УДК 621.376.9
doi:10.31799/1684-8853-2026-5-56-72
EDN: CMAJJN

Научные статьи
Articles

Способ формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей псевдослучайной последовательности

С. В. Штанько[а], *доктор техн. наук, доцент, orcid.org/0000-0002-8391-8911, vka@mil.ru*
В. А. Крягин[а], *преподаватель, orcid.org/0009-0002-7529-283X*
П. Н. Топчий[а], *преподаватель, orcid.org/0009-0008-4678-7685*
Д. А. Аникин[б], *начальник отдела, orcid.org/0009-0003-8295-312X*
[а]*Военно-космическая академия им. А. Ф. Можайского, Ждановская наб., 13, Санкт-Петербург, 197198, РФ*
[б]*Министерство обороны Российской Федерации, Знаменка ул., 19, Москва, 119160, РФ*

Введение: *радиостеганографические методы, основанные на встраивании стегосигнала в открытый сигнал-контейнер на физическом уровне, позволяют решить задачу обеспечения конфиденциальности информации и, в отличие от криптографических методов, скрыть сам факт передачи информации по радиоканалу, однако требуют обеспечения энергетической скрытности стегосигнала и стойкости к попыткам его обнаружения злоумышленником.* ***Цель:*** *разработать способ энергетического маскирования радиосигнала внутри сигнала-контейнера на основе дополнительной фазовой манипуляции и нелинейной расширяющей псевдослучайной последовательности, обеспечивающего скрытую передачу информации по стегоканалу с заданной помехоустойчивостью для легального абонента и невозможность обнаружения стегосигнала злоумышленником.* ***Результаты:*** *предложен способ формирования стегосигнала путем дополнительной фазовой манипуляции малым углом вектора фазоманипулированного сигнала-контейнера. Угол отклонения выбирался из условия маскировки энергии одного чипа в пределах дисперсии фазового шума. Расширение спектра стегосигнала выполнялось нелинейной псевдослучайной последовательностью, формируемой генератором нелинейной псевдослучайной последовательности, стойкой к анализу. Получены аналитические соотношения для вероятности правильного обнаружения и вероятности битовой ошибки. Показано, что при длине расширяющей последовательности 16 383 элемента легальный абонент достигал вероятности правильного обнаружения 0,9972 при отношении энергии чипа к спектральной плотности шума $q = -33$ дБ, тогда как злоумышленник при поэлементном приеме не может обнаружить стегосигнал при $q < 0$ дБ. Вероятность битовой ошибки менее 10^{-8} достигалась при $q = -30$ дБ, а злоумышленнику требовалось более 12 дБ — разница составила 42 дБ. Разработан стенд полунатурного моделирования на базе программно-определяемых радиоустройств; отклонение экспериментальных данных от расчетных не превысило пяти процентов.* ***Практическая значимость:*** *способ применим к широкому классу цифровых радиосистем с фазовой манипуляцией и может использоваться для передачи данных по встроенному каналу в системах критической информационной инфраструктуры.*

Ключевые слова *— фазовая манипуляция, псевдослучайная последовательность, фазовая диаграмма, сигнал-контейнер, расширяющая последовательность, корреляционный прием, стегосигнал, стегосообщение, нелинейная расширяющая последовательность.*

Для цитирования: Штанько С. В., Крягин В. А., Топчий П. Н., Аникин Д. А. Способ формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей псевдослучайной последовательности. *Информационно-управляющие системы*, 2026, № 5, с. 56–72. doi:10.31799/1684-8853-2026-5-56-72, EDN: CMAJJN
For citation: Shtanko S. V., Kryagin V. A., Topchiy P. N., Anikin D. A. A method for generating a radio steganographic signal based on additional phase modulation and a nonlinear pseudorandom expansion sequence. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 56–72 (In Russian). doi:10.31799/1684-8853-2026-5-56-72, EDN: CMAJJN

Введение

В современных условиях развитие глобальных систем связи и передачи данных приводит к непрерывному возрастанию требований к безопасности информации, циркулирующей в таких системах, в частности, ее составляющей — конфиденциальности. Особенно актуально это для объектов критической информационной инфраструктуры [1], под которыми понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы специального назначения, предназначенные для управления субъектами критической информационной инфраструктуры (МВД, МЧС, здравоохранения, транспортной инфраструктуры и т. д.). В более значительной степени подвержены угрозам нарушения конфиденциальности системы, элементы которых объединены радиоканалами, ввиду их пространственной доступности [2].

Основу системы обеспечения конфиденциальности информации в указанных системах, как правило, составляют криптографические методы. Их применение реализует ограничение (предотвращение) доступа к семантике передаваемых

данных для всех, кроме пользователей, обладающих некоторыми закрытыми параметрами — ключами. Результаты анализа потоков данных (трафика), включая интенсивность, объем и динамику передачи сообщений, сами по себе могут быть источником информации для злоумышленника, даже без получения доступа к смыслу передаваемых данных. Поэтому для некоторых задач желательным является не только сокрытие смысла передаваемой информации, но и самого факта ее передачи. Для решения задач скрытой передачи данных по встроенному каналу используются стеганографические методы, позволяющие встраивать некоторую дополнительную информацию (стегосообщение) в открытую информацию (контейнер). Такие методы реализуются на уровне обработки информации и не зависят от носителя (канала передачи) информации. Например, широко известен подход, связанный с внедрением скрытой информации в двоичные файлы (изображения, видео). При этом без знания ключевой информации злоумышленник не может не только получить доступ к смыслу встроенной информации, но и установить сам факт ее наличия [3].

Аналогичный подход может быть применен и на физическом уровне. В этом случае уже элементы сигнала, являющегося носителем дополнительной информации, встраиваются в сигнал — носитель основной информации. Радиостеганографические методы основаны на встраивании стегосигнала в сигнал-контейнер (открытый носитель). В этом случае под сокрытием передачи информации следует понимать не только невозможность ее обнаружения при перехвате и получения доступа к ее смыслу, но и сокрытие самого факта передачи по каналу радиосвязи какой-либо информации помимо той, которая содержится в сигнале-контейнере. Поскольку такие методы реализуются фактически на физическом уровне, это значительно затрудняет потенциальному злоумышленнику не только задачу анализа добытых данных, в том числе на предмет содержания в контейнере встроенной информации, но и регистрацию и прием сигнала-носителя такой информации (стегосигнала).

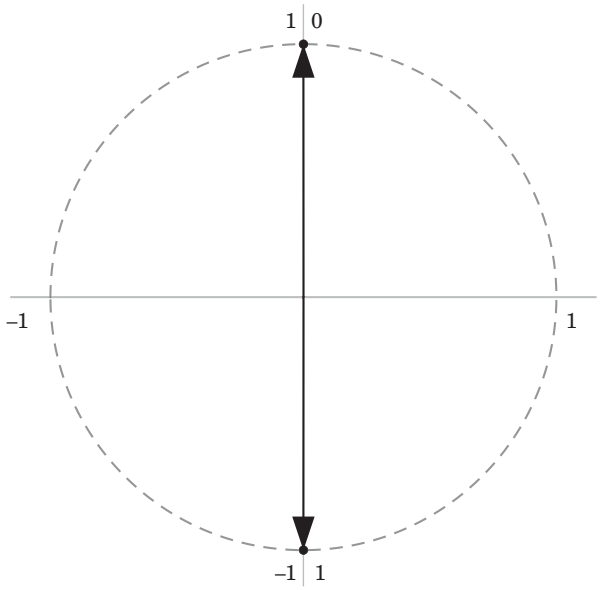
В статье предлагается способ формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей псевдослучайной последовательности, позволяющий осуществлять прием стегосигнала с требуемой помехоустойчивостью легальному абоненту с одной стороны и значительно ограничивающий возможности злоумышленника по обнаружению и приему стегосигнала с другой. Ряд частных результатов, положенных в основу настоящей работы, докладывался авторами ранее применительно к смежным задачам — передаче информации по космическим радиолиниям [4] и защите навигационных сигналов от имитационных воздействий [5]. В настоящей статье они впервые объединены в рамках единого способа формирования радиостеганографического сигнала, что и составляет ее основной научный результат.

Описание способа формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей псевдослучайной последовательности

В основе предлагаемого способа лежит использование дополнительной фазовой манипуляции малым углом в структуре существующего радиосигнала-контейнера. На первом этапе для упрощения понимания в качестве сигнала-контейнера рассмотрим бинарный (двухпозиционный) фазоманипулированный сигнал ФМ-2 с 0 – π манипуляцией (рис. 1), описываемый аналитическим выражением

$$S_{\text{ФМ2}}(t) = AG(t)\cos(\omega_0 t), \qquad (1)$$

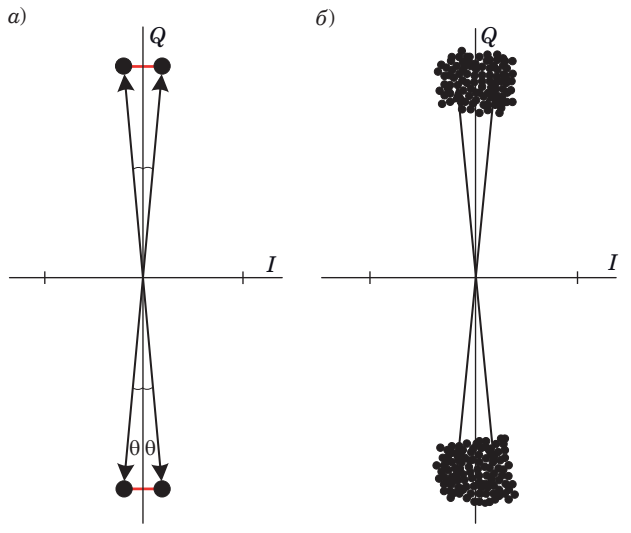
где A — амплитуда сигнала; $G(t)$ — бинарная расширяющая псевдослучайная последовательность (ПСП), модулированная информационной последовательностью, принимающая значения ±1 и обеспечивающая инверсию фазы несущей (0 – π манипуляция); ω_0 — несущая частота.



■ ***Рис. 1.*** Фазовая диаграмма сигнала ФМ-2
■ ***Fig. 1.*** Phase diagram of the FM-2 signal

Опишем способ внедрения (маскирования) двоичного стегосигнала в сигнал-контейнер (1). Чтобы внедрить данные, необходимо дополнительно изменять (модулировать) параметры сигнала-контейнера, но делать это необходимо так, чтобы посторонний наблюдатель не мог зарегистрировать эти изменения (принять стегосигнал). Внедрение происходит путем формирования дополнительной фазовой составляющей на основе сигнала-контейнера (1). С этой целью будем отклонять вектор, описывающий сигнал-контейнер в каждом из возможных положений, на дополнительный угол $\pm\theta$ (рис. 2, *а*) так, чтобы значение модуля вектора разности не превышало величину, соответствующую дисперсии шумов. Угол θ определим следующим образом: $\theta = \theta_0 \cdot L_{ст}(t) \cdot B(t)$, где $L_{ст}(t)$ — бит встраиваемого сообщения; $B(t)$ — бинарная ПСП, принимающая значения ± 1. Вектор сигнала-контейнера при его отклонении на дополнительный угол модуляции θ должен находиться в пределах зоны неопределенности, ограниченной дисперсией фазового шума (рис. 2, *б*).

