

УДК 004.056.5

## РАЗРАБОТКА АЛГОРИТМА И ВИЗУАЛИЗАЦИЯ ПРОСТРАНСТВЕННОГО РАСПРЕДЕЛЕНИЯ ТРАСС ДОСТАВКИ СООБЩЕНИЙ В УСЛОВИЯХ УГРОЗЫ НЕСАНКЦИОНИРОВАННОГО СЪЕМА

Стволовая А.К., Павликов С.Н.

*Владивостокский государственный университет экономики и сервиса, Владивосток, e-mail: anastasiy1911@mail.ru*

Информационные технологии стали неотъемлемой частью современного общества. В наше время очень часто сталкиваются с проблемой несанкционированного использования передаваемой информации. Очень важна безопасная передача информации от одного объекта к другому с повышенной защищенностью, будь это денежный перевод или документация. Уже существуют методы, базирующиеся на новых способах нелинейных преобразований, что приводит к новому витку развития методов нападения и защиты. Поэтому необходим поиск других новых методов, что является актуальной задачей, обеспечения сохранности информации путем логической, информационной, тактической, энергетической и других скрытностей передачи. При этом следует уделить внимание и скрытности приема. В статье предложен новый способ повышения скрытности канала, что приводит к росту ресурсных затрат противника. Проведенные исследования с помощью системы математического моделирования Mathcad показали, что деления информации на две части достаточно, это значительно усложняет перехват и съем информации. Представленная визуализация показывает работу метода зашумления, маскирования и кодирования, которые можно использовать как совместно, так и в отдельности. Визуализация проводилась с помощью среды разработки Visual Studio, код написан на языке программирования C#. При написании кода буквенные сочетания передаются не только по различным трассам доставки сообщений, но и используют различную частоту.

**Ключевые слова:** информация, информационный канал, защита, метод

## DEVELOPMENT OF ALGORITHM AND VISUALIZATION OF SPATIAL DISTRIBUTION OF COMMUNICATION DELIVERY TRACKS IN CONDITIONS OF THREAT OF UNAUTHORIZED REMOVAL

Stvolovaya A.K., Pavlikov S.N.

*Vladivostok State University of Economics and Service, Vladivostok, e-mail: anastasiy1911@mail.ru*

Information technology has become an integral part of modern society. In our time, very often they face the problem of unauthorized use of transmitted information. Very important is the safe transfer of information from one object to another with increased security, be it a money transfer or documentation. Already there are methods based on new ways of nonlinear transformations, which leads to a new round of development of methods of attack and defense. However, the existence of such directions is known and their implementation triggers a mechanism for developing new ways of attack and reducing their effectiveness due to the limited representation of the theory of signal separation, channels and methods of their transformation. Therefore, it is necessary to search for other methods, which is an urgent task, ensuring the preservation of information through logical, information, tactical, energy and other secrets of transmission. In this case, attention should be given to the secretiveness of the reception. In this article suggests a new way to increase the channel's secrecy, which leads to an increase in the enemy's resource costs. The conducted researches with the help of the mathematical modeling system Mathcad have shown that the division of information into two parts is enough, this greatly complicates the interception and information retrieval. Therefore, studies were used when dividing into one and two letters, traces. The presented visualization shows the operation of the method of noisiness, masking and coding, which can be used both jointly and separately. Visualization was carried out using the Visual Studio development environment, the code is written in the C # programming language. When writing the code, letter combinations are transmitted not only along different message delivery routes, but also use a different frequency.

**Keywords:** the information, a channel, protection, methods

Популярными в наше время являются методы защиты [1], которые используют расширенный спектр задач нелинейной трансформации сигнала [2].

Вопросами расширения данных модификаций в радиосвязи занимались: К. Шеннон, В.Ф. Комарович, Барадеи, И.А. Голяницкий, В.Г. Кулаков, Н.Н. Клименко, А.Н. Обухов, В.И. Борисов и другие.

