ISSN 0868–5886 НАУЧНОЕ ПРИБОРОСТРОЕНИЕ, 2024, том 34, № 2, с. 112–120

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 621.391

© А. А. Гавришев, Д. Л. Осипов, 2024

АНАЛИЗ СВОЙСТВ СВЕРХШИРОКОПОЛОСНЫХ СИГНАЛОВ, ВЛИЯЮЩИХ НА СКРЫТНОСТЬ И НАДЕЖНОСТЬ ПЕРЕДАЧИ ДАННЫХ В СИСТЕМАХ РАДИОСВЯЗИ

Проведен анализ использования последовательностей сверхширокополосных сигналов (СШПС), сформированных на основе BPSK-модуляции для обеспечения скрытности и надежности передачи данных в системах радиосвязи. Проведена оценка их свойств с помощью показателей BDS-статистики и пик-фактора. В результате проведенных исследований установлено, что для выбранных условий исследования в целом подходящими являются последовательности СШПС, основанные на решении уравнения Эйлера – Лагранжа, характеризующиеся большей скрытностью от постороннего наблюдателя, чем другие исследованные последовательности СШПС. Так же показано, что все исследуемые последовательности СШПС обладают приемлемым значением пик-фактора. Отмечено, что последовательности СШПС, построенные на основе широко используемых импульсов, например моноциклы Гаусса, а также стандартизированные системы радиосвязи, не позволяют в полной мере обеспечить скрытность передачи данных в системах радиосвязи, поэтому их нецелесообразно использовать в СШПС-системах радиосвязи с высокими требованиями по обеспечению скрытности передачи данных. Проведенные исследования позволили дополнить знания о последовательностях СШПС для обеспечения скрытной и надежной передачи данных в системах радиосвязи.

Кл. сл.: сверхширокополосные сигналы, системы связи, скрытность, надежность

ВВЕДЕНИЕ

Системы радиосвязи на основе сверхширокополосных сигналов (СШПС) являются перспективным направлением развития беспроводной передачи данных на малые расстояния. К их достоинствам следует отнести низкое энергопотребление, относительную простоту построения аппаратуры и высокую эффективность использования спектра. СШПС-системы радиосвязи представляют большой интерес для разработчиков и производителей телекоммуникационного оборудования, поскольку позволяют работать на безлицензионной основе, а особенности передаваемых сигналов подразумевают отсутствие мощных усилителей и сложных компонентов обработки сигналов в составе приемо-передающих комплексов. По сравнению с узкополосными системами СШПС-системы более успешно решают задачи повышения скорости и скрытности передачи данных. Реализация данных преимуществ подразумевает разработку особых методов формирования, обработки, передачи и приема сигналов [1, 2].

Вместе с тем вопросам оценки скрытности СШПС-систем радиосвязи уделено недостаточно внимания. Известно [3–10], что скрытность радиосигналов позволяет противостоять их обнаружению и измерению их параметров, обеспечивая таким образом, защиту от несанкционированного доступа. Так, в работе [3] указано, что узкополосные, широкополосные сигналы и СШПС имеют различную ширину спектра, что влияет на вероятность их обнаружения с помощью средств радиоразведки — чем больше ширина спектра передаваемого сигнала, тем труднее его обнаружить и, соответственно, выше его скрытность. Проведенные исследования показывают, что последовательности СШПС обладают наибольшей скрытностью по энергетическим показателям по сравнению с узкополосными и широкополосными сигналами. В работах [4–6] проведены исследования СШПС по критериям, характеризующим их энергетические характеристики, скрытность передачи информации и некоторые другие. Показано, что возможна оптимизация определенного типа последовательности сигналов, позволяющая улучшить отмеченные выше показатели качества. В работе [7] проведено численное моделирование СШПС-системы радиосвязи с расширением спектра. Исследованы спектральные и корреляционные характеристики передаваемых в канале связи СШПС. Полученные результаты показывают, что передаваемые в канале связи сигналы по энергетическим показателям имеют вид, схожий с флуктуационным шумом, что свидетельствует о низкой вероятности их перехвата. В работе [8] рассмотре-

но применение СШПС для дистанционного управления робототехническими комплексами. Приводятся результаты эксперимента по оценке скрытности передаваемых СШПС в эфире, проведенного с помощью анализатора спектра. Показано, что при удалении анализатора спектра на расстояние более 3 м от антенны приемопередатчика передаваемые СШПС не обнаруживаются. В работе [9] утверждается, что атаки на стандартизированные СШПС-системы радиосвязи на физическом уровне могут позволить злоумышленникам подделывать передаваемые данные. Такие атаки могут позволить злоумышленникам совершать различные противоправные действия с устройствами, в которых используются стандартизированные СШПС-системы радиосвязи. Предложен подход по повышению структурной скрытности передаваемых СШПС. Отмечено, что даже при перехвате передаваемых СШПС злоумышленник не сможет раскрыть структуру передаваемых сигналов из-за использования предложенного подхода. В работе [10] представлен один из подходов к оценке скрытности передаваемых СШПС, основанный на показателе равномерности спектра. Отмечено, что совершенные по показателю скрытности СШПС должны обладать равномерным спектром, близким по форме к прямоугольнику.

Как видно из приведенных данных, в известной литературе по СШПС-системам радиосвязи наиболее часто для оценки их скрытности используются методы, основанные на энергетических показателях. Указанные методы, хотя и являются наиболее часто используемыми для оценки скрытности различных типов радиосигналов, однако они обладают рядом недостатков. Так, известно [11–13], что энергетические показатели могут давать заниженные оценки скрытности радиосигналов. Исходя из этого, актуальным является оценка скрытности СШПС с помощью альтернативных методов оценки скрытности, например методов на основе нелинейной динамики и др. [11–13].

Кроме этого, в опубликованных работах не уделено достаточно внимания некоторым вопросам оценки надежности СШПС-систем радиосвязи, в частности оценке пик-фактора передаваемых СШПС как одного из показателей надежности. Известно [14–17], что увеличенное значение пик-фактора негативно влияет на помехоустойчивость и энергетическую эффективность радиопередающего устройства. Так, в публикациях [1, 2, 18] указано, что нормативные требования в различных странах накладывают ограничения на использование СШПС-систем радиосвязи. Отмечено, что пик-фактор СШПС играет важную роль в таких системах радиосвязи и может оказывать значительное влияние на энергетическую эффективность радиопередающего устройства. В [19] указано, что СШПС, используемые в различных практических приложениях, например в радиолокации, могут обладать большим пик-фактором и накладывать некоторые ограничения на работу таких устройств. Исходя из этого, разработчикам и производителям таких систем радиосвязи необходимо обращать более пристальное внимание на характеристики используемых СШПС, в том числе на форму СШПС и их пик-фактор.

Таким образом, можно утверждать, что исследование пик-фактора СШПС как одного из показателей надежности СШПС-систем радиосвязи является актуальным и требует дальнейшей проработки.

Целью статьи является оценка свойств последовательностей СШПС для обеспечения скрытной и надежной передачи данных в системах радиосвязи с помощью показателей BDS-статистики и пик-фактора.