Очевидно, что в этом случае посимвольное обнаружение и прием будут невозможны ввиду малой энергии стегосигнала. Однако, если модулировать стегосигнал расширяющей последовательностью и осуществлять корреляционный прием с накоплением символов расширяющей ПСП, используя достаточно большой период накопления, можно добиться требуемого отношения сигнал/шум для стегосигнала. Платой за это будет относительно низкая скорость передачи данных.

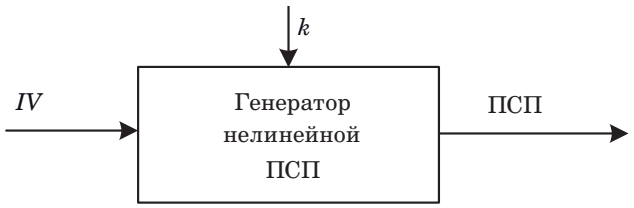


■ ***Рис. 2.*** Фазовая диаграмма сигнала-контейнера с дополнительной модуляцией, формирующей стегосигнал при отсутствии (*а*) и наличии (*б*) шума

■ ***Fig. 2.*** Constellation diagram of the cover signal with additional modulation forming the stego signal in the absence (*а*) and in the presence (*б*) of noise

В этом случае вектор разности, полученный в результате отклонения на угол $+\theta$, соответствует чипу расширяющей ПСП стегосигнала «1», $-\theta$ — «0». Другими словами, знак отклонения на дополнительный угол определяется произведением информационного бита $L_{ст}(t)$ и символа расширяющей ПСП $B(t)$. При корреляционном приеме с известной последовательностью $B(t)$ легальный абонент восстанавливает биты $L_{ст}(t)$ путем накопления энергии за период ПСП. Расчеты, подтвержденные экспериментом, показывают, что существует возможность выбора такого диапазона значений параметров сигнала-контейнера и стегосигнала (длительность символа сигнала-контейнера; угол θ, определяющий энергию стегосигнала; период накопления; количество чипов расширяющей ПСП в информационном символе стегосигнала и т. д.), при котором энергии информационного символа, накопленного легальным абонентом сигнала при условии знания им расширяющей ПСП стегосигнала, достаточно для его качественного (с заданной помехоустойчивостью) обнаружения и корреляционного приема. В то же время в условиях отсутствия сведений о структуре расширяющей ПСП у потенциального злоумышленника накопление и выделение им энергии информационного символа невозможно, а энергии одного чипа расширяющей ПСП недостаточно для его выделения и почипового обнаружения и приема.

Для того чтобы вероятный злоумышленник не имел возможности подобрать структуру расширяющей ПСП стегосигнала, в качестве таковой следует использовать нелинейную последовательность, отличающуюся высокой структурной скрытностью (формируемую с использованием специальных нелинейных функций) [6]. При этом необходимо учитывать, что такая последовательность должна иметь хорошие корреляционные свойства, позволяющие реализовывать корреляционный прием и обработку такого сигнала с требуемой помехоустойчивостью [7, 8]. Известно, что качественные криптографические алгоритмы обладают корреляционными свойствами, близкими к корреляционным свойствам истинно случайной последовательности при условии достаточно большого периода накопления [9, 10]. В этом смысле их использование позволит осуществлять корреляционный прием с требуемым качеством при условии выполнения достаточно жестких требований к вопросам синхронизации в процессе выделения стегоканала из канала-контейнера, однако эта задача может быть успешно решена с помощью самого сигнала-контейнера. Выполненные оценки показывают, что для последовательностей указанного типа при достаточно большом периоде накопления (16 000 элементов) максимальный уровень боковых лепестков автокорреляционной функции не превышает –28 дБ



IV – параметр начального состояния генератора

■ ***Рис. 3.*** Способ формирования нелинейной ПСП

■ ***Fig. 3.*** Nonlinear pseudorandom sequence generation method

относительно главного максимума, а уровень взаимно-корреляционной функции не превышает –27 дБ, что не хуже соответствующих показателей линейных ПСП той же длины и не приводит к снижению помехоустойчивости корреляционного приема.

В качестве расширяющей можно использовать, например, нелинейную ПСП, получаемую с помощью генератора ПСП, работающего на основе криптографического алгоритма «Кузнечик» [6]. Для этого источник и получатель должны обладать общим закрытым параметром, являющимся аналогом ключа k (рис. 3), на основе которого они смогут формировать идентичную нелинейную ПСП, используемую для расширения спектра сигнала и корреляционного приема соответственно.

Последовательность вырабатывается в режиме гаммирования с обратной связью по выходу: вектор начального состояния IV зашифровывается на ключе k, результат каждой итерации подается на вход следующей, а искомая последовательность образуется конкатенацией полученных блоков:

$$Y_1 = E(IV, k),\ Y_i = E(Y_{i-1}, k),\ B = Y_1 \| Y_2 \| \ldots \| Y_n,$$

где IV — вектор начального состояния (128 бит); k — ключ (256 бит); $E(\cdot)$ — функция зашифрования 128-битного блока.

Стороны, обладающие общими k и IV, при наличии синхронизации формируют идентичную апериодическую последовательность требуемой длины. Предложенный способ сохраняет работоспособность при использовании любого алгоритма с требуемой стойкостью и скоростью выработки.

Вычислительная сложность формирования такой ПСП невелика. Требуемая скорость ее выработки определяется чиповой скоростью сигнала-носителя и для широкополосных радиосистем составляет единицы-десятки мегабит в секунду, что на два-три порядка ниже производительности известных программных и аппаратных реализаций алгоритма «Кузнечик» и обеспечивает формирование ПСП в реальном времени со значительным запасом.

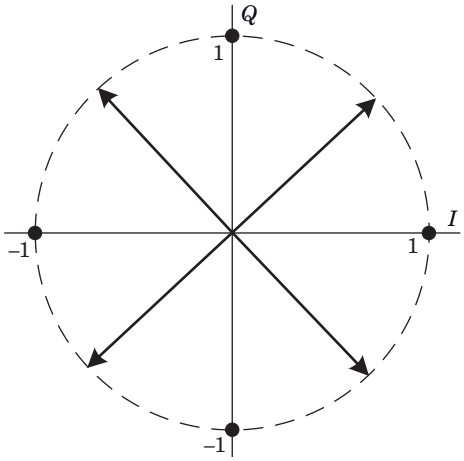
Следует отметить, что реализация описанного подхода в значительной степени затруднена сложностью поиска и обнаружения стегосигнала, поскольку элементарный чип последовательности обладает очень низкой энергией. Однако при предъявлении достаточно высоких требований к синхронизации сигнала-контейнера и стегосигнала и их когерентной обработке данная проблема успешно может быть решена, поскольку синхронизация будет осуществляться при помощи сигнала-носителя, а поиск стегосигнала будет выполняться по элементам структуры сигнала-носителя (например, по специальным синхропосылкам). В этом смысле удобным представляется использование в качестве сигнала-носителя сигнала цифровой широкополосной радиосистемы, реализующей высокую степень синхронизации и использующей радиосигнал с квадратурным уплотнением. Такой сигнал можно рассматривать как четырехуровневый фазоманипулированный радиосигнал ФМ-4 [11–13]. В этом случае доплеровский сдвиг и многолучевое распространение отрабатываются штатными средствами системы-носителя. Доплеровская расстройка устраняется слежением за несущей сигнала-контейнера, а многолучевость разрешается корреляционной обработкой широкополосного сигнала-контейнера, поскольку при разности хода лучей, превышающей длительность чипа, побочные лучи разделяются и не искажают основной корреляционный пик. Синхронизация стегоканала выполняется не по слабому стегосигналу, а по сигналу-контейнеру, поэтому малый угол дополнительной фазовой модуляции ее не усложняет. В реализованном макете тактовая синхронизация стегоканала осуществлялась по периодической метке, представляющей собой заранее заданную короткую двоичную последовательность, передаваемую в канале-контейнере.

Рассмотрим для примера в качестве сигнала-контейнера (носителя) радиосигнал цифровой широкополосной радиосистемы с квадратурным уплотнением. Пусть сигнал представляет собой фазоманипулированный радиосигнал ФМ-4. Аналитическая запись такого радиосигнала с квадратурным уплотнением имеет вид

$$S_{\text{кон}}(t) = AG_I(t)\cos(\omega_0 t) - AG_Q(t)\sin(\omega_0 t), \quad (2)$$

где A — амплитуда квадратурных компонент радиосигнала; $G_{I,Q}$ — модулирующие последовательности соответствующих квадратурных составляющих, принимающие значения ±1; ω_0 — круговая несущая частота.

Сигнальное созвездие для всех возможных комбинаций значений G_I и G_Q представлено на рис. 4.



■ ***Рис. 4.*** Фазовая диаграмма сигнала-контейнера ФМ-4
■ ***Fig. 4.*** Phase diagram of the FM-4 signal container

Маскированный сигнал (стегосигнал) формируется следующим образом. Каждый символ встраиваемого сообщения $L_{ст}(t)$ модулирует по фазе расширяющую последовательность стегосообщения – нелинейную ПСП с высокой структурной скрытностью $B(t)$, формируемую с помощью ключа k генератором нелинейной ПСП, $S_{ст}(t) = L_{ст}(t) \otimes B(t)$. В данном случае при формировании стегосигнала так же, как и при формировании сигнала-контейнера, используется метод прямого расширения спектра сигнала с помощью нелинейной ПСП, при этом принято ограничение: длительность символа расширяющей последовательности стегосигнала должна быть кратной длительности передаваемого символа расширяющей последовательности сигнала-контейнера.

Для того чтобы изменения фазы, соответствующие символам расширяющей последовательности стегосигнала $S_{ст}(t)$, были неразличимы на уровне шумов [14], угол θ выбирается из условия маскировки энергии одного чипа стегосигнала в фазовом шуме: $\theta_0^2 \le \sigma_\varphi^2$. При этом каждый информационный бит соответствует N чипам расширяющей ПСП, и только накопленная за период расширения энергия, пропорциональная $N\theta_0^2$, обеспечивает требуемое отношение сигнал/шум при корреляционном приеме. Другими словами, выбор больших значений базы стегосигнала позволяет обеспечить заданную помехоустойчивость, однако платой за это является снижение скорости передачи информации в стегоканале.