Целью работы является увеличение пропускной способности канала; повышение скрытности при доставке сообщения передаваемого адресату по радиоканалу, на базе

методов управления траекториями доставки элементов сообщений; снижение вероятности перехвата информации, позволяющее увеличивать защищенность сообщений.

Задачи, которые потребуется решить в ходе работы:

1. Классификация методов скрытности радиоканала; уточнение критериев оценки эффективности за счет двух связанных методов.

2. Разработка нового метода повышения скрытности на основе: разделения и пространственного кодирования.

3. Разработка нового метода повышения скрытности за счет зашумления на передающей и приемной сторонах.

4. Разработка программного кода метода и его визуализация.

Приведенные в работе технологии формируют новое направление в развитии телекоммуникационных систем и общей теории связи при решении задач скрытности, помехозащищенности и повышения эффективности использования расширенного понятия связного ресурса [3]. В ходе написания работы был проведен патентный поиск, аналоги приведены в таблице.

Также уже были опубликованы статьи на данную тему, что еще раз подтверждает ее актуальность. Всероссийские конкурсы, такие как: «УМНИК-2014», «УМНИК-2016», «Всероссийский инженерный конкурс ВИК – 2016»; международные конференции: 64 – 62-я молодежная научно-техническая конференции «МОЛОДЕЖЬ. НАУКА. ИННОВАЦИИ»; XIX РФ и Китайской Народной Республики; конкурс Благотворительного фонда В. Потанина; открытый университет Сколково, – по достоинству оценили наработки в области научной деятельности и отметили значимость работы.

Предлагается проанализировать несколько категорий методов пространственного разделения, из числа которых применяются: способы селекции согласно дальностям, направлениям и их сочетания. Классификация методов представлена на рис. 1 [4].

Исследования были выполнены для различных методов разделения сообщений, сигналов, каналов, пакетов, трасс доставки и их комбинаций. Сравнение методов защиты за счет разделения радиоканалов приведено на рис. 2 [5].

Сущность метода распределения трасс заключается в делении информации на несколько частей. Подразумевается деление информационных блоков на несколько составляющих. Значительная доля данных – информация, вторая – ключ. Разделение совершается следующим способом: первоначальный информационный блок проходит несколько этапов трансформации на передающей стороне с последующим восстановлением в приемной аппаратуре. Далее вырезанные блоки ключа также преобразуются из спектра во временную область и подаются на радиопередатчик, для излучения, так же как и ложная информация.

Способы защиты информации в радиоканале

№ п/п	Название	Информационный ресурс
1	Способ защиты информации в метеорном радиоканале	Патент РФ № 2265957, 25.02.2004
		Патент СССР № 1462498, 28.02.1989
		Патент США № 5119500, 02.06.1992
		Патент РФ № 2211533, 27.08.2003
2	Способ передачи-приема сигнала в многопользовательской системе радиосвязи с множеством передающих и множеством приемных антенн	Патент РФ № 2398359, 28.01.2008
		Патент РФ № 2303330, 20.07.2007
3	Способ передачи и приема цифровой информации в тропосферных линиях связи	Патент РФ № 2475962, 18.06.2010
		Патент РФ № 2013014, 10.07.2010



Рис. 1. Классификация методов скрытности

Методы защиты		
Кодовое разделение	Частотное разделение	Корреляционное разделение
Адрес канала указывается кодированным сигналом, посылаемым на линию связи. Разделение на приемной стороне осуществляется декодирующим устройством, направляющим сообщения по выбранному каналу. Код адреса может быть последовательным/параллельным. В последнем случае используется отдельная линия связи или индивидуальный частотный канал на каждый разряд кода. Кодовое разделение каналов позволяет производить опрос каналов в произвольном порядке, что делает удобным его использование в системах передачи данных и адаптивных телеизмерительных системах.	Для различных каналов в полосе частот линии связи отводятся непересекающиеся участки.	Эффективность корреляционного метода разделения состоит в том, что он позволяет значительно ослабить влияние перекрестных помех, а это особенно существенно в случае перекрывающихся спектров сигналов.
	<b>Временное разделение</b>	<b>Разделение по форме</b>
	Сигналы датчиков передаются только в отведенные для них непересекающиеся отрезки времени.	Для разделения сигналов, различающихся по форме, используются операции, наиболее чувствительные к изменению формы, – обычно дифференцирование, интегрирование и вычитание.
	<b>Пространственное разделение</b>	<b>Разделение по уровню</b>
Разделение по пространственным каналам.	В системах с разделением по уровню параметром разделения служит амплитуда сигналов, принимающая ряд дискретных значений.	

