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

А.К.Стволовая

Владивостокский государственный университет экономики и сервиса

Кафедра информационных технологий и систем

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 математических задачах.Однако наличие таких направлений известно и их внедрение запускает механизм разработки новых способов нападения и снижения их эффективности за счет ограниченного представления теории разделения сигналов, каналов и методов их трансформации. Поэтому необходим поиск других 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.

Известные методы защиты [1] базируется на сложных математических задачах: криптографии, кодирования, модуляции, организации протоколов взаимодействия и разделения сигналов [2].

Вопросами расширения пространства многоуровневых математических моделей радиосвязи в разное время занимались такие исследователи, как 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, позволяющего 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.

В ходе написания работы был проведен патентный поиск.

№ п/п	Название	Информационный ресурс
1.	Способ защиты информации в метеорном радиоканале путем шифрования случайным природным процессом	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

Также уже были зафиксированы 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 Международная научно-практическая конференция студентов, аспирантов и молодых ученых «ИНТЕЛЛЕКТУАЛЬНЫЙ ПОТЕНЦИАЛ ВУЗОВ – НА РАЗВИТИЕ ДАЛЬНЕВОСТОЧНОГО РЕГИОНА РОССИИ И СТРАН АТР»; международный научный форум магистрантов, аспирантов и молодых учёных и вузов Ассоциации Дальнего Востока и Сибири Российской Федерации и северо-восточных регионов Китайской Народной Республики (АВРИК); конкурс Благотворительного фонда В. Потанина; открытый университет Сколково; по достоинству оценили наработки в области научной деятельности и отметили значимость работы.

Предлагается рассмотреть группу методов пространственного разделения, среди которых используются: методы селекции по дальностям, по направлениям и их сочетания. Уже существуют следующие методы скрытности, представленные на рисунке 1. [3]

Рисунок 1 - Классификация методов скрытности

Исследования были выполнены для различных методов разделения сообщений, сигналов, каналов, пакетов, трасс доставки и их комбинаций. Оценка скрытности методов разделения радиоканалов и сравнительные характеристики приведены на рисунке 2. [4]

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.
	Временное разделение	***Разделение по форме***
	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.
	Пространственное разделение	***Разделение по уровню***
	Разделение по пространственным каналам.	В системах с разделением по уровню параметром разделения служит амплитуда сигналов, принимающая ряд дискретных значений.

Рисунок 2 - Методы защиты информации

Сущность метода распределения трасс заключается в делении информации на несколько частей. Подразумевается деление информационных блоков на несколько составляющих. Первая – большая часть информации, вторая – ключ. Разделение происходит следующим образом: исходный информационный сигнал во времени переводится в спектр, из спектра вычитаются заданные компоненты в виде дискретных составляющих, оставшийся обрезанный сигнал переводится снова во временную область и потом подается к антенне для излучения. Затем вырезанные части ключа также преобразуются из спектра во временную область и подаются на передатчик,для излучения, также как и ложная информация.

Антенны передатчиков, формируют излучение передаваемой информации по направлению к определенной заданной точке. Ключ формируется другой антенной системой и направляется под углом так, чтобы обрезанная информационная составляющая и ключ сложились синфазно в заданной точке пространства. Вокруг полезной передаваемой информации излучается ложная информация. Это происходит с целью создания фона чтобы отвлечь внимание противной стороны.

Приемной стороне известно в какой точке необходимо будет осуществлять съем информации, в этом направлении и будет сфокусирована приемная антенна. В этой точке уже будут сложены обрезанная информация и ключ, в результате принимающая сторона имеет возможность получить часть нужной информации. После того как необходимые данные будут приняты в заданный момент времени, система перестроится для приема информации в следующей точке и в другой участок времени.

Преимуществом является то, что информационная система имеет ограниченное количество каналов. Если мы увеличиваем количество ложной информации, трасс передачи информации, частот то мы тем самым снижаем скорость передачи и упрощаем процесс по вскрытию механизма закрытия информации противной стороны.

Реализация предлагаемого метода подразумевает ряд условий:

1) Выбранные точки должны быть видны на приемной и передающей стороне одновременно.

Приемник и передатчик могут не находиться в зоне прямой видимости, но точка, в которую излучается информация, должна быть видна двум сторонам.