Рассмотрим полную аналитическую модель совмещенного сигнала $S_{сов}(t)$, содержащего стегосигнал $S_{ст}(t)$ в сигнале-контейнере $S_{кон}(t)$. Совмещенный сигнал образуется дополнительной фазовой модуляцией сигнала-контейнера стегосигналом:

$$S_{сов}(t) = \\ = AG_I(t)\cos[\omega_0 t + \theta(t)] - AG_Q(t)\sin[\omega_0 t + \theta(t)]. \quad (3)$$

Эквивалентная запись совмещенного сигнала в комплексной форме имеет вид

$$\tilde{S}_{сов}(t) = \tilde{S}_{кон}(t)e^{j\theta(t)}; \quad (4)$$

$$S_{сов}(t) = \Re\left\{\tilde{S}_{кон}(t)e^{j\theta(t)}\right\}; \quad (5)$$

$$\tilde{S}_{кон}(t) = A[G_I(t) + jG_Q(t)]e^{j\omega_0 t}. \quad (6)$$

Выражение (3) для малых углов $\theta(t) << 1$ можно представить в виде приближенного выражения, полученного разложением в ряд Тейлора:

$$S_{сов}(t) \approx S_{кон}(t)\cos[\theta(t)] + S^{\perp}_{кон}(t)\sin[\theta(t)]. \quad (7)$$

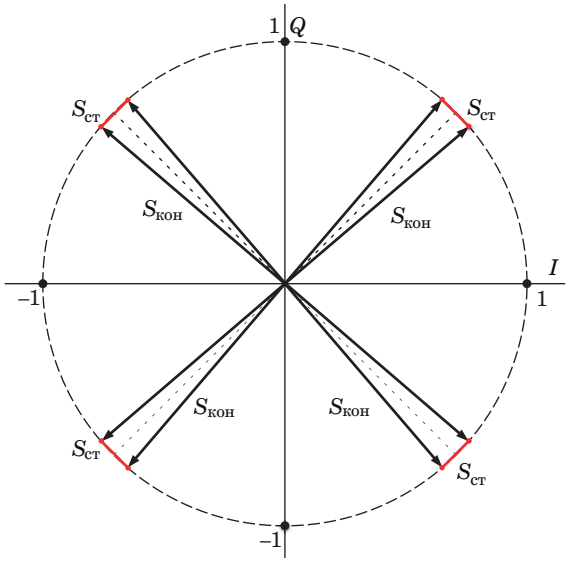
При $\cos\theta \approx 1$, $\sin\theta \approx \theta$

$$S_{кон}(t) = AG_I(t)\cos\omega_0 t - AG_Q(t)\sin\omega_0 t; \quad (8)$$

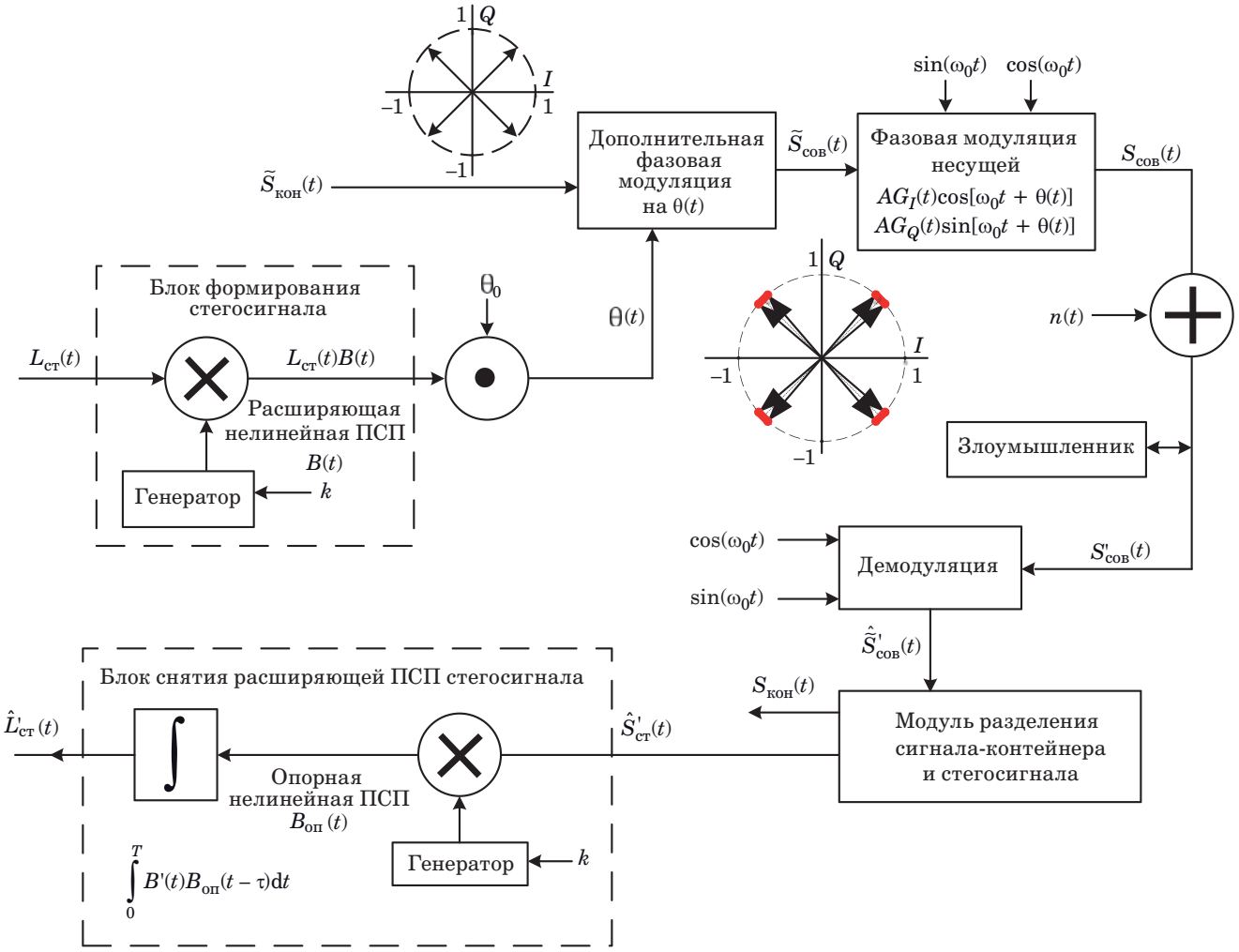
$$S_{сов}(t) \approx S_{кон}(t) + \theta(t) \cdot S^{\perp}_{кон}(t), \quad (9)$$

где $S^{\perp}_{кон}(t) = AG_Q(t)\cos\omega_0 t + AG_I(t)\sin\omega_0 t$ – сигнал, ортогональный сигналу-контейнеру в комплексной плоскости (I, Q), определяющий направление поворота созвездия.

Поясним физический смысл приведенных соотношений. Дополнительная фазовая манипуляция $\theta(t)$ поворачивает комплексный вектор сигнала-контейнера в каждой позиции созвездия (определяемой комбинацией $G_I(t)$, $G_Q(t)$) на угол $\pm\theta(t)$ по закону чипов расширяющей последовательности стегосигнала. Величина θ_0 выбирается из условия энергетической маскировки. Фазовая диаграмма совмещенного сигнала представлена на рис. 5.



■ ***Рис. 5.*** Фазовая диаграмма совмещенного сигнала
■ ***Fig. 5.*** Phase diagram of the combined signal



■ ***Рис. 6.*** Модель процесса формирования, передачи и приема совмещенного сигнала
■ ***Fig. 6.*** Model of combined signal generation, transmission, and reception process

Затем полученный совмещенный сигнал моделирует высокочастотный сигнал и передается абоненту-получателю. Модель процесса формирования, передачи и приема совмещенного сигнала (стегосигнала и сигнала-контейнера) представлена на рис. 6.

При приеме совмещенного комплексного радиосигнала $S'_{сов}(t)$ в смеси с шумом $n(t)$ абонент-получатель производит его демодуляцию и выделение стегосигнала из совмещенного. Для этого после демодуляции абонент-получатель осуществляет разделение сигнала-контейнера и стегосигнала. С этой целью на основе принятой комплексной огибающей $\hat{\tilde{S}}'_{сов}(t)$ формируется оценка сигнала-контейнера $\tilde{S}'_{кон}(t)$ путем принятия решений по символам расширяющей последовательности контейнера. Стегосигнал выделяется как разность принятого совмещенного сигнала и оценки контейнера:

$$\hat{S}'_{ст} = \hat{\tilde{S}}'_{сов} - \hat{S}'_{кон},$$

что соответствует выделению ортогональной составляющей $\theta(t)\cdot S^{\perp}_{кон}(t)$ в соответствии с приближенным выражением (9). Полученный таким образом сигнал $\hat{S}'_{ст}(t)$ поступает на блок снятия расширяющей ПСП стегосигнала.

Для осуществления корреляционной обработки полученной реализации стегосигнала абонент-получатель, зная ключ алгоритма формирования k, формирует опорный сигнал, соответствующий нелинейной расширяющей последовательности $B_{оп}(t)$:

$$R(\tau) = \int_0^T B'(t)\,B_{оп}(t-\tau)\,dt, \qquad (10)$$

где $B_{оп}(t)$ — опорная нелинейная ПСП; T — интервал корреляции (накопления).

Сформировать опорную нелинейную ПСП и осуществить корреляционный прием, а также сформировать стегосигнал с использованием расширяющей ПСП $B_{оп}(t)$ может только абонент, обладающий ключом k.

Оценка сложности реализации воздействий злоумышленником при применении способа формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей ПСП

Особенностью предлагаемого подхода является тот факт, что при его реализации для возможного злоумышленника сложной задачей является не только получение доступа к смыслу передаваемой в стегосигнале информации, но и установление самого факта наличия дополнительного канала передачи данных.

Рассмотрим действия злоумышленника при попытке получить доступ к дополнительному каналу при условии, что он знает (или обоснованно предполагает), что такой канал существует. В этом случае для него возможны две стратегии:

— злоумышленник пытается установить закон формирования расширяющей ПСП дополнительного канала, чтобы осуществить накопление необходимого количества чипов ПСП и реализовать корреляционный прием;

— злоумышленник пытается выделить отдельные чипы расширяющей ПСП и осуществить посимвольный прием (в том числе в режиме постобработки).

Стойкость описанного способа к первой стратегии злоумышленника полностью определяется стойкостью специального алгоритма, используемого для формирования нелинейной расширяющей ПСП, и не является предметом данной статьи, однако отметим, что в этих целях может использоваться любой криптографический алгоритм, обладающий необходимой устойчивостью к анализу и скоростью формирования.