Рис. 2. Методы защиты информации

Антенны передатчиков формируют излучение отправленной информации согласно заданной точке. Ключ формируется другой антенной и излучается в направлении таким образом, чтобы обрезанный информационный блок и ключ сформировались синфазно в установленной точке пространства. Около полезной передаваемой информации также излучается ложная информация. Данные действия применяются для отвлечения внимания противника.

Приемной стороне заранее сообщается, в какой точке необходимо совершить снятие информации, в этом направлении и будет сфокусирована приемная радиоантенна. В данном пункте уже будут скомпонованы блок обрезанной информации и ключ, в итоге принимающая сторона получает нужную информацию. После принятия первой части данных система преобразуется для снятия информации в следующей точке на другом участке времени [6].

Алгоритм работы метода приведен на рис. 3.

Преимуществом является то, что информационная система содержит ограниченную численность каналов. В случае увеличения ложной информации мы усложняем снятие данных противной стороной.

Осуществление предлагаемого способа подразумевает ряд критериев:

1. Подобранные точки должны быть видны приемной и передающей стороне. Приемные и передающие антенны располагаются для соблюдения условия совместно наблюдения точки переизлучения.

2. Область, в которую передается информация, должна определяться сектором в дан-

ных границах. Противная сторона должна будет просматривать большое количество возможных вариантов трасс, а изменение их во времени приведет к тому, что вероятность вскрытия станет мала. Перебор точек приведет злоумышленника к перегрузке информационной системы и остановке съема.

Для усиления представленного метода предлагается использовать метод маскирования. Пока известно, что маскирование предусматривает защиту передатчика. Возможны более сложные варианты использования направленности передатчика/приемника и зашумление. Эффективность будет определяться в виде произведения характеристик направленности каждого из элементов схемы.

Для реализации данного метода написана программа, визуализация варианта построения трассы представлена на рис. 4.

На рис. 5 представлен более сложный вариант передачи информации с использованием двух трасс.

Опыт работы в крупной телекоммуникационной компании позволяет заметить, что корпорации сталкиваются с проблемой передачи информации в отдаленных пунктах. Не везде в Приморском крае есть возможность провести коммуникации до определенного здания. С такими проблемами сталкиваются такие предприятия, как базы отдыха «Синяя сопка», воинские части, расположенные далеко от городских территорий. Метод предполагает передачу информации по радиоканалу, что позволит использовать его в данных местах. Также система предполагает защиту информации от несанкционированного съема, что является важным для любой компании: игровая зона, МВД, биз-

нес-центры, рыбодобывающие компании. Гибкость предлагаемой системы позволит в любой момент поменять условия доставки, что снизит до нуля вероятность перехвата.

Анализ результатов моделирования по пространственному преобразованию трасс распространения показал:

1. Даже при делении информации на два блока по пространству повышается скрытность радиоканала, что не позволяет станции радиоразведки (РР) восстановить информацию.

2. Для перехвата информации станция РР должна формировать множество каналов приема с последующим их перебором, что потребует увеличения аппаратных, вычислительных и временных ресурсов.

3. Предложенные варианты расширяют пространства маневра построения трасс через виртуальные отражатели, контроль которых становится или недоступным или неприемлемым для станций радиоразведки.

4. Развитие автоматизированных систем мониторинга пространства в будущем сможет снизить эффективность данного метода,

поэтому требуется усилить предложенный метод скрытности дополнительным эффектом. Поэтому предложена новая процедура зашумления канала. Для большей надежности предложено выполнить маскирование как передатчика, так и приемника [7].