2) Область пространства, в которой передается информация, должна определяться сектором в заданных пределах. Например, задан конкретный сектор от антенны передающей стороны и такой же сектор с приемной стороны, их пересечением и будет определена область передачи данных. Противная сторона вынуждена будет просматривать множество точек, но, не зная, как собирается информация во времени и каким образом осуществляется переход с одной точки на

другую, возможность вскрытия будет минимальна. Это и может привести к перегрузке информационной системы злоумышленников и прекращению несанкционированного съема.

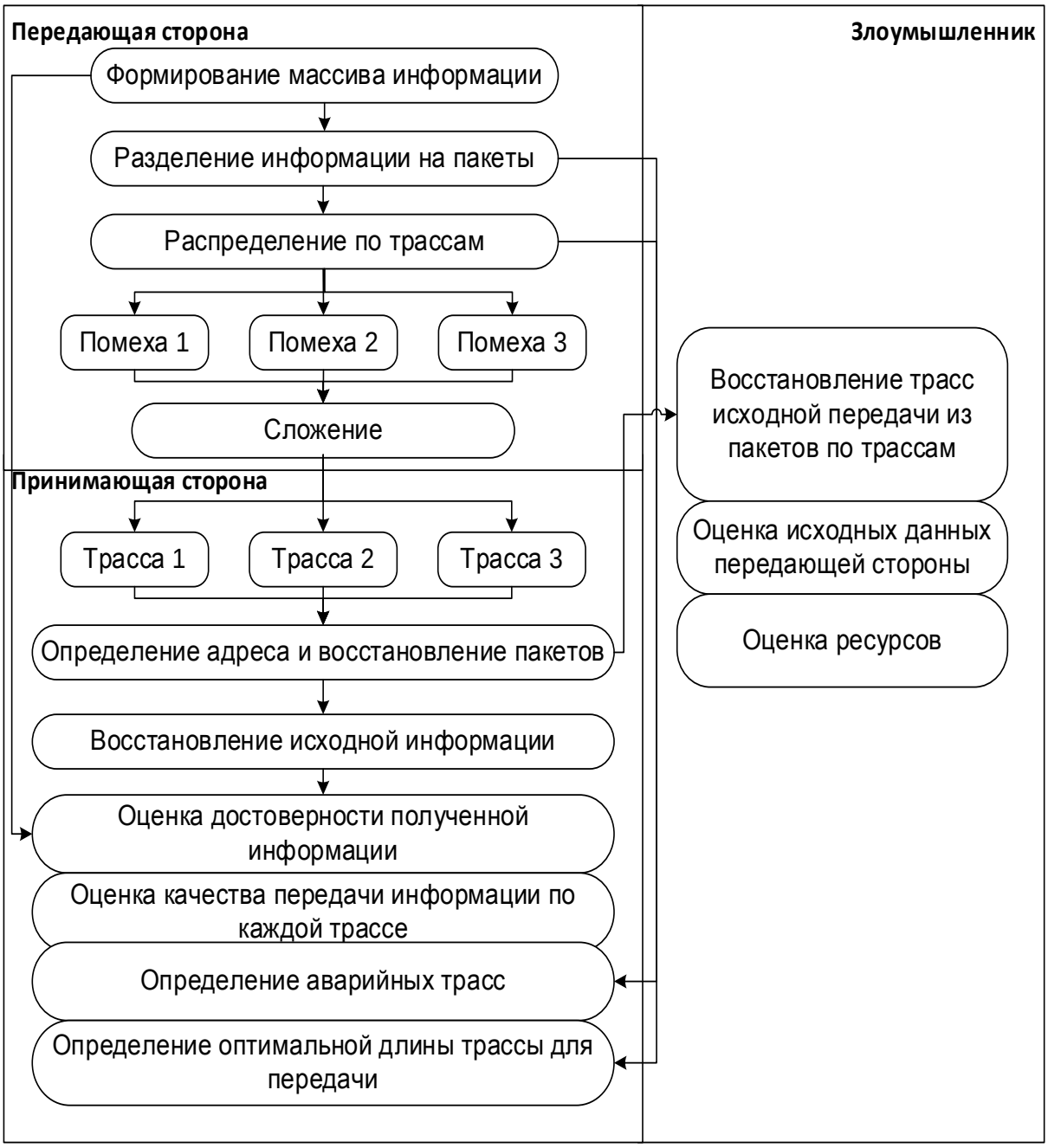

Рисунок 3 – Алгоритм работы метода

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 данного метода написана программа, визуализация представлена на рисунке 4.