Стойкость способа ко второй стратегии определяется энергетическими характеристиками стегосигнала и сигнала-контейнера. Покажем, что существует возможность выбора таких энергетических параметров, которые, с одной стороны, позволяют осуществлять корреляционный прием легальному абоненту при условии наличия у него знаний о законе формирования расширяющей ПСП, а с другой стороны, лишают злоумышленника возможности посимвольной обработки даже при наличии у него гипотетических элементов антенны и приемного тракта с наилучшими для него характеристиками.

Рассмотрим пример, иллюстрирующий выбор параметров стегосигнала, при которых возможности злоумышленника обнаружить и принять его, в том числе с использованием узконаправленных антенн с большим коэффициентом усиления, ограничены. Пусть длительность символа передаваемой информации в стегосигнале $\tau_с = 0{,}016$ с. Выберем мощность стегосигнала так, чтобы пик корреляционной функции на приемной стороне был достаточен для его обнаружения, а спектральная плотность мощности сигнала при этом оставалась существенно ниже уровня шума [5]. В этом случае злоумышленник, не располагающий структурой расширяющей последовательности, прием осуществить не сможет. Тогда накопление на интервале корреляционной обработки, равном длительности символа стегосигнала, эквивалентно сужению полосы до $\Delta f = 62{,}5$ Гц [5].

Оценим фоновый шум на входе приемника для наихудшего случая, включая тепловой шум антенны, потери в тракте, шум усилителя. Эквивалентную шумовую температуру антенны зададим $T_а^{ш} = 290$ К. Мощность шума составляет

$$P_а^{ш} = k\Delta f T_а^{ш}, \qquad (11)$$

где $k = 1{,}38 \cdot 10^{-23}$ Дж/К — постоянная Больцмана.

Подстановка указанных значений дает $P_а^{ш} \approx$ $\approx$ –186 дБВт. Пусть до приемника доходит около –161 дБВт мощности стегосигнала, тогда отношение сигнал/шум 25 дБ обеспечивает корреляционный прием [4]. Злоумышленнику, которому известна лишь длительность символа, но не структура последовательности, приходится регистрировать смесь сигнала с шумом в полосе, обратной длительности чипа $\tau_ч$. Если на один информационный символ (период накопления) отводится 8191 чип расширяющей ПСП, эта полоса возрастает до $\Delta F_{нар} = 1/\tau_ч = L/\tau_с \approx 0{,}5$ МГц. Даже для гипотетической антенны с $T_а^{ш} = 150$ К мощность шума в ней составит –149 дБВт — на 12 дБ выше мощности сигнала, что практически исключает почиповый прием стегосигнала [4].

Оценим вероятность правильного приема при осуществлении обнаружения стегосигнала легальным абонентом, знающим структуру расширяющей ПСП, и злоумышленником, не обладающим этим знанием. Будем полагать вероятность ложной тревоги $P_{л.т} = 0{,}1$ [5]. Вероятность правильного обнаружения при когерентном приеме в простейшем случае определяется соотношением [15, 16]

$$P_{п.о} = \Phi\left(\sqrt{2q} - \Phi^{-1}\left(1 - P_{л.т}\right)\right), \qquad (12)$$

где $\Phi(x) = \dfrac{2}{\sqrt{2\pi}}\int_0^x e^{-\frac{t^2}{2}}\,dt$ — функция Крампа;

q — эффективное отношение сигнал/шум: для злоумышленника $q = q_ч$, для легального абонента $q = q_ч L = q_с$, $q_ч = E_ч/N_0$ — отношение энергии $E_ч$ одного чипа к N_0, а $q_с = E_с / N_0$ — отношение энергии $E_с$ символа к N_0.

Как было показано в [5], «поскольку злоумышленник не знает структуры расширяющей нелинейной ПСП и специального ключа, будем полагать, что он пытается осуществлять поэлементный прием. Энергия сигнала, определяющая вероятность его правильного обнаружения злоумышленником $P_{п.о}$, в этом случае определяется амплитудой сигнала и длительностью одного чипа расширяющей ПСП $\tau_ч$. Для легального абонента, напротив, энергия сигнала будет определяться длительностью информационного символа $\tau_с = \tau_ч B = \tau_ч L$, где B — база сигнала, численно равная длине расширяющей ПСП L. Таким образом, эквивалентное отношение сигнал/шум для легального абонента будет в B раз больше: $q_с = q_ч B$». Для иллюстрации различия в показателях помехоустойчивости и представления их наглядного сравнения на одном графике будем нормировать отношение сигнал/шум на энергию одного чипа расширяющей ПСП и рассматривать величину $E_ч/N_0$, при этом для легального абонента эффективное отношение сигнал/шум в решающем устройстве $q = q_с = q_ч L$, а для злоумышленника $q = q_ч$. При этом реальная эквивалентная шумовая полоса для легального абонента определяется интервалом накопления $\tau_с$ и примерно равна $1/\tau_с$, тогда как для злоумышленника, работающего по чипам, — $1/\tau_ч$.

Зависимости вероятности правильного обнаружения стегосигнала от отношения сигнал/шум q (отношения энергии чипа расширяющей ПСП $E_ч$ к спектральной плотности мощности шума N_0) приведены на рис. 7, *а* [5] для вероятности ложной тревоги $P_{л.т} = 0{,}1$. Кривая *1* описывает поэлементный прием злоумышленником, а кривые *2*, *3* и *4* — прием легальным абонентом при длинах расширяющей нелинейной ПСП $L = 511$, 8191 и 16 383 элемента.

При $q < 0$ дБ поэлементный прием для злоумышленника практически нереализуем [17, 18], тогда как легальный абонент, располагающий структурой расширяющей ПСП длиной $L = 16\,383$ элемента, уже при $q = -33$ дБ достигает вероятности правильного обнаружения $P_{п.о} = 0{,}9972$ [5].

Следует подчеркнуть, что для злоумышленника, не обладающего знанием опорной ПСП, принята упрощенная (и оптимистичная для него) модель приемника. Предполагается, что решение принимается по символу при эффективном отношении сигнал/шум $q_ч$, без выигрыша от корреляции с ПСП. В реальных условиях отсутствие ПСП приводит к еще более низкой вероятности правильного обнаружения символа, поэтому полученные оценки для злоумышленника фактически являются верхней границей его возможностей.

Теперь оценим возможность искажения информационного символа стегосигнала для легального абонента, осуществляющего корреляционный прием, и для злоумышленника, пытающегося осуществить поэлементный прием.

Количественной мерой искажения символа (элемента стегосообщения) будем полагать вероятность битовой ошибки в переданном стегосообщении, определяемую в соответствии с выражением

$$P_0 = Q\left(\sqrt{\frac{E(1-\rho)}{N_0}}\right), \qquad (13)$$

где $Q(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}\,\mathrm{d}t$ — гауссов интеграл ошибок; ρ — временной коэффициент взаимной корреляции, который принимает значения от –1 до 1 включительно.

Для сигналов, использующих фазовую манипуляцию несущей частоты на 0 – π, значение $\rho = -1$. Таким образом, в данном случае вероятность битовой ошибки определяется следующим выражением:

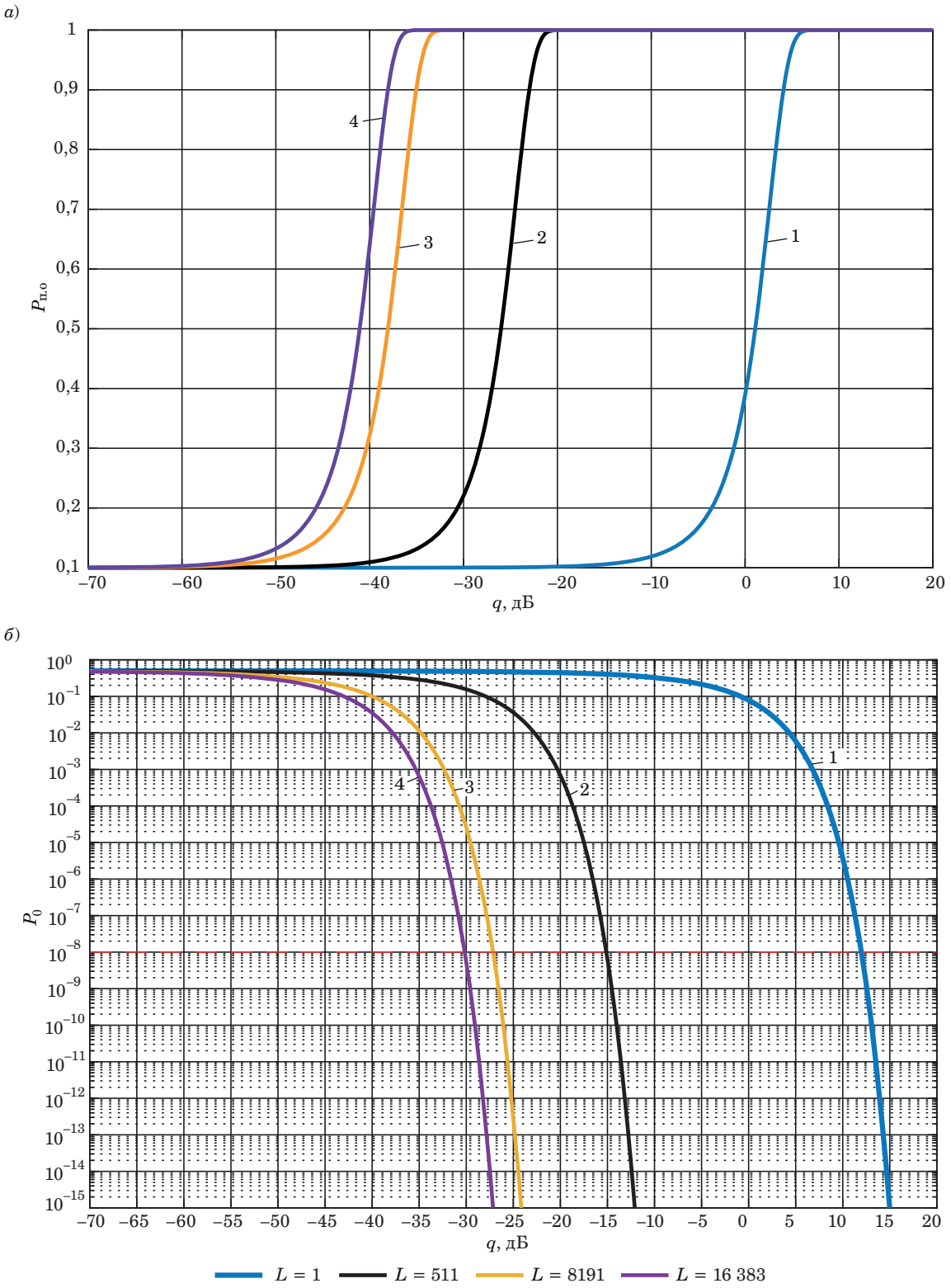
$$P_0 = Q\left(\sqrt{\frac{2E}{N_0}}\right). \qquad (14)$$

В выражениях (13), (14) величина P_0 рассматривается как вероятность ошибки информационного символа при бинарном приеме. Для легального абонента, реализующего корреляционный прием по полной расширяющей ПСП длиной L, энергия символа пропорциональна $E_с = E_ч L$, а соответствующее отношение сигнал/шум $q = q_с = q_ч L$. Для злоумышленника, осуществляющего поэлементный (почиповый) прием и не использующего знание ПСП, решение по тому же информационному символу принимается при существенно меньшей эффективной энергии, близкой к $E_ч$, т. е. при гораздо меньшем E/N_0 в (13), (14), а эффективное отношение сигнал/шум $q = q_ч$.

