УДК 621.396.001

Дидковский Р.М., к.т.н. *(Черкасский государственный технологический университет)*
Бокла Н.И., асп. *(Государст. университет информационно-коммуникационных технологий)*

МОДЕЛИРОВАНИЕ СИСТЕМЫ СВЯЗИ С РАСШИРЕНИЕМ СПЕКТРА ПОСЛЕДОВАТЕЛЬНОСТЬЮ БАРКЕРА

Дідковський Р.М., Бокла Н.І. Моделювання систем зв'язку з розширенням спектру послідовністю Баркера. Розглянуто принципи побудови імітаційної обчислювальної моделі широкосмугової системи зв'язку з фазоманіпульованими сигналами. Запропонована структура та напрямки застосування таких моделей.

Ключові слова: ШИРОКОСМУГОВІ СИСТЕМИ ЗВ'ЯЗКУ, ФАЗОВА МАНІПУЛЯЦІЯ, ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ

Дидковский Р.М., Бокла Н.И. Моделирование системы связи с расширением спектра последовательностью Баркера. Рассмотрены принципы построения имитационной вычислительной модели широкополосной системы связи с фазоманипулированными сигналами. Предложена структура и направления применения таких моделей.

Ключевые слова: ШИРОКОПОЛОСНЫЕ СИСТЕМЫ СВЯЗИ, ФАЗОВАЯ МАНИПУЛЯЦИЯ, ИМИТАЦИОННОЕ **МОДЕЛИРОВАНИЕ**.

Didkowskyi R.M., Bokla N.I. Modeling of spread-spectrum communication system utilizing Barker sequence. In the work the construction principles of communication systems computer simulation model with wideband phase-shift-keying signals are being reviewed. The structure and direction of application of such models is proposed.

Keywords: WIDEBAND COMMUNICATION SYSTEM, PHASE-SHIFT-KEYING, COMPUTER SIMULATION MODELING.

Введение. Широкополосные и сверхширокополосные системы связи – одно из наиболее интенсивно развивающихся направлений в теории и практике радиотехнических устройств и систем [1]. Методы формирования и обработки сложных шумоподобных сигналов в таких системах продолжают активно совершенствоваться [2]. При этом имитационное компьютерное моделирование выступает в роли эффективного инструмента, позволяющего решать ряд важных задач, а именно:

– исследование свойств существующих систем в полностью управляемых условиях, которые трудно создать в ходе физического эксперимента;

– оптимизация структуры и алгоритмов функционирования блоков и устройств в ходе модернизации существующей или разработки новой системы;

– исследование влияния на систему условий ее функционирования (помеховая обстановка, многолучевое распространение сигнала, доплеровский сдвиг частоты).

Одним из наиболее распространенных (в том числе и в коммерческих приложениях) методов расширения спектра является фазовая манипуляция сигнала по закону некоторой псевдослучайной последовательности (метод прямой последовательности). С этой точки зрения значительный интерес (в силу своих оптимальных автокорреляционных свойств) представляют так называемые последовательности Баркера [3]. Именно они будут использованы в данной работе в качестве расширяющей последовательности.

Следует отметить, что предложенные ранее модели [4] зачастую останавливаются в своей детализации на уровне огибающей сигнала, что не позволяет решать многие из перечисленных выше задач. Следовательно, актуальным вопросом является построение вычислительной имитационной модели системы связи расширенного спектра, достаточно приближенной к физике протекающих в этой системе процессов [5]. Вопрос тем более актуален, поскольку современные вычислительные средства позволяют достаточно просто реализовать модель такого типа и в приемлемое время выполнить соответствующий имитационный эксперимент.

Таким образом, целью данной работы является разработка имитационной вычислительной модели системы связи с бинарной фазовой манипуляцией и расширением спектра с помощью последовательности Баркера. Применение построенной модели рассмотрим на примере исследования устойчивости системы к ошибкам синхронизации по частоте, фазе и времени.

Построение модели. Структурная схема модели изображена на рис. 1. Она, в общем, отображает структуру приемо-передающих устройств и канала в системах связи с расширением спектра методом прямой последовательности [6].