ОСНОВНАЯ ЧАСТЬ

Исследовательская часть

Известно [20], что форма СШПС оказывает существенное влияние на характеристики систем радиосвязи, в которых они используются. Современные исследования, посвященные вопросам формирования СШПС, в большинстве случаев применяют в качестве базовых моноимпульсы Гаусса и их производные [1, 2, 21, 22]. Кроме этого, также активно используются импульсы Рэлея и импульсы на основе функций Лагерра [1, 2], импульсы на основе полиномов Лежандра [23, 24] и некоторые другие. Также в ряде работ предлагается большое количество новых классов СШПС, например импульсы на основе решения уравнения Эйлера – Лагранжа [4–6], на основе хаотических сигналов [25, 26], импульсы, описанные стандартом IEEE 802.15.4 [27], и многие другие.

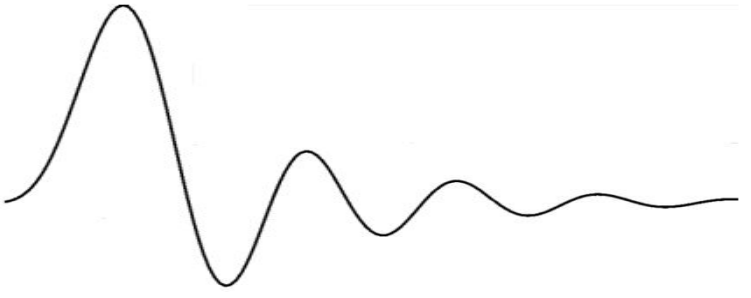
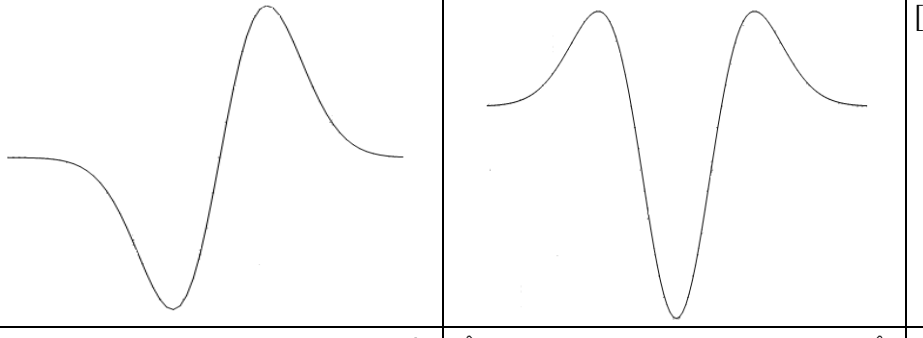
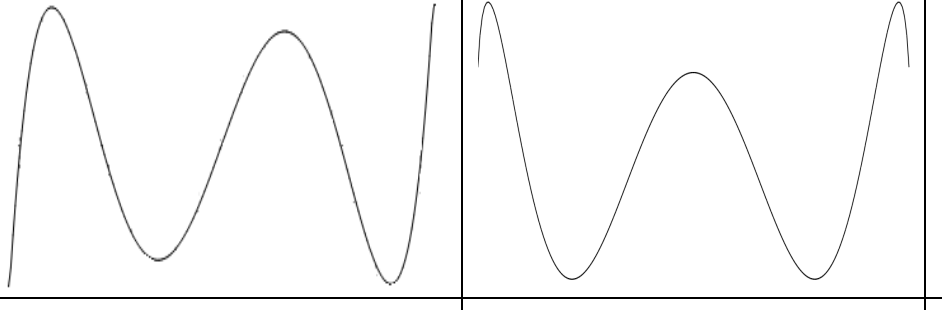
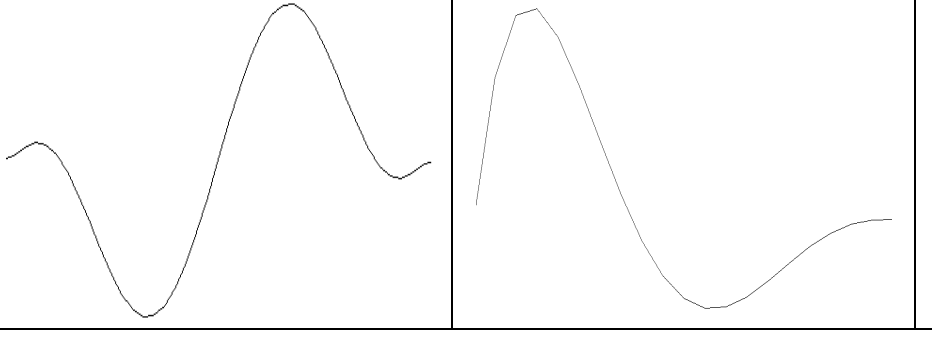
Для проведения исследований авторами были отобраны следующие виды СШПС, приведенные в табл. 1.

Для передачи информации необходимо оперировать потоком данных, представленным в виде последовательности импульсов СШПС [28–30]. Под последовательностью СШПС обычно понимается совокупность импульсов (см. табл. 1), расположенных на некотором конечном интервале времени, рассматриваемая как составной сигнал. В общем случае простейший вид передаваемой последовательности СШПС возможно записать следующим образом [28–30]:

$$S_n(t,t_0,T)=\sum_{k=0}^{N-1} s\left[t-t_0-(k-\mu)T\right], \qquad (1)$$

где t_0 — время прихода последовательности; T —

Табл. 1. Отобранные виды СШПС

Название	Временна́я диаграмма	Источник
Импульс, описанный стандартом IEEE 802.15.4		[27]
Моноцикл Гаусса различного порядка		[1, 2, 20, 22]
Импульсы на основе полиномов Лежандра		[23, 24]
Импульсы на основе решения уравнения Эйлера – Лагранжа		[4–6]

период следования СШПС; k — порядковый номер СШПС, начинающийся с 0; N — общее число импульсов в последовательности; μ — параметр, определяющий точку последовательности, с которой связано время ее прихода; $s(t)$ — описывает временну́ю форму одиночного сигнала.

В настоящее время в СШПС-системах радиосвязи одними из наиболее часто используемых являются следующие виды модуляции [28–30]: амплитудно-импульсная модуляция (PAM-модуляция), позиционно-импульсная модуляция (PPM-модуляция), двоичная фазовая модуляция (BPSK-модуляция). Каждая из них имеет свои достоинства и недостатки. В качестве базовой авторами была выбрана BPSK-модуляция.