Отметим, что для злоумышленника величина P_0 в (13), (14) отражает вероятность ошибки при решении по одному чипу расширяющей ПСП. При восстановлении всего информационного символа в целом эта вероятность будет еще выше [4, 5].

Как уже отмечалось, у легального абонента энергия определяется длительностью информационного символа $\tau_с = \tau_ч B$ (против длительности чипа $\tau_ч$ у злоумышленника), что дает ему выигрыш в отношении сигнал/шум в B раз: $q_с = q_ч B$ [4].

Зависимости вероятности битовой ошибки принятого стегосообщения от эквивалентного отношения сигнал/шум приведены на рис. 7, *б:* кривая *1* описывает прием злоумышленником,



■ ***Рис. 7.*** Зависимость вероятности правильного обнаружения стегосигнала (*а*) [5] и битовой ошибки (*б*) от отношения сигнал/шум: *1* — прием злоумышленником; *2–4* — прием легальным абонентом при расширяющей нелинейной ПСП

■ ***Fig. 7.*** Dependence of the stego signal detection probability (*a*) [5] and bit error probability (*б*) on the signal-to-noise ratio: *1* — reception by an adversary; *2–4* — reception by a legitimate subscriber using an expanding nonlinear pseudorandom sequence

кривые *2*, *3* и *4* — прием легальным абонентом при длинах расширяющей нелинейной ПСП L = 511, 8191 и 16 383 элемента [4].

Из графиков видно, что требуемая достоверность информационного обмена (вероятность битовой ошибки) при передаче информационного сообщения меньше 10^{-8} [12] у легального абонента при применении расширяющей нелинейной ПСП длиной L = 16 383 элемента достигается при q = –30 дБ, в то время как для злоумышленника — при q = 12 дБ, что в реальных условиях эксплуатации достичь сложно.

Таким образом, расчеты, подтвержденные экспериментом, показывают, что существует возможность выбора такого диапазона значений параметров сигнала-контейнера и стегосигнала (длительности символов сигнала-контейнера, угла, определяющего энергию стегосигнала, периода накопления, количества символов расширяющей нелинейной ПСП в информационном символе стегосигнала и т. д.), при которых энергии информационного символа, накопленного легальным абонентом сигнала при условии знания им расширяющей нелинейной ПСП стегосигнала, достаточно для его качественного (с заданной помехоустойчивостью) обнаружения и корреляционного приема.

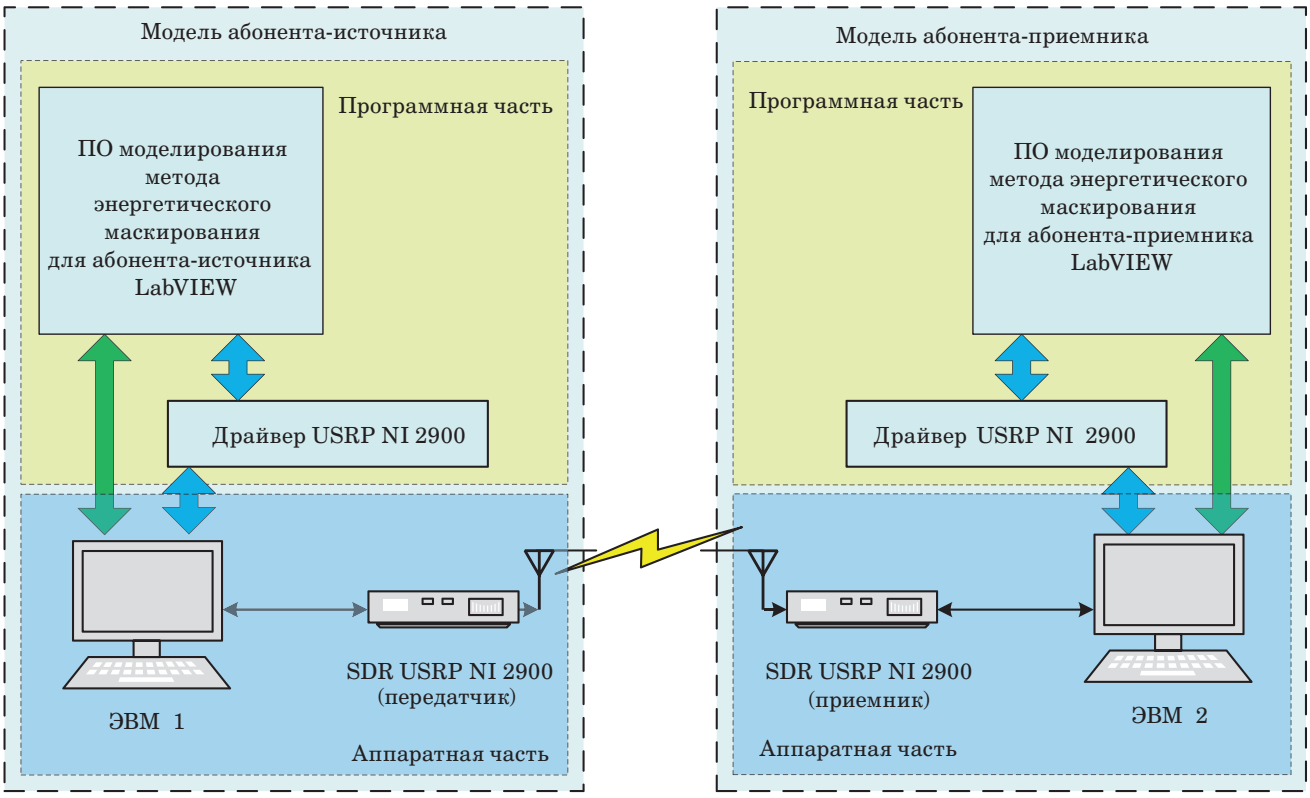
В то же время в условиях отсутствия сведений о расширяющей нелинейной ПСП у потенциального злоумышленника накопление энергии и выделение им информационного символа невозможно, а энергии одного чипа недостаточно для почипового обнаружения и приема.

Программная реализация способа формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей ПСП

Для оценки возможности физической реализации предложенного способа разработаны программное обеспечение (ПО) компьютерного моделирования и стенд полунатурного моделирования способа формирования радиостеганографического сигнала.

Основная часть ПО моделирования выполнена на языке G в среде графического программирования LabVIEW [19].

Стенд полунатурного моделирования (рис. 8) представляет собой аппаратно-программный комплекс, включающий модели абонента-источника и абонента-приемника.



■ ***Рис. 8.*** Структурная схема стенда полунатурного моделирования способа формирования радиостеганографического сигнала

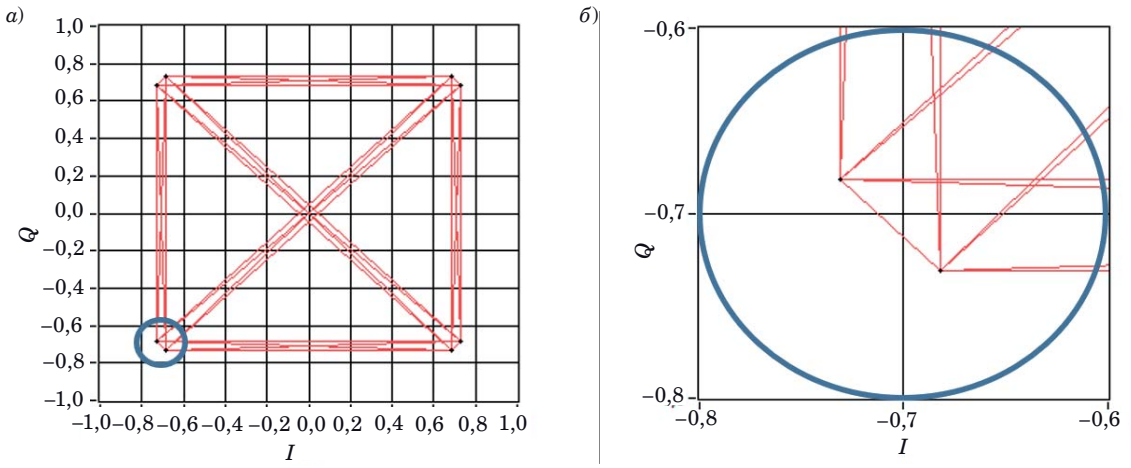
■ ***Fig. 8.*** Structural diagram of the stand for semi-natural modeling of the formation method radio steganographic signal

Для формирования радиоканала в качестве приемо-передающих устройств использовались программно-определяемые радиоустройства USRP NI 2900 (Software-defined radio, SDR). Устройство NI USRP 2900 — это настраиваемый дуплексный приемопередатчик с несущей частотой от 70 МГц до 6 ГГц и полосой пропускания 56 МГц. Одно из устройств выполняет передачу совмещенного сигнала, а второе — прием этого сигнала, реализуя таким образом физическую модель радиоканала передачи информации. Непосредственно логику формирования и обработки совмещенного сигнала в ходе выполнения алгоритма определяет разработанное ПО моделирования соответствующего способа формирования радиостеганографического сигнала, загруженное в устройства USRP NI 2900.

Выполнено моделирование процесса передачи информации с использованием способа формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей ПСП. Предложенный способ позволяет выполнять совместную передачу информации по каналу-контейнеру и передачу по стегоканалу.

Квадратурная диаграмма передаваемой информации по каналу-контейнеру и стегоканалу на панели приборов программы LabVIEW показана на рис. 9. На рис. 9, *а* представлена квадратурная диаграмма при одинаковых масштабах осей *I* и *Q*. На ней различимы четыре позиции сигнала-контейнера с напряжением 1 В (чипы со значением «0» и «1» расширяющей ПСП по двум квадратурным составляющим), тогда как две позиции стегосигнала (±0,01 В) при таком масштабе практически неразличимы. Увеличение масштаба осей (рис. 9, *б*) позволяет различить разные позиции стегосигнала в пределах одной позиции сигнала-контейнера.

