM-16 в пределах ОСШ 0 дБ**

Table 1. **Comparison of BER of QPSK, BPSK, Chirp and QAM-16 signals within 0 dB SNR**

SNR, дБ	BER (QPSK)	BER (BPSK)	BER (ЛЧМ)	BER (QAM-16)
0	0,2931	0,0841	0	0,7391
–1	0,3426	0,1061	0	0,7632
–5	0,5003	0,2148	0	0,8383
–20	0,7142	0,4499	0,001	0,9083

Среди рассматриваемых сигналов ЛЧМ является наиболее пригодным для передачи информации под шумами и будет рассматриваться в дальнейшем для изучения влияния АБГШ в канале на энергетическую скрытность.

Описание используемого метода оценки энергетической скрытности

Моделирование передачи информации под воздействием шумов в канале связи позволяет оценить пригодность применения того или иного сигнала в скрытной системе связи. Однако для принятия решения о выборе сигнала необходимо оценить степень энергетической скрытности, так как от этого параметра во многом зависит итоговая видимость сигнала средствами РЭБ [18–20].

В литературе описаны различные способы получения оценки энергетической скрытности сигналов. В данной работе для получения оценки будем использовать метод оценки по энергии передаваемого символа.

В качестве основного показателя энергетической скрытности используется вероятность обнаружения излучаемого сигнала при условии, что противник не знает точной структуры и параметров сигнала, которая может быть вычислена по формулам

$$P_0 = 0{,}5 - \int_0^{\Delta i} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx; \qquad (1)$$

$$\Delta i = \tilde{\Pi} - q_{вх}^2 \sqrt{W_p T_p}, \qquad (2)$$

где $\tilde{\Pi}$ – порог срабатывания; q – отношение сигнал/помеха на входе обнаружителя; W_p –

полоса радиочастот сигнала; T_p – время работы на передачу.

Отношение сигнала к помехе может быть представлено согласно формуле

$$q_{\text{вх}}^2 = \frac{2E_s}{N_0}, \quad (3)$$

где E_s – энергия сигнала в расчете на 1 бит; N – спектральная плотность шума.

Для сообщения конечной длины энергия символа может быть найдена по формуле

$$E_s = \frac{\int_0^{T_p} s^2(t)\,dt}{K}, \quad (4)$$

где $s(t)$ – сигнал; K – число информационных бит (может быть найдено как произведение скорости передачи на время работы).

Сигнал $s(t)$ для случая передачи ЛЧМ-сигнала может быть найден как

$$s = S_0 \cos\left[\varphi_0 + 2\pi\left(F_{\max} - F_{\min}\right)t\right] = \\ = S_0 \cos\left[2\pi\left(F_{\max} - F_{\min}\right)t\right],$$

где S_0 – амплитуда сигнала; φ_0 – начальная фаза (для упрощения расчетов примем ее равной нулю); t – время.

С использованием приведенных выше формул в Matlab была составлена модель, позволяющая оценить степень энергетической скрытности сигнала ЛЧМ при различных параметрах.

При математическом моделировании используются следующие начальные параметры:

- амплитуда сигнала на входе приемника 0,2 мкВ;
- время работы на передачу – 0,1 мкс;
- полоса частот – 125 кГц;
- ОСШ и порог срабатывания выбираются по ходу моделирования.

Оценка влияния АБГШ на энергетическую скрытность ЛЧМ-сигнала

Результаты измерения степени энергетической скрытности ЛЧМ-сигнала представлены в таблице 2.

Увеличение уровня шума в канале приводит к изменению амплитуды передаваемого сигнала и, соответственно, к увеличению показателя энергии на бит. Если бы рассматриваемый сигнал передавался при положительных ОСШ, то ухудшение помеховой обстановки, вероятно, ухудшило бы энергетическую скрытность, так как увеличение энергии, приходящейся на бит, обычно приводит к увеличению вероятности обнаружения сигнала.

Однако рассматриваемый ЛЧМ-сигнал передавался при ОСШ от 0 до –28 дБ, то есть информационный сигнал не только обладает малой амплитудой и мощностью, но и передается настолько глубоко под шумами, что вероятность обнаружения сигнала стремится к нулю. Поэтому при моделировании увеличение мощности шума не привело к увеличению вероятности обнаружения сигнала. Напротив, с ухудшением ОСШ вероятность обнаружения сигнала продолжала снижаться.