Таким образом, в работе предложен метод защиты информации в радиоканале, значительно затрудняющий съем информации. Разработка метода пространственного преобразования позволяет повысить скрытность передаваемой информации и увеличить защищенность сообщений.

Классификация методов скрытности радиоканала и уточнение критериев оценки эффективности за счет двух связанных методов помогли в разработке нового метода повышения скрытности на основе: разделения и пространственного кодирования. Разработан план и проведен эксперимент по оценке эффективности метода пространственного разделения. Определены условия и ограничения метода. Разработано техническое решение, в Роспатент отправлена заявка на полезную модель.



Рис. 3. Алгоритм работы метода

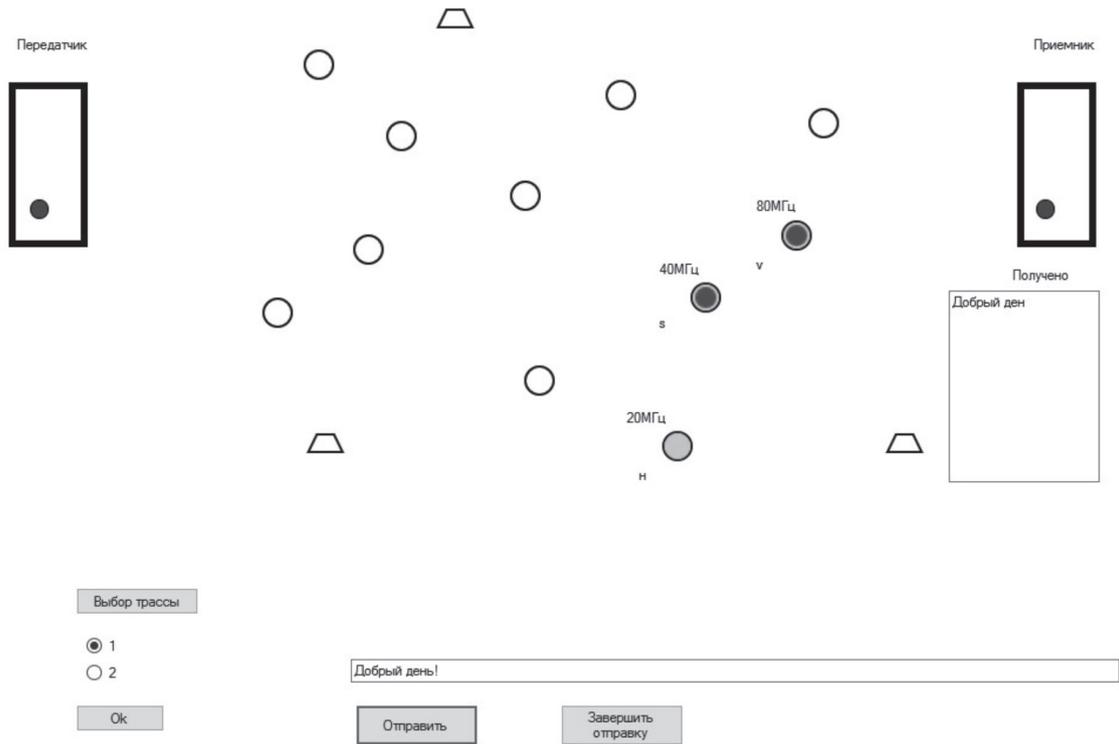


Рис. 4. Передача информации по первой трассе

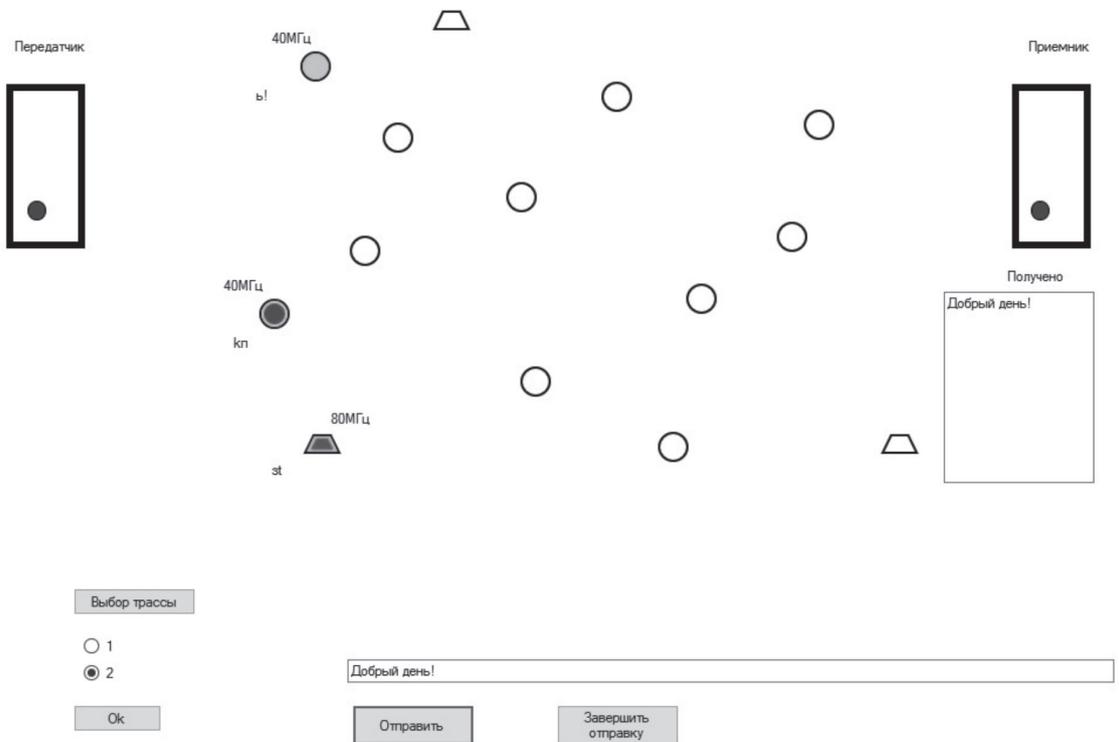


Рис. 5. Передача информации по двум трассам

Цели работы достигнуты, система позволяет повысить скрытность сообщений при доставке адресату, что снижает вероятность перехвата.

#### Список литературы

1. Помехоустойчивость и эффективность систем передачи информации / А.Г. Зюко, А.И. Фалько, И.П. Панфилов, Л.В. Банкет, П.В. Иващенко; под ред. А.Г. Зюко. – М: Радио и связь, 1985. – 272 с.