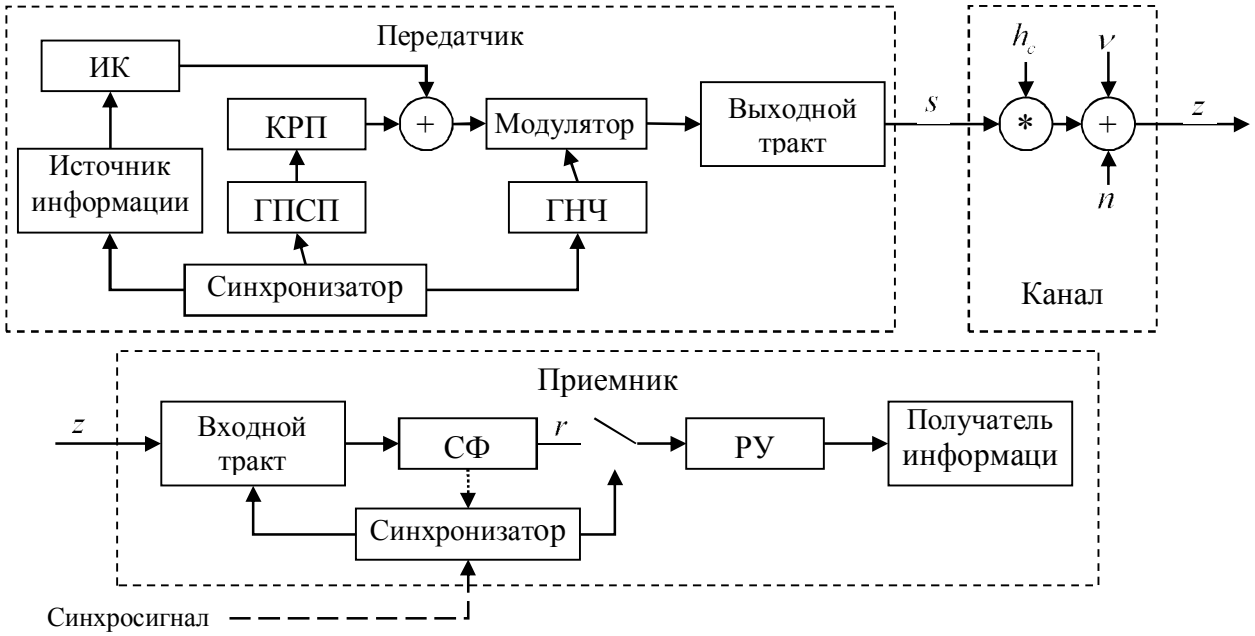

Рис. 1. Структурная схема имитационной вычислительной модели

Рассмотрим приведенную схему подробнее. Информационный кодер (ИК) превращает битовый поток, исходящий от источника информации, в первичный цифровой сигнал $\theta_{inf}(t)$, определяющий информационный закон изменения фазы. Кодер расширяющей последовательности (КРП) превращает битовый поток генератора псевдослучайной последовательности (ГПСП) в сигнал $\theta_{ss}(t)$. Сигнал $\theta_{ss}(t)$ задает закон изменения фазы для расширения спектра. Отметим, что скорость битового потока ГПСП относится к битовой скорости источника информации как $\frac{N_C \cdot \log_2(M_C)}{\log_2(M)}$, где N_C – количество символов ПСП, приходящихся на один информационный символ; M_C – количество позиций модулирующего сигнала $\theta_{ss}(t)$; M – количество позиций сигнала $\theta_{inf}(t)$.

Следовательно, если T – символьный интервал системы, то длительность символа ПСП равняется $\tau_0 = T / N_C$. Сигналы $\theta_{inf}(t)$ и $\theta_{ss}(t)$ объединяются в сумматоре и поступают на вход фазового модулятора. На другой вход модулятора поступает сигнал генератора несущей частоты (ГНЧ) вида $x(t) = A\sin(2\pi f_1 t + \varphi_1)$, где A – амплитуда; f_1 – частота; φ_1 – начальная фаза гармонического колебания.

Синхронизатор согласовывает по времени циклы работы источника информации, ГПСП и ГНЧ. Если обозначить $R = 1/T$ – символьную скорость передачи информации, а $f_0 = 1/\tau_0$ – частоту следования символов ПСП, то роль синхронизатора в передатчике можно разъяснить как обеспечение строгой кратности (с соответствующими коэффициентами) величин R, f_0 и f_1. Кроме того синхронизатор должен обеспечить согласование начала рабочего цикла ГПСП и ГНЧ с началом символьного интервала информационного сообщения. В результате на выходе модулятора наблюдаем сигнал вида

$$s(t) = A\sin(2\pi f_1 t + \theta_{inf}(t) + \theta_{ss}(t) + \varphi_1). \quad \textbf{(1)}$$

Выходной тракт передатчика в общем случае может осуществлять перенос частот и усиление сигнала перед его подачей на антенно-фидерные устройства. Однако в модели

функциональность этого блока ограничена нормировкой амплитуды сигнала для достижения необходимого значения мощности P_x: $A = \sqrt{2P_x}$.

Преобразование математической модели сигнала передатчика (1) в вычислительную модель требует перехода к дискретному времени. Все функции времени, используемые в модели, должны быть вычислены во временных узлах t_0, t_1, ..., t_{i-1}, t_i, t_{i+1}, ..., t_{N-1}, где $t_i = t_\Delta \cdot i$, $i = 0,1,2,...,N-1$, t_Δ – период дискретизации; t_{N-1} – длительность наблюдения.

Например, функция (1) представлена в модели вектором действительных чисел $\bar{s} = (s(t_0),\ s(t_1),\ ...,\ s(t_i),\ ...,\ s(t_{N-1}))$; N определяет размерность вектора $\bar{s}$. Обозначим $f_\Delta = 1/t_\Delta$ – частоту дискретизации. Следует отметить, что адекватные результаты моделирования можно получить, если $f_\Delta \geq 8f_1$. В дальнейших исследованиях $f_\Delta = 16f_1$.

На рис. 2 приведены примеры графиков функций $\theta_{inf}(t)$, $\theta_{ss}(t)$ и $s(t)$ при использовании бинарной фазовой манипуляции. В качестве расширяющей последовательности здесь использован код Баркера длиной $N_C = 13$ при этом соотношение частот $f_1 = f_0 = 13R$, а единица измерения оси времени на рисунке – длительность символа ГПСП τ_0.