Таблица 2. **Вероятность обнаружения ЛЧМ сигнала в зависимости от порогового значения при заданном ОСШ**

Table 2. **The probability of detecting a chirp signal depending on the threshold value for a given SNR**

Пороговое значение, мкВ	Энергия на бит						
	0,0008	0,014	0,027	0,04	0,09	0,131	0,26
	ОСШ, дБ						
	0	–0	–18	–20	–3	–25	–28
0,1	0,24	0,031	$5{,}3 \cdot 10^{-17}$	$5{,}4 \cdot 10^{-17}$	$6{,}2 \cdot 10^{-17}$	$7{,}4 \cdot 10^{-17}$	$7{,}8 \cdot 10^{-17}$
0,16	0,067	0,0093	$5{,}4 \cdot 10^{-17}$	$5{,}5 \cdot 10^{-17}$	$6{,}5 \cdot 10^{-17}$	$7{,}6 \cdot 10^{-17}$	$2{,}8 \cdot 10^{-16}$
0,25	0,0062	0,00056	$5{,}4 \cdot 10^{-17}$	$5{,}5 \cdot 10^{-17}$	$6{,}5 \cdot 10^{-17}$	$6{,}8 \cdot 10^{-17}$	$8{,}4 \cdot 10^{-16}$
0,35	0,00023	0,000011	$5{,}5 \cdot 10^{-17}$	$5{,}8 \cdot 10^{-17}$	$6{,}8 \cdot 10^{-17}$	$2{,}4 \cdot 10^{-17}$	$2 \cdot 10^{-15}$
0,5	0,0000034	0,00000047	$5{,}8 \cdot 10^{-17}$	$6{,}2 \cdot 10^{-17}$	$7{,}2 \cdot 10^{-17}$	$1 \cdot 10^{-16}$	$4{,}4 \cdot 10^{-15}$

Моделирование показало, что при передаче ЛЧМ-сигнала под шумами, наибольшее влияние на вероятность обнаружения сигнала оказывает чувствительность средств радиолокации противника.

Полученные результаты позволяют утверждать, что ЛЧМ-сигнал может использоваться для обеспечения бескомпроматной передачи сообщений в случае, если сигнал передается в течение коротких промежутков времени при отрицательных ОСШ.

Заключение

В результате проделанной работы сигналы BPSK, QPSK, QAM-16 и ЛЧМ были проверены на помехоустойчивость, а также проанализиро-

ваны на пригодность в использовании для обеспечения бескомпроматной передачи.

В результате проверки было установлено, что среди многопозиционных сигналов наиболее устойчивым к помехам является сигнал QAM-16; благодаря этому, а также своим хорошим показателям энергетической скрытности сигнал QAM может быть выбран в качестве передающего в радиосистемах специального назначения.

Сигнал ЛЧМ обладает наилучшей устойчивостью к АБГШ. Сигнал позволяет осуществлять безошибочную передачу при ОСШ от –18 дБ и выше. Полученные результаты позволяют утверждать, что сигнал ЛЧМ может применяться в системах, рассчитанных на применение в затрудненной помеховой обстановке.

Среди рассматриваемых сигналов ЛЧМ оказался единственным, обеспечивающим приемлемое качество связи при передаче сигнала с ОСШ на уровне 0 дБ и менее, поэтому он был исследован на обеспечение энергетической скрытности под воздействием шумов. Результаты исследования показали, что, несмотря на рост энергии на бит от наложения шумов, сигнал ЛЧМ может передаваться при таких низких ОСШ, что средства наблюдения практически не могут зарегистрировать сигнал в эфире.

Фактические данные, полученные в результате исследования, требуют экспериментального подтверждения.

Предложенные в статье положения имеют значение для использования в практике разработки радиотехнических систем специального назначения.

Библиографические ссылки

1. *Перунов Ю. М.*, *Куприянов А. И.* Методы и средства радиоэлектронной борьбы : монография. Вологда : Инфра-Инженерия, 2021. 376 с.

2. *Берикашвили В. Ш.* Основы радиоэлектроники. Системы передачи информации. 2-е изд. М. : Юрайт, 2019. 105 с.

3. *Тихонов С. С.*, *Кудрявцев А. М.*, *Дворников С. В.* Энергетическая скрытность сигналов ППРЧ, сформированных в базисах функций сплайн-характеров // Информация и космос. 2017. № 2. С. 35–41.

