# ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ И БЕЗОПАСНОСТЬ ОБОРУДОВАНИЯ

УДК 623.624

## ОБ ОЦЕНКЕ ПОМЕХОЗАЩИЩЕННОСТИ СПУТНИКОВЫХ РАДИОНАВИГАЦИОННЫХ СИСТЕМ

*Жук А.П., Орел Д.В.*

В работе предложен вариант оценки помехозащищенности спутниковых радионавигационных систем с повышенной структурной скрытностью навигационных сигналов с помощью выражения, учитывающего снижение априорной неопределенности параметров навигационных сигналов в процессе функционирования системы радиоэлектронного противодействия.

***Ключевые слова:*** помехозащищенность, спутниковая радионавигация, структурная скрытность, имитирующая помеха, радиоэлектронное противодействие.

Рост зависимости различных технических, телекоммуникационных, транспортных и других систем от координатно-временного обеспечения навигации на основе спутниковых радионавигационных систем (СРНС) приводит к повышению их уязвимости в случае технического сбоя, который может произойти в результате преднамеренного воздействия на радиоканал «навигационный космический аппарат – аппаратура потребителей» [1]. Среди всех видов радиоэлектронного подавления аппаратуры потребителей (АП) СРНС можно выделить подавление навигационных сигналов (НС) с помощью организации радиопомех (jamming). В связи с этим возникает потребность количественной оценки помехозащищенности СРНС в условиях воздействия на нее организованных радиопомех.

В ряде работ представлены соотношения для оценки помехозащищенности СРНС [2; 4]. Однако они не позволяют оценить помехозащищенность СРНС в случае стохастического применения НС. Целью данной статьи является разработка варианта оценки помехозащищенности СРНС с повышенной структурной скрытностью НС и уточнение выражения для оценки вероятности разведки параметров НС.

Используя общее понятие помехозащищенности радиотехнической системы применительно к интерфейсу пользователей СРНС [3], ее можно охарактеризовать следующим показателем вероятности успешного решения навигационной задачи в условиях радиоэлектронного подавления (РЭП):

$$P_{\text{ПЗ}} = P_{\text{РНЗ0}} + P_{ПД}\left(P_{РНЗ1} - P_{РНЗ0}\right), \qquad (1)$$

где $P_{ПД}$ – вероятность подавления СРНС, характеризует скрытность системы; $P_{\text{РНЗ0}}$ – вероятность успешного выполнения своей задачи СРНС при отсутствии РЭП; $P_{РЭП1}$ – вероятность успешного выполнения задачи СРНС в условиях РЭП.

Рассмотрим составляющие, используемые при определении вероятности успешного решения навигационной задачи СРНС. Эффективность функционирования СРНС, характеризуемая вероятностью успешного решения навигационной задачи в условиях отсутствия РЭП $P_{\text{РНЗ0}}$, определяется в основном вероятностью успешного выполнения первичной обработки информации, в ходе которой применяются статистические алгоритмы, обеспечивающие выделение НС на фоне помех и оценивание их информационных параметров [3].

Первичная обработка информации в АП реализуется решением следующих задач [2]:

- двумерный поиск НС по задержке и частоте, обнаружение и подтверждение наличия сигнала (характеризуется вероятностью ошибочных решений при поиске и обнаружении $P_{\text{ПО}}$);
- слежение за доплеровским сдвигом сигнала и его оценивание (характеризуется вероятностью срыва слежения за частотой в системе фазовой автоподстройки частоты $P_{cf}$ канала слежения за частотой АП);
- слежение за задержкой огибающей сигнала и его оценивание (характеризуется вероятностью срыва слежения за задержкой $P_{c\tau}$);
- демодуляция сигнала (характеризуется вероятностью ошибочных решений на бит информации $P_{\text{ОБ}}$).