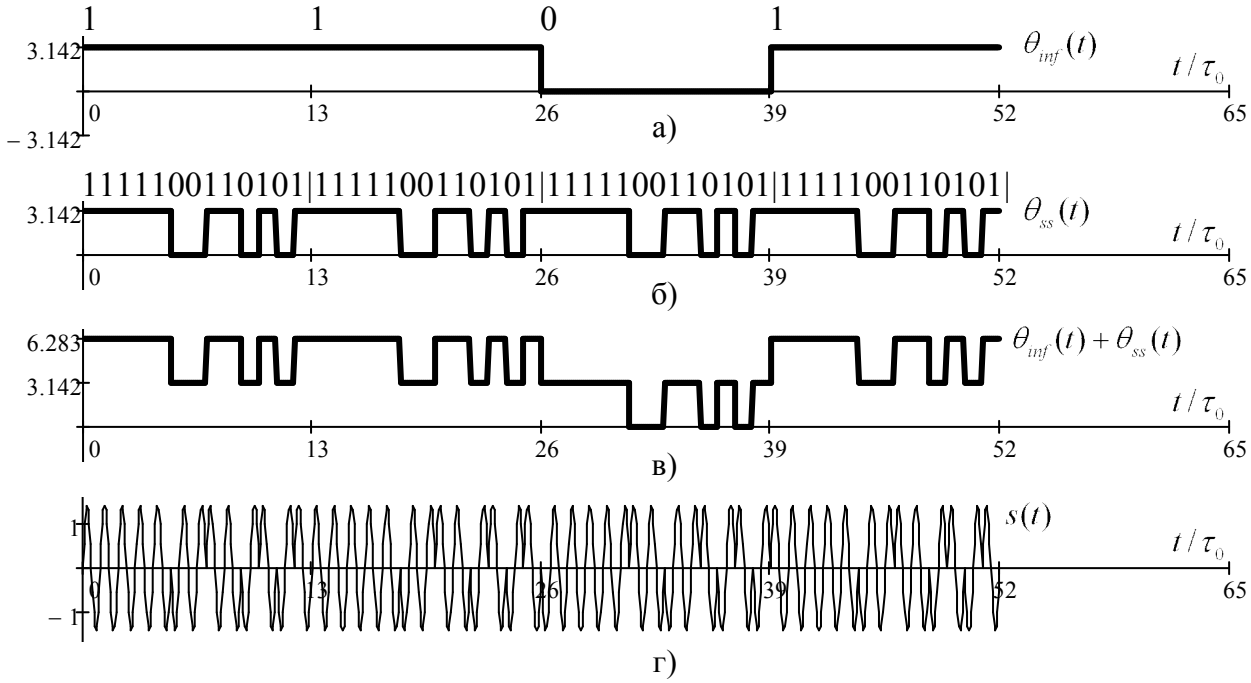

Рис. 2. Информационные биты и информационный модулирующий сигнал $\theta_{inf}(t)$ **(а);** циклическая последовательность Баркера и сигнал модуляции расширения спектра $\theta_{ss}(t)$ **(б);** сигнал на входе модулятора **(в);** сигнал $s(t)$ на выходе модулятора **(г)**

В данном исследовании будем использовать именно бинарную фазовую манипуляцию, хотя модель рассчитана также и на многопозиционную фазовую манипуляцию гармонического сигнала.

Следующий этап – моделирование канала связи. В общем случае на входе приемника наблюдается сигнал вида

$$z(t) = s(k_t t - t_c) \cdot h_c(t) + \nu(t) + n(t), \qquad \textbf{(2)}$$

где $h_c(t)$ – импульсная характеристика канала; k_t – коэффициент рассогласования масштаба времени (определяется отличием в частоте тактового генератора в синхронизаторах передатчика и приемника, а также доплеровским сдвигом частоты); t_c – ошибка синхронизации по времени; $\nu(t)$ – квазигармонические помехи; $n(t)$ – аддитивный белый гауссов шум (БГШ).

Влияние на сигнал многолучевого канала в упрощенном виде можно представить как дополнительное смещение фазы принимаемого сигнала φ_c. Моделирование квазигармонических помех можно осуществить в соответствии с математической моделью, изложенной в [7]. Однако исследование влияния на систему квазигармонических помех выходит за пределы данного исследования. Исходя из сказанного, формулу (2) можно переписать в развернутом виде так

$$z(t) = A\sin(2\pi f_1(k_t t - t_c) + \theta_{inf}(k_t t - t_c) + \theta_{ss}(k_t t - t_c) + \varphi_c + \varphi_1) + n(t). \quad \textbf{(3)}$$

Моделью БГШ является вектор $\overline{n}$ независимых реализаций гауссовой случайной величины с нулевым математическим ожиданием и дисперсией D_n. Значение дисперсии этой величины выбирается так, чтобы обеспечить заданное значение отношения сигнал-шум $h^2 = E_b / N_0$, где E_b – энергия передачи бита, N_0 – спектральная плотность мощности БГШ. Из [3] известно, что $h^2 = E_b / N_0 = \rho^2 B$, где $B = N_C$ – база сигнала, $\rho^2 = P_x / P_n$ – отношение сигнал-шум по мощности, P_n – мощность БГШ в полосе частот сигнала. Учитывая теорему Котельникова, можем записать $P_n = D_n \cdot 2f_0 / f_\Delta$, тогда $D_n = P_x f_\Delta N_C / (2f_0 h^2)$. Если зафиксировать в (3) $A = \sqrt{2}$, то есть $P_x = 1$, то получим $D_n = \dfrac{f_\Delta N_C}{2f_0 h^2}$.