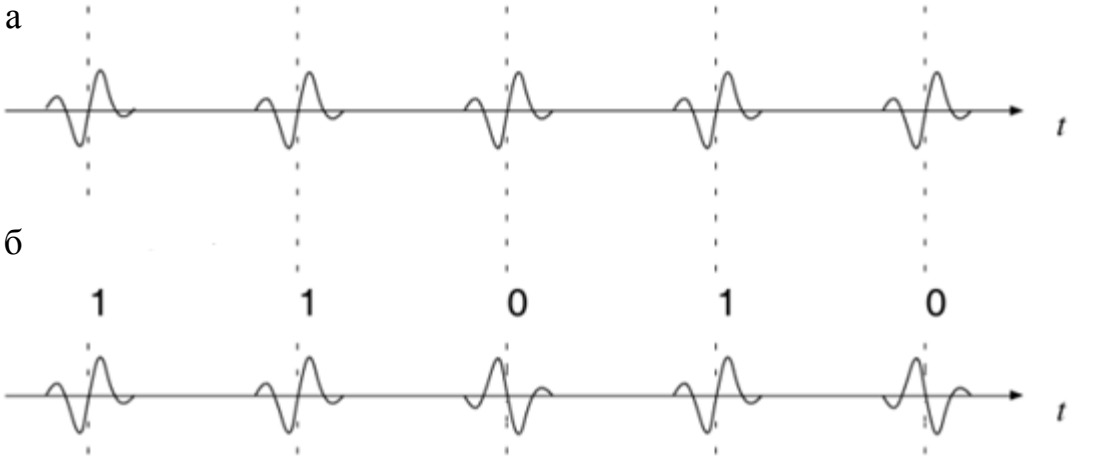


Рис. Метод BPSK-модуляции для СШПС-систем радиосвязи [28].
а — немодулированная последовательность, б — модулированная последовательность

При BPSK-модуляции для передачи используются два типа импульсов [28–30]: прямой и инверсный, т.е. сдвинутый относительно прямого импульса по фазе на 180°. Эти два импульса применяются для передачи логического нуля и единицы. Метод BPSK-модуляции имеет очень хорошие показатели помехоустойчивости. Иллюстрация принципа метода BPSK-модуляции применительно к СШПС-системам радиосвязи показана на рис.

С учетом выражения (1) и рекомендаций из работ [11, 12, 28–30], авторами было проведено моделирование передаваемых в канале связи СШПС, сформированных на основе BPSK-модуляции. В качестве последовательностей СШПС использовались импульсы, представленные в табл. 1. Для каждого из указанных видов импульсов было сформировано 50 последовательностей СШПС, в которых исходные передаваемые данные (логические нуль и единица) задавались с помощью генератора бинарных псевдослучайных последовательностей и модулировались импульсами, представленными в табл. 1.

Проведем количественную оценку скрытности и надежности полученных последовательностей СШПС с помощью BDS-статистики и пик-фактора. Положим, что исследуемые последовательности СШПС передаются в идеальном канале связи.

Для осуществления количественной оценки скрытности обратимся к BDS-статистике. Известно [11–13], что BDS-статистика базируется на статистических свойствах корреляционной размерности исследуемого процесса в фазовом пространстве, которая в свою очередь определяется корреляционным интегралом. Эти данные дают в отдельных случаях больше информации о классе процесса (случайные, хаотические, регулярные), чем энергетические показатели. В соответствии с [11–13], BDS-статистика в ряде случаев может выступать в качестве меры энергетической скрытности передаваемых сигналов. BDS-статистика основана на статистической величине $w(\varepsilon)$, описываемой следующим выражением:

$$w_{m,N}(\varepsilon) = \sqrt{N-m+1}\,\frac{C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m}{\sigma_{m,N}(\varepsilon)}, \qquad (2)$$

где $C_{m,N}(\varepsilon)$ и $C_{1,N-m}(\varepsilon)$ — корреляционные интегралы, а $\sigma_{m,N}(\varepsilon)$ — среднеквадратичное отклонение.

Табл. 2. Усредненные значения BDS-статистики $\overline{w(\varepsilon)}$ исследуемых последовательностей СШПС

Название	BDS-статистика $\overline{w(\varepsilon)}$
Импульс, описанный стандартом IEEE 802.15.4	[68÷80]
Моноциклы Гаусса различного порядка	[98÷110]
Импульсы на основе полиномов Лежандра	[244÷300]
Импульсы на основе решения уравнения Эйлера – Лагранжа	[28÷65]

В табл. 2 приведены усредненные значения BDS-статистики $\overline{w(\varepsilon)}$, описываемой выражением (2), полученные для исследуемых последовательностей СШПС.

Как видно из табл. 2, исследуемые последовательности СШПС обладают значениями BDS-статистики $\overline{w(\varepsilon)} \in [28,300]$. Среди них наименьшим значением BDS-статистики обладают последовательности СШПС, в которых используются импульсы на основе решения уравнения Эйлера – Лагранжа ($\overline{w(\varepsilon)} \in [28,65]$). Последовательности СШПС, построенные на основе широко используемых импульсов, например моноциклов Гаусса, обладают значениями BDS-статистики $\overline{w(\varepsilon)} \in [98,110]$, близкими к хаотическим сигналам [11–13]. Последовательности СШПС, описанные в стандарте IEEE 802.15.4, занимают промежуточное значение между исследуемыми последовательностями СШПС по показателю скрытности ($\overline{w(\varepsilon)} \in [68,80]$), приближаясь по значению BDS-статистики к авторегрессионому процессу и близким к ним [11–13]. Полученные результаты показывают, что последовательности СШПС в целом обладают сложной структурой, однако они также обнаруживаются с помощью BDS-статистики. Указанный результат совпадает с известными исследованиями [4, 9, 10].

Проведем количественную оценку исследуемых последовательностей СШПС с помощью одного из показателей надежности функционирования передачи данных в системах радиосвязи. В качестве такого показателя обратимся к показателю пик-фактора сигналов [14–17], вычисляемого с помощью следующего выражения:

$$P = \frac{U_{\max}}{\sigma}, \qquad (3)$$

где $U_{\max}$ — максимальное значение сигнала, σ — среднеквадратичное значение сигнала.

В табл. 3 приведены значения пик-фактора P, описываемого выражением (3), полученные для исследуемых последовательностей СШПС.

Как видно из табл. 3, исследуемые последовательности СШПС обладают значением пик-фактора $P \in [1.5, 3.3]$. Согласно известным исследованиям [14–17], для современных систем связи значение пик-фактора передаваемых сигналов, вычисленное с помощью выражения (3), должно находиться примерно в диапазоне $P \in [1, 4]$. Отсюда можно заключить, что исследуемые последовательности СШПС в целом подходят для передачи данных в системах радиосвязи, т.к. обладают приемлемым пик-фактором.

Сравнительный анализ полученных данных

В табл. 4 приведены обобщенные выводы по проведенным исследованиям. Сравнительный анализ полученных данных (табл. 4) показывает, что для выбранных условий исследования в целом подходящими являются последовательности СШПС [4–6], основанные на решении уравнения Эйлера – Лагранжа.

Табл. 3. Значения пик-фактора P исследуемых последовательностей СШПС

Название	Пик-фактор P
Импульс, описанный стандартом IEEE 802.15.4	[2÷2.6]
Моноциклы Гаусса различного порядка	[1.9÷2.5]
Импульсы на основе полиномов Лежандра	[1.5÷3]
Импульсы на основе решения уравнения Эйлера – Лагранжа	[2.1÷3.3]

Табл. 4. Обобщенные выводы по проведенным исследованиям

Название	BDS-статистика	Пик-фактор
Импульс, описанный стандартом IEEE 802.15.4	+/–	+
Моноциклы Гаусса различного порядка	+/–	+
Импульсы на основе полиномов Лежандра	+/–	+
Импульсы на основе решения уравнения Эйлера – Лагранжа	+	+

Указанные последовательности СШПС обладают значением BDS-статистики, наиболее близким к значению $w(\bar{\varepsilon}) \le |1.96|$, определяющему белый шум [11–13], и приемлемым пик-фактором. Поэтому последовательности СШПС указанного типа целесообразно применять в СШПС-системах радиосвязи для повышения скрытности и надежности передачи данных. Последовательности СШПС, построенные на основе широко используемых импульсов, например моноциклах Гаусса [1, 2, 21, 22], не позволяют в полной мере обеспечить скрытность передачи данных в системах радиосвязи, поэтому их нецелесообразно использовать в СШПС-системах радиосвязи с высокими требованиями по обеспечению скрытности передачи данных. Указанный результат совпадает с известными исследованиями [4, 9–13].