4. *Saarnisaari Harri & Vartiainen Johanna* (2022) Signal detection with spectrum windows, Heliyon, 8, e10054, 10.1016/j.heliyon.2022.e10054

5. *Lipski Michael & Kompella Sastry & Narayanan Ram* (2021) Practical Implementation of Adaptive Threshold Energy Detection using Software Defined Radio. IEEE Transactions on Aerospace and Electronic Systems, 57, 1227-1241. 10.1109/TAES.2020.3040059

6. *Howard Stephen & Weinberg Graham* (2019) Optimal Predictive Inference and Non-Coherent CFAR Detectors. IEEE Transactions on Aerospace and Electronic Systems, pp. 1-1. 10.1109/TAES.2019.2951185

7. *Tao Li*, *Wai Ho Mow*, *Vincent Lau*, *Manhung Siu*, *Roger S.K. Cheng*, *Ross D Murch* (2007). Robust joint interference detection and decoding for OFDM-based cognitive radio systems with unknown interference. IEEE J. Sel. A. Commun. 25, 3 (April 2007), 566-575. https://doi.org/10.1109/JSAC.2007.070407

8. *Ostovari P. and Wu J.* (2017) Fault-Tolerant and Secure Data Transmission Using Random Linear Network Coding: 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 2017, pp. 1-9. DOI: 10.1109/ICCCN.2017.8038417

9. *Jain M. and Lenka S. K.* (2015) Secret data transmission using vital image steganography over transposition cipher: International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 2015, pp. 1026-1029. DOI: 10.1109/ICGCIoT.2015.7380614

10. *Patil A. S.*, *Sundari G. and Joshi V. M.* (2022) STONE: Secret-data Transmission On Novelty Encryption, 2022, IEEE 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 2022, pp. 1-6. DOI: 10.1109/I2CT54291.2022.9824466

11. *Lee C. F.*, *Shen J. J.*, *Agrawal S.*, *Wang Y. X. and Lee Y. H.* (2020) Data Hiding Method Based on 3D Magic Cube, IEEE Access, vol. 8, pp. 39445-39453. DOI: 10.1109/ACCESS.2020.2975385

12. *Довбня В. Г.*, *Коптев Д. С.*, *Бабанин И. Г.* Оценка потенциальной помехоустойчивости приема цифровых сигналов, используемых в современных и перспективных системах радиорелейной и спутниковой связи // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2020. Т. 10, № 1. С. 21–35.

13. *Афанасьев Д. С.* Цифровая обработка ЛЧМ-сигнала // Известия СПБГЭТУ – ЛЭТИ. 2022. Т. 15, № 4. С. 44–48.

14. *Будко П. А.*, *Будко Н. П.*, *Виноградeнко А. М.* Способы повышения помехоустойчивости в автоматизированных системах контроля // Системы управления, связи и безопасности. 2020. № 2. С. 176–211. DOI: 10.24411/2410-9916-2020-10206

15. *Волхонская Е. В.*, *Коротей Е. В.*, *Власова К. В.*, *Рушко М. В.* Модельное исследование помехоустойчивости приема радиосигналов с QPSK, BPSK, 8psk и DBPSK // Известия КГТУ. 2017. № 46. С. 165–174.

16. *Нгуен Ван Зунг.* Помехоустойчивость корреляционного приемника сигналов с многопозиционной фазовой манипуляцией при наличии ретранслированной помехи // Журнал радиоэлектроники. 2019. № 3. URL: http://jre.cplire.ru/jre/mar19/4/text.pdf DOI: 10.30898/1684-1719.2019.3.4

17. *Рушко М. В.* Разработка программного комплекса по оценке качества цифрового канала связи морской подвижной спутниковой службы // Вестник Балтийского федерального университета им. И. Канта. Серия: Физико-математические и технические науки. 2019. № 2. С. 47–55.

18. *Куприянов А. И.* Скрытность сверхузкополосных сигналов // Техника средств связи. 2021. № 2 (154). С. 2–11.

19. *Абрамов А. В.* Обеспечение скрытности работы средств связи за счет синтеза и инверсной фильтрации широкополосных шумоподобных сигналов // I-methods. 2019. С. 39–51

20. *Евстафьев Г. А.*, *Селянская Е. А.* Метод обеспечения структурной скрытности сигнала // Системы синхронизации, формирования и обработки сигналов. 2021. Т. 12, № 4. С. 39–45. EDN WMFFKQ.

