Научная статья
УДК 621.391
https://doi.org/10.31854/1813-324X-2025-11-1-26-33
EDN:EHOZQY



# Система радиосвязи с широкополосными сигналами в условиях присутствия ретранслированных помех

**Валерий Иванович Коржик** ✉, korzhik.vi@sut.ru
**Рафаэль Рифгатович Биккенин**, bikkenin.rr@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

**Аннотация**

*В настоящее время помехоустойчивость приема в условиях действия преднамеренных помех, похожих на передаваемые сигналы, играет решающую роль при передаче данных, содержащих важную информацию. В системах радиосвязи с широкополосными сигналами, называемых также сигналами с расширенным спектром, обеспечивалась защита от преднамеренных помех, формируемых постановщиком в условиях априорной неопределенности о передаваемых сигналах. Однако в настоящее время противодействующая сторона способна выявить параметры этих сигналов (вид модуляции, скорость передачи, длительность посылок и др.). Поэтому необходима разработка новых методов защиты от современных угроз для безопасной и помехоустойчивой передачи сообщений, в том числе и при создании ретранслированных помех.*

***Цель** статьи – повышение помехоустойчивости передачи широкополосных сигналов при действии ретранслированных помех, мощность которых превышает мощность применяемых сигналов.*

***Сущность** предлагаемого решения заключается в использовании для передачи информации широкополосных фазочастотномодулированных сигналов, формируемых при помощи независимых непредсказуемых псевдослучайных последовательностей, различных на передаваемой и непередаваемой частотах. Мгновенные фазы сигналов при этом рандомизируются независимо при передаче на битовых интервалах. С применением современного математического аппарата выводится соотношение для расчета вероятности битовой ошибки. Доказывается, что при правильно выбранных параметрах вероятности битовых ошибок приближаются к величинам, при которых возможно эффективное применение кодов, корректирующих независимые ошибки, что позволит обеспечить надежную доставку важной информации в заданные сроки.*

***Научная новизна** решения состоит в применении для защиты передаваемой информации непредсказуемой псевдослучайной последовательности также на непередаваемой в текущий момент частоте, в рандомизированном сдвиге фазы на каждом битовом интервале при формировании широкополосного сигнала и, кроме того, в оптимизации параметров предлагаемой системы радиосвязи.*

***Теоретическая значимость** состоит в корректном выводе формул для расчета вероятности битовой ошибки и оценке возможности дальнейшего применения корректирующих кодов.*

***Практическая значимость** заключается в возможности проектирования широкополосных систем радиосвязи, обладающих необходимой помехоустойчивостью при действии ретранслированных помех с энергетическим превосходством над легитимными сигналами.*

**Ключевые слова:** *широкополосные сигналы, ретранслированные помехи, псевдослучайные последовательности, некогерентный прием, коды корректирующие ошибки*

**Ссылка для цитирования:** Коржик В.И., Биккенин Р.Р. Система радиосвязи с широкополосными сигналами в условиях присутствия ретранслированных помех // Труды учебных заведений связи. 2025. Т. 11. № 1. С. 26–33. DOI:10.31854/1813-324X-2025-11-1-26-33. EDN:EHOZQY

Original research
https://doi.org/10.31854/1813-324X-2025-11-1-26-33
EDN:EHOZQY

# Wireless System Using Spread Spectrum Signals under the Conditions of Possible Jamming by Retransmitted Interference

**Valery I. Korzhik** ✉, korzhik.vi@sut.ru
**Rafael R. Bikkenin**, bikkenin.rr@sut.ru

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

**Annotation**

*Presently, it is very important to design wireless systems that are resistant to jamming by adversary. It is well known technology to execute so called spread spectrum signals in order to prevent such attacks, especially under the conditions when enemy is superior i1n power against legitimate users. Moreover, adversary is able to estimate legitime signal parameter (type of modulation, duration of intervals ctr) However, such approach be vulnerable in the case of the use by adversary so called retransmitted interferences.*

***The purpose*** *of this article is to increase the efficiency of spread spectrum signals transmission under the action of retransmitted interference, the power of which exceeds the power of the legitimate signals.*

***The essence*** *of the proposed solution is to use spread spectrum phase-frequency modulated signals for information transmission, generated using independent unpredictable pseudorandom sequences that are different at the transmitted and non-transmitted frequencies. Instant phases are randomized independently for bit intervals at the transmitting side. Theoretically, using appropriated mathematical technique, the formula is derived for calculating of the bit error probability for the proposed system with different choice of its parameters. It is proved that for correctly selected parameters, the probabilities of bit errors are approaching to such values that occurs qcceptable to use next* error correcting codes*, which will ensure reliable delivery of important information.*

***The scientific novelty*** *of our method consists in the use an unpredictable pseudorandom sequence at a frequency that is not currently being transmitted, in a randomized phase shift at each bit interval when forming a broadband signal, as well as in optimizing the parameters for the proposed radio communication system, that improved significantly further use of error-correcting code.*

