УДК 621.393

**В.В. Лебедянцев, Е.В. Морозов**

# Оценки информационной защищенности и помехоустойчивости инвариантной системы связи

Для нового класса систем связи, использующих инварианты каналов связи, получены оценки информационной защищенности и помехоустойчивости к белому шуму.
**Ключевые слова:** группа преобразований канала связи, инварианты канала связи, помехоустойчивость, информационная защищенность.

Инвариантные системы связи представляют собой новый, пока ещё малоизученный класс систем. С учетом этого актуальными являются задачи оценки их информационной защищенности и помехоустойчивости.

Инвариантные системы связи для передачи значений информационного процесса используют инварианты группы преобразований, которая описывает преобразования сигналов в канале связи [1]. Так, например, изменения сигналов в линейных каналах связи вследствие неидеальности частотно-временных характеристик соответствуют преобразованиям аффинной группы. Основным инвариантом этой группы являются «отношения трех точек» [2], что применительно к задачам связи означает сохранение каналом отношения длин векторов сигналов с подобными формами:

$$J = \frac{\left|\bar{s}_{\text{вх}_1}\right|}{\left|\bar{s}_{\text{вх}_2}\right|} = \frac{\left|\bar{s}_{\text{вых}_1}\right|}{\left|\bar{s}_{\text{вых}_2}\right|}, \qquad (1)$$

где $\bar{s}_{\text{вх}_1}$, $\bar{s}_{\text{вх}_2}$, $\bar{s}_{\text{вых}_1}$ и $\bar{s}_{\text{вых}_2}$ – соответственно векторы входных и выходных сигналов, причем должно быть $\bar{s}_{\text{вх}_1} = \alpha \bar{s}_{\text{вх}_2}$, $\alpha$ – любое число.

Из (1) легко получить алгоритмы относительной амплитудной модуляции и демодуляции (ОАМ):

$$\bar{s}_i = J_i \bar{s}_{on}; \qquad J_i = \frac{\left|\bar{s}_i\right|}{\left|\bar{s}_{on}\right|}. \qquad (2)$$

Здесь $J_i$ – обозначает значение $i$-го информационного элемента; $\bar{s}_{on}$ – вектор опорного сигнала, передаваемого, например, в начале блока информационных сигналов $s_i(t)$; $J_i, \left|\bar{s}_i\right|, \left|\bar{s}_{on}\right|$ – соответственно оценки значений информационных элементов, длин векторов информационных и опорных сигналов на выходе канала связи.

В общем случае опорный сигнал может занимать любое место в блоке сигналов, опорных сигналов может быть несколько и т.д. Это при необходимости следует использовать для обеспечения информационной защищенности процесса передачи.

Инварианты канала вследствие своей неизменности (хотя сигналы в канале связи изменяются) представляют собой идеальную форму для безыскаженной передачи информации.

Конечно, в каналах связи действуют ещё аддитивные и мультипликативные помехи. Однако их влияние на передаваемые сигналы также можно описать соответствующей группой преобразований, для которой требуется найти собственной инвариант. В частности, группой преобразований, характеризующей воздействия на сигналы аддитивных помех, является группа сдвигов. Инвариант этой группы представляет собой расстояние между линиями направлений сдвигов сигнальных точек вследствие воздействия помех в пространстве представления сигналов [1].

Используя сочетания инвариантов группы сдвигов и аффинной группы преобразований, можно обеспечить безыскаженную передачу информации по линейным каналам с аддитивными помехами.

При наличии в канале белого шума вследствие равновероятности любого направления сдвига сигнальных точек найти инвариант группы сдвига не представляется возможным. В связи с этим представляет интерес оценка помехоустойчивости инвариантной системы связи к воздействию белого шума.

В [3] приведена оценка помехоустойчивости для случая, когда вычисления оценок информационных элементов $J_i$ осуществляются в соответствии с алгоритмом (2).

Улучшить помехоустойчивость можно применением методов оптимального приема сигналов. Так, если считать, что форма принимаемых сигналов на приемной стороне известна (информационные и опорные сигналы имеют подобные формы, а оценка опорного сигнала $s_{on}(t)$ принятая в начале, конце или внутри блока сигналов, хранится в памяти приемника), то алгоритм получения наилучших оценок будет следующим:

$$\min_{J_i} \int_0^T \left[ s(t) - J_i s_{on}(t) \right]^2 dt , \qquad (3)$$

где $T$ – длительность сигнала на выходе канала.

В результате аналитических преобразований получено следующее выражение для плотности вероятности погрешности оценок $\Delta J_i$:

$$\omega(\Delta J_i) = \frac{1}{\delta\sqrt{2\pi(1+2J_i^2)}} \exp\left[ -\frac{\Delta J_i}{\delta^2(1+2J_i^2)} \right], \qquad (4)$$

где $\delta$ – среднеквадратическое значение белого шума.

Таким образом, погрешность оценок $\Delta J_i$ является случайной величиной с гауссовской плотностью вероятности с дисперсией $\delta^2(1+2J_i^2)$ и нулевым математическим ожиданием.

На рис. 1 приведены результаты имитационного моделирования инвариантной системы связи. Целью исследования было сравнение помехоустойчивости различных методов оценки значений информационных элементов.