Последовательности СШПС, описанные в стандарте IEEE 802.15.4, хоть и обладают уровнем скрытности выше, чем широко используемые последовательности СШПС, однако меньшим, чем последовательности СШПС на основе решения уравнения Эйлера – Лагранжа. Кроме того, стандартизированные системы радиосвязи наиболее часто являются объектами атак злоумышленников из-за подробного описания всех их характеристик [4, 9–13]. Исходя из этого, их также нецелесообразно использовать в СШПС-системах радиосвязи с высокими требованиями по обеспечению скрытности передачи данных.

ЗАКЛЮЧЕНИЕ

Таким образом, в данной работе проведен анализ использования последовательностей СШПС, сформированных на основе BPSK-модуляции, для обеспечения скрытности и надежности передачи данных в системах радиосвязи. Проведена оценка их свойств с помощью показателей BDS-статистики и пик-фактора. В результате проведенных исследований установлено, что для выбранных условий исследования в целом подходящими являются последовательности СШПС [4–6], основанные на решении уравнения Эйлера – Лагранжа, характеризующиеся большей скрытностью от постороннего наблюдателя, чем другие исследованные последовательности СШПС, т.к. их значение BDS-статистики находится ближе к белому шуму [11–13]. Также показано, что все исследуемые последовательности СШПС обладают приемлемым значением пик-фактора. Отмечено, что последовательности СШПС, построенные на основе широко используемых импульсов, например моноциклов Гаусса [1, 2, 21, 22], а также стандартизированные системы радиосвязи [27] не позволяют в полной мере обеспечить скрытность передачи данных в системах радиосвязи, поэтому их нецелесообразно использовать в СШПС-системах радиосвязи с высокими требованиями по обеспечению скрытности передачи данных. Указанный результат совпадает с известными исследованиями [4, 9–13].

Проведенные исследования позволили дополнить знания о последовательностях СШПС для обеспечения скрытной и надежной передачи данных в системах радиосвязи. Дальнейшие работы в указанной области авторы связывают с исследованием СШПС-систем радиосвязи с другими распространенными видами модуляции. Кроме того, перспективным является направление исследований в области обеспечения скрытности и надежности СШПС-систем радиосвязи на основе хаотических сигналов.

СПИСОК ЛИТЕРАТУРЫ

1. *Абдрахманова Г.И.* Повышение эффективности сверхширокополосных систем связи на основе оптимизации формы импульсов. Автореф. дис. ... канд. техн. наук. Уфа, 2013. 19 с.
2. *Грахова Е.П., Мешков И.К., Багманов В.Х., Виноградова И.Л.* Моделирование СШП радиоимпульсов на основе производных Гаусса и Рэлея с учетом спектральной маски ГКРЧ // Электротехнические и информационные комплексы и системы. 2014. Т. 10, № 3. С. 62–69. URL: https://cyberleninka.ru/article/n/modelirovanie-sshp-radioimpulsov-na-osnove-proizvodnyh-gaussa-i-releya-s-uchetom-spektralnoy-maski-gkrch
3. *Каргашин В.Л.* Проблемы обнаружения и идентификации радиосигналов средств негласного контроля информации // Специальная техника. 2000. № 4. С. 45–53. URL: https://web.archive.org/web/20070206105910/http://st.ess.ru/publications/4_2000/kargashin/kargashin.pdf
4. *Корниенко А.В., Буй Л.Н.* Сравнение моделей сверхширокополосных сигналов по нескольким показателям качества // Вестник Рязанской государственной радиотехнической академии. 2005. № 16. С. 109–111. URL: https://elibrary.ru/item.asp?id=11743366
5. *Кириллов С.Н., Корниенко А.В., Буй Л.Н.* Влияние среды распространения на форму сверхширокополосных сигналов в системах передачи информации // Материалы XIV Международной научно-технической конференции "Проблемы передачи и обработки информации в сетях и системах телекоммуникаций". 2005, Рязань: РГРТА. С 61–62.
6. *Буй Л.Н.* Энергетические потери при пеленгации сверхширокополосных сигналов // Вестник Рязанского государственного радиотехнического университета. 2007. № 20. С. 117–120.
7. *Калинин В.И., Радченко Д.Е., Черепенин В.А.* Численное моделирование шумовой системы передачи