Сигнал $z(t)$ поступает на вход согласованного фильтра (СФ). В случае многопозиционной модуляции СФ состоит из нескольких каскадов (соответственно количеству позиций модуляции), а решающее устройство (РУ) функционирует по мажоритарному принципу.

Если же модуляция бинарная, то СФ состоит из одного каскада. Ядро фильтра $h(t)$ совпадает с сигналом (1), определенным на одном символьном интервале и инвертированном во времени. Пусть этот сигнал соответствует передаче, например, символа 1. Обозначим $r(t)$ – сигнал на выходе фильтра, а r^* – значение функции $r(t)$ в предполагаемый момент окончания текущего (k-го) символьного интервала, то есть $r^* = r(kT - t_c)$. При этих условиях РУ работает по правилу $r^* \underset{H_0}{\overset{H_1}{\gtrless}} 0$, где H_1 – гипотеза о приеме символа 1, а H_0 – гипотеза о приеме символа 0. Как можно более точное определение момента окончания символьного интервала и выборка соответствующих значений функции $r(t)$ – одна из основных задач синхронизатора приемника.

Процедура синхронизации может обеспечиваться двумя принципиально разными способами. Первый предполагает, что хронирующий сигнал поступает извне по специальному каналу с высоким отношением сигнал-шум (пунктирная линия на рис. 1). Синхросигнал может исходить от внешнего высокоточного источника. Такой синхросигнал обычно тактирует как синхронизатор приемника, так и синхронизатор передатчика. Источником синхросигнала может быть и передатчик (он выступает ведущим устройством, а приемник – ведомым). В любом случае такой режим работы системы будем называть синхронным, и будем считать, что рассогласование масштаба времени в синхронном режиме отсутствует, то есть $k_t = 1$.

Однако расширение спектра сигнала позволяет осуществить автосинхронизацию системы. При этом источником синхросигнала является СФ приемника (точечная линия на рис. 1). Такой режим работы системы будем называть асинхронным.

В асинхронном режиме указателем момента окончания символьного интервала является главный пик функции $r(t)$. Грубая синхронизация определяется по пересечению огибающей модуля функции $r(t)$ порогового уровня γ, а точная синхронизация может быть осуществлена путем поиска положения максимума функции $|r(t)|$ внутри интервала, где $|r(t)| > \gamma$.

На рис. 3 проиллюстрирован вид выхода СФ (при отсутствии аддитивных помех), определение знака $r(t)$ с помощью РУ в конце символьного интервала и биты принятого сообщения. На этом же рисунке показана функция $|r(t)|$ и оптимальный пороговый уровень γ, который можно вычислить как среднее арифметическое между максимумом главного пика и максимумом боковых пиков функции $|r(t)|$ (при отсутствии помех). Поскольку для последовательностей Баркера максимум модуля бокового пика автокорреляционной функции равняется $1/N_C$, то в данном случае $\gamma = (N_C + 1)/(2N_C)$.

Особенностью вычислительной модели приемника является только, то, что все процессы происходят в дискретном времени. Например, если вектор $\bar{z}$ есть представление в модели сигнала (3), то $r(t)$ (выход СФ) вычисляется как цифровая свертка $\bar{z}$ и вектора $\bar{h}$, который является дискретным представлением ядра $h(t)$: $r_i = \sum_{j=0}^{N_T-1} z_{i-j} \cdot h_j$, где $N_T = T/t_\Delta$ – размерность вектора $\bar{h}$.

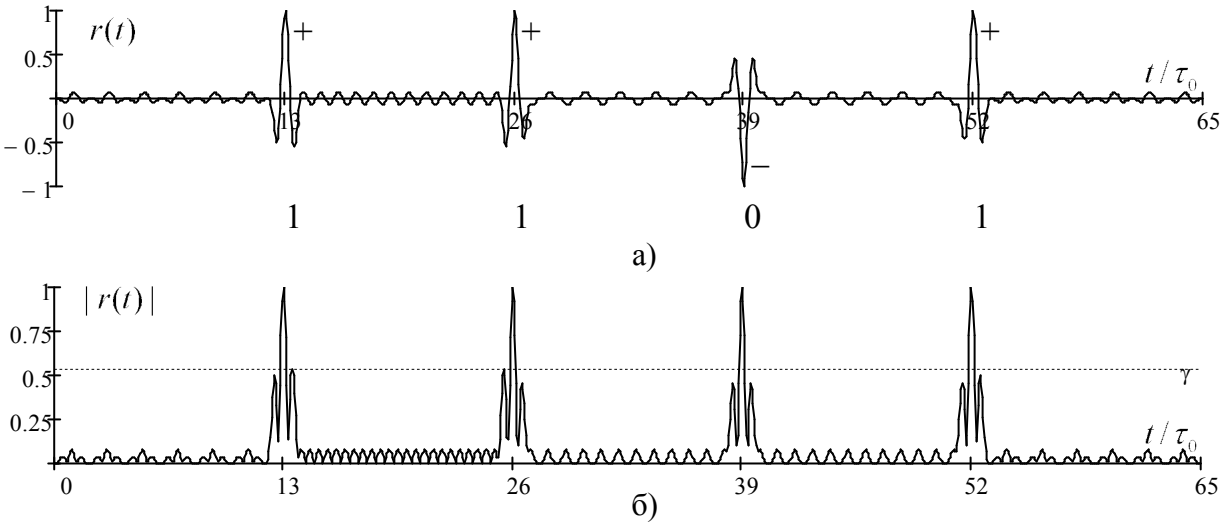

Рис. 3. Функция $r(t)$ на выходе СФ и процедура детектирования **(а);**
функция $|r(t)|$ и пороговый уровень синхронизатора γ **(б)**