References

1. Perunov U.M., Kupriyanov A.I. (2021) *Metody i sredstva radiojelektronnoj bor'by* [Methods and funds of electronic warfare]. Vologda: Infra-Inzheneriya Publ., 2021, 376 p. (in Russ.).

2. Berikashvili V.S (2019) *Osnovy radiojelektroniki. Sistemy peredachi informacii* [Fundamentals of radio electronics. Information transmission systems]. Moscow: Yurait Publ., 2019, 105 p. (in Russ.).

3. Tikhonov S.S.., Kudryavtsev A.M., Dvornikov S.V. (2017) [Energy concealment of the signals of FHSS formed in the bases of spline-characters functions]. *Informatcia i cosmos*, 2017, no. 2, pp. 35-41 (in Russ.).

4. Saarnisaari Harri & Vartiainen Johanna (2022) Signal detection with spectrum windows, Heliyon, 8, e10054, 10.1016/j.heliyon.2022.e10054

5. Lipski Michael & Kompella Sastry & Narayanan Ram (2021) Practical Implementation of Adaptive Threshold Energy Detection using Software Defined Radio. IEEE Transactions on Aerospace and Electronic Systems, 57, 1227-1241. 10.1109/TAES.2020.3040059

6. *Howard Stephen & Weinberg Graham* (2019) Optimal Predictive Inference and Non-Coherent CFAR Detectors. IEEE Transactions on Aerospace and Electronic Systems, pp. 1-1. 10.1109/TAES.2019.2951185

7. Tao Li, Wai Ho Mow, Vincent Lau, Manhung Siu, Roger S.K. Cheng, Ross D Murch (2007). Robust joint interference detection and decoding for OFDM-based cognitive radio systems with unknown interference: IEEE J. Sel. A. Commun, 25, 3 (April 2007), 566-575. https://doi.org/10.1109/JSAC.2007.070407

8. Ostovari P. and Wu J. (2017) Fault-Tolerant and Secure Data Transmission Using Random Linear Network Coding: 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 2017, pp. 1-9. DOI: 10.1109/ICCCN.2017.8038417

9. Jain M. and Lenka S.K. (2015) Secret data transmission using vital image steganography over transposition cipher: International Conference on Green Computing and Internet of Things (ICGCIoT), Greater Noida, India, 2015, pp. 1026-1029. DOI: 10.1109/ICGCIoT.2015.7380614

10. Patil A.S., Sundari G. and Joshi V.M. (2022) STONE: Secret-data Transmission On Novelty Encryption, 2022, IEEE 7th International conference for Convergence in Technology (I2CT), Mumbai, India, 2022, pp. 1-6. DOI: 10.1109/I2CT54291.2022.9824466

11. Lee C.F., Shen J.J., Agrawal S., Wang Y.X. and Lee Y.H. (2020) Data Hiding Method Based on 3D Magic Cube, IEEE Access, vol. 8, pp. 39445-39453. DOI: 10.1109/ACCESS.2020.2975385

12. Dovbnja V.G., Koptev D.S., Babanin I.G. (2020) [Evaluation of the potential noise immunity of digital signals reception used in modern and future systems of radio relay and satellite communications]. *Izvestija Jugo-Zapadnogo gosudarstvennogo universiteta. Serija: Upravlenie, vychislitel'naja tehnika, informatika. Medicinskoe priborostroenie*, 2020, vol. 10, no. 1, pp. 21-35 (in Russ.).

13. Afanas'ev D.S (2022) [Digital Chirp Processing]. *Izvestija SPBGJeTU - LjeTI*, 2022, vol. 15, no. 4, pp. 44-48.

14. Budko P.A., Budko N.P., Vinogradenko A.M. (2020) [Ways to increase noise immunity in automated control systems]. *Sistemy upravlenija, svjazi i bezopasnosti*, 2020, no. 2, pp. 176-211 (in Russ.). DOI: 10.24411/2410-9916-2020-10206

15. Volhonskaja E.V., Korotej E.V., Vlasova K.V., Rushko M.V. (2017) [Model study of the noise immunity of radio signal reception with QPSK, BPSK, 8psk and DBPSK]. *Izvestija KGTU*, 2017, no. 46, pp. 165-174 (in Russ.).