информации с расширением спектра // Журнал радиоэлектроники. 2014. № 10. (18 с.).
URL: http://jre.cplire.ru/jre/oct14/8/text.pdf
8. *Шибаев А.А.* О применении сверхширокополосной радиолинии в организационной структуре роботизированного комплекса // Сборник трудов Первой международной научной конференции "The 2017 Symposiumon Cybersecurity of the Digital Economy (CDE'17)". СПб.: Издательский дом "Афина", 2017. С. 392–394.
9. *Singh M., Leu P., Capkun S.* UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks // Network and Distributed Systems Security (NDSS) Symposium. 2019. (16 p.).
DOI: 10.14722/ndss.2019.23109
10. *Сеньков М.А., Киселев К.В., Быков А.А.* Разработка математической модели показателя равномерности радиочастотного спектра сверхширокополосного сигнала // Современные наукоемкие технологии. 2020. № 12, ч. 1. С. 107–112. DOI: 10.17513/snt.38418
11. *Гавришев А.А.* Моделирование и количественно-качественный анализ распространенных защищенных систем связи // Прикладная информатика. 2018. Т. 13, № 5 (77). С. 84–122. URL:
http://www.appliedinformatics.ru/r/articles/?article_keyword_4=&crosscutting_issue=229&category=0&author=1756
12. *Осипов Д.Л., Гавришев А.А.* Анализ использования отфильтрованных с помощью полосового фильтра хаотических сигналов для передачи данных в системах радиосвязи // Научное приборостроение. 2021. Т. 31. № 2. С. 93–104. DOI 10.18358/np-31-2-i93104
13. *Васюта К.С.* Классификация процессов в инфокоммуникационных радиотехнических системах с применением BDS-статистики // Проблемы телекоммуникаций. 2012. № 4 (9). С. 63–71.
URL: https://elibrary.ru/item.asp?id=20260336
14. *Логинов С.С.* Цифровые радиоэлектронные устройства и системы с динамическим хаосом и вариацией шага временной сетки. Дис. ... д-ра. техн. наук. Казань, 2015. 228 с.
15. *Гавришев А.А., Гавришев А.Н.* К вопросу о расчете значений пик-фактора сигналов, генерируемых распространенными скрытными системами связи // Вестник НЦБЖД. 2020. № 3 (45). С. 149–157. URL: https://elibrary.ru/item.asp?id=43928669
16. *Козел В.М., Подворная Д.А., Ковалев К.А.* Пик-фактор сигналов систем сухопутной подвижной службы 5G // Доклады БГУИР. 2020. Т. 18, № 6. С. 5–10. DOI: 10.35596/1729-7648-2020-18-6-5-10
17. *Дворников С.В., Марков Е.В., Маноши Э.А.* Повышение помехозащищенности передач декаметровых радиоканалов в условиях непреднамеренных помех // T-Comm: Телекоммуникации и транспорт. 2021. Т. 15, № 6. С. 4–9. DOI: 10.36724/2072-8735-2021-15-6-4-9
18. *Corral C.A., Emami Sh.* Peak Power and Implementation Considerationsfor UWB // IEEE802. 2005. (4 p.). URL:
https://www.ieee802.org/15/pub/05/15-05-0236-00-004a-peak-power-and-implementation-considerations-uwb.pdf
19. Recommendation ITU-R SM.1755-0: Characteristics of ultra-wideband technology. 2006.
URL: https://www.itu.int/rec/R-REC-SM.1755/en
20. *Имнореев И.Я.* Сверхширокополосные радары: Новые возможности, необычные проблемы, системные особенности // Вестник МГТУ. Сер. Приборостроение. 1998. № 4. С. 25–56.
URL: https://vestnikprib.ru/catalog/rec/rloc/801.html
21. *Дворников С.В., Пшеничников А.В., Дворников С.С., Борисов В.В., Потапов Г.С.* Система сверхширокополосной сверхкороткоимпульсной связи // Радиопромышленность. 2021. Т. 31, № 1. С. 16–27. URL: https://www.elibrary.ru/item.asp?id=45540851
22. *Кунилов А.Л., Ивойлова М.М.* Способ приема сверхкороткоимпульсного сигнала в виде моноцикла Гаусса. Патент РФ RU2737005C1 от 24.11.2020. URL: https://patents.google.com/patent/RU2737005C1/ru
23. *Tsai Ch.-Y., Jeng Sh.-K.* Design of a Legendre-polynominail-based orthogonal pulse generator for ultra-wideband communication // IEEE Conference: Antennas and propagation Society International Symposium. 2005. Vol. 2B. P. 680–683. DOI: 10.1109/APS.2005.1552105
24. *M'foubat A.O., Elbahhar F., Tatkeu Ch.* Novel ultra-wideband multi-user receiver for transportation systems communication // IET Networks. 2014. Vol. 3, iss. 3. P. 169–175. DOI: 10.1049/iet-net.2012.0081
25. *Дмитриев А.С., Клецов А.В., Лактюшкин А.М., Панас А.И., Старков С.О.* Сверхширокополосная беспроводная связь на основе динамического хаоса // Радиотехника и электроника. 2006. № 10. С. 1193–1209. URL: https://elibrary.ru/item.asp?id=17656509
26. *Kuzmin L.V., Efremova E.V., Itskov V.V.* Modulation, Shaping and Replicability of UWB Chaotic Radiopulses for Wireless Sensor Applications // Sensors. 2023. Vol. 23, iss. 15. Id. 6864. DOI: 10.3390/s23156864
27. *Coppens D., Shahid A., Lemey S., Herbruggen B., Marshall Ch., Poorter E.* An Overview of UWB Standards and Organizations (IEEE 802.15.4, FiRa, Apple): Interoperability Aspects and Future Research Directions // IEEE Access. 2022. URL: https://arxiv.org/pdf/2202.02190.pdf
28. *Носов В.И., Калинин В.О.* Исследование методов повышения помехоустойчивости короткоимпульсных сверхширокополосных систем радиосвязи. Новосибирск: СибГУТИ, 2017. 244 с.
29. *Беличенко В.П., Буянов Ю.И., Кошелев В.И.* Сверхширокополосные импульсные радиосистемы. Новосибирск: Наука, 2015. 473 с.
30. *Muhr E., Vauche R., Bourdel S., Gaubert J. et al.* High Output Dynamic UWB Pulse Generator for BPSK Modulations // IEEE International Conference on Ultra Wideband (IC UWB), Sydney, Australia, 2013. P. 170–174. DOI: 10.1109/ICUWB.2013.6663842

НИЯУ МИФИ, г. Москва, Россия (*Гавришев А.А.*)

СКФУ, г. Ставрополь, Россия (*Осипов Д.Л.*)

Контакты: *Гавришев Алексей Андреевич*, alexxx.2008@inbox.ru

Материал поступил в редакцию 21.02.2024

ANALYSIS OF THE PROPERTIES OF ULTRA-WIDEBAND SIGNALS AFFECTING THE SECRECY AND RELIABILITY OF DATA TRANSMISSION IN RADIO COMMUNICATION SYSTEMS

A. A. Gavrishev[1], D. L. Osipov[2]

[1]*NRNU MEPhI, Moscow, Russia*
[2]*NCFU, Stavropol, Russia*

The analysis of the use of sequences of ultra-wideband (UWB) signals formed on the basis of BPSK modulation to ensure the secrecy and reliability of data transmission in radio communication systems is carried out. Their properties were evaluated using BDS-statistics and peak factor indicators. As a result of the conducted research, it was found that for the selected research conditions, the UWB sequences based on the solution of the Euler – Lagrange equation, characterized by greater secrecy from an outside observer than other studied UWB sequences, are generally suitable. It is also shown that all the studied UWB sequences have an acceptable peak factor value. It is noted that UWB sequences based on widely used pulses, for example, Gauss monocycles, as well as standardized radio communication systems, do not fully ensure the secrecy of data transmission in radio communication systems, therefore, it is impractical to use them in UWB radio communication systems with high requirements for ensuring the secrecy of data transmission. The conducted research has made it possible to supplement knowledge about UWB sequences to ensure covert and reliable data transmission in radio communication systems.