Отсюда вероятность успешного выполнения задачи СРНС [4]:

$$P_{\text{РНЗi}} = \left(1 - P_{\text{ПО}}\right)\cdot\left(1 - P_{cf}\right)\cdot\left(1 - P_{c\tau}\right)\cdot\left(1 - P_{\text{ОБ}}\right). \qquad (2)$$

В соответствии с [4] при отсутствии организованных помех СРНС имеет следующие показатели $P_{\text{ПО}} = 1{,}75\cdot10^{-2}$, $P_{cf} = 5\cdot10^{-2}$, $P_{c\tau} = 3\cdot10^{-3}$, $P_{\text{ОБ}} = 2\cdot10^{-12}$. Таким образом, вероятность успешного выполнения своей задачи СРНС при от-

сутствии радиоэлектронного подавления составляет $P_{\text{РНЗО}} = 0{,}93$. Этого достаточно для решения навигационной задачи в транспортных и телекоммуникационных системах, за исключением задач высокоточного определения координат на местности, необходимых в особых случаях [1]. Для повышения $P_{\text{РНЗО}}$ используется обработка НС на дополнительных частотах и от дополнительных СРНС, в результате удается достичь значения показателя $P_{\text{РНЗО}} = 0{,}9999$; которого достаточно для потребителей с повышенными требованиями к точности определения координат.

В условиях РЭП вероятность подавления СРНС $P_{ПД}$ в [3] предложено определять в виде

$$P_{\text{ПД}} = P_{\text{РЗ}} P_{ИСП} P_{ПП}, \qquad (3)$$

где $P_{\text{РЗ}} = P\{H_{\text{РЗ}}\}$ – вероятность того, что параметры $\vec{\Theta} = (\Theta_1, \ldots, \Theta_m)$ сигналов $s_j(t, \vec{\Theta})$, $j = \overline{1, M}$, $M \geq 1$, $t \in [0, T_0]$, используемых в СРНС, будут определены (разведаны) системой РЭП (гипотеза $H_{\text{РЗ}}$); $P_{\text{ИСП}} = P\{H_{\text{ИСП}} \mid H_{\text{РЗ}}\}$ – вероятность использования РЭП (гипотеза $H_{\text{ИСП}}$) при условии, что параметры $\vec{\Theta} = (\Theta_1, \ldots, \Theta_m)$, $m \geq 1$ сигналов разведаны с точностью, необходимой для организации радиоэлектронного подавления (гипотеза $H_{\text{РЗ}}$); $P_{\text{ПП}} = P\{H_{\text{ПП}} \mid (H_{\text{ИСП}} \cap H_{\text{РЗ}})\}$ – вероятность воздействия помехи на приемник СРНС (гипотеза $H_{\text{ПП}}$) при условии, что параметры сигналов разведаны (оценены) с заданной точностью (гипотеза $H_{\text{РЗ}}$) и средства РЭП использованы (гипотеза $H_{\text{ИСП}}$).

Во всех существующих и проектируемых СРНС, в том числе в СРНС Глонасс, а также спутниковых системах дифференциальной коррекции SBAS, планируется использование технологии кодового разделения сигналов между навигационными космическими аппаратами (НКА). Структура сигналов из системы квазиортогональных сигналов, используемых в вышеупомянутых системах, может быть представлена следующим образом [2]:

$$U_i(t) = U_m \mathrm{Q_i}(t - \tau) D_i(t - \tau) \times \\ \times \sin\left[2\pi(L \pm f_{\text{д}}) + \varphi\right], i \in [1, n_{\text{КА}}], \qquad (4)$$

где $U_m$ – амплитуда сигнала; $\mathrm{Q_i}(t - \tau)$ – манипулирующая функция, представляющая собой тип модуляции и расширяющую последовательность; $D_i(t - \tau)$ – манипулирующая функция, представляющая собой передаваемые навигационные данные; $L$ – несущая частота; $f_{\text{д}}$ – доплеровское смещение частоты; $\varphi$ – начальная фаза сигнала; $\tau$ – задержка сигнала по времени; $i$ – номер НКА; $n_{\text{КА}}$ – общее число НКА в рассматриваемой СРНС. В выражении (4) приведены все параметры НС.