Исследование помехоустойчивости системы. Следует отметить, что при условии точной синхронизации ($k_t = 1$, $\varphi_c = 0$, $t_c = 0$) потенциальная помехоустойчивость исследуемой системы связи не отличается от помехоустойчивости классической системы с когерентным приемом фазоманипулированного сигнала [7]. Следовательно, вероятность ошибки приемника определяется равенством $P_b = 1 - \Phi(\sqrt{2h^2})$, где $\Phi(\xi)$ – интеграл вероятностей $\Phi(\xi) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\xi} \exp\left(-\frac{u^2}{2}\right) du$.

Рассмотрим влияние ошибок синхронизации разного типа на форму сигнала (3), график функции $r(t)$ и помехоустойчивость системы. Рис. 4 иллюстрирует влияние ошибки фазовой синхронизации на форму сигналов. Построения выполнены для кода Баркера длиной $N_C = 13$ при соотношении частот $f_1 = 4f_0 = 52R$ и $\varphi_c = \pi/4$. Соответствующие сигналы при $\varphi_c = 0$ изображены точечной линией (для сравнения). Как видно из рис. 4 смещение фазы приводит к изменению формы излома сигнала $s(t)$ в точках разрыва модулирующего сигнала $\theta_{inf}(t) + \theta_{ss}(t)$. Кроме того происходит соответствующий фазовый сдвиг гармонического заполнения внутри пика функции $r(t)$ (при сохранении формы огибающей пика).

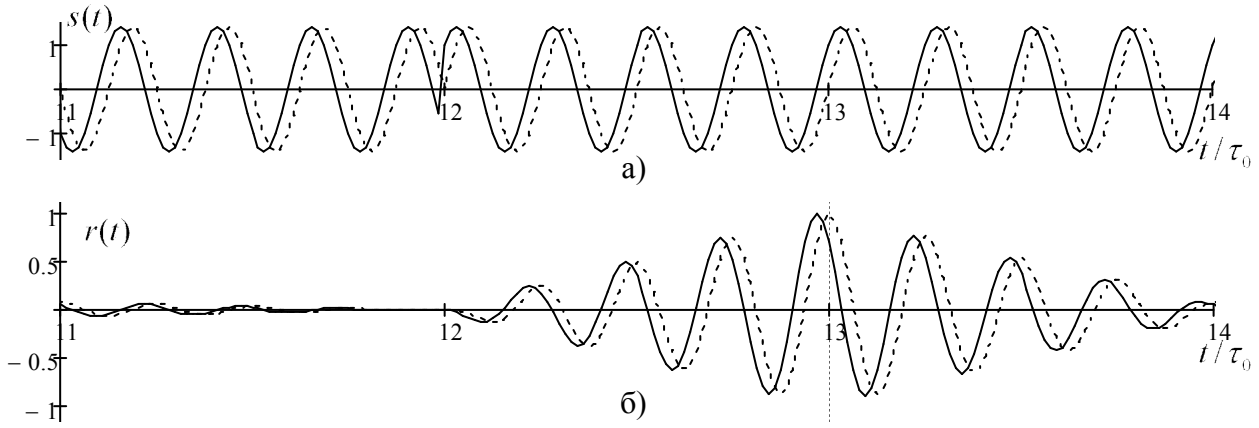

Рис. 4. Изменение формы сигналов $s(t)$ **(а)** и $r(t)$ **(б)** при ошибке фазовой синхронизации

В результате при синхронном режиме работы системы в точке выборки значения функции $r(t)$ будем иметь $r^* = r(kT)\cos\varphi_c$. Отсюда следует, что $\cos^2\varphi_c$ выражает потери отношения сигнал-шум, поэтому вероятность ошибки приема информационного бита P_b в данном случае вычисляется по формуле $P_b = 1 - \Phi(\sqrt{2h^2}\cos\varphi_c)$.

Влияние смещения фазы на помехоустойчивость системы связи объясняет рис. 5. Непрерывными кривыми на рисунке показаны теоретические зависимости, полученные по указанной выше формуле, точки отвечают результатам имитационных вычислительных экспериментов. Следует отметить, что при $\varphi_c = \pi/2$ среднее значение r^* будет равно 0 и результат детектирования не определен (случаен). Дальнейшее увеличение φ_c приведет к обратной работе детектора.