Keywords: UWB, communication systems, secrecy, reliability

REFERENCES

1. Abdrakhmanova G.I. *Povyshenie ehffektivnosti sverkhshirokopolosnykh sistem svyazi na osnove optimizatsii formy impul'sov*. Avtoref. diss. kand. techn. nauk [abstr. cand. techn. sci. diss. Improving the efficiency of ultra-wideband communication systems based on pulse shape optimization.]. Ufa, 2013. 19 p. (In Russ.).
2. Grakhova E.P., Meshkov I.K., Bagmanov V.Kh., Vinogradova I.L. [UWB radio pulses design based on the derivative Gaussian and Rayleigh pulses relevant to the spectral mask of radiofrequencies committee]. *Ehlektrotekhnicheskie i informatsionnye kompleksy i sistemy* [Electrical engineering and information complexes and systems], 2014, vol. 10, no. 3, pp. 62–69. (In Russ.).
3. Kargashin V.L. [Problems of detection and identification of radio signals of means of tacit information control]. *Spetsial'naya tekhnika* [Special machinery], 2000, no. 4, pp. 45–53. (In Russ.).
4. Kornienko A.V., Bye L.N. [Comparison of models ultra-wideband signals on several parameters of quality]. *Vestnik Ryazanskoi gosudarstvennoi radiotekhnicheskoi akademii* [Bulletin of the Ryazan State Radio Engineering Academy], 2005, no. 16, pp. 109–111. (In Russ.).
5. Kirillov S.N., Kornienko A.V., Bye L.N. [Influence of the propagation medium on the form of ultra-wideband signals in information transmission systems]. *Materialy XIV Mezhdunarodnoi nauchno-tekhnicheskoi konferentsii "Problemy peredachi i obrabotki informatsii v setyakh i sistemakh telekommunikatsii"* [Proc. 14th Int. Conf. "Problems of information transmission and processing in telecommunication networks and systems"], 2005, Ryazan, RSREU named after V.F. Utkin. pp. 61–62. (In Russ.).
6. Bye L.N. [Energy losses during direction finding of ultra-wideband signals]. *Vestnik Ryazanskogo gosudarstvennogo radiotekhnicheskogo universiteta* [Vestnik of Ryazan State Radio Engineering University], 2007, no. 20, pp. 117–120. (In Russ.).
7. Kalinin V.I., Radchenko D.E., Cherepenin V.A. [Numerical modelling of a noise information transmission system with spectrum expansion]. *Zhurnal radioehlektroniki* [Journal of radio electronics], 2014, no. 10. (18 p.). URL: http://jre.cplire.ru/jre/oct14/8/text.pdf (In Russ.).

8. Shibaev A.A. [About application of ultra-wideband radio line in the organisational structure of the robotic complex]. *Sbornik trudov Pervoi mezhdunarodnoi nauchnoi konferentsii "The 2017 Symposiumon Cybersecurity of the Digital Economy (CDE'17)"* [Proc. 1th Int. Conf. "The 2017 Symposiumon Cybersecurity of the Digital Economy (CDE'17)"]. Saint Petersburg, Afina Publ., 2017. pp. 392–394. (In Russ.).
9. Singh M., Leu P., Capkun S. UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks. *Network and Distributed Systems Security (NDSS) Symposium*, 2019. (16 p.). DOI: 10.14722/ndss.2019.23109
10. Senkov M.A., Kiselev K.V., Bykov A.A. [Development of a mathematical modelan indicator of the uniformity of the radio frequency spectrum of an ultra-wideband signal]. *Sovremennye naukoemkie tekhnologii* [Modern science-intensive technologies], 2020, no. 12-1, pp. 107–112. (In Russ.).
11. Gavrishev A.A. [Modeling and quantitative and qualitative analysis of common secure communication systems]. *Prikladnaya informatika* [Journal of applied informatics], 2018, vol. 13, no. 5 (77), pp. 84–122. (In Russ.).
12. Osipov D.L., Gavrishev A.A. [Analysis of the use of chaotic signals filtered with a bandpass filter for data transfer operation in radio communication systems]. *Nauchnoe Priborostroenie* [Scientific Instrumentation], 2021, vol. 31, no. 2, pp. 93–104. DOI: 10.18358/np-31-2-i93104 (In Russ.).
13. Vasyuta K.S. [Classification of processes in infocommunication radio-technical systems with application of BDS-statistics]. *Problemy telekommunikatsii* [The problems of telecommunications], 2012, no. 4 (9), pp. 63–71. (In Russ.).
14. Loginov S.S. *Tsifrovye radioehlektronnye ustroistva i sistemy s dinamicheskim khaosom i variatsiei shaga vremennoi setki*. Diss. dokt. techn. nauk [Digital radio electronic devices and systems with dynamic chaos and time grid step variation. Doct. techn. sci. diss.]. Kazan, 2015. 228 p. (In Russ.).
15. Gavrishev A.A., Gavrishev A.N. [To the question of calculating the peak factor values of signals generated by common hidden communication systems]. *Vestnik NTSBZHD* [Bulletin of the NCBWC], 2020, no. 3 (45), pp. 149–157. (In Russ.).
16. Kozel V.M., Podvornaya D.A., Kovalev K.A. Peal factor of signals of 5G mobile service systems. *Doklady BGUIR* [BSUIR reports], 2020, vol. 18, no. 6, pp. 5–10. DOI: 10.35596/1729-7648-2020-18-6-5-10 (In Russ.).
17. Dvornikov S.V., Markov E.V., Manoshi A.A. [Ncreasing immunity of decameter radio channel transmissions under unintended interference]. *T-Comm: Telekommunikatsii i transport* [T-COMM], 2021, vol. 15, no. 6, pp. 4–9. DOI: 10.36724/2072-8735-2021-15-6-4-9 (In Russ.).
18. Corral C.A., Emami Sh. Peak Power and Implementation Considerationsfor UWB. *IEEE802*, 2005. (4 p.). URL: https://www.ieee802.org/15/pub/05/15-05-0236-00-004a-peak-power-and-implementation-considerations-uwb.pdf
19. *Recommendation ITU-R SM.1755-0: Characteristics of ultra-wideband technology*. 2006. URL: https://www.itu.int/rec/R-REC-SM.1755/en
20. Immoreev I.Ya. [Ultra-wideband radars: New opportunities, unusual problems, system peculiarities]. *Vestnik MGTU. Seriya Priborostroenie* [Herald of the Bauman Moscow State Technical University. Series instrument engineering], 1998, no. 4, pp. 25–56. (In Russ.).
21. Dvornikov S.V., Pshenichnikov A.V., Dvornikov S.S., Borisov V.V., Potapov G.S. [Ultra-wideband ultra-short pulse communication system]. *Radiopromyshlennost'* [Radio industry], 2021, vol. 31, no. 1, pp. 16–27. URL: https://www.elibrary.ru/item.asp?id=45540851 (In Russ.).
22. Kunilov A.L., Ivoilova M.M. *Sposob priema sverkhkorotkoimpul'snogo signala v vide monotsikla Gaussa. Patent RF no. RU2737005C1* [Method of receiving ultrashort pulse signal in the form of Gauss monocycle]. Prioritet 24.11.2020. (In Russ.). URL: https://patents.google.com/patent/RU2737005C1/ru
23. Tsai Ch.-Y., Jeng Sh.-K. Design of a Legendre-polynominail-based orthogonal pulse generator for ultra-wideband communication. *IEEE Conference: Antennas and propagation Society International Symposium*, 2005, vol. 2B, pp. 680–683. DOI: 10.1109/APS.2005.1552105
24. M'foubat A.O., Elbahhar F., Tatkeu Ch. Novel ultra-wideband multi-user receiver for transportation systems communication. *IET Networks*, 2014, vol. 3, iss. 3, pp. 169–175. DOI: 10.1049/iet-net.2012.0081
25. Dmitriev A.S., Kletsov A.V., Laktyushkin A.M., Panas A.I., Starkov S.O. [Ultrawideband wireless communications based on dynamic chaos]. *Radiotehnika i elektronika* [Journal of Communications Technology and Electronics], 2006, vol. 51, no. 10, pp. 1193–1209. (In Russ.).
26. Kuzmin L.V., Efremova E.V., Itskov V.V. Modulation, Shaping and Replicability of UWB Chaotic Radiopulses for Wireless Sensor Applications. *Sensors*, 2023, vol. 23, iss. 15, Id. 6864. DOI: 10.3390/s23156864
27. Coppens D., Shahid A., Lemey S., Herbruggen B., Marshall Ch., Poorter E. An Overview of UWB Standards and Organizations (IEEE 802.15.4, FiRa, Apple): Interoperability Aspects and Future Research Directions. *IEEE Access*, 2022. URL: https://arxiv.org/pdf/2202.02190.pdf
28. Nosov V.I., Kalinin V.O. *Issledovanie metodov povysheniya pomekhoustoichivosti korotkoimpul'snykh sverkhshirokopolosnykh sistem radiosvyazi* [Investigation of methods to improve noise immunity of short-pulse ultra-wideband radio communication systems]. Novosibirsk, STUTIS, 2017. 244 p. (In Russ.).
29. Belichenko V.P., Buyanov YU.I., Koshelev V.I. *Sverkhshirokopolosnye impul'snye radiosistemy* [Ultra-wideband pulse radio systems]. Novosibirsk, Nauka Publ., 2015. 473 p. (In Russ.).
30. Muhr E., Vauche R., Bourdel S., Gaubert J. et al. High Output Dynamic UWB Pulse Generator for BPSK Modulations. *IEEE International Conference on Ultra Wideband (IC UWB)*, Sydney, Australia, 2013, pp.170–174. DOI: 10.1109/ICUWB.2013.6663842