16. Nguen Van Zung (2019) [Noise immunity of a correlation receiver of signals with multiposition phase shift keying in the presence of retransmitted interference]. *Zhurnal radiojelektroniki*, 2019, no. 3 (in Russ.). Available at: http://jre.cplire.ru/jre/mar19/4/text.pdf DOI: 10.30898/1684-1719.2019.3.4

17. Rushko M.V. (2019) [Development of a software package for assessing the quality of a digital communication channel of the maritime mobile satellite service]. *Vestnik Baltijskogo federal'nogo universiteta im. I. Kanta. Serija: Fiziko-matematicheskie i tehnicheskie nauki*, 2019, no. 2, pp. 47-55 (in Russ.).

18. Kupriyanov A.I. (2021) [The secrecy of super-narrowband signals. Means of communication equipment]. *Tehnika sredstv svjazi*, 2021, no. 2, pp. 2-11 (in Russ.).

19. Abramov A.V. (2019) [Ensuring of secrecy of communications through synthesis and inverse filtering of broadband noise-like signals]. *I-methods*, 2019, pp. 39-51 (in Russ.).

20. Yevstafev G.A., Selyanskaya E.A. (2021) [Signal Structural Stealth Method]. *Sistemy sinhronizacii, formirovanija i obrabotki signalov*, 2021, vol. 12, no. 4, pp. 39-45. EDN WMFFKQ.

Evaluation of Additive White Gaussian Noise Influence on the Energy Stealthiness of Complex Signals

L.A. Senatorov, Post-graduate, Kalashnikov ISTU, Izhevsk, Russia
V.V. Khvorenkov, DSc in Engineering, Professor, Kalashnikov ISTU, Izhevsk, Russia
A.V. Savelyev, DSc in Engineering, Professor, "SRZ" JSC, Sarapul, Russia

While designing special-purpose radio communication systems, it is important to take into account the work of potential adversaries or intruders who have electronic warfare and electronic countermeasure, whose task is to disrupt radio communications or intercept transmitted messages.

Today, a number of methods are known to counteract electronic warfare, the main of them are aimed to avoid destructive influences of radio warfare. In this area, the issue of creating "uncompromising" radio transmitting devices is promising. The term "incompromising" means that a radio transmitting device is capable of transmitting a covert signal in such a way that the enemy's electronic warfare equipment could not fixate the broadcast. The secrecy of the signal is ensured by a set of technical and organizational measures. When studying secrecy issues, the greatest attention is paid to energy secrecy, since this component mainly depends on design decisions at the design stage.

The article deals with the problem of obtaining an estimate of the influence of AWGN on the probability of correct signal transmission. The influence of noise and interference is considered as an important element of electronic warfare and countering enemy electronic warfare. The purpose of the article is to study the effect of noise on the degree of energy secrecy of signals.

The influence of AWGN and phase noise for BPSK, QPSK, QAM-16 and chirp signals has been evaluated. Based on the results, some regularities are described that make it possible to evaluate the effect of AWGN and phase noise on the noise immunity of these signals.

Studies of the chirp signal on the degree of energy secrecy under the influence of noise have been carried out. As a result of the study, conclusions were drawn about the influence of external noise on the degree of energy secrecy of signals, the chirp signal was recognized as potentially suitable for use in special communication systems.

Keywords: noise immunity, Matlab, BPSK, QPSK, chirp signals, quadrature signals, energy stealthiness, signal stealth, uncompromising signals.

Получено 24.08.2023

Образец цитирования

Сенаторов Л. А., *Хворенков В. В.*, *Савельев А. В.* Оценка влияния аддитивного белого гауссова шума на энергетическую скрытность сложных сигналов // Вестник ИжГТУ имени М. Т. Калашникова. 2023. Т. 26, № 3. С. 75–81. DOI: 10.22213/2413-1172-2023-3-75-81.

For Citation

Senatorov L.A., Khvorenkov V.V., Savelyev A.V. (2023) [Evaluation of Additive White Gaussian Noise Influence on the Energy Stealthiness of Complex Signals]. *Vestnik IzhGTU imeni M.T. Kalashnikova*, 2023, vol. 26, no. 32, pp. 75-81 (in Russ.). DOI: 10.22213/2413-1172-2023-3-75-81.