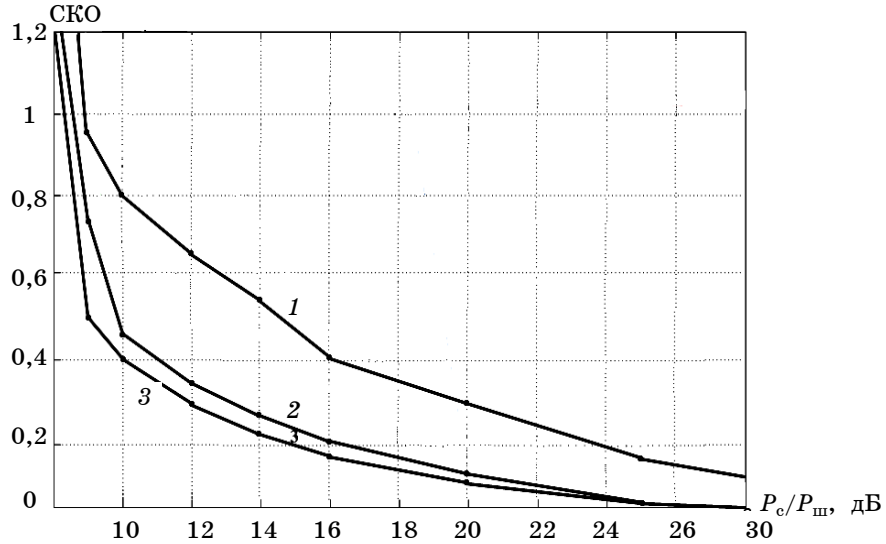


Рис. 1. Сравнение помехоустойчивости различных методов оценки значений информационных элементов в инвариантной системе связи: *1* – метод непосредственного деления оценок длин векторов и опорных сигналов; *2* – метод максимального правдоподобия с использованием усредненной оценки длины вектора опорного сигнала; *3* – метод максимального правдоподобия с использованием усредненных реализаций опорного сигнала

Как показали результаты имитационного моделирования, применение для вычисления оценок значений информационных элементов метода максимального правдоподобия позволило более чем в два раза уменьшить погрешность (кривая *2*) по отношению к методу вычисления путем непосредственного деления оценок длин векторов информационных и опорных сигналов (кривая *1*).

Определим теперь степень информационной защищенности инвариантной системы связи.

Информационную защищенность формируют следующие факторы:

а) новизна алгоритма передачи информации;

б) отсутствие необходимости в адаптации приемника к свойствам используемого канала посредством различных обучающих сигнальных последовательностей;

в) возможность произвольного расположения опорного сигнала внутри блока сигналов;

г) возможность применения составного опорного сигнала, отдельные слагаемые которого расположены внутри блока сигналов секретным образом.

Пусть опорный сигнал разделен на $m$ слагаемых, а длина всего блока сигналов равна $n$. Тогда, очевидно, что число возможных конфигураций систем временного расположения слагаемых опорного сигнала внутри блока будет равно числу сочетаний из $n$ по $m$ элементов.

Помимо такого «примитивного» способа засекречивания процедуры вычисления оценки опорного сигнала путем суммирования отдельных его слагаемых, возможно осуществить вычисления его уровня посредством некоторой линейной секретной функции от $m$ аргументов, которыми являются m служебных сигналов $\overline{s}_{cc}$, секретным образом расположенных в блоке сигналов:

$$\overline{s}_{on} = a_1\overline{s}_{cc} + a_2\overline{s}_{cc} + \ldots + a_m\overline{s}_{cc}.$$

Очевидно, что набор значений $\{a_i\}$ будет является ещё одной секретной информацией, способной повысить информационную безопасность инвариантной системы связи.

Нетрудно найти число вариантов комбинаций слагаемых опорных сигналов, определяющее информационную защищенность инвариантной системы связи:

$$N = C_n^m \cdot k^m,$$

где $k$ – число возможных значений, которые могут иметь коэффициенты $a_i$.

Таким образом, инвариантные системы связи являются весьма привлекательными в определенных ситуациях, когда, например, свойства канала известны не полностью, необходимо минимизировать время вхождения в связь, обеспечить информационную безопасность на физическом уровне семиуровневой модели OSI.

*Литература*

1. Лебедянцев В.В. Разработка и исследование методов анализа и синтеза инвариантных систем связи: дис. ... д-ра техн. наук. – Новосибирск: СибГУТИ,1995. – 253 с.

2. Ефимов Н.В. Высшая геометрия. – М.: Наука,1978. – 576 с.

3. Лебедянцев В.В. К оценке помехоустойчивости инвариантной системы связи / В.В. Лебедянцев, Д.С. Качан, Е.В. Морозов // Вестник СибГУТИ (Новосибирск). – 2009. – № 4. – С. 68–72.

---

**Лебедянцев Валерий Васильевич**
Доктор техн. наук, профессор, зав. каф. автоматической электросвязи СибГУТИ, г. Новосибирск
Тел.: (383) 269-82-42
Эл. адрес: lebvv@sibsutis.ru

**Морозов Евгений Викторович**
Ассистент каф. автоматической электросвязи СибГУТИ, г. Новосибирск
Тел.: (383) 269-82-42
Эл. адрес: joni6127@rambler.ru

V.V. Lebedjantsev, E.V. Morozov

**Estimations of information security and noise stabilities of the invariant communication system**

For a new class of the communication systems using invariant of communication channels, estimations of information security and a noise stability to white noise are received.

**Keywords:** group of transformations of a communication channel, invariant a communication channel, a noise stability, information security.