***The theoretical significance*** *consists in the correct proof of the formula for the bit error probabilities and further estimation the conditions for application of error correction codes.*

***The practical significance*** *lies in design of interference proof wireless communication system that after some further elaboration of synchronization system and error correction codes, can be applied in practice under very hard interference environment.*

**Keywords:** *spread spectrum signals, retransmitted interference, pseudorandom sequences, non-coherent receiver, error correcting codes*

**For citation:** Korzhik V.I., Bikkenin R.R. Wireless System Using Spread Spectrum Signals under the Conditions of Possible Jamming by Retransmitted Interference. *Proceedings of Telecommunication Universities.* 2025;11(1):26–33. (in Russ.) DOI:10.31854/1813-324X-2025-11-1-26-33. EDN:EHOZQY

## Введение

Построение систем связи, защищенных от воздействия преднамеренных помех, остается актуальной задачей и в настоящее время. Давно известно [1–4], что эффективным средством защиты от таких помех является использование так называемых *широкополосных сигналов* (ШПС) или иначе – *сигналов с расширенным спектром*. В данной статье рассматриваются только методы *прямого расширения спектра*. В этом случае каждый бит сообщения передается при помощи последовательного генерирования *псевдослучайной последовательности* (ПСП) бит с дополнительной — типично фазовой или частотной модуляцией каждого элемента (*чипа*) этой последовательности.

В работах [1–4] было показано, что, по крайней мере, при когерентном приеме фазомодулированных двоичных сигналов на каждом чипе и невозможности оценки фаз сигналов в каждом чипе постановщиком помех вероятность ошибок принимаемого сообщения $P_e$ будет экспоненциально убывать к нулю при возрастании параметра $q\sqrt{n}$, где $q = U_c^2/U_п^2$ – отношение сигнал / шум в точке приема, а $n$ – база ШПС. Отсюда следует, что при невозможности оценки фаз сигналов в каждом чипе постановщиком помех при условии, что $q \ll 1$, т. е., когда постановщик помех имеет значительное преимущество по мощности по сравнению с легальным пользователем, за счет увеличения базы сигнала $n$ можно обеспечить любую приемлемую для легального пользователя вероятность ошибки бита $P_e$. (Однако, заметим, что при этом происходит обратно пропорциональное $n$ уменьшение скорости передачи сообщений).

Совершенно другой сценарий возникает при возможности создания противником так называемой *ретранслированной модулированной помехи.* В этом случае постановщик помех за минимально короткое время способен обнаружить работающую легитимную станцию, определить параметры ее сигнала (вид модуляции, скорость передачи, длительность посылок и др.), по которым сформировать помеху, а затем настроить свой передатчик и осуществить его излучение. Интервал времени, затрачиваемый на последние процедуры, называется временем реакции станции помех $T_р$. В современных станциях помех $T_р \leq 100$ мкс [5].

При определенных условиях, создавая ретранслированную помеху, постановщик помех имеет возможность демодулировать каждый чип легитимного сигнала на интервале значительно меньшем, чем длительность этого чипа $T_{ch}$, и затем модулировать оставшуюся часть этого чипа случайным образом, сохраняя или инвертируя ее. Схема такого сценария показана на рисунке 1, где $d_{12}$ – расстояние от передающей легитимной станции до станции помех; $d_{13}$ – от передающей до приемной станции легитимных пользователей; $d_{23}$ – от передатчика станции помех до легитимной приемной станции.

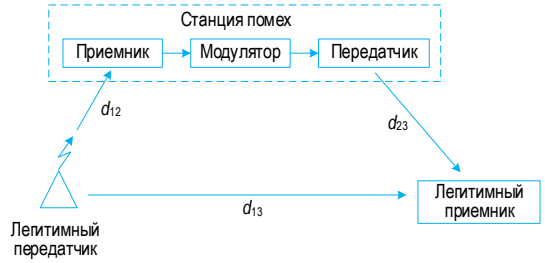


**Рис. 1. Схема сценария создания ретранслированных помех широкополосному сигналу**

*Fig. 1. A Scheme of a Scenario for Retransmitted Interference Creating against Legitimate Spread Spectrum Signal*

Тогда условие малого запаздывания ретранслированной помехи относительно легитимного сигнала можно записать в следующем виде:

$$T_р + \frac{(d_{12} + d_{23} - d_{13})}{C} \ll T_{ch},$$

где $C$ – скорость распространения радиоволн (света); $T_{ch}$ – длительность одного чипа.

Рассмотрим, для примера, частный, но практически реальный случай, когда $d_{12} = 1$ км, $d_{23} = 0{,}5$ км, а «треугольник» распространения радиоволн представим, как треугольник с углом 90 °, напротив стороны длиной $d_{13}$. Тогда $d_{13} = \sqrt{d_{12}^2 + d_{23}^2}$. (Очевидно, что и для любого заданного треугольника расчет расстояния $d_{13}$ не представляет труда). Для рассматриваемого случая получим, что $d_{13} \approx 1{,}12$ км, а $T_р + (d_{12} + d_{23} - d_{13})/C \approx 101$ мкс. Если длительность чипа ШПС равна $T_{ch} = 1$ мс, что соответствует скорости битовой передачи информации $v = 1/(nT_{ch})$, то при этом запаздывание помех относительно полезного сигнала оказывается примерно равным $T_{ch}/10$, т. е. допустимой величине. (Конечно, при другом расположении станций относительно друг друга запаздывание помехи может оказаться и значительно больше, чем $T_{ch}/10$). Рассмотрим далее наиболее благоприятный случай для постановщика помех, когда время запаздывания принимается равным нулю.

В следующих разделах настоящей статьи рассматривается математическая модель системы радиосвязи, предлагаются новые передающие и приемные части алгоритмов, использующих ШПС, рассчитывается вероятность ошибки бита для данного метода и формулируются дополнительные задачи, которые необходимо решить для практической реализации предлагаемой системы защиты ШПС от преднамеренных ретранслированных помех. (Заметим, что данная статья является значительным расширением работы тех же авторов, опубликованной в трудах Международной научно-технической конференции [6]).

## 2. Описание алгоритмов модуляции и демодуляции для ШПС, защищенных от преднамеренных ретранслированных помех

Модулятор формирует сигналы $S_i(t), i = 0, 1$, $t \in (0, T_b)$ для передачи по радиоканалу двоичного символа $i = 0$ или $i = 1$ на битовом интервале $(0, T_b)$ по следующему правилу:

$$S_i(t) = \begin{cases} U_s\, \pi(t) \sin \omega_0 t, \text{для } i = 0 \\ U_s\, \pi'(t) \sin \omega_1 t, \text{для } i = 1' \end{cases} \qquad (1)$$

где $U_s$ – амплитуда сигнала; $\omega_0$ – несущая частота при передаче бита $i = 0$; $\omega_1$ – несущая частота при передаче бита $i = 1$:

$$\pi(t) = \sum_{j=1}^{n} a_j \, \pi(t - jT_{ch}),$$

$$\pi'(t) = \sum_{j=1}^{n} a'_j \, \pi(t - jT_{ch}),$$

$$\pi(t - jT_{ch}) = \begin{cases} 1, t \in [(j-1)T_{ch}, jT_{ch}] \\ 0, t \in [(j-1)T_{ch}, jT_{ch}] \end{cases},$$

где $T_{ch}$ – длительность «чипа» ШПС; $a_j \in \pm 1$ – $j$-й элемент ПСП на передаваемой частоте; $a'_j \in \pm 1$ – $j$-й элемент ПСП на непередаваемой на данном бите частоте; $n = T_b/T_{ch}$ – количество «чипов» на битовом интервале в ШПС (база).

Важнейшим требованием, предъявляемым к ПСП $a'_j$, $j = 1, 2, \ldots, n$, является *непредсказуемость* данной последовательности, если известна ПСП на передаваемой частоте $a_j, j = 1, 2, \ldots, n$, а также непредсказуемость ПСП, если известны все предыдущие элементы ПСП. (К пояснению данного требования авторы еще вернуться при обсуждении процедуры демодуляции).

Канал связи между легитимными пользователями и канал для передачи помехи будем описывать моделью постоянного (незамирающего) канала со случайной фазой ВЧ-несущей. Таким образом, предполагается, что здесь реализуется модель канала *прямой видимости*, т. е. без многолучевости и замираний. Тогда сигнал, принимаемый легитимным демодулятором, будет иметь вид:

$$Z(t) = \mu S_i\left(t, \varphi_{s_i}\right) + n_i(t), i = (0, 1), 0 \le t \le T_b, \quad (2)$$

где $\mu S_i\left(t, \varphi_{s_i}\right)$ – сигнал, представленный в (1); $\varphi_{s_i}$ – случайная фаза, добавляемая в канале связи; $\mu$ – коэффициент затухания сигнала в канале связи; $n_i(t)$ – преднамеренная помеха, создаваемая на передаваемой (или непередаваемой) частоте.

(Заметим, что постановщику помех очевидно известно, на какой частоте передается сигнал для каждого чипа).

Поскольку при обработке на приеме принимаемой смеси ШПС с помехой возникает эффект «обеления» помехи, т. е. она приобретает свойства, подобные естественному шуму, оптимальным демодулятором для легитимного канала связи можно считать оптимальный некогерентный (квадратурный) приемник [7], использующий известные ПСП, как для передаваемой, так и для непередаваемой частот, алгоритм которого имеет вид (3), где $rect(x) = \begin{cases} 0, x \ge 0 \\ 1, x < 0 \end{cases}$.

