УДК 614.8: 654.078
doi: 10.34987/vestnik.sibpsa.2020.18.3.010

К вопросу об обеспечении имитозащиты в системах, основанных на использовании аварийных радиобуев

Гавришев А.А.
ФГАОУ ВО Северо-Кавказский федеральный университет

Аннотация:

Рассмотрены системы, основанные на использовании аварийных радиобуев. Отмечено, что одним из их основных недостатков является доступность передаваемой информации постороннему наблюдателю. Уставлено, что для устранения указанного недостатка в известных системах применяются шумоподобные сигналы. Однако в большинстве известных работ не уделяется достаточно внимания вопросам обеспечения имитозащиты указанных систем от подмены передаваемых данных. С учетом трудов [2; 13], разработана имитозащищенная система, основанная на использовании аварийных радиобуев. Приведена структурная схема разработанной имитозащищенной системы, описан порядок ее функционирования. С помощью разработанной системы, в отличие от большинства известных систем, возможно провести идентификацию и верификацию поисковой станции для целей передачи или отказа в передаче на нее требуемой информации.

Ключевые слова: чрезвычайные ситуации, аварийный радиобуй, имитозащита, подмена передаваемых данных.

On the issue of providing imitation protection in systems based on the use of emergency beacons

A.A. Gavrishev
FSAEI HPE NCFU

Abstract:

Systems based on the use of emergency beacons are considered. It is noted that one of their main disadvantages is the availability of transmitted information to an outside observer. It is established that noise-like signals are used in known systems to eliminate this disadvantage. However, most of the well-known works do not pay enough attention to the issues of providing imitation protection of these systems from spoofing the transmitted data. Taking into account the work [2; 13], an imitation protection system based on the use of emergency beacons was developed. A block diagram of the developed imitation protection system is given, and the order of its functioning is described. The developed system, unlike most known systems, can be used to identify and verify the search station for the purpose of transmitting or refusing to transmit the required information to it.

Keywords: emergency situation, emergency beacon, imitation protection, spoofing.

Введение

В настоящее время одним из самых важных направлений построения систем обеспечения информацией о местоположении по радиоканалу между мобильным объектом и базовой станцией является развитие систем, основанных на использовании аварийных радиобуев (АР), передающих на поисковую станцию сигна-

лы о местоположении терпящих бедствие самолетов, вертолетов, кораблей, робототехнических комплексов, групп или отдельных людей, находящихся в труднодоступных и опасных районах [1-5]. Одним из основных недостатков известных систем, основанных на использовании АР, в соответствии с работами [1; 2; 4; 5], является доступность передаваемой информации между АР и поисковой станцией постороннему наблюдателю. В соответствии с работами [1; 2; 6-8] это может привести к тому, что передаваемые данные могут быть перехвачены, просмотрены, подменены или подавлены помехами, что потенциально может привести к негативным последствиям. В данной статье авторы хотят обратиться к вопросам обеспечения имитозащиты в системах, основанных на использовании АР, которые мало освещаются в известной литературе.

Целью данной статьи является разработка имитозащищенной системы, основанной на использовании АР.

Основная часть

Из литературы и списков трудов к ней известно [6-8], что защита передаваемой по радиоканалу информации от деструктивных воздействий достигается путем обеспечения энергетической скрытности сигналов-переносчиков информации, структурной скрытности передаваемых сигналов и информационной скрытности передаваемого сообщения. Известно [6-8], что энергетическая и структурная скрытность являются важнейшими характеристиками передаваемых сигналов в условиях деструктивных воздействий и в настоящее время в основном обеспечиваются использованием шумоподобных сигналов. По отношению к системам, основанным на использовании АР, в соответствии с работами [1; 2; 4; 5], активное применение находят сложные сигналы, в частности, фазоманипулированные сигналы; импульсные сигналы, основанные на применении частотного и временного уплотнения и некоторые другие. Указанные сигналы хоть и могут обеспечить необходимую энергетическую и структурную скрытность передаваемых сигналов, однако они могут быть уязвимы по отношению к деструктивным воздействиям, связанным с подменой передаваемых данных. В частности, известно [9; 10], что одним из наиболее эффективных подходов по осуществлению подмены передаваемых данных в беспроводных каналах связи является использование структурных помех, подобных полезному передаваемому радиосигналу. Таким образом, деструктивное воздействие структурных помех можно рассматривать как частный случай имитовоздействия [9; 10], то есть как подмену передаваемых сигналов. Действительно, при радиоэлектронном подавлении канала связи с помощью структурных помех, как правило, используют помехи, близкие по своей частотно-временной структуре подавляемым сигналам. При этом сам процесс такого деструктивного воздействия будет заключаться в подмене истинного сигнала помехой. За счет этого на решающем элементе демодулятора может создаваться ситуация, при которой демодулируемые символы носят или случайный характер, или же, в идеальном случае, соответствуют комбинации, навязываемой структурной помехой [9; 10]. Это потенциально может привести к негативным последствиям в условиях поисково-спасательных операций, ликвидации чрезвычайных ситуаций, решения иных специальных задач.

Для устранения указанного недостатка в некоторых системах, основанных на использовании АР, в частности в [2], предлагается использовать систему «свой-чужой», основанную на использовании идентифицирующей и верифицирующей информации (ИВИ), и блока принятия решения с дешифратором ИВИ. Общая схема функционирования указанной системы «свой-чужой», основанной на использовании ИВИ, и блока принятия решения с дешифратором ИВИ для систем, основанных на использовании АР, может быть описана в общем виде следующим образом [2; 11]:

- данные о местоположении АР передаются только в ответ на запрос;
- запрос содержит информацию, идентифицирующую конкретного инициатора запроса из числа возможных инициаторов запроса;
- запрос содержит также информацию, верифицирующую данного конкретного инициатора запроса, то есть подтверждающую его право получить требуемую информацию о местоположении;
- ответ АР инициируется, только если дается санкционирование от дешифраторов ИВИ.

Вместе с тем, в известных работах [1; 2; 4; 5], не указана конкретная реализация системы «свой-чужой» для систем, основанных на использовании АР, хотя данный вопрос представляет практический и научный интерес. В соответствии с известной литературой [12; 13] в общем виде системы «свой-чужой» реализуются с помощью добавