УДК 621.396

Д. В. Орёл, А. П. Жук

ФГАОУ ВПО «Северо-Кавказский федеральный университет»

Метод повышения помехозащищённости навигационного сигнала спутниковой радионавигационной системы

В статье представлен метод повышения помехозащищённости навигационного сигнала спутниковой радионавигационной системы на основе повышения его структурной скрытности, за счёт стохастического использования увеличенного количества систем квазиортогональных кодовых последовательностей, получаемых путем функциональных преобразований псевдослучайных аргументов.

Ключевые слова: помехозащищённость, структурная скрытность, спутниковая радионавигация, система кодовых последовательностей.

Активное развитие рынка и существенное расширение сфер использования навигационно-временного обеспечения (НВО) на основе глобальных навигационных спутниковых систем (ГНСС) ведут к росту зависимости различных систем от НВО, получаемого на основе ГНСС. К таким системам относятся в том числе и критически важные для функционирования государств и регионов: крупные транспортные узлы, энергетические системы, магистральные телекоммуникационные системы, международные биржи и другие объекты [1]. Согласно докладу Британской королевской инженерной академии, 6% валового внутреннего продукта Европейского Союза (800 миллиардов евро в год) в 2011 году уже зависело от НВО ГНСС [2].

Дестабилизация работы ГНСС может привести к нарушению функционирования других, зависящих от них, жизненно важных систем: возможны аварии и крушения судов, нарушения работы аэропортов, морских и речных портов, финансовых, телекоммуникационных и энергетических систем [1]. Таким образом, в результате нарушения работы ГНСС могут быть реализованы угрозы как локального, так и регионального и государственного масштаба. С целью реализации обозначенных угроз растёт интерес различных лиц, компаний и служб к технологиям организации умышленных злонамеренных воздействий на интерфейс потребителей ГНСС. При этом преследуется широкий спектр целей: недобросовестная конкуренция, терроризм, диверсии и др.

Интерфейс потребителей ГНСС включает в себя аппаратуру формирования и излучения НС в околоземное пространство, совокупность излучаемых НС и навигационную аппаратуру потребителей, способную принимать НС. Среди видов возможных злонамеренных воздействий на интерфейс потребителей ГНСС особо можно выделить следующие:

- подавление навигационного сигнала (НС) с помощью организации имитирующих радиопомех (jamming);
- навязывание навигационной аппаратуре потребителя (НАП) ложного НС (spoofing).

Подавление применяется для блокирования НС, в результате которого НАП утрачивает возможность определять координаты и осуществлять синхронизацию с временной шкалой ГНСС. Целью подмены НС является нарушение работы ГНСС таким образом, что координаты объекта определяются не верно.

Целью статьи является разработка метода повышения помехозащищённости НС ГНСС для повышения вероятности решения навигационной задачи НАП в условиях злонамеренных воздействий на НС.

Рассмотрим более подробно каждый тип злонамеренного воздействия на интерфейс потребителей ГНСС.

Для радиоэлектронного подавления (РЭП) НАП ГНСС пригодны активные маскирующие организованные помехи. В качестве критерия эффективности помех при РЭП НС ГНСС целесообразно использовать коэффициент подавления [3]:

$$\eta_p = P_{SB}/P_{\text{РД}}; \quad P_{SB} = 2,5 \cdot 10^{-16},$$

где P_{SB} — максимальный ожидаемый уровень сигнала на входе НАП; $P_{\text{РД}}$ — уровень помехи $P(t)$ на входе НАП, достаточный для нарушения функционирования каналов первичной обработки НАП.

Для РЭП НАП СРНС из маскирующих помех наиболее пригодны прицельные и заградительные непрерывные шумовые помехи, которые реализуются на основе квазибелого шума (ШП) и гармонических процессов (ГП) [3]. Для организации эффективных шумовых помех требуется разведка несущей частоты НС и его фазы.

Имитирующие помехи относятся к классу «интеллектуальных» помех [3]. Имитирующие помехи разделяются на прицельные, следящие и заградительные (ЗСП). К недостаткам следящей и прицельной имитирующих помех следует отнести сложность получения необходимых для их формирования целеуказаний. Более простой в реализации является заградительная имитирующая помеха (ЗИП), поскольку она не требует формирования точных временных целеуказаний.

В табл. 1 представлены показатели воздействия рассмотренных типов помех на каналы первичной обработки информации НАП для случая, когда расстояние между НАП и станцией РЭП не превышает 100 км.

Таблица 1

Показатели воздействия различных типов помех на НАП ГНСС

Канал НАП	Тип помехи	Вероятность РЭП	Энергетический потенциал, PnGn (дБВт)	Коэффициент подавления, η_p
Канал обнаружения	ШП	$P_{\text{ПД1}} = 0,5$	28,5	$1,5 \cdot 10^{-3}$
	ГП	$P_{\text{ПД1}} = 0,5$	28,5	$1,5 \cdot 10^{-3}$
	ЗСП	$P_{\text{ПД1}} = 0,67$	10,5	$5 \cdot 10^{-2}$
			16,4	10^{-1}
Канал слежения за частотой	ШП	$P_{\text{ПД2}} = 0,32$	39,5	$2,5 \cdot 10^{-3}$
	ГП	$P_{\text{ПД2}} = 0,32$	44,4	$4,17 \cdot 10^{-3}$
Канал слежения за задержкой	ШП	$P_{\text{ПД3}} = 0,5$	30,4	$[4,3 \cdot 10^{-6}; 10^{-3}]$
	ГП	$P_{\text{ПД3}} = 0,5$	74	$[4,3 \cdot 10^{-10}; 10^{-7}]$
	ЗСП	$P_{\text{ПД3}} = 0,67$	10,5	$5 \cdot 10^{-3}$
			16,4	10^{-1}
Канал демодуляции	ШП	$P_{\text{ПД4}} = 0,1$	38,7	$8,3 \cdot 10^{-4}$
	ГП	$P_{\text{ПД4}} = 0,1$	38,7	$2,5 \cdot 10^{-5}$

Анализ табл. 1 показывает, что использование имитирующих помех наиболее эффективно, поскольку для их организации требуется энергетический ресурс станции РЭП, не превышающий 20 дБВт. Кроме того, они инвариантны к использованию комбинированных навигационных систем, в то время как эффективность шумовых помех против таких систем снижается [3].

Поэтому для повышения вероятности успешного решения навигационной задачи с использованием ГНСС следует, прежде всего, обеспечить противодействие организации имитирующих помех.

Рассмотрим второй тип злонамеренного воздействия на интерфейс потребителей ГНСС — навязывание ложного НС. На рынке имеются устройства, позволяющие имитировать

сигналы ГНСС. К ним относятся как станции тестирования НАП, так и специальные приборы - псевдоспутники, помогающие улучшить геометрию созвездия навигационных космических аппаратов (НКА) в условиях ограниченного приёма. Подобные приборы способны воспроизводить точные копии НС, транслируемых НКА, имитировать воздействие помех и различные виды задержек НС.

Основным содержанием решения навигационной задачи на основе ГНСС является определение пространственных координат потребителя, составляющих вектора его скорости, а также текущего времени. Поэтому в процессе решения навигационной задачи должен быть определён расширенный вектор состояний потребителя П, который в инерциальной геоцентрической системе координат $OX_0Y_0Z_0$ можно представить в виде

$$\text{П} = \begin{bmatrix} x & y & z & t & V_x & V_y & V_z \end{bmatrix},$$

где x, y, z — координаты потребителя, V_x, V_y, V_z — составляющие вектора скорости потребителя, t — текущее время.

Составляющие вектора П недоступны для непосредственного измерения с помощью радиосредств. У принятого радиосигнала могут измеряться некоторые его параметры, например задержка τ или доплеровское смещение частоты $f_{\text{д}}$, называемые радионавигационными параметрами. На основе этих параметров могут быть вычислены такие связанные с ними навигационные параметры, как дальность от НКА до потребителя:

$$\text{Д} = c\tau$$

и радиальная скорость движения потребителя:

$$V_p = f_{\text{д}}\lambda,$$

где c — скорость света, λ — длина волны излучаемого НС.

Для манипулирования этими данными необходимо воспроизвести копию НС каждого видимого НКА и совершить манипуляцию навигационными параметрами НС для неверного определения местоположения и формирования ложного курса следования подвижного объекта.

Оба рассматриваемых вида злонамеренных воздействий основываются на использовании процессов, имитирующих НС. Отличие заключается лишь в том, что при подмене НС необходимо воспроизвести не только структуру дальномерного кода, но также и структуру навигационного сообщения. В связи с этим актуальной является задача повышения защищённости интерфейса потребителей ГНСС от рассмотренных типов злонамеренных воздействий.

Возможным направлением противодействия рассмотренным типам злонамеренного воздействия на интерфейс потребителей ГНСС является повышение помехозащищённости НС ГНСС. Поскольку ключевым этапом для организации обоих типов злонамеренных воздействий является радиоразведка, соответственно наиболее важной составляющей повышения помехозащищённости НС является повышение скрытности – способности ГНСС противостоять мерам радиоразведки (мониторинга). В соответствии с этапами радиоразведки выделяют следующие виды скрытности.

1) Энергетическая: противодействие выявлению сигнала на фоне шума.

2) Структурная: противодействие определению структуры сигналов.

3) Информационная: противодействие раскрытию передаваемой информации.

ГНСС функционируют непрерывно, параметры открытых НС общеизвестны и статичны. Для успешности навигации необходимо принимать НС не менее 4 спутников, расположенных на разных градусах возвышения над горизонтом, что ограничивает использование

направленных антенн. В портативной НАП использование направленных антенн невозможно в силу необходимости обеспечения их работоспособности при любой ориентации НАП в пространстве.

НС с кодовым разделением каналов (КРК), используемые во всех существующих ГНСС, обладают достаточно высокой энергетической скрытностью. Несущая частота и ширина спектра НС регламентированы международными договорённостями и произвольное манипулирование данными параметрами недопустимо.

Информационная скрытность реализуется криптографическими методами. Их использование позволит защититься от имитации НС, но окажется неэффективным против подавления НС.

Структурную скрытность открытых НС на сегодняшний день можно считать неудовлетворительной. Для КРК используется одна система квазиортогональных кодовых последовательностей. Все параметры открытых НС описаны в интерфейсных контрольных документах, что позволяет осуществлять генерацию ЗИП для подавления НС. Таким образом, можно сделать вывод, что для повышения помехозащищённости ГНСС необходимо повышение структурной скрытности НС. Наиболее перспективным в этом плане представляется метод повышения структурной скрытности путём стохастической смены манипулирующих функций, используемых для КРК.

Количество используемых при этом структур систем квазиортогональных кодовых последовательностей должно быть настолько большим, чтобы их использование без повторения могло осуществляться в течение длительного времени, а система радиоразведки не могла хранить весь набор используемых систем последовательностей в своей памяти. Необходимое количество систем кодовых последовательностей для обеспечения структурной скрытности НС в течение 15 лет составляет $A_{rs} = 4{,}7304 \cdot 10^{11}$. При этом каждая система содержит 50 квазиортогональных кодовых последовательностей.

Сами используемые кодовые последовательности должны иметь высокую сложность разгадывания и обладать корреляционными и статистическими свойствами, удовлетворяющими требованиям их применимости для НС. Под высокой сложностью разгадывания подразумевается стойкость алгоритма формирования кодовых последовательностей к возможности предсказания её структуры. Так, кодовые последовательности, формируемые на основе регистров сдвига с линейными обратными связями, содержащих n разрядов, обладают низкой сложностью разгадывания, поскольку достаточно принять $2n$ последовательно идущих элементов, чтобы на основе алгоритма Берлекемпа–Месси восстановить структуру регистра сдвига с линейными обратными связями [4]. Под хорошими статистическими свойствами понимается сбалансированность кода, соответствие числа серий элементов закону k-распределённости и близость боковых пиков корреляционных функций к границе Велча.

По виду алгоритма формирования системы квазиортогональных кодовых последовательностей делятся на два класса: линейные и нелинейные. Линейные алгоритмы позволяют получать большие системы последовательностей с оптимальными статистическими и корреляционными свойствами, но при этом последовательности имеют низкую сложность разгадывания. Кроме того, на основе известных алгоритмов возможно получить лишь $4{,}17 \cdot 10^8$ систем квазиортогональных кодовых последовательностей объёмом по 50 последовательностей. Недостаточное количество и низкая сложность разгадывания обуславливают невозможность использования линейных алгоритмов формирования систем квазиортогональных кодовых последовательностей для повышения помехозащищённости НС.