2. Стволовая А.К. Метод защиты информации в мобильных системах связи: материалы междунар. науч. конф. – Владивосток: Изд-во ВГУЭС, 2017. – С. 211–215.
3. Орлов В.В. Методы скрытой передачи информации в телекоммуникационных сетях: автореф. дис. ... канд. техн. наук. – Самара, 2012. – 16 с.
4. Юдин И.А. Методы защиты информации от несанкционированного доступа // Инновации и инвестиции: электронный научный журнал. – 2016. – № 6 [Электронный ресурс]. – URL: <https://elibrary.ru/item.asp?id=28310345> (дата обращения: 10.12.2017).
5. Оптимизация телекоммуникационных систем [Текст]: монография / С.С. Веселова, С.Н. Павликов, Е.И. Убанкин, Е.А. Шевцова. – Владивосток: Мор. гос. ун-т, 2013. – С. 100.
6. Михайлов Д.Ю. Метод защиты радиоканала // Развитие Дальнего Востока в контексте политических и экономических изменений в Азиатско-Тихоокеанском регионе: материалы Третьего международного магистерского форума / под общ. ред. д-ра экон. наук А.П. Латкина. – Владивосток: Изд-во ВГУЭС 2016. – С. 99–103.
7. Стволовая А.К., Павликов С.Н. Система радиосвязи с повышенной разведзащищенностью // Заявка Патент России № 2017136894.