Наилучшая стратегия помехи для данной легитимной системы ШПС связи состоит в следующем: с вероятностью $1/2$ находится битовый интервал и на нем не передается помеха, и с вероятностью также $1/2$ выбирается битовый интервал и на нем создается инверсная помеха на передаваемой частоте и шумовая помеха на непередаваемой частоте. Это следует из результатов [8], где доказано, что оптимальная помеха как простым, так и сложным сигналам с дискретной фазовой модуляцией, синтезированная без учета информации о начальных фазах передаваемых сигналов, представляет собой также фазомодулированное колебание со значениями информационной фазы, изменяющимися на 180 ° с постоянной величиной амплитуды и со случайной начальной фазой, равномерно распределенной на интервале от 0 до $2\pi$, несущая частота и длительность посылок которой совпадают с соответствующими параметрами сигнала, а моменты смены информационной фазы или полярности элементов помехи и сигнала на входе подавляемого приемника совпадают по времени. При энергетическом превосходстве такой помехи над сигналом в приемнике будет регистрироваться помеха вместо передаваемого сигнала.

После подстановки получаемых в таких случаях принимаемого полезного сигнала с помехой $Z(t)$ в (3) и проведения несложных тригонометрических преобразований находим решающее правило легитимного приемника (4), где $U_{\text{п}}$ – амплитуда помехи; $\varphi = \varphi_s - \varphi_{\text{п}}$ – разность фаз сигнала и помехи; $\varepsilon, \hat{\varepsilon}$ – взаимно независимые гауссовские случайные величины (в силу *центральной предельной теоремы теории вероятностей*), имеющие нулевые математические ожидания и дисперсии $\sigma^2 = U_{\text{п}}^2 T_{ch}^2 n/4$.

$$i = rect\left[\left(\sum_{j=1}^{n} a_j \int_{T_{ch}(j-1)}^{T_{ch}j} Z(t)\cos\omega_0 t dt\right)^2 + \left(\sum_{j=1}^{n} a_j \int_{T_{ch}(j-1)}^{T_{ch}j} Z(t)\sin\omega_0 t dt\right)^2 - \right.$$
$$\left. - \left(\sum_{j=1}^{n} a'_{j+1} \int_{T_{ch}(j-1)}^{T_{ch}j} Z(t)\cos\omega_1 t dt\right)^2 - \left(\sum_{j=1}^{n} a'_{j+1} \int_{T_{ch}(j-1)}^{T_{ch}j} Z(t)\sin\omega_1 t dt\right)^2\right]. \quad (3)$$

$$i = rect\left[\frac{n^2 T_{ch}^2}{4}(U_s^2 + U_{\text{п}}^2 + 2U_s U_{\text{п}}\cos\varphi) - (\varepsilon^2 + \hat{\varepsilon}^2)\right]. \quad (4)$$

Вероятность регистрации бита $i = 1$, когда в действительности передавался бит $i = 0$, равна вероятности того события, что выражение в скобках в формуле (4) будет отрицательным и зависящим от φ, т. е. иметь вид (5), где $\eta = (\varepsilon^2 + \hat{\varepsilon}^2)$; $A = \frac{n^2 T_{ch}^2}{4}(U_s^2 + U_{\text{п}}^2 + 2U_s U_{\text{п}} \cos\varphi)$.

Предполагая (как и раньше), что ε и $\hat{\varepsilon}$ – независимые гауссовские величины с параметрами $(0, \sigma^2)$, получаем, что $\eta = (\varepsilon^2 + \hat{\varepsilon}^2)$ будет случайной величиной, распределенной по *экспоненциальному закону*, т. е. η имеет плотность вероятности (6).

Подставляя (6) в (5), вычисляя интеграл и учитывая, что $\sigma^2 = U_{\text{п}}^2 T_{ch}^2 n/4$, получим (7), где $q_0 = U_s^2/U_{\text{п}0}^2$ – отношение мощностей *сигнал / шум* на передаваемой частоте $\omega_0$; $q_1 = U_s^2/U_{\text{п}1}^2$ – отношение мощностей *сигнал / шум* на непередаваемой частоте $\omega_1$.