Нелинейные алгоритмы формирования систем квазиортогональных кодовых последовательностей позволяют получать последовательности с высокой сложностью разгадывания структуры. Однако с ростом количества получаемых систем последовательностей их корреляционные и статистические свойства существенно ухудшаются, в результате чего они не отвечают условиям применимости в НС ГНСС.

Таким образом, известные алгоритмы формирования систем квазиортогональных кодовых последовательностей не позволяют получить необходимое количество систем последовательностей с требуемыми свойствами. В связи с этим возникает задача разработки метода формирования систем квазиортогональных кодовых последовательностей, позволяющего получить их требуемое количество и обладающих необходимыми свойствами.

Для решения этой задачи был разработан метод получения увеличенного количества систем квазиортогональных кодовых последовательностей на основе функциональных преобразований псевдослучайных аргументов. В основе разработанного метода лежит положение о том, что, зная закон распределения аргументов, представляющих собой случайные величины, часто можно установить закон распределения случайных величин, представляющих собой значений функции от аргументов [5]. В случае, если известны характеристики исходной случайной величины (аргумента), такие как математическое ожидание, дисперсия, плотность вероятности, также возможным становится определение аналогичных характеристик и для итоговой случайной величины (результата функционального преобразования).

На основе вышеописанных положений реализуется метод обратного преобразования, так называемое преобразование Н.В. Смирнова [6] — метод генерации псевдослучайных величин с заданной функцией распределения, путём модификации работы генератора равномерно распределённых псевдослучайных чисел.

Пусть $G(x)$ является функцией произвольного распределения. Если функция $G : \boldsymbol{R} \to [0,1]$ строго монотонна на всей своей области определения, то она биективна, а следовательно, имеет обратную функцию G^{-1}: $[0,1] \to \boldsymbol{R}$. Иначе говоря, для генерации псевдослучайной величины с функцией распределения G необходимо построить детерминированную функцию $\tau = G^{-1}(x)$ и получить искомые случайные числа как значения этой функции от аргумента, являющегося случайной псевдовеличиной с равномерным законом распределения на интервале $[0,1]$. Если $x_1, \ldots, x_n \sim X[0,1]$ — выборка из стандартного непрерывного равномерного распределения, тогда $\tau_1, \ldots, \tau_n$ — выборка из интересующего нас распределения, где $\tau_i = G^{-1}(x_i)$, $i = 1, \ldots, n$.

Особенностью разработанного метода получения увеличенного количества систем квазиортогональных кодовых последовательностей является использование полученных в результате функционального преобразования псевдослучайных чисел в качестве параметра, определяющего длину серий последовательно идущих элементов одного знака в двоичной кодовой последовательности. Реализация рассматриваемого метода на практике включает в себя следующие основные этапы.

1) Формирование исходного ряда равномерно распределённых псевдослучайных чисел rnd.

2) Функциональное преобразование псевдослучайных чисел с помощью выбранной функции:
$$\tau_i = G^{-1}(rnd_i).$$

3) Дискретизация полученных значений функции τ_i с выбранным шагом d:
$$t_i =]\tau_i/d[\,.$$

4) Получение двоичной последовательности, в которой t_i определяет длину серии последовательно идущих элементов одного знака:
$$n_{t_{i-1}+1} \ldots n_{t_{i-1}+t_i} = (-1)^i \cdot (a_{t_{i-1}+1} \ldots a_{t_{i-1}+t_i}),$$
где $a_1 \ldots a_N$ — последовательность единичных элементов.