Квадратурная диаграмма сигнала-контейнера, принятого в смеси с шумом, показана на рис. 10 [4].



■ ***Рис. 9.*** Фазовая диаграмма совмещенного сигнала: *а* — в масштабе всего сигнала; *б* — в увеличенном масштабе [4]
■ ***Fig. 9.*** Constellation diagram of the combined signal: *а* — full view; *б* — enlarged view [4]

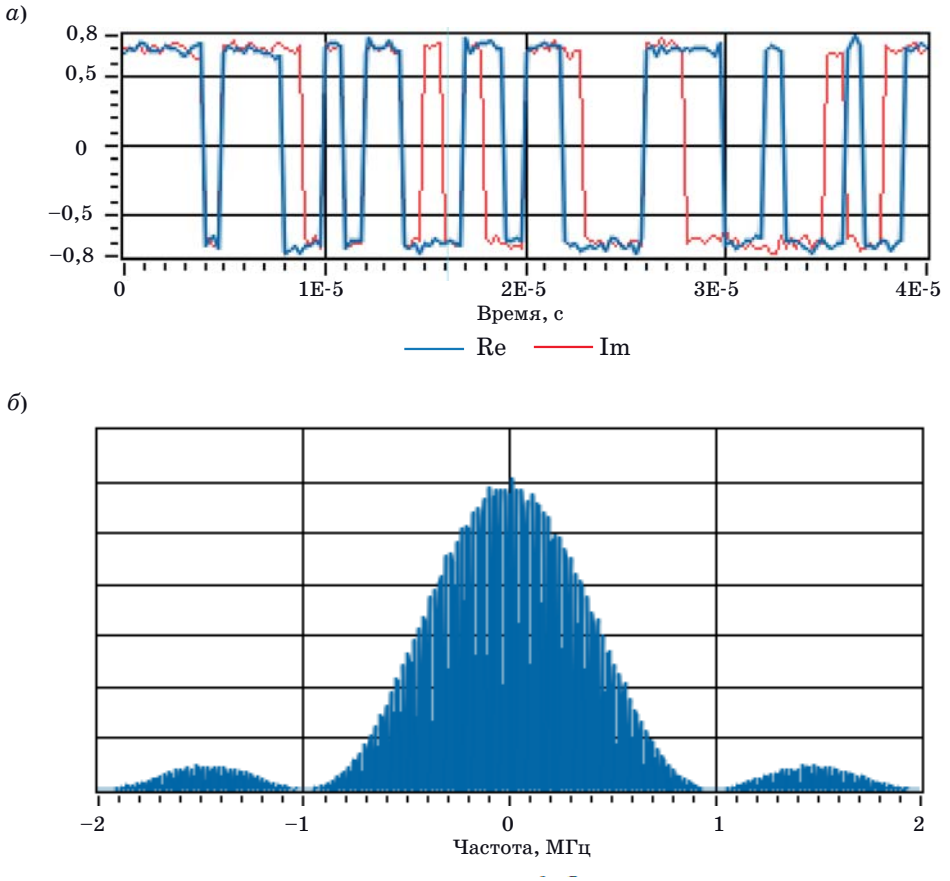


■ ***Рис. 10.*** Фазовая диаграмма принимаемого сигнала-контейнера в смеси с шумом [4]
■ ***Fig. 10.*** Phase diagram of the received container signal in a mixture with noise [4]

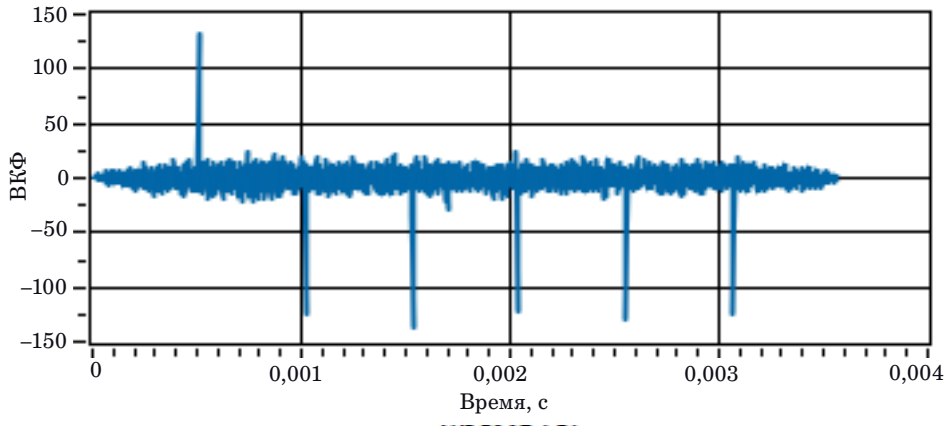
Осциллограмма и спектр принятого совмещенного сигнала показаны на рис. 11, *а* и *б*. Сигнал-контейнер легко различим и во временной, и в частотной областях, и на квадратурной диаграмме, тогда как стегосигнал теряется в шуме и на фоне контейнера. Его выделение без знания структуры нелинейной ПСП невозможно [4].

Полученная в результате свертки демодулированного сигнала с опорной ПСП корреляционная функция (рис. 12) содержит положительные и отрицательные пики (свертка с опорными сигналами символов «0» и «1») [4].

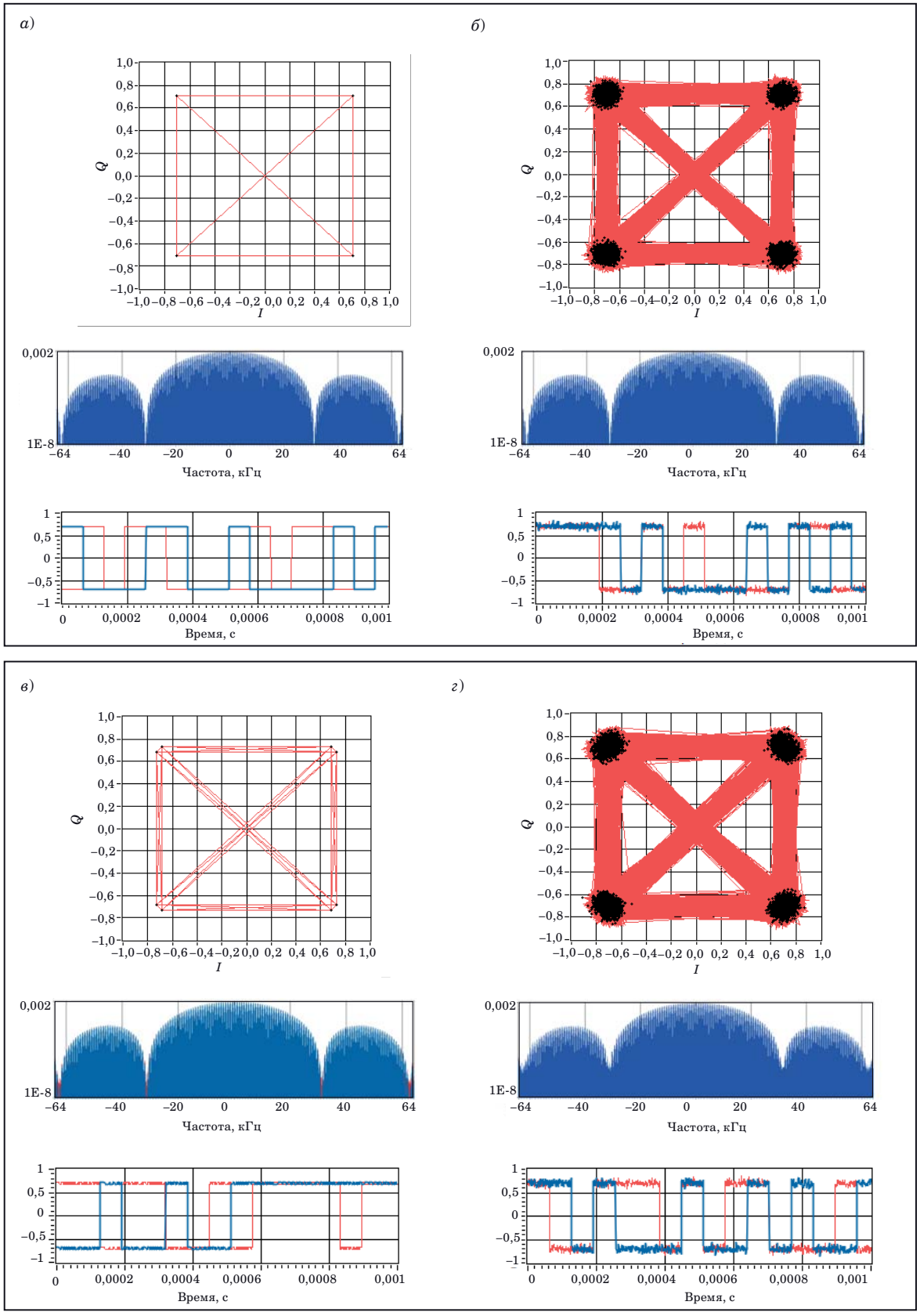
На рис. 13 сопоставлены квадратурные диаграммы, спектры и временные диаграммы «пустого» сигнала-контейнера и совмещенного сигнала



■ ***Рис. 11.*** Осциллограмма (*а*) и спектр (*б*) принимаемого совмещенного сигнала в смеси с шумом
■ ***Fig. 11.*** Oscillogram (*а*) and spectrum (*б*) of the received combined signal mixed with noise



■ ***Рис. 12.*** Взаимная корреляционная функция принимаемого стегосигнала
■ ***Fig. 12.*** Cross-correlation function of the received stego signal



■ ***Рис. 13.*** Фазовые диаграммы, спектры и временные диаграммы: *а* — «пустой» сигнал-контейнер без шума; *б* — «пустой» сигнал-контейнер в смеси с шумом; *в* – совмещенный сигнал без шума; *г* — совмещенный сигнал в смеси с шумом

■ ***Fig. 13.*** Constellation diagrams, spectra, and time-domain waveforms: *а* — cover signal without noise; *б* — cover signal with noise; *в* – combined signal without noise; *г* — combined signal with noise

без шума и в смеси с шумом. Как следует из сравнения рис. 13, *а* и *в*, встраивание стегосигнала смещает точки квадратурного созвездия лишь незначительно и заметно только в отсутствие шума. В реальном канале (рис. 13, *б*, *г*) совмещенный сигнал и «пустой» контейнер визуально и статистически неотличимы. Ни по квадратурной диаграмме, ни по спектру, ни по временной диаграмме факт наличия стегосигнала без знания ключа формирования расширяющей ПСП не обнаруживается.

Результаты эксперимента с использованием разработанного ПО подтверждают реализуемость предложенного способа формирования радиостеганографического сигнала на основе дополнительной фазовой модуляции и нелинейной расширяющей ПСП, а также возможность выбора таких параметров, которые позволят осуществлять обнаружение, прием и обработку стегосигнала легальными абонентами при невозможности его обнаружения злоумышленником.