Для РЭП СРНС возможно использование различных помех, эффективность которых будет во многом зависеть от вероятности разведки параметров НС в процессе осуществления радиомониторинга противоборствующей стороной, который включает в себя следующие основные задачи [2].

1. Установление энергетического контакта подсистемы радиомониторинга с источниками радиоизлучений.

2. Выделение полезного сигнала на основе классификации при многокомпонентной радиообстановке и многоальтернативных ситуациях.

3. Автосопровождение радиоизлучений.

4. Оценивание информационных параметров НС и формирование целеуказаний для постановки эффективных помех.

5. Демодуляция НС.

Для СРНС характерно наличие большого объема априорной информации о траекториях полетов НКА, энергетических, частотных, временных и статистических характеристиках существующих открытых НС. При этом априорно неизвестными параметрами, которые необходимо оценить в результате радиомониторинга, являются амплитуда, доплеровское смещение частоты и временное запаздывание огибающей сигнала.

Учитывая непрерывный характер функционирования СРНС, будем считать, что временные ограничения работы станции РЭП отсутствуют. В таком случае логично предположить, что вероятность разведки параметров существующих открытых НС будет стремиться к единице. Определение возможностей противоборствующей стороны является сложно формализуемой задачей, поэтому для упрощения оценки вероятности успешного решения навигационной задачи в условиях РЭП будем руководствоваться предположением, что при успешной разведке параметров НС ($P_{\text{РЗ}} \to 1$) показатели вероятности использования РЭП и воздействия помехи на сигнал также будут стремиться к единице ($P_{\text{ИСП}} \to 1$ и $P_{\text{ПП}} \to 1$).

Рассмотрим наиболее эффективные типы помех, которые могут быть использованы для РЭП СРНС. Для РЭП АП СРНС наиболее пригодны прицельные и заградительные непрерывные шумовые помехи, а также активные имитирующие помехи [4]. В качестве критерия эффективности помех при РЭП АП СРНС целесообразно использовать коэффициент подавления [3]:

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

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

Шумовые помехи реализуются на основе квазибелого шума и гармонических процессов, которые могут быть описаны следующим образом [4].

1. Шумоподобная помеха (ШП) типа «квазибелый» шум

$$P_1(t) = U_{\text{мш}}(t)\cos\left[\omega_{p1}t + \varphi_{p1}(t)\right];$$
$$\omega_{p1} \approx \omega_0;\ \ \omega_0 = 2\pi L, \qquad (6)$$

где $U_{\text{мш}}(t)$ – закон изменения огибающей помехи; $\varphi_{p1}(t)$ – закон изменения фазы помехи; $\omega_{p1}$ – средняя частота помехи; $L$ – несущая частота НС.

2. Гармоническая помеха (ГП)

$$P_2(t) = U_{mp}\cos\left[\omega_{p2}t + \varphi_{p2}\right];$$
$$\omega_{p2} \in \left[\omega_0 - \pi\Delta f_{\text{ЛТ}};\omega_0 + \pi\Delta f_{\text{ЛТ}}\right], \qquad (7)$$

где $U_{mp}$ – амплитуда помехи; $\omega_{p2}$ – угловая частота помехи; $\varphi_{p2}$ – начальная фаза помехи; $f_{\text{ЛТ}}$ – полоса пропускания канала.

Для организации эффективных шумовых помех требуется разведка несущей частоты НС и его фазы. Активные имитирующие помехи формируются процессами, сходными с НС. Имитирующие помехи относятся к классу «интеллектуальных» помех [3]. Имитирующие помехи разделяются на прицельные, следящие и заградительные:

3. Прицельная имитирующая помеха

$$P_{\text{i1}}(t) = K_i S_i(t - \Delta\tau), \qquad (8)$$

где $S_i(t)$ описывается выражением (5).

Процесс $P_{\text{i1}}(t)$ подобен НС $S_i(t)$ с частотным и временным рассогласованием, а также с фиксированным значением фазы огибающей манипулирующей функции, где $K_i$ – коэффициент, учитывающий уровень прицельной имитирующей помехи.