Предполагая, что разность фаз φ сигнала и помехи равномерно распределена на интервале от 0 до 2π, получаем в (8) вероятность ошибки $P_e$, усредняя $P_e(\varphi)$ на указанном интервале. (В дальнейшем это утверждение обосновывается тем, что, как будет отмечено впоследствии, эта фаза принудительно рандомизируется на каждом битовом интервале в передатчике. И тогда, как известно, при любых начальных распределениях φ, суммарная фаза будет иметь равномерное распределение на интервале от 0 до 2π. В (8) $I_0\left(\frac{nq_1}{\sqrt{q_0}}\right)$ – модифицированная функция Бесселя первого рода и нулевого порядка [9]:

$$I_0\left(\frac{nq_1}{\sqrt{q_0}}\right) = \frac{1}{2\pi}\int_0^{2\pi} \exp\left[\left(\frac{nq_1}{\sqrt{q_0}}\cos\varphi\right)\right] d\varphi.$$

Найдем оптимальное значение $q_0$, которое обеспечивает постановщику помех наибольшую вероятность ошибки $P_e$. Введем в (8) новую переменную $y = 1/\sqrt{q_0}$. Тогда вместо (8) получим (9).

Для нахождения максимума $P_e(y)$ вычислим производную от (9) и приравняем ее к нулю (10), что эквивалентно решению уравнения (11). (Заметим, что при выводе (10) авторы воспользовались известным фактом [9], что:

$$\frac{dI_0(y)}{dy} = I_1(y),$$

где $I_1(y)$ – модифицированная функция Бесселя первого рода первого порядка).

После простых преобразований (11) получим окончательно уравнение (12), где $a = nq_1$.

Численное решение уравнения (12) дает при $a \geq 5$ приближенный результат $y \approx 1$, т. е. $q_0 \approx 1$. Заметим, что выбор $q_0 = 1$ является физически очевидным, поскольку создание противофазной помехи при совпадении ПСП сигнала на передаваемой частоте и этой помехи, позволит приблизить к нулю сумму сигнала и такой помехи только при одинаковых значениях их амплитуд и фаз.

$$P_e(\varphi) = Pr\left[\frac{n^2 T_{ch}^2}{4}(U_s^2 + U_{\text{п}}^2 + 2U_s U_{\text{п}} \cos\varphi) - (\varepsilon^2 + \hat{\varepsilon}^2) \leq 0\right] = Pr\{\eta \geq A\}. \quad (5)$$

$$w(\eta) = \begin{cases} \frac{1}{2\sigma^2}\exp(-\eta/2\sigma^2), \eta \geq 0 \\ 0, \eta < 0. \end{cases} \quad (6)$$

$$P_e(\varphi) = \int_A^\infty \omega(\eta)\, d\eta = \int_A^\infty \frac{1}{2\sigma^2} e^{-\frac{\eta}{2\sigma^2}}\, d\eta = e^{-\frac{A}{2\sigma^2}} = \exp\left[-\frac{n}{2}\left(q_1 + \frac{q_1}{q_0} + 2\frac{q_1}{\sqrt{q_0}}\cos\varphi\right)\right]. \quad (7)$$

$$P_e = \frac{1}{2\pi}\int_0^{2\pi} \exp\left[-\frac{n}{2}\left(q_1 + \frac{q_1}{q_0} + 2\frac{q_1}{\sqrt{q_0}}\cos\varphi\right)\right] d\varphi = \exp\left[-\frac{n}{2}\left(q_1 + \frac{q_1}{q_0}\right)\right]\frac{1}{2\pi}\int_0^{2\pi} \exp\left(\frac{nq_1}{\sqrt{q_0}}\cos\varphi\right) d\varphi =$$
$$= \exp\left[-\frac{n}{2}\left(q_1 + \frac{q_1}{q_0}\right)\right] I_0\left(\frac{nq_1}{\sqrt{q_0}}\right). \quad (8)$$

$$P_e(y) = \exp\left[-\frac{nq_1}{2}(1 + y^2)\right] I_0(nq_1 y). \quad (9)$$

$$\frac{dP_e(y)}{dy} = -\exp\left[-\frac{nq_1}{2}(1 + y^2)\right] I_0(nq_1 y) nq_1 y + \exp\left[-\frac{nq_1}{2}(1 + y^2)\right] I_1(nq_1 y) nq_1 = 0. \quad (10)$$

$$-I_0(nq_1 y) nq_1 y + I_1(nq_1 y) nq_1 = 0. \quad (11)$$

$$I_1(ay) = y I_0(ay). \quad (12)$$

Что же касается непередаваемой частоты ($\omega_1$, при передаче бита $i = 0$), то на ней необходимо создать максимальный отклик приемника для обеспечения ошибки на этом битовом интервале: постановщик помех должен стремиться к выбору максимальной величины $q_1$. Однако для противодействия получения постановщиком помех максимального отклика на непередаваемой частоте, т. е. максимизации величин $(\varepsilon^2 + \hat{\varepsilon}^2)$, при демодуляции сигнала необходимо, чтобы ПСП $a'_j, j = \overline{1,n}$ на непередаваемой частоте не совпадала бы с ПСП $a_j, j = \overline{1,n}$ на передаваемой частоте этого бита и, более того, знание постановщиком помех ПСП $a_j$ (за счет свойств ретрансляции) никак не помогало бы предсказанию $a'_j$. Иначе на приеме будет выполняться когерентное сложение сигналов на чипах (см. последние два элемента в круглых скобках (3)). И тогда отклик на непередаваемой частоте увеличится и не будет иметь плотности вероятности (6).