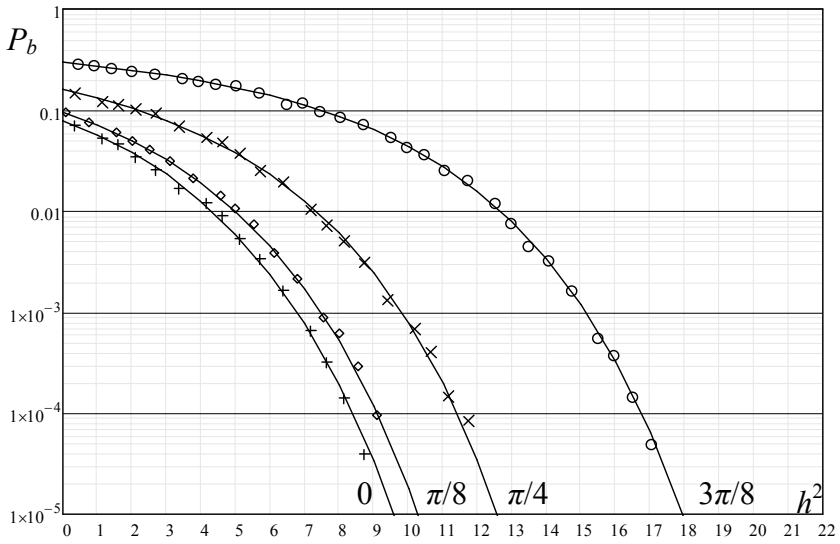

Рис. 5. Зависимости P_b от h^2 при различных значениях φ_c в синхронном режиме

В асинхронном режиме возникновение ошибки приема информационного бита зависит от срабатывания трех устройств: грубой синхронизации, точной синхронизации и РУ. Поэтому аналитическое исследование вероятности ошибки P_b является достаточно сложной задачей. Однако результаты вычислительных экспериментов позволяют составить представление о влиянии фазового смещения φ_c на помехоустойчивость системы в асинхронном режиме. На рис. 6 изображены экспериментальные оценки зависимостей P_b от h^2. Непрерывные кривые соответствуют отсутствию ошибки $\varphi_c = 0$, длинный штрих – $\varphi_c = \pi/8$, точечные кривые – $\varphi_c = \pi/4$, штрих-пунктирные – $\varphi_c = 3\pi/8$.

Анализ результатов показывает, что система точной синхронизации успешно компенсирует фазовые смещения меньшие $\pi/4$. В асинхронном режиме потери связанные с рассинхронизацией фазы гораздо меньше, чем в синхронном режиме. Однако добавка ошибок синхронизации к общему результату приводит к значительным потерям (около 7 дБ при $f_1 = f_0$).

Следует отметить, что уве-личение частоты несущей при фиксированной часто-те следования эле-ментов ПСП уменьшает помехо-устойчивость системы.

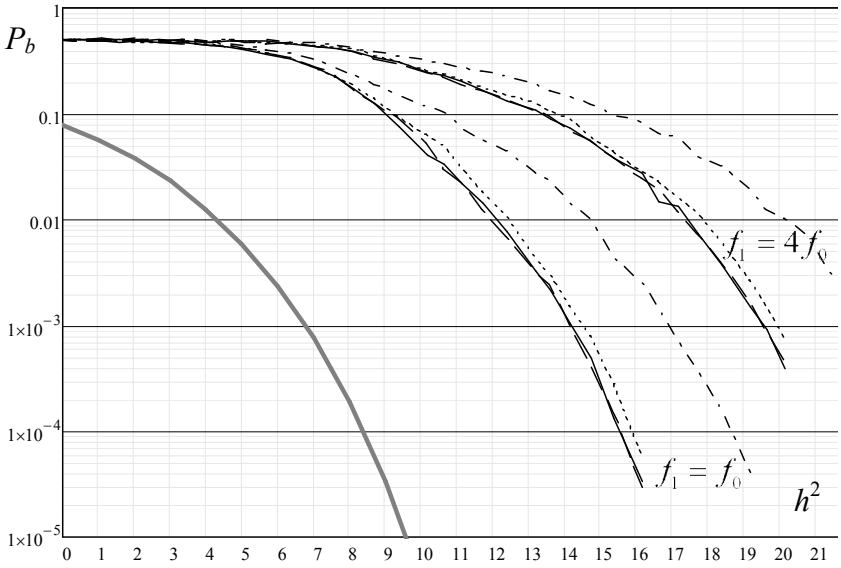

Рис. 6. Зависимости P_b от h^2 при различных значениях φ_c в асинхронном режиме

Рассмотрим теперь ***ошибку синхронизации по времени.*** Поскольку в асинхронном режиме момент выборки значения $r(t)$ определяется каждый раз синхронизатором, то регулярная ошибка синхронизации времени характерна только для синхронного режима (см. рис. 7).

В данном случае сигналы $s(t)$ и $r(t)$ сохраняют свою форму, только лишь смещаются по оси времени. В этом случае $r^* = \left(1 - \frac{|t|}{\tau_0} T\right) \cos(2\pi f_1 t_c)$.

Отсюда следует, что при малых значениях t_c потери помехоустойчивости могут быть приближенно выражены через фазовую ошибку $\varphi_c = 2\pi f_1 t_c$.

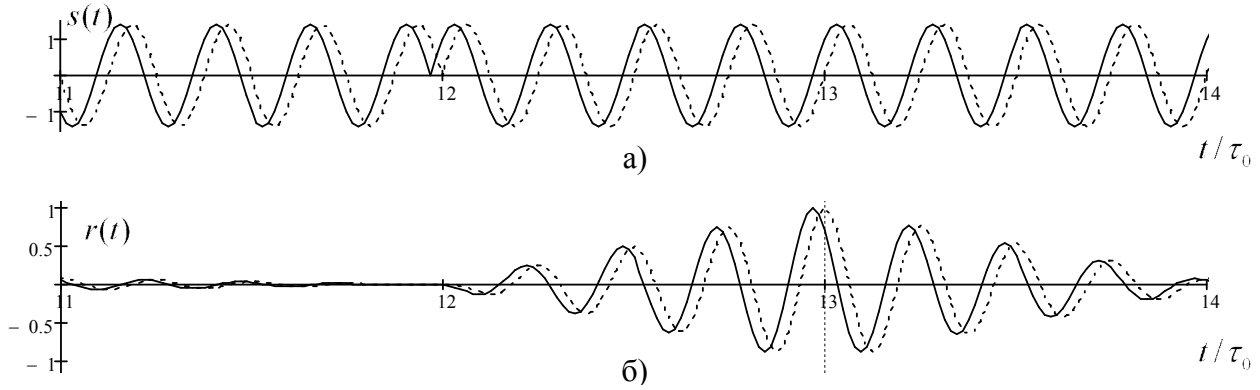

Рис. 7. Изменение формы сигналов $s(t)$ **(а)** и $r(t)$ **(б)** при ошибке синхронизации по времени