4. Следящая имитирующая помеха

$$P_{i2}(t) = K_i S_i(t - \tau(t));\ \tau(t) = r(t)/c \qquad (9)$$

подобна прицельной имитирующей помехе, но с переменной начальной фазой манипулирующей функции, закон изменения которой соответствует изменению расстояния $r(t)$ от АП до станции РЭП.

5. Заградительная имитирующая помеха (ЗИП)

$$P_{i3}(t) = \sum_{j=1}^{n_p} K_i S_i(t - \tau_{pj}), \qquad (10)$$

имитирующая набор НС $S_i(t)$ с одинаковым частотным рассогласованием для всех компонентов и разным временным рассогласованием для каждого компонента. К недостаткам следящей и прицельной имитирующих помех следует отнести сложность получения необходимых для их формирования параметров сигнала. Более простой в реализации является ЗИП, поскольку она не требует для формирования точных временных параметров сигнала.

Для организации эффективных имитирующих помех требуется разведка не только несущей частоты и фазы НС, но и амплитуды НС и манипулирующих функций, представляющих собой кодовую последовательность для разделения сигналов и навигационные данные.

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

Противоборствующая сторона стремится достичь цели РЭП СРНС с наименьшими затратами энергетических ресурсов. Оценим минимальную мощность, требуемую для гарантированного РЭП НС. На основе данных из таблицы 1 оценим вероятность успешного выполнения задачи СРНС в условиях РЭП $P_{\text{РНЗ1}}$ для следующих случаев.

1) Станцией РЭП используется сочетание ЗИП и ШП/ГП. Принимая, что $P_{\text{РЗ}} \to 1$, $P_{\text{РЗ}} = P_{\text{РНЗ1}}$. Тогда вероятность успешного решения навигационной задачи СРНС будет иметь следующее значение: $P_{\text{ПЗ}_1} = 0{,}0667$.

2) Станцией РЭП используются только ЗИП. В этом случае подавляются два канала первичной обработки информации. Тогда вероятность успешного решения навигационной задачи СРНС: $P_{\text{РЗ}_2} = 0{,}1089$.

3) Станцией РЭП используются только ГП/ШП. Тогда вероятность успешного решения навигационной задачи СРНС: $P_{\text{ПЗ}_3} = 0{,}153$.

4) Станцией РЭП используются только ГП/ШП. При этом рассмотрим минимально приемлемую для станции РЭП вероятность подавления $P_{\text{ПД}} = 0{,}5$. Для этого достаточно подавить один из каналов первичной обработки информации с такой же вероятностью 0,5. В этом случае целесообразно воздействовать на канал обнаружения. Тогда вероятность успешного выполнения задачи СРНС в условиях РЭП: $P_{\text{ПЗ}_4} = 0{,}5$.

Таблица 1. Показатели воздействия различных типов помех на АП СРНС

| Канал АП | Тип помехи | Вероятность РЭП | Энергетический потенциал PnGn (дБВт) | Коэффициент подавления $\eta_p$ |
|---|---|---|---|---|
| Канал обнаружения | ШП | $P_{ПД1} = 0,5$ | 28,5 | $\eta_{p11} = 1,5 \cdot 10^{-3}$ |
| | ГП | $P_{ПД1} = 0,5$ | 28,5 | $\eta_{p12} = 1,5 \cdot 10^{-3}$ |
| | ЗИП | $P_{ПД1} = 0,67$ | 10,5<br>16,4 | $\eta_{p13} = 5 \cdot 10^{-2}$<br>$\eta_{p13} = 10^{-1}$ |
| Канал слежения за частотой | ШП | $P_{ПД2} = 0,32$ | 39,5 | $\eta_{p21} = 2,5 \cdot 10^{-3}$ |
| | ГП | $P_{ПД2} = 0,32$ | 44,4 | $\eta_{p22} = 4,17 \cdot 10^{-3}$ |
| Канал слежения за задержкой | ШП | $P_{ПД3} = 0,5$ | 30,4 | $\eta_{31} \in \overline{4,3 \cdot 10^{-6}; 10^{-3}}$ |
| | ГП | $P_{ПД3} = 0,5$ | 74 | $\eta_{32} \in \overline{4,3 \cdot 10^{-10}; 10^{-7}}$ |
| | ЗИП | $P_{ПД3} = 0,67$ | 10,5<br>16,4 | $\eta_{p33} = 5 \cdot 10^{-3}$<br>$\eta_{p33} = 10^{-1}$ |
| Канал демодуляции | ШП | $P_{ПД4} = 0,1$ | 38,7 | $\eta_{p41} = 8,3 \cdot 10^{-4}$ |
| | ГП | $P_{ПД4} = 0,1$ | 38,7 | $\eta_{p42} = 2,5 \cdot 10^{-5}$ |