Заключение

В работе предложен новый способ формирования скрытого (маскированного) сигнала, основанный на использовании дополнительной фазовой манипуляции и нелинейной расширяющей ПСП, реализующий метод радиостеганографии, который, с одной стороны, позволяет легальным абонентам принимать скрытый сигнал с необходимым качеством, а с другой — существенно ограничивает возможности злоумышленника по его обнаружению и приему.

Показано, что при применении способа для передачи информации по стегоканалу можно выбрать параметры стегосигнала (индекс модуляции, период накопления, количество чипов расширяющей ПСП в информационном символе стегосигнала и т. д.), при которых энергии информационного символа, накопленной легальным абонентом при условии знания им расширяющей ПСП, достаточно для его обнаружения и корреляционного приема, а также целесообразно использовать расширение спектра сигнала нелинейной ПСП, обладающей высокой структурной скрытностью.

Основные результаты:

1. Получены аналитические соотношения для выбора параметров стегосигнала, обеспечивающих $P_{\text{п.о}} > 0{,}9972$ для легального получателя при $P_{\text{п.о}} \approx 0{,}1$ для злоумышленника.

2. Показано, что при использовании ПСП длиной $L = 16\,383$ легальный приемник обеспечивает $P_{\text{п.о}} < 10^{-8}$ при $q = -30$ дБ, в то время как злоумышленнику требуется $q > 12$ дБ, что на 42 дБ выше.

3. Экспериментально подтверждена работоспособность метода на стенде с USRP NI 2900. Отклонение экспериментальных данных от расчетных не превышает 5 %.

4. Способ применим к широкому классу цифровых радиосистем: WiFi, LTE, DVB-T и др. [20–22].

Таким образом, предложенный радиостеганографический способ, определенный на физическом уровне, может использоваться практически в любой цифровой радиосистеме, например в сетях Wi-Fi 802.11, цифровых мобильных сетях, цифровом телевидении, навигационных системах и т. д. [23, 24].

Направления дальнейших исследований:

1) анализ влияния многолучевого распространения и доплеровского сдвига;

2) адаптивный выбор параметров стегосигнала в зависимости от условий канала;

3) разработка протоколов обмена ключами для синхронизации ПСП;

4) исследование возможности одновременной передачи нескольких стегосигналов.

Литература

1. **Долженков С. С., Максимова Е. А.** Исследование антропоморфических видов организации межобъектного взаимодействия на уровне субъекта критической информационной инфраструктуры. *Вестник Санкт-Петербургского университета государственной противопожарной службы МЧС России*, 2025, № 1, с. 94–108. doi:10.61260/2218-130X-2025-1-94-108, EDN: MEPVXZ
2. **Cuevas D., Gutiérrez M., Ibáñez J., Santamaría I.** Low probability of detection communication using noncoherent grassmannian signaling. *Proceedings of the 2025 59th Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, USA, 2025, pp. 514–518. doi:10.1109/IEEECONF67917.2025.11443893
3. **D'Oro S., Restuccia F., Melodia T.** Hiding data in plain sight: Undetectable wireless communications through pseudo-noise asymmetric shift keying. *Proceedings of the IEEE INFOCOM 2019*, Paris, 2019, pp. 1585–1593. doi:10.1109/INFOCOM.2019.8737581
4. **Штанько С. В., Крягин В. А.** Применение сигнально-кодовой конструкции с дополнительной квадратурной модуляцией при передаче информации по космическим радиолиниям. *СПбНТОРЭС: труды ежегодной научно-технической конференции*, СПб., 2023, № 1(78), с. 167–170. EDN: RWLXQM
5. **Штанько С. В., Крягин В. А.** Вопросы практической реализации способа передачи навигационных сигналов с использованием дополнительного канала для передачи навигационных меток. *Навигация и гидрография*, 2025, № 3(80), с. 37–48. EDN: JFWGFB

6. **Беляев С. С., Будько М. Б., Будько М. Ю., Гирик А. В., Грозов В. А.** Построение функции генерации криптографически стойких псевдослучайных последовательностей на базе алгоритма «Кузнечик». *Вопросы кибербезопасности*, 2021, № 4(44), с. 25–34. doi:10.21681/2311-3456-2021-4-25-34, EDN: GBNJBU
7. **Дегтярев А. Н., Афонин И. Л., Поляков А. Л.** Корреляционный прием одномерных полосовых сигналов в условиях действия межсимвольной интерференции и межканальных помех с периодическим опорным сигналом. *Радиоэлектроника. Наносистемы. Информационные технологии*, 2025, т. 17, № 3, с. 279–284. doi:10.17725/j.rensit.2025.17.279, EDN: IFGMJF
8. **Кондрашов Ю. В., Бирюков М. А., Сазонов В. В., Ротенбергер А. А.** Влияние корреляционных функций широкополосных сигналов на помехоустойчивость их приема в многолучевых каналах связи. *Электросвязь*, 2022, № 3, с. 10–15. doi:10.34832/ELSV.2022.28.3.001, EDN: NGNWBJ
9. **Бобровский В. В.** Особенности корреляционной обработки шумоподобных сигналов в электроразведочной аппаратуре. *Геофизические исследования*, 2022, т. 23, № 2, с. 39–54. doi:10.21455/gr2022.2-3, EDN: DCPGAB
10. **Чесноков М. Н., Литвинов А. А., Соловьев А. А., Волгушев Д. Б.** Помехозащищенность приема ортогональных стохастических широкополосных сигналов в условиях воздействия запаздывающих помех. *Успехи современной радиоэлектроники*, 2021, т. 75, № 4, с. 48–56. doi:10.18127/j20700784-202104-07, EDN: ZGBQUX
11. **Кисельников А. Е.** *Алгоритмы идентификации типов искажения сигналов с цифровой модуляцией на основе анализа вектора ошибок*: дис. … канд. техн. наук, Ярославль, ЯрГУ, 2021, 132 с. EDN: AVDIRR
12. **Михайлик Д. А., Малыгин И. В.** Расчет устойчивости системы спутниковой связи на основе широкополосных сигналов по отношению к импульсным и флуктуационным помехам. *Ural Radio Engineering Journal*, 2023, т. 7, № 2, с. 153–165. doi:10.15826/urej.2023.7.2.004, EDN: KOQCWC
13. **Chen C., Zeng X., Ao M., Li C., Zhou F., Ye F.** Security protection of GNSS reference station data based on bespoke steganography embedding algorithm. *Proceedings of the IEEE International Conference on Communications (ICC 2025)*, Chengdu, 2025, pp. 197–202. doi:10.1109/ICC51173.2025.11069711
14. **Aggarwal R., Dagefu F., Kong J., Choi J., Kim B., Spasojevic P.** On covertness of DSSS against Energy and cycle detectors under link QoS requirements. *Proceedings of the IEEE 101st Vehicular Technology Conference (VTC2025-Spring)*, Oslo, 2025, pp. 1–6. doi:10.1109/VTC2025-Spring.2025.00001
15. **Дегтярев А. Н., Афонин И. Л., Поляков А. Л., Зеленкевич Д. Ю.** Повышение помехоустойчивости обнаружителя сигнала. *Радиоэлектроника. Наносистемы. Информационные технологии*, 2025, т. 17, № 4, с. 409–418. doi:10.17725/j.rensit.2025.17.409, EDN: CVTQSU
16. **Потапов А. А.** Определение порогов обнаружения радиосигналов для метода энергетического детектора. *Журнал радиоэлектроники*, 2021, № 9. doi:10.30898/1684-1719.2021.9.3, EDN: BGELRC
17. **Иванов Н. М.** Обнаружение и пеленгование новых слабых сигналов в присутствии мощных помех. *Радиотехника*, 2025, т. 89, № 11, с. 131–137. doi:10.18127/j00338486-202511-15, EDN: FVTQYR
18. **Потапов А. А.** Радиомониторинг низкоуровневых радиосигналов посредством анализа периодических спектральных выборок. *Нелинейный мир*, 2021, т. 19, № 3, с. 5–17. doi:10.18127/j20700970-202103-01, EDN: BZXRPI
19. **Абрамов А. А., Якуш Н. А.** Разработка методики поверки USRP для высокоточного исследования радиосистем. *Труды МАИ*, 2022, № 127. doi:10.34759/trd-2022-127-12, EDN: MZLARX
20. **Гавришев А. А., Осипов Д. Л.** Оценка скрытности OFDM сигналов, основанных на BPSK модуляции, с помощью методов нелинейной динамики. *TComm: Телекоммуникации и транспорт*, 2022, т. 16, № 9, с. 13–19. doi:10.36724/2072-8735-2022-16-9-13-19, EDN: GICCDT
21. **Bonati L., D'Oro S., Restuccia F., Basagni S., Melodia T.** SteaLTE: Private 5G cellular connectivity as a service with full-stack wireless steganography. *IEEE INFOCOM 2021 — IEEE Conference on Computer Communications*, Vancouver, BC, Canada, 2021, pp. 1–10. doi:10.1109/INFOCOM42981.2021.9488889
22. **Grzesiak K., Piotrowski Z., Kelner J. M.** A wireless covert channel based on dirty constellation with phase drift. *Electronics*, 2021, vol. 10, no. 6, art. 647. doi:10.3390/electronics10060647
23. **Карцан И. Н.** Математическая модель защищенного канала связи для морских исследований методом стеганографии. *Informatics. Economics. Management*, 2024, т. 3, № 2, с. 415–424. doi:10.47813/2782-5280-2024-3-2-0415-0424, EDN: MPYZSM
24. **Grzesiak K., Piotrowski Z., Kelner J. M.** Covert channel based on quasi-orthogonal coding. *Electronics*, 2023, vol. 12, no. 10, art. 2249. doi:10.3390/electronics12102249

UDC 621.376.9
doi:10.31799/1684-8853-2026-5-56-72
EDN: CMAJJN

A method for generating a radio steganographic signal based on additional phase modulation and a nonlinear pseudorandom expansion sequence

S. V. Shtanko[a], Dr. Sc., Tech., Associate Professor, orcid.org/0000-0002-8391-8911, vka@mil.ru
V. A. Kryagin[a], Lecturer, orcid.org/0009-0002-7529-283X
P. N. Topchiy[a], Lecturer, orcid.org/0009-0008-4678-7685
D. A. Anikin[b], Head of Department, orcid.org/0009-0003-8295-312X
[a]A. F. Mozhaiskii Military Space Academy, 13, Zhdanovskaia Emb., 197198, Saint-Petersburg, Russian Federation
[b]Ministry of Defense of the Russian Federation, 19, Znamenka St., 119160, Moscow, Russian Federation