Наиболее губительным для системы является расхождение масштабов времени в передатчике и приемнике. В совокупности с доплеровским сдвигом частоты оно приводит к возникновению ошибки частотной синхронизации.

В синхронном режиме такая ошибка может быть представлена как накапливаемая ошибка временной синхронизации (рис. 8). При достаточной длине пакета и отсутствии подстройки частоты результатом будет полная потеря связи. Поэтому считаем, что в синхронном режиме расхождение масштабов времени пренебрежимо мало.

Влияние ошибки данного типа на помехоустойчивость системы в асинхронном режиме проиллюстрировано на рис. 9.

Кривые зависимости P_b от h^2 получены в результате проведения имитационного вычислительного эксперимента для следующих значений k_t: 1) $k_t = 1$ (непрерывная кривая); 2) $k_t = 1{,}01$ (кривая с длинным штрихом); 3) $k_t = 1{,}02$ (штрих-пунктирная кривая). Из рисунка видно, что при увеличении частоты несущей потери помехоустойчивости связанные с ошибкой синхронизации масштаба времени уменьшаются.

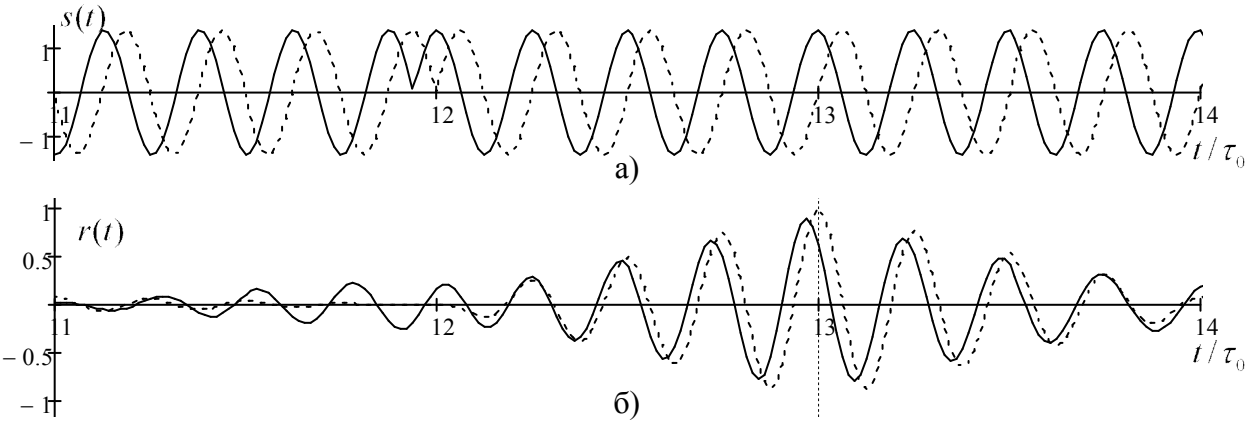

Рис. 8. Изменение формы сигналов $s(t)$ **(а)** и $r(t)$ **(б)** при ошибке синхронизации по времени

Выводы. Предложенная в работе методика имитационного моделирования широкополосных систем связи может быть эффективным инструментом исследования существующих и прогнозирования свойств разрабатываемых систем.

Рассмотренная модель допускает ряд упрощений в структуре приемо-передающих устройств. Например, в практических системах в синхронном режиме, как правило, применяется устройство точной синхронизации, позволяющее компенсировать малые расхождения в оценке времени передатчиком и приемником.