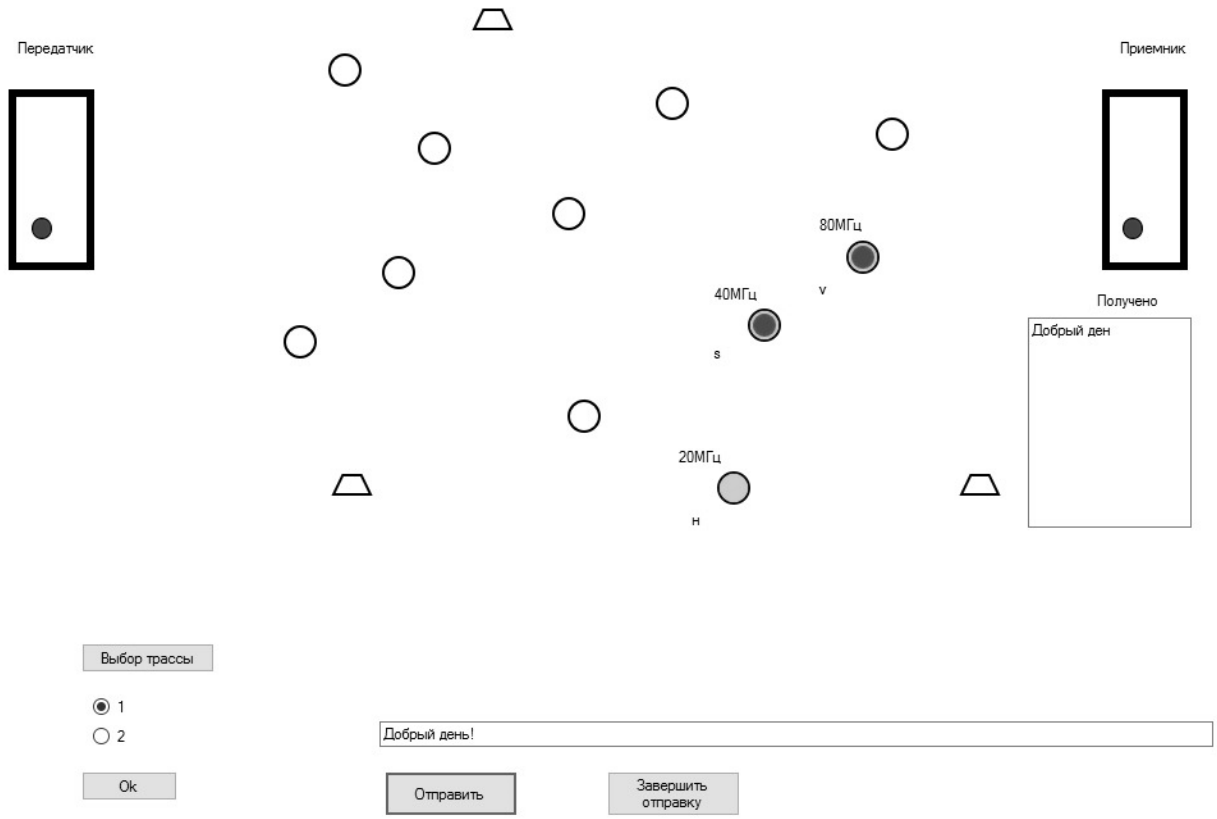

Рисунок 4 – Передача информации по первой трассе

На рисунке 5 представлен более сложный вариант передачи с использованием второй трассы.