На рис. 1 представлен минимальный необходимый энергетический потенциал средств РЭП для рассмотренных выше четырех случаев организации РЭП СРНС. Анализ таблицы 1 и рис. 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 [4].

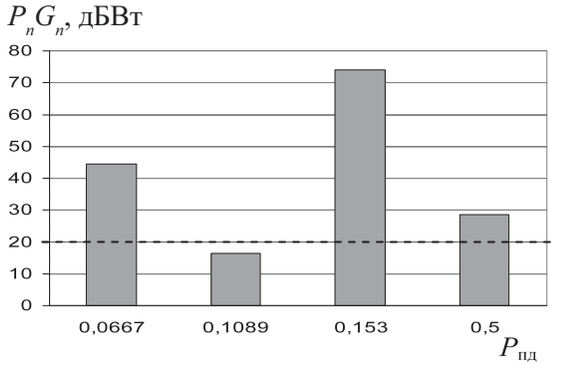


Рис. 1. Минимальный необходимый энергетический потенциал для организации РЭП СРНС

На основании вышеизложенного для повышения вероятности успешного решения навигационной задачи СРНС следует прежде всего обеспечить противодействие организации имитирующих помех.

Направлением повышения помехозащищенности в условиях воздействия имитирующих помех является повышение скрытности радиосистемы для противодействия этапу радиомониторинга при организации РЭП. Скрытность многоканальной радиосистемы определяется скрытностью рабочей группы сигналов [4]. Структурной называется скрытность, определяемая мощностью $A$ (числом элементов) множества $X$ возможных структур сигналов. Таким образом, априорная неопределенность структуры манипулирующих функций $\mathrm{Q_i}(t)$ называется структурной скрытностью СРНС. В случае стохастической смены кодовых последовательностей манипулирующая функция сигнала является априорно неизвестной, и в процессе радиомониторинга необходимо предусмотреть ее распознавание.

В общем случае вероятность разведки параметров радиосигнала, упомянутой в формуле (3), оценивается следующим образом:

$$P_{\text{РЗ}} = \sum_{i=1}^{n} p_i P_{РЗi} , \qquad (11)$$

где $P_{РЗ_i}$ – вероятность разведки $i$-го параметра НС, $p_i$ – весовой коэффициент, определяющий значимость разведки $i$-го параметра НС для организации того или иного типа радиопомехи, $\sum p_i = 1$. Как следует из вышеописанного, для организации имитирующих помех СРНС наибольшее значение имеет вероятность разведки структуры манипулирующих функций $\mathrm{Q_i}(t)$, которая оценивается следующим образом [5]:

$$P_{РЗi} = 1/R , \qquad (12)$$

где $R$ – число возможных вариантов структуры манипулирующих функций $\mathrm{Q_i}(t)$.

Рассмотрим задачу системы радиомониторинга НС СРНС с повышенной структурной скрытностью. В отличие от одиночного сигнала выявление рабочей группы из $m$ сигналов представляет собой неоднозначную задачу. Число $R$ вариантов выбора $m$ без повторений различных событий из общего их числа $A$ равно числу сочетаний из $A$ по $m$ [5],

$$R = \binom{A}{m} = \frac{A!}{(A-m)!m!}, \quad (13)$$

где $A = 2^N$ – полное количество двоичных кодовых последовательностей длины $N$.