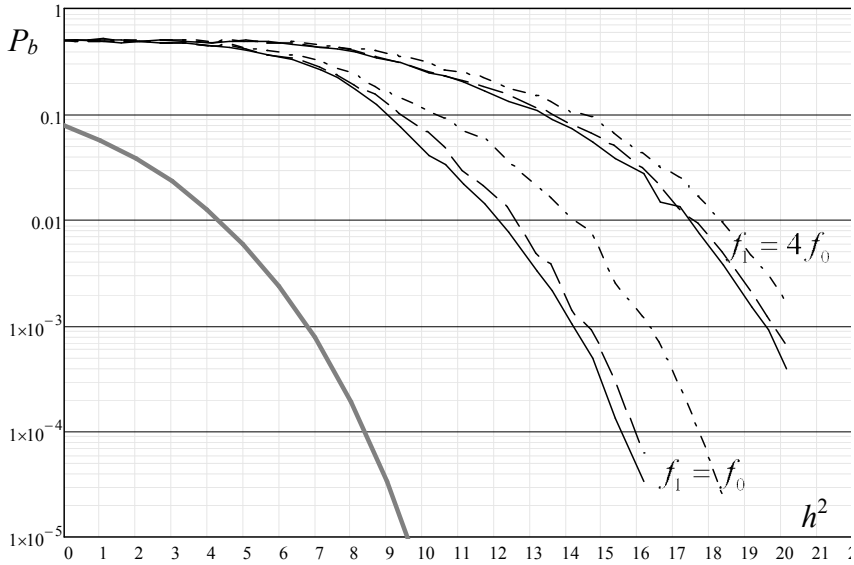

Рис. 9. Зависимости P_b от h^2 при различных значениях k_t в асинхронном режиме

Из проведенных исследований видно, что решение проблемы фазовой синхронизации может быть найдено при применении RAKE-приемника, состоящего из 8-ми ветвей отличающихся сдвигом фазы ядра СФ на $\pi/4$. Количество ветвей можно сократить до 4-х, если передавать детерминированный бит в преамбуле каждого пакета для компенсации обратной работы РУ (сдвиг фазы на π). Такие решения также известны в практике построения систем данного типа.

При необходимости модель может быть дополнена соответствующими модулями. Однако в данной работе мы преследовали иную цель, а именно: предложить методику моделирования систем связи с расширением спектра прямой последовательностью, позволяющую “заглянуть” внутрь процессов, происходящих в системе, а также получить оценки некоторых зависимостей трудно вычисляемых аналитически.

Дальнейшие исследования в этом направлении связаны с исследованием влияния на характеристики системы перехода к применению многопозиционной фазовой модуляции для расширения спектра.

Литература

1. Мазурков М.И. Системы широкополосной радиосвязи: учеб. пособие для студ. вузов / М.И. Мазурков. – О.: Наука и техника, 2010. – 340 с.

2. Семенко А.І. Особливості проектування телекомунікаційних систем з широкосмуговим шумоподібним сигналом / А.І. Семенко // Вісник Державного університету інформаційно-комуніуаційних технологій. – 2007. – Спецвипуск. – С.108-114.

3. Варакин Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. – М.: Радио и связь, 1985. – 384 с.

4. Быков В.В. Цифровое моделирование в статистической радиотехнике / В.В. Быков. – М.: Сов. Радио, 1971. – 328 с.

5. Комашинский В.И. Системы подвижной радиосвязи с пакетной передачей информации. Основы моделирования / В.И. Комашинский, А.В. Максимов. – М.: Горячая линия – Телеком, 2007. – 176 с.

6. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Издательский дом "Вильямс", 2004. – 1104 с.

7. Тихонов В.И. Статистический анализ и синтез радиотехнических устройств и систем: учеб. пособие для вузов / В.И. Тихонов, В.Н. Харисов. – М.: Радио и связь, 1991. – 608 с.

УДК 511.216

Яремчук Ю.Є., к.т.н. (*Вінницький національний технічний університет*)

ОТРИМАННЯ АНАЛІТИЧНИХ ЗАЛЕЖНОСТЕЙ ПРИСКОРЕНОГО ОБЧИСЛЕННЯ ЕЛЕМЕНТІВ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ ДЛЯ РОЗРОБКИ АСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Яремчук Ю.Є. Отримання аналітичних залежностей прискореного обчислення елементів рекурентних послідовностей для розробки асиметричних криптографічних протоколів. В роботі розглянуто рекурентну U_k-послідовність, для якої встановлено аналітичні залежності прискореного обчислення елементів цієї послідовності через елементи V_k-послідовності. Розглянуті послідовності, а також сукупність отриманих аналітичних залежностей можуть стати основою для розробки асиметричних криптографічних протоколів.

Ключові слова: КРИПТОГРАФІЯ, МАТЕМАТИЧНИЙ АПАРАТ, РЕКУРЕНТНА ПОСЛІДОВНІСТЬ, U_k-ПОСЛІДОВНІСТЬ, V_k-ПОСЛІДОВНІСТЬ

Яремчук Ю.Е. Получение аналитических зависимостей ускоренного вычисления элементов рекуррентных последовательностей для разработки асимметричных криптографических протоколов. В работе рассмотрено рекуррентную U_k-последовательность, для которой установлены аналитические зависимости ускоренного вычисления элементов этой последовательности через элементы V_k-последовательности. Рассмотренные последовательности, а также совокупность полученных аналитических зависимостей, могут стать основой для разработки асимметричных криптографических протоколов.

Ключевые слова: КРИПТОГРАФИЯ, МАТЕМАТИЧЕСКИЙ АППАРАТ, РЕКУРРЕНТНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ, U_k-ПОСЛЕДОВАТЕЛЬНОСТЬ, V_k-ПОСЛЕДОВАТЕЛЬНОСТЬ

Iaremchuk Iu.Ie. Receipt of analytical dependences speed-up calculation of elements of recurrent sequences for development of asymmetric cryptographic protocols. The recurrent is in-process considered U_k-sequence for which analytical dependences of speed-up calculation of elements of this sequence are set through elements V_k-sequences. This sequences, and also aggregate of the got analytical dependences, can to be foundation for development of asymmetric cryptographic protocols.

Keywords: CRYPTOGRAPHY, MATHEMATICAL APPARATUS, RECURRENT SEQUENCE, U_k-SEQUENCE, V_k-SEQUENCE

Вступ. Рекурентні послідовності в загальному вигляді породжується співвідношенням $u_n = a_1 u_{n-1} + a_2 u_{n-2} + \ldots + a_k u_{n-k}$ виходячи з початкових елементів u_0, u_1, ... , u_k