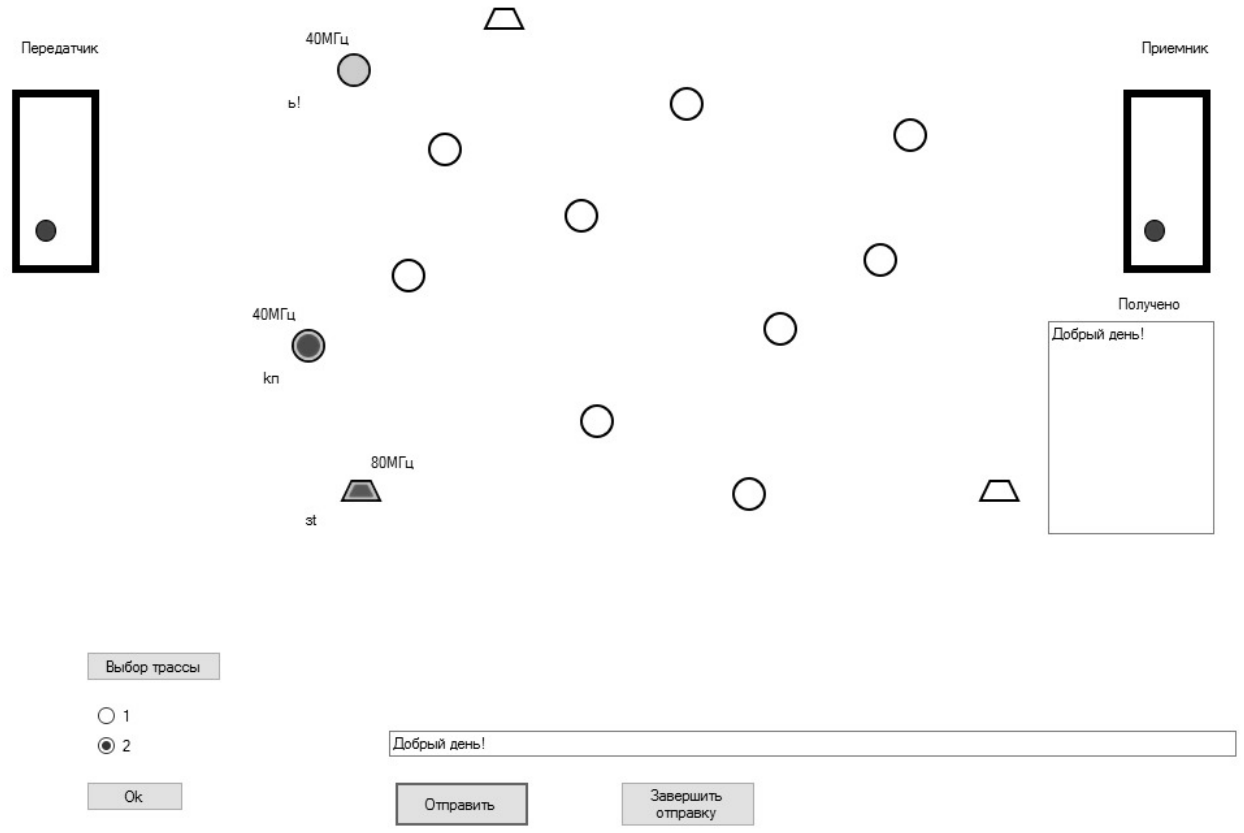

Рисунок 5 - Передача информации по второй трассе

Работая в крупной телекоммуникационный компании хочу 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», воинскиечасти, 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: Игорная зона, МВД, бизнес 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 и не позволяет станции радиоразведки восстановить информацию;
2) Для перехвата информации станции 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 смогут

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.

Итак, 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 помогло 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. Уже разработано техническое решение, в Роспатент отправлена

заявка на полезную модель. Планируется привести алгоритм работы метода в более презентабельный вид с использованием уже написанного программного кода.

Цели работы достигнуты, система позволяет повысить скрытность сообщений при доставке адресату, что снижает вероятность перехвата. Использование метода возможно для любой компании, что позволит решить следующие проблемы:

1) Запрет собственниками зданий на проведение телекоммуникаций по фасадам в бизнес центах, исторических зданиях;
2) Отдаленных объектов, нуждающихся в телекоммуникациях;
3) Доступ посторонних лиц к данным компаний.

Список использованных источников:

1. Зюко А.Г., Фалько А.И., Панфилов И.П. Помехоустойчивость и эффективность систем передачи информации// -М.Радио и связь.-1985.-с. 170-182.
2. Спутниковые технологии в обеспечении безопасности мореплавания/ С.С.Веселова, С.Н. Павликов// Вестник Морского государственного университета 2012.Вып.– с. 165.
3. Орлов В.В. Методы скрытой передачи информации в телекоммуникационных сетях: Автореф.дис. на соиск. канд. техн. наук: -2012.16с.
4. Юдин И.А. Методы защиты информации от несанкционированного доступа/ И.А. Юдин. Режим доступа: [https://elibrary.ru/item.asp?id=28310345].