Недостатком представленного подхода к оценке вероятности разгадывания параметров сигнала, основанного на равной вероятности всех возможных значений параметров НС, является отсутствие учета накопления разведывательной информации подсистемой радиомониторинга станции РЭП, что в большинстве случаев существенно ускоряет процесс радиоразведки. Предположим, что в СРНС производится стохастическая смена кодовых последовательностей, а подсистема радиомониторинга станция РЭП, накапливая информацию об используемых последовательностях, уменьшает априорную неопределенность структуры манипулирующих функций $\mathrm{Q_i}(t)$. Тогда в общем случае вероятность разведки параметра сигнала в *i*-ый момент времени будет иметь вид:

$$P_{\text{РЗ}i} = 1/(n - M_i), \quad (14)$$

где $M_i$ – число разведанных значений параметра сигнала от начала наблюдения до *i*-го момента времени.

Как известно, не все двоичные последовательности пригодны для использования в системах радиосвязи. Одним из критериев, накладывающих ограничения на применимость последовательностей, может служить их взаимная корреляция. Число кодовых последовательностей, удовлетворяющих требованиям взаимной корреляции, ограниченно и определяется выражением [5]

$$A_{cc} = \sqrt{2/(\pi N)}\ 2^N. \quad (15)$$

В таблице 2 приведены значения $A_{cc}$ для некоторых длин последовательностей.

Таблица 2. Число кодовых последовательностей, удовлетворяющих требованиям по взаимной корреляции

| $N$ | 4095 | 8190 | 10230 |
|---|---|---|---|
| $A_{cc}$ | $6{,}5 \cdot 10^{1230}$ | $2{,}12 \cdot 10^{2461}$ | $2{,}14 \cdot 10^{3075}$ |

Поскольку длительность периода последовательности близка к единицам мС, за этот интервал времени будет разведано *m* структур кодовых последовательностей. С учетом этого преобразуем выражение (14):

$$R_k = \frac{(A_{cc} - mk)!}{(A_{cc} - m(k+1))!m!};\ k = [0, \ldots, n], \quad (16)$$

где *k* – число символов навигационного сообщения, разведанных системой радиомониторинга. Тогда вероятность разведки структуры манипулирующих функций $\mathrm{Q_i}(t)$ будет равна:

$$P_{\text{РЗ}i} = 1/R_k. \quad (17)$$

Основываясь на расчетном сроке эксплуатации спутников СРНС Глонасс, не превосходящем 15 лет, а также на темпах развития технологий, достаточным показателем повышения структурной скрытности СРНС можно считать использование неповторяющихся кодовых последовательностей, сменяемых на каждом информационном символе НС, на всех НКА созвездия СРНС в течение 15 лет. Следует отметить, что к последовательностям предъявляется весь набор требований по спектральным и корреляционным свойствам. В таком случае требуемое количество неповторяющихся последовательностей при 50 КА (по аналогии с СРНС Galileo) составит $A_r = 2{,}3652 \cdot 10^{12}$. Как видно из таблицы 2, для рассматриваемых размерностей *N* кодовых последовательностей их количество $A_{cc}$ существенно больше требуемого значения.

Анализ формулы (17) с учетом данных, представленных в таблице 2, позволяет сделать вывод о том, что вероятность разведки манипулирующей функции $\mathrm{Q_i}(t)$, необходимая для постановки ЗИП, при больших *N* стремится к нулю: $P_{\text{РЗ}} \to 0$. В этом случае, согласно выражению (3), вероятность подавления СРНС также будет стремиться к нулю $P_{\text{ПД}} \to 0$. Поэтому стохастическое применение НС является достаточно эффективным способом противодействия имитирующей помехе.

Анализ выражения (1) показывает, что при сохранении прочих равных условий снижение вероятности подавления СРНС $P_{\text{ПД}}$ ведет к повышению вероятности успешного решения навигационной задачи в условиях радиоэлектронного подавления $P_{\text{ПЗ}}$, что свидетельствует о повышении ее помехозащищенности.