Introduction: The development of global communication systems has increased the standards for information confidentiality, especially in critical information infrastructure systems whose elements are interconnected via radio channels. Cryptographic methods conceal the meaning of transmitted data but do not hide the very fact of information exchange. Radio steganographic methods based on embedding a stego signal into an open carrier signal at the physical layer address this issue; however, they require energy concealment of the stego signal and robustness against an attacker's detection attempts. **Purpose:** To develop a method of energy masking for a radio signal inside a carrier signal based on additional phase manipulation and a nonlinear spreading pseudorandom sequence, which provides covert information transmission over a stego channel with a specified noise immunity for the legitimate user and prevents an attacker from detecting the stego signal. **Results:** The proposed method forms the stego signal by applying an additional small-angle phase manipulation to the vector of the phase-modulated carrier signal. The deviation angle has been chosen so that the energy of a single chip could remain masked within the phase-noise variance. The spectrum of the stego signal has been spread by a nonlinear pseudorandom sequence generated by a nonlinear pseudorandom sequence generator resistant to analytical attacks. Analytical expressions for the probability of correct detection and the bit error probability have been obtained. The findings show that, for a spreading sequence length of 16383 chips, the legitimate user has achieved a detection probability of 0.9972 at a chip-energy-to-noise spectral density ratio of $q = -33$ dB, whereas an attacker employing chip-by-chip reception has failed to detect the stego signal for $q < 0$ dB. A bit error probability below 10^{-8} has been achieved at $q = -30$ dB, while an attacker has required more than 12 dB, which has given a 42 dB advantage. A semi-hardware testbed based on software-defined radios has been developed; the deviation of experimental results from analytical estimates has not exceeded five percent. **Practical relevance:** The method is applicable to a wide class of digital phase-modulated radio systems and can be used for data transmission over an embedded channel in critical information infrastructure systems.

Keywords — phase manipulation, pseudorandom sequence, phase diagram, container signal, expanding sequence, correlation technique, stego signal, stego message, nonlinear expanding sequence.

For citation: Shtanko S. V. , Kryagin V. A., Topchiy P. N. , Anikin D. A. A method for generating a radio steganographic signal based on additional phase modulation and a nonlinear pseudorandom expansion sequence. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 56–72 (In Russian). doi:10.31799/1684-8853-2026-5-56-72, EDN: CMAJJN

References

1. Dolzhenkov S. S., Maksimova E. A. Study of anthropomorphic types of organization of interobject interaction at the level of a subject of critical information infrastructure. *Vestnik Saint-Petersburg University of State Fire Service of EMERCOM of Russia*, 2025, no. 1, pp. 94–108 (In Russian). doi:10.61260/2218-130X-2025-1-94-108, EDN: MEPVXZ
2. Cuevas D., Gutiérrez M., Ibáñez J., Santamaría I. Low probability of detection communication using noncoherent grassmannian signaling. *Proceedings of the 2025 59th Asilomar Conference on Signals, Systems, and Computers*, Pacific Grove, CA, USA, 2025, pp. 514–518. doi:10.1109/IEEECONF67917.2025.11443893
3. D'Oro S., Restuccia F., Melodia T. Hiding data in plain sight: Undetectable wireless communications through pseudo-noise asymmetric shift keying. *Proceedings of the IEEE INFOCOM 2019*, Paris, 2019, pp. 1585–1593. doi:10.1109/INFOCOM.2019.8737581
4. Shtanko S. V., Kryagin V. A. The use of a signal-code structure with additional quadrature modulation when transmitting information over space radio lines. *SPbNTORES: trudy ezhegodnoi nauchno-tekhnicheskoi konferentsii* [SPbNTORES: Proceedings of the Annual Scientific and Technical Conference]. Saint-Petersburg, 2023, no. 1(78), pp. 167–170 (In Russian). EDN: RWLXQM
5. Shtanko S. V., Kryagin V. A. Issues of practical implementation of the method of transmitting navigation signals using an additional channel for transmitting navigation tags. *Navigation and Hydrography*, 2025, no. 3(80), pp. 37–48 (In Russian). EDN: JFWGFB
6. Beliaev S., Budko M., Budko M., Guirik A., Grozov V. Development of a pseudo-random sequence generation function based on the "Kuznechik" cryptographic algorithm. *Voprosy kiberbezopasnosti*, 2021, no. 4(44), pp. 25–34 (In Russian). doi:10.21681/2311-3456-2021-4-25-34, EDN: GBNJBU
7. Degtiarev A. N., Afonin I. L., Poliakov A. L. Correlation reception of one-dimensional bandpass signals under conditions of inter-symbol interference and inter-channel interference with a periodic reference signal. *Radioelectronics. Nanosystems. Information Technologies*, 2025, vol. 17, no. 3, pp. 279–284 (In Russian). doi:10.17725/j.rensit.2025.17.279, EDN: IFGMJF
8. Kondrashov Yu. V., Biriukov M. A., Sazonov V. V., Rotenberger A. A. Influence of correlation functions of broadband signals on the noise immunity of their reception in multipath communication channels. *Elektrosviaz'*, 2022, no. 3, pp. 10–15 (In Russian). doi:10.34832/ELSV.2022.28.3.001, EDN: NGNWBJ
9. Bobrovskii V. V. Peculiarities of correlation processing of pseudonoise signals in electrical prospecting equipment. *Geophysical Research*, 2022, vol. 23, no. 2, pp. 39–54 (In Russian). doi:10.21455/gr2022.2-3, EDN: DCPGAB
10. Chesnokov M. N., Litvinov A. A., Soloviev A. A., Volgushev D. B. Performance of orthogonal stochastic code signals in the presence of delayed interference. *Achievements of Modern Radioelectronics*, 2021, vol. 75, no. 4, pp. 48–56 (In Russian). doi:10.18127/j20700784-202104-07, EDN: ZGBQUX
11. Kisel'nikov A. E. *Algoritmy identifikatsii tipov iskazheniia signalov s tsifrovoi moduliatsiei na osnove analiza vektora oshibok*. Dis. kand. tekhn. nauk [Algorithms for identifying types of distortion of digitally modulated signals based on error vector analysis. PhD tech. sci. diss.]. Yaroslavl, IarGU Publ., 2021. 132 p. (In Russian). EDN: AVDIRR
12. Mikhailik D. A., Malygin I. V. Estimation of the immunity of a satellite communication system based on wideband signals in relation to impulse and fluctuating interferences. *Ural Radio Engineering Journal*, 2023, vol. 7, no. 2, pp. 153–165 (In Russian). doi:10.15826/urej.2023.7.2.004. EDN: KOQCWC
13. Chen C., Zeng X., Ao M., Li C., Zhou F., Ye F. Security protection of GNSS reference station data based on bespoke steganography embedding algorithm. *Proceedings of the IEEE International Conference on Communications (ICC 2025)*, Chengdu, 2025, pp. 197–202. doi:10.1109/ICC51173.2025.11069711
14. Aggarwal R., Dagefu F., Kong J., Choi J., Kim B., Spasojevic P. On covertness of DSSS against Energy and cycle detectors under link QoS requirements. *Proceedings of the IEEE 101st Vehicular Technology Conference (VTC2025-Spring)*, Oslo, 2025, pp. 1–6. doi:10.1109/VTC2025-Spring.2025.00001

15. Degtiarev A. N., Afonin I. L., Poliakov A. L., Zelenkevich D. Yu. Improving the noise immunity of the signal detector. *Radioelectronics. Nanosystems. Information Technologies*, 2025, vol. 17, no. 4, pp. 409–418 (In Russian). doi:10.17725/j.rensit.2025.17.409, EDN: CVTQSU
16. Potapov A. A. Radio signals detection thresholds estimation for energy detection technique. *Journal of Radio Electronics*, 2021, no. 9 (In Russian). doi:10.30898/1684-1719.2021.9.3, EDN: BGELRC
17. Ivanov N. M. Detecting and direction finding of new weak signals in presence of high-power noise. *Radioengineering*, 2025, vol. 89, no. 11, pp. 131–137 (In Russian). doi:10.18127/j00338486-202511-15, EDN: FVTQYR
18. Potapov A. A. Low-level signals radiomonitoring using periodic spectrum samples analysis. *Nonlinear World*, 2021, vol. 19, no. 3, pp. 5–17 (In Russian). doi:10.18127/j20700970-202103-01, EDN: BZXRPI
19. Abramov A. A., Yakush N. A. Development of USRP verification methodology for high-precision radio system research. *Trudy MAI*, 2022, no. 127 (In Russian). doi:10.34759/trd-2022-127-12, EDN: MZLARX
20. Gavrishev A. A., Osipov D. L. Evaluation of the stealth of OFDM-signals based on BPSK modulation, using nonlinear dynamics methods. *T-Comm*, 2022, vol. 16, no. 9, pp. 13–19 (In Russian). doi:10.36724/2072-8735-2022-16-9-13-19, EDN: GICCDT
21. Bonati L., D'Oro S., Restuccia F., Basagni S., Melodia T. SteaLTE: Private 5G cellular connectivity as a service with full-stack wireless steganography. *IEEE INFOCOM 2021 – IEEE Conference on Computer Communications*, Vancouver, BC, Canada, 2021, pp. 1–10. doi:10.1109/INFOCOM42981.2021.9488889
22. Grzesiak K., Piotrowski Z., Kelner J. M. A wireless covert channel based on dirty constellation with phase drift. *Electronics*, 2021, vol. 10, no. 6, art. 647. doi:10.3390/electronics10060647
23. Kartsan I. N. Mathematical model of secure communication channel for marine research by steganography method. *Informatics. Economics. Management*, 2024, vol. 3, no. 2, pp. 415–424 (In Russian). doi:10.47813/2782-5280-2024-3-2-0415-0424, EDN: MPYZSM
24. Grzesiak K., Piotrowski Z., Kelner J. M. Covert channel based on quasi-orthogonal coding. *Electronics*, 2023, vol. 12, no. 10, art. 2249. doi:10.3390/electronics12102249

УВАЖАЕМЫЕ АВТОРЫ!

Научная электронная библиотека (НЭБ) продолжает работу по реализации проекта SCIENCE INDEX. После того как Вы зарегистрируетесь на сайте НЭБ (http://elibrary.ru/defaultx.asp), будет создана Ваша личная страничка, содержание которой составят не только Ваши персональные данные, но и перечень всех Ваших печатных трудов, имеющихся в базе данных НЭБ, включая диссертации, патенты и тезисы к конференциям, а также сравнительные индексы цитирования: РИНЦ (Российский индекс научного цитирования), h (индекс Хирша) от Web of Science и h от Scopus. После создания базового варианта Вашей персональной страницы Вы получите код доступа, который позволит Вам редактировать информацию, помогая создавать максимально объективную картину Вашей научной активности и цитирования Ваших трудов.