Contacts: *Gavrishev Aleksej Andreevich,*
alexxx.2008@inbox.ru

Article received by the editorial office on 21.02.2024

INTRODUCTION

Radio communication systems based on ultra-wideband signals (UWB) are a promising direction for the development of wireless data transmission over short distances. Their advantages include low energy consumption, relative simplicity of equipment construction, and high efficiency of spectrum use. UWB radio communication systems are of great interest to developers and manufacturers of telecommunications equipment since they allow operation on a license-free basis, and the features of the transmitted signals imply the absence of powerful amplifiers and complex signal processing components as part of transceiver complexes. Compared to narrowband systems, UWB systems more successfully solve the problems of increasing the speed and secrecy of data transmission. The implementation of these advantages implies the development of special methods for generating, processing, transmitting, and receiving signals [1, 2].

Insufficient attention has been paid to the issue of assessing the secrecy of UWB radio communication systems. It is known [3–10] that the secrecy of radio signals makes it possible to resist their detection and measurement of their parameters, thus providing protection against unauthorized access. Thus, in work [3] it is indicated that narrowband, broadband, and UWB signals have different spectrum widths, which affects the likelihood of their detection using radio reconnaissance means — the greater the spectrum width of the transmitted signal, the more difficult it is to detect it, and, accordingly, its secrecy is higher. The studies conducted show that UWB sequences have the greatest secrecy in terms of energy indicators compared to narrow-band and wide-band signals. In works [4–6], studies of UWB were carried out according to criteria characterizing their energy characteristics, secrecy of information transmission, and some others. It is shown that it is possible to optimize a certain type of signal sequence, which makes it possible to improve the quality indicators noted above.

In [7], a numerical simulation of a UWB radio communication system with spread spectrum was carried out. The spectral and correlation characteristics of the UWB transmissions in the communication channel have been studied. The results obtained show that the signals transmitted in the communication channel in terms of energy indicators have a form similar to fluctuation noise, which indicates a low probability of their interception. Work [8] discusses the use of UWB signals for remote control of robotic complexes. The results of an experiment to assess the secrecy of transmitted UWB signals on the air, carried out using a spectrum analyzer, are presented. It has been shown that when the spectrum analyzer is removed at a distance of more than 3 m from the transceiver antenna, transmitted UWB signals are not detected. Work [9] states that attacks on standardized UWB radio communication systems at the physical level can allow attackers to falsify transmitted data. Such attacks can allow attackers to perform various illegal actions with devices that use standardized UWB radio communication systems. An approach has been proposed to increase the structural secrecy of transmitted UWB signals. It is noted that even the interception of the transmitted UWB signals by intruders will not reveal the structure of the transmitted signals due to the use of the proposed approach. Work [10] presents one of the approaches to assessing the secrecy of transmitted UWB signals based on the spectrum uniformity index. It is noted that UWB signals that are perfect in terms of stealth indicators must have a uniform spectrum, close in shape to a rectangle.

As can be seen from the data presented, in the known literature on UWB radio communication systems, methods based on energy indicators are most often used to assess their secrecy. These methods, although they are the most frequently used to assess the secrecy of various types of radio signals, have a number of disadvantages. Thus, it is known [11–13] that energy indicators can underestimate the secrecy of radio signals. Based on this, it is relevant to assess the secrecy of the UWB signals using alternative methods for assessing secrecy, for example methods based on nonlinear dynamics, etc. [11–13].

The published works do not pay enough attention to some issues of assessing the reliability of UWB radio communication systems, in particular, assessing the peak factor of transmitted UWB as one of the reliability indicators. It is known [14–17] that an increased peak factor negatively affects the noise immunity and energy efficiency of a radio transmitting device. Thus, publications [1, 2, 18] state that regulatory requirements in various countries impose restrictions on the use of UWB radio communication systems. It is noted that the UWB peak factor plays an important role in such radio communication systems and can have a significant impact on the energy efficiency of the radio transmitting device. It is stated in [19] that UWB signals used in various practical applications, for example, radar, can have a large peak factor and impose some restrictions on the operation of such devices. Based on this, developers and manufacturers of such radio communication systems need to pay closer attention to the characteristics of the used UWB signals, including the shape of the UWB and their peak factor.

Thus, it can be argued that the study of the UWB peak factor as one of the indicators of the reliability of UWB radio communication systems is relevant and requires further study.

The purpose of the article is to evaluate the properties of UWB sequences to ensure secretive and relia-

ble data transmission in radio communication systems using BDS statistics indicators and the peak factor.

MAIN PART

Research part

It is known [20] that the shape of UWB signals has a significant impact on the characteristics of the radio communication systems in which they are used. Modern studies devoted to the formation of UWB signals, in most cases, use Gaussian monopulses and their derivatives as base ones [1, 2, 21, 22]. In addition, Rayleigh pulses and impulses based on Laguerre functions [1, 2], impulses based on Legendre polynomials [23, 24] and some others are also actively used. Also, a number of works propose a large number of new classes of UWB signals, for example, pulses based on solving the Euler – Lagrange equation [4–6], based on chaotic signals [25, 26], pulses described by the IEEE 802.15.4 standard [27], and many others.

To conduct research, the authors selected the following types of UWB signals, given in Tab. 1.

Tab. 1. Selected types of UWB signals

To transmit information, it is necessary to operate with a data stream presented in the form of a sequence of UWB pulses [28–30]. The UWB sequence is usually understood as a set of pulses (see Tab. 1) located over a certain finite time interval, considered a composite signal.

In the general case, the simplest form of the transmitted UWB sequence can be written as follows [28–30]:

$$S_n(t,t_0,T)=\sum_{k=0}^{N-1}s\left[t-t_0-(k-\mu)T\right], \qquad (1)$$

where t_0 is the arrival time of the sequence; T is the repetition period of the UWB signals; k is the serial number of the UWB signals, starting from 0; N is the total number of pulses in the sequence; μ is a parameter that determines the point of the sequence with which its arrival time is associated; $s(t)$ describes the time shape of a single signal.