Поскольку, с одной стороны, такой метод заведомо приводит к увеличению вероятности ошибки бита $P_e$, а, с другой стороны, его легко исключить, обеспечив независимость ПСП $a_j$ и $a'_j$ на передаваемой и на непередаваемой частотах, соответственно, то расчет $P_e$ для такого случая мы производить не будем.

Описанный выше алгоритм защиты от ретранслированных помех имеет одну негативную особенность, заключающуюся в том, что ошибки, возникающие среди передаваемых бит, могут оказаться сильно коррелированными. Это приведет к сложностям при использовании кодов, корректирующих независимые ошибки. Если же для ослабления этого фактора произвести декорреляцию ошибок при помощи, например *перемежения* битовых символов [7], то такой подход может привести к значительной задержке принимаемых сигналов. Поэтому мы предлагаем ввести на передаче принудительные фазовые сдвиги сигналов на каждом битовом интервале, причем обеспечить статистическую независимость этих фазовых сдвигов при помощи дополнительного чисто случайного генератора. Тогда можно будет полагать, что модель ошибок при использовании корректирующих кодов будет соответствовать биномиальной модели, что существенно упростит выбор кодов, исправляющих лишь независимые ошибки.

Упрощая формулу (8) для случая $q_0 = 1$, получим:

$$P_e = \exp\left[-\frac{n}{2}\left(q_1 + \frac{q_1}{q_0}\right)\right] I_0\left(\frac{nq_1}{\sqrt{q_0}}\right) = \\ = \exp(-nq_1) I_0(nq_1) = \exp(-a) I_0(a), \quad (13)$$

где $a = nq_1$.

В таблице 1 представлены результаты расчета вероятностей битовых ошибок $P_e$, полученных при использовании формулы (13) и выборе оптимизированного параметра $q_0 \approx 1$, а также для различных значений параметра $a = nq_1$.

**ТАБЛИЦА 1. Результаты вычислений вероятностей битовой ошибки $P_e$ по (13) при $q_0 = 1$ и различных значениях параметра $a = nq_1$**

*TABLE 1. Results of the Bit Error Probability Calculation by (13) under and Different Values*

| $a$ | 10 | 20 | 50 | 100 | 1000 | 5000 | 10000 |
|---|---|---|---|---|---|---|---|
| $P_e$ | 0,13 | 0,0905 | 0,057 | 0,0399 | 0,012 | 0,00564 | 0,00399 |

Результаты, представленные в таблице 1, показывают, что, например, даже при двухкратном превосходстве по мощности помехи над полезным сигналом, когда $q_1 = 0{,}5$, а база легитимного сигнала $n = 100$, параметр $a = 50$, и ему будет тогда соответствовать вероятность ошибки $P_e \approx 0{,}057$.

Согласно формуле Шеннона, для пропускной способности двоичного симметричного канала без памяти [10] выражение для расчета пропускной способности можно записать в следующем виде:

$$C = 1 + P_e \log_2 P_e + (1 - P_e)\log_2(1 - P_e). \quad (14)$$

Подставляя $P_e \approx 0{,}057$ в (14), получим $C \approx 0{,}449$, что дает надежду на повышение достоверности при использовании даже жесткого декодирования корректирующими кодами (например, LDPC, *аббр. от англ.* Low-Density Parity-Check Code, кодами с малой плотностью проверок на четность [11, 12] или турбокодами [11, 13]) без катастрофического снижения скорости передачи данных по легитимному каналу.

Произведем ориентировочный расчет времени задержки передачи данных для предложенного метода. Ранее в статье было отмечено, что можно ожидать битовой скорости до 10 кбит/с в канале связи. Тогда длительность одного чипа будет равна 0,1 мс, и, следовательно, длительность соответствующей передачи одного бита при $n = 100$ оказывается 10 мс. Если теперь выбрать корректирующий код с длиной блока 100 и кодовой скоростью 0,4 (см. выражение (14)), получим, что 40 бит данных могут быть надежно (при адекватном выборе кода) переданы легитимному корреспонденту примерно за время 1 с. Конечно, это достаточно большая величина, при которой могут быть надежно приняты разве лишь короткие сообщения. Но такая оценка позволяет понять, насколько эффективны ШПС при возможности создания ретранслированных помех. Очевидно, что такая оценка может быть уточнена с учетом реальных параметров сигналов и ограничений на требуемое время доставки определенных объемов данных.