Как было отмечено в [7], кодовые последовательности обладают оптимальными корреляционными характеристиками в том случае, когда серии элементов в них подчиняются закону k-распределённости ($G = 1/2^k$). Такое распределение серий элементов достигается в полной мере при использовании в предлагаемом методе функции вида

$$G^{-1} = \log_2 \frac{1}{rnd}.$$

При достаточно большом периоде генератора псевдослучайных чисел (ГПСЧ) можно получить большое число неповторяющихся кодовых последовательностей: при длине периода ГПСЧ, равного l, количество кодовых последовательностей, которое теоретически может быть получено при использовании единственного функционального преобразования, составит $Q \approx 2l/N$, где N — длина кодовых последовательностей в битах. Поскольку расчётное время эксплуатация НКА не превышает 15 лет, достаточно обеспечить защищённость НС на указанный период. Необходимое количество кодовых последовательностей для обеспечения защищённости НС в течение 15 лет составляет $A = 2{,}3652 \cdot 10^{12}$. При этом должно выполняться следующее неравенство: $Q \geqslant A$. Тогда при длине последовательностей $N = 10\,230$ бит $l \geqslant 1{,}2098 \cdot 10^{16}$. ГПСЧ «Вихрь Мерсенна» имеет период $l = (2^{19937} - 1)/32 \approx 1,3486 \cdot 10^{6000}$, который многократно превосходит значение A и удовлетворяет приведённому неравенству. Поскольку вышесказанное доказывает, что при использовании ГПСЧ «Вихрь Мерсенна» возможно с помощью лишь одной функции получить необходимое количество последовательностей для повышения структурной скрытности НС в течение 15 лет, то целесообразно использовать единственную функцию:

$$\tau = \log_2 \frac{1}{rnd}.$$

При этом выбор начального бита ГПСЧ в качестве секрета позволит обеспечить высокую структурную скрытность кодовых последовательностей.

Проведённый вычислительный эксперимент по моделированию систем квазиортогональных кодовых последовательностей на основе разработанного метода позволяет получать системы кодовых последовательностей, удовлетворяющих корреляционным и статистическим требованиям и имеющих высокую сложность разгадывания структуры [8]. При этом выше обосновано, что возможно получить их количество, необходимое для повышения структурной скрытности НС в течение 15 лет.

Таким образом, повысить помехозащищённость интерфейса потребителей ГНСС предлагается путём повышения структурной скрытности НС ГНСС, которую в свою очередь предлагается осуществить за счёт стохастического использования увеличенного количества систем квазиортогональных кодовых последовательностей на основе метода функциональных преобразований псевдослучайных аргументов.

Настоящая работа имеет потенциальную практическую значимость, поскольку в настоящее время ведутся работы по проектированию перспективных специальных НС для НКА Глонасс-КМ отечественной ГНСС ГЛОНАСС. Предложенный в рамках настоящей работы метод повышения помехозащищённости интерфейса потребителей ГНСС может быть использован для перспективных НС ГНСС ГЛОНАСС. Его использование повысит вероятность успешного решения навигационной задачи в условиях злонамеренного воздействия на НС.

Литература

1. *Орёл Д.В.* Анализ угроз функционирования аппаратуры гражданских потребителей глобальных спутниковых радионавигационных систем // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. — Ростов-на-Дону : ПЦ «Университет» СКФ МТУСИ, 2011. — С. 44–48.

2. Global Navigation Space Systems: reliance and vulnerabilities // Report of The Royal Academy of Engineering. – London : March, 2011. — 48 p.

3. *Дятлов А.П., Дятлов П.А., Кульбикаян Б.Х.* Радиоэлектронная борьба со спутниковыми радионавигационными системами. — М. : Радио и связь, 2004. — 226 с.

4. Общесистемные вопросы защиты информации: монография / под. ред. Е.М. Сухарева. — Кн. 1. — М. : Радиотехника, 2003. — 296 с.

5. *Вентцель Е.С.* Теория вероятностей. — Издание четвёртое, стереотипное. — М. : Наука, 1969. — 576 с.

6. *Вадзинский Р.Н.* Справочник по вероятностным распределениям. — СПб. : Наука, 2001. — 295 с.; ил. 116.

7. *Ипатов В.П.* Периодические дискретные сигналы с оптимальными корреляционными свойствами. — М. : Радио и связь, 1992. — 152 с.

8. *Жук А.П., Орёл Д.В.* Моделирование кодовых последовательностей для сигналов глобальных спутниковых радионавигационных систем с кодовым разделением каналов // Материалы XVI Международной научно-технической конференции «Радиолокация. Навигация. Связь». — Воронеж : НПФ «Саквоее», 2010. — С. 2111–2119.

Поступила в редакцию 16.04.2013.