Таким образом, в итоге можно сделать следующие выводы.

1. Анализ необходимого энергетического потенциала и эффективности средств РЭП свидетельствует о наибольшей уязвимости СРНС от воздействия имитирующих помех.

2. Предложено выражение

$$P_{\text{ПЗ}} = P_{\text{РНЗ0}} + \left( \frac{p_c (A_{cc} - m(k+1))! m!}{(A_{cc} - mk)!} + \sum_{i=1}^{n-1} P_{Pзi} p_i \right) \times$$

$$\times P_{ИСП} P_{ПП} \left( P_{РНЗ1} - P_{РНЗ0} \right),$$

которое, в отличие от известных, позволяет оценить помехозащищенность СРНС в условиях стохастического применения ей НС с учетом снижения априорной неопределенности параметров НС в процессе функционирования системы РЭП.

## Литература


1. Global Navigation Space Systems: reliance and vulnerabilities // Report of The Royal Academy of Engineering. London: March, 2011. – 48 p.
2. Дятлов А.П., Кульбикаян Б.Х. Радиомониторинг излучений спутниковых радионавигационных систем. М.: Радио и связь, 2006. – 270 с.
3. Борисов В.И., Зинчук В.М. Помехозащищенность систем радиосвязи. Вероятностно-временной подход. М.: РадиоСофт, 2008. – 260 с.
4. Дятлов А.П., Дятлов П.А., Кульбикаян Б.Х. Радиоэлектронная борьба со спутниковыми радионавигационными системами. М.: Радио и связь, 2004. – 226 с.
5. Основы теории скрытности. Под ред. З.М. Каневского. Воронеж: Изд. ВГУ, 2006. – 197 с.


## ABOUT THE NOISE IMMUNITY EVALUATION OF SATELLITE RADIO NAVIGATION SYSTEMS

**Zhuk A.P., Orel D.V.**

**This work introduces the way to evaluate the noise immunity of satellite radio navigation systems with high structural secrecy of navigation signals by using the expression, that takes into account the reduction of prior uncertainty parameters of navigation signals during the jamming complex system works.**

***Keywords:*** *noise immunity, satellite radio navigation, structural secrecy, simulating interference, radio electronic strike.*

Жук Александр Павлович, к.т.н., профессор Кафедры «Организация и технологии защиты информации» (ОТЗИ) Ставропольского государственного университета (СтавГУ). Тел. (8-652) 35-74-09; 8-918-884-14-81. E-mail: alekszhuk@mail.ru

Орел Дмитрий Викторович, ассистент Кафедры ОТЗИ СтавГУ. Тел. (8-652) 95-56-36; 8-918-740-11-74. E-mail: kde.def@gmail.com

УДК 004.056

# ПРИНЦИПЫ МНОГОУРОВНЕВОЙ ЗАЩИТЫ ИНФОРМАЦИИ

*Алексеев А.П., Макаров М.И.*

Рассмотрены принципы защиты информации, основанные на создании нескольких барьеров: криптографического, стеганографического, алгоритмического и пространственно-временного распыления.

***Ключевые слова:*** защита информации, криптография, стеганография, барьеры, пространственно-временное распыление информации.

## Введение

Защита передаваемой и хранимой информации в настоящее время базируется на принципах, фундаментально разработанных в криптографии и стеганографии. С помощью криптографических методов защищаемое сообщение преобразуется в набор символов, нечитаемый без ключа [1]. Приемы стеганографии позволяют создать скрытый канал связи, который сложно обнаружить даже с помощью специальных методов обработки информации [2].

Специалистами проведено большое число результативных криптографических атак на известные шифры [3] и на стеганографические методы защиты [2]. Наличие успешно проведенных атак говорит об имеющейся уязвимости существующих принципов защиты информации.

Процесс разработки средств защиты информации и средств атаки на шифры и методы сокрытия сообщений носит соревновательный (итерационный) характер. Как правило, через несколько лет после создания широко распространенного шифра появляется эффек-