## 3. Заключение

В предложенной вниманию читателей журнала «Труды учебных заведений связи» статье авторы предлагают систему ШПС в условиях радиоэлектронного подавления и, в частности, для наиболее тяжелого ее сценария – создания ретранслированной помехи, которая при превосходстве ее мощности над мощностью сигналов способна полностью подавить легитимную линию связи, использующую традиционные методы ШПС. Такой сценарий не принадлежит к фантазиям авторов, а соответствует реальной ситуации, когда станция помех расположена достаточно близко от подавляемого приемника.

Хотя использование фазомодулированных и частотно-модулированных сигналов, по-видимому, не является новым, однако авторы полагают, что применение непредсказуемой ПСП на непередаваемой частоте может претендовать на некоторую оригинальность. Также оригинальным является рандомизированный сдвиг фаз на каждом битовом интервале, что существенно улучшает дальнейшее применение корректирующих ошибки кодов.

Заметим, что теоретический расчет вероятностей битовых ошибок $P_e$ по формуле (13), а также оптимизация параметра $q_0$, являются новыми результатами. Причем важно отметить, что достоверность получения этих результатов не требует никакой дополнительной экспериментальной проверки исходной модели, поскольку нормализация помехи $(\varepsilon^2 + \hat{\varepsilon}^2)$ в (4) достаточно надежно обеспечивается при хороших свойствах датчика ПСП и достаточно большой базе сложного сигнала $n$, а равномерная случайность и взаимная независимость на битовых интервалах фазы $\varphi$ выполняется принудительно при помощи хорошего генератора шума.

Конечно, было бы интересно проверить всю предложенную модель системы связи в условиях ретранслированных помех при помощи имитационного компьютерного моделирования, но, как было только что отмечено, это не является необходимым для подтверждения достоверности теоретических выводов.

Заметим, однако, что прежде, чем пытаться реализовать данную систему на практике, необходимо тщательно проработать алгоритм синхронизации по битовым и блоковым интервалам в условиях помех, в том числе и специально ориентированных на подавление именно такой системы связи [14, 15]. Наконец, для того, чтобы окончательно убедиться в отсутствии дополнительных уязвимостей предлагаемой системы связи от воздействия радиоэлектронного подавления, необходимо проверить, не сможет ли постановщик помех с высокой точностью оценить мгновенную фазу передаваемого легитимного сигнала, поскольку в противном случае он сумеет создать в точности противофазную помеху (см. $\varphi = \pi$ в формуле (5)), и тогда реализуется полный «обрыв» легитимного канала передачи данных.

Интересно отметить, что в отличие от случая применения ШПС при отсутствии ретранслированных помех (т. е. при «невычислимости» ПСП постановщиком помех), вероятность битовой ошибки $P_e$ достаточно быстро убывает с ростом базы сигнала $n$ (см. [1–4]). В то же время, как видно из таблицы 1, при фиксированной величине $q_1$ вероятность ошибки $P_e$ с ростом $n$ убывает сравнительно медленно. По-видимому, это та «цена», которую необходимо «заплатить» за присутствие ретранслированной помехи. Тем не менее $P_e$, хоть и медленно, но, все же монотонно убывает, что позволяет обеспечить надежную связь при дальнейшем использовании корректирующих кодов.

**Список источников**


1. Proakis J. Digital Communications. N.Y.: McGraw-Hill, 1995.
2. Dixon R.C. Spread Spectrum Systems. John Willy and Sons, 1979.
3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Пер. с англ. М.: Вильямс, 2007. 1104 с.
4. Голдсмит А. Беспроводные коммуникации. Пер. с англ. М.: Техносфера, 2011. 904 с. EDN:QMWIPL
5. Борисов В.И., Зинчук В.М., Лимарев А.Е. [и др.] Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. М.: Радио и связь, 2003. 384 с. EDN:QMMHCF
6. Korjik V., Bikkenin R. Performance analysis of the enhanced PN spread spectrum system in the presence of jamming by modulated retransmitted signal // Proceedings of the 5th International Symposium on Spread Spectrum Techniques and Applications (Sun City, South Africa, 04–04 September 1998). IEEE, 1998. PP. 809–811. DOI:10.1109/ISSSTA.1998.722490
7. Финк Л.М. Теория передачи дискретных сообщений. М.: Советское радио, 1970. 728 с.
8. Агафонов А.А., Ложкин К.Ю., Поддубный В.Н. Методология и результаты синтеза и оценки эффективности преднамеренных помех приемникам дискретных сигналов // Радиотехника и электроника. 2003. Т. 48. № 8. С. 956–962. EDN:OOQISJ
9. Справочник по специальным функциям с формулами, графиками и таблицами / Под ред. М. Абрамовица и И. Стиган. Пер. с англ. М.: Наука, 1979. 832 с.
10. Шеннон К.Э. Работы по теории информации и кибернетике. Пер. с англ. М.: Изд-во иностр. лит., 1963. 830 с.
11. MacKay D.J.C., Neal R.M. Near Shannon Limit Performance of Low-Density Parity Check Codes // Electronics Letters. 1996. Vol. 32. Iss. 18. DOI:10.1049/el:19961141