Currently, the following types of modulation are among the most frequently used in UWB radio communication systems [28–30]: pulse amplitude modulation (PAM modulation), pulse position modulation (PPM modulation), and binary phase modulation (BPSK modulation). Each of them has its own advantages and disadvantages. The authors chose BPSK modulation as the base one.

With BPSK modulation, two types of pulses are used for transmission [28–30]: direct and inverse, i.e., phase shifted relative to the direct pulse by 180°. These two pulses are used to transmit logical zero and one. The BPSK modulation method has very good noise immunity characteristics. An illustration of the principle of the BPSK modulation method applied to UWB radio communication systems is shown in Fig.

Fig. BPSK modulation method for UWB radio communication systems [28].
а — unmodulated sequence, б — modulated sequence

Taking into account expression (1) and recommendations from works [11, 12, 28–30], the authors carried out modeling of UWB signals transmitted in the communication channel, formed on the basis of BPSK modulation. The pulses presented in Tab. 1 were used as UWB sequences. For each of the indicated types of pulses, 50 UWB sequences were generated, in which the initial transmitted data (logical zero and one) were specified using a binary pseudo-random sequence generator and modulated by the pulses presented in Tab. 1.

Let us carry out a quantitative assessment of the secrecy and reliability of the obtained UWB sequences using BDS statistics and the peak factor. Let us assume that the studied UWB sequences are transmitted through an ideal communication channel.

To carry out a quantitative assessment of secrecy, let us turn to BDS statistics. It is known [11–13] that BDS statistics are based on the statistical properties of the correlation dimension of the process under study in phase space. The correlation dimension is determined by the correlation integral. In some cases, these data provide more information about the class of the process (random, chaotic, or regular) than energy indicators. In accordance with [11–13], BDS statistics can, in some cases, act as a measure of the energy secrecy of transmitted signals. BDS statistics are based on the statistical value $w(\varepsilon)$ described by the following expression:

$$w_{m,N}(\varepsilon)=\sqrt{N-m+1}\,\frac{C_{m,N}(\varepsilon)-C_{1,N-m}(\varepsilon)^m}{\sigma_{m,N}(\varepsilon)}, \qquad (2)$$

where $C_{m,N}(\varepsilon)$ and $C_{1,N-m}(\varepsilon)$ are correlation integrals, and $\sigma_{m,N}(\varepsilon)$ is the standard deviation.

Tab. 2 shows the averaged values of the BDS statistics described by expression (2) and obtained for the studied UWB sequences.

Tab. 2. Average values of BDS statistics $\overline{w(\varepsilon)}$ for the studied UWB sequences

As can be seen from Tab. 2, the studied UWB sequences have BDS statistics values $\overline{w(\varepsilon)} \in [28,300]$. Among them, the UWB sequences that use pulses based on the solution of the Euler – Lagrange equation ($\overline{w(\varepsilon)} \in [28,65]$) have the lowest values of BDS statistics. UWB sequences constructed on the basis of widely used pulses, for example, Gaussian monocycles, have BDS statistics values $\overline{w(\varepsilon)} \in [98,110]$, close to chaotic signals [11–13]. The UWB sequences described in the IEEE 802.15.4 standard have an intermediate value between the studied UWB sequences in terms of the stealth indicator ($\overline{w(\varepsilon)} \in [68,80]$), approaching the autoregressive process and relative methods [11–13] in terms of BDS statistics. The results obtained show that UWB sequences in general have a complex structure, but they can be detected using BDS statistics. This result coincides with well-known studies [4, 9, 10].

Let us carry out a quantitative assessment of the studied UWB sequences using one of the indicators of the reliability of data transmission in radio communication systems.

As such an indicator, let us turn to the signal peak factor [14–17], calculated using the following expression:

$$P = \frac{U_{\max}}{\sigma}, \qquad (3)$$

where $U_{\max}$ is the maximum signal value, σ is the root mean square value of the signal.

Tab. 3 shows the values of the peak factor P, described by expression (3) and obtained for the studied UWB sequences.

Tab. 3. Peak factor P values of the studied UWB sequences

As can be seen from Tab. 3, the studied UWB sequences have a peak factor value. According to well-known studies [14–17], for modern communication systems, the peak factor value of transmitted signals, calculated using expression (3), should be approximately in the range We can conclude that the studied UWB sequences are generally suitable for data transmission in radio communication systems because they have an acceptable peak factor.

Comparative analysis of the data obtained

Tab. 4 shows generalized conclusions on the conducted research. A comparative analysis of the obtained data (Tab. 4) shows that for the selected research conditions, the UWB sequences [4–6] based on the solution of the Euler–Lagrange equation are generally suitable.

Tab. 4. Generalized conclusions from the studies conducted

The indicated UWB sequences have a BDS statistics value that is closest to the value $w(\overline{\varepsilon}) \le |1.96|$, defining white noise [11–13] and an acceptable peak factor. Therefore, it is advisable to use UWB sequences of the specified type in UWB radio communication systems to increase the secrecy and reliability of data transmission. UWB sequences, built on the basis of widely used pulses, for example, Gaussian monocycles [1, 2, 21, 22], do not fully ensure the secrecy of data transmission in radio communication systems, so they are inappropriate to use in UWB radio communication systems with high requirements. - measures to ensure the secrecy of data transmission. The specified result matches well-known studies [4, 9–13].

The UWB sequences described in the IEEE 802.15.4 standard, although they have a level of secrecy higher than the widely used UWB sequences but less than the UWB sequences based on solving the Euler-Lagrange equation. In addition, standardized radio communication systems are most often the targets of attacks by intruders due to the detailed description of all their characteristics [4, 9–13]. Based on this, it is also inappropriate to use them in UWB radio communication systems with high requirements for ensuring the secrecy of data transmission.

CONCLUSION

Thus, this work analyzes the use of UWB sequences generated on the basis of BPSK modulation to ensure the secrecy and reliability of data transmission in radio communication systems. Their properties were assessed using BDS statistics and peak factor indicators. As a result of the conducted research, it was established that for the selected research conditions, the UWB sequences are generally suitable [4–6], based on the solution of the Euler–Lagrange equation, characterized by greater secrecy from an outside observer than other studied UWB sequences because their BDS statistics value is closer to white noise [11–13]. It is also shown that all the studied UWB sequences have an acceptable peak factor value. It is noted that UWB sequences built on the basis of widely used pulses, for example, Gaussian monocycles [1, 2, 21, 22], as well as standardized radio communication systems [27], do not fully ensure the secrecy of

data transmission in radio communication systems, therefore, it is inappropriate to use them in UWB radio communication systems with high requirements for ensuring the secrecy of data transmission. This result coincides with well-known studies [4, 9–13].

The conducted research made it possible to supplement knowledge about UWB sequences to ensure secretive and reliable data transmission in radio communication systems. The authors associate further research in this area with the study of UWB radio communication systems and other common types of modulation. The direction of research in the field of ensuring secrecy and reliability of UWB radio communication systems based on chaotic signals is also promising.