12. MacKay D.J.C. Information Theory, Inference and Learning Algorithms. Cambridge University Press, 2003. 640 p.
13. Berrou C., Glavieux A., Thitmajshima P. Near optimum error correcting coding and decoding: Turbo-codes // IEEE Transactions on Commutations. 1996. Vol. 44. Iss. 10. PP. 1261–1271. DOI:10.1109/26.539767
14. Журавлев В.И. Поиск и синхронизация в широкополосных системах. М.: Радио и связь, 1986. 240 с. EDN:WIYMEJ
15. Борисов В.И., Зинчук В.М., Лимарев А.Е., Мухин Н.П., Нахмансон Г.С. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью. М.: Радио и связь, 2003. 640 с.

**References**

1. Proakis J. *Digital Communications*. N.Y.: McGraw-Hill; 1995.
2. Dixon R.C. *Spread Spectrum Systems*. John Willy and Sons; 1979.
3. Sklar B. *Digital Communications. Fundamentals and Applications*. Prentice Hall; 2001.
4. Goldsmith A. *Wireless Communications*. Cambridge University Press; 2005.
5. Borisov V.I., Zinchuk V.M, Limarev A.E., Muhin N.P., Shestopalov V.I. ECM-Resistance of Frequency-Hopping of Spread – Spectrum Communications Systems. Moscow: Radio and Communications Publ.; 2003. 384 p. (in Russ.) EDN:QMMHCF
6. Korjik V., Bikkenin R. Performance analysis of the enhanced PN spread spectrum system in the presence of jamming by modulated retransmitted signal. *Proceedings of the 5th International Symposium on Spread Spectrum Techniques and Applications*, 04–04 September 1998, Sun City, South Africa. IEEE; 1998. p.809–811. DOI:10.1109/ISSSTA.1998.722490
7. Fink L.M. *Theory of Transmission of Discrete Messages.* Moscow: Soviet Radio Publ.; 1970. 728 p. (in Russ.)
8. Agafonov A.A., Lozhkin K.Yu., Poddubny V.N. Methodology and Results of Synthesis and Estimation of the Efficiency of Malicious Interferences for Discrete Signal Receivers. *Journal of Radio Electronics.* 2003;48(8):956–962. (in Russ.) EDN:OOQISJ
9. Abramowitz M. Stegun I.A. *Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables*. National Bureau of Standards Applied Mathematics Series. 55. Issued June 1964.
10. Shannon C.E. A mathematical theory of communication. *Bell System Technical Journal*. 1948;27:379–423 and 623–656.
11. MacKay D.J.C., Neal R.M. Near Shannon Limit Performance of Low-Density Parity Check Codes. *Electronics Letters*. 1996;32(18). DOI:10.1049/el:19961141
12. MacKay D.J.C. *Information Theory, Inference and Learning Algorithms*. Cambridge University Press; 2003. 640 p.
13. Berrou C., Glavieux A., Thitmajshima P. Near optimum error correcting coding and decoding: Turbo-codes. *IEEE Transactions on Commutations*. 1996;44(10):1261–1271. DOI:10.1109/26.539767
14. Zhuravlev V.I. *Search and Synchronization in Spread Spectrum Systems*. Moscow: Radio and Communications Publ.; 1986. 240 p. (in Russ.) EDN:WIYMEJ
15. Borisov V.I., Zinchuk V.M., Limarev A.E., Mukhin N.P., Nakhmanson G.S. Noise Immunity of radio communication systems with Spread Spectrum Signal by Carrier Pseudorandom Sequence Modulation. Moscow: Radio and Communications, Publ.; 2003. 640 p. (in Russ.)

Статья поступила в редакцию 24.01.2025; одобрена после рецензирования 03.02.2025; принята к публикации 17.02.2025.
The article was submitted 24.01.2025; approved after reviewing 03.02.2025; accepted for publication 17.02.2025.

# Информация об авторах:

**КОРЖИК Валерий Иванович** — доктор технических наук, профессор, профессор кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
https://orcid.org/0000-0002-8347-6527

**БИККЕНИН Рафаэль Рифгатович** — доктор технических наук, профессор, профессор кафедры электроники Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича

Коржик В.И. является членом редакционного совета журнала «Труды учебных заведений связи» с 2016 г., но не имеет никакого отношения к решению опубликовать эту статью. Статья прошла принятую в журнале процедуру рецензирования. Об иных конфликтах интересов авторы не заявляли.

Korzhik V.I. has been a member of the journal "Proceedings of Telecommunication Universities" Editorial Council since 2016, but has nothing to do with the decision to publish this article. The article has passed the review procedure accepted in the journal. The authors have not declared any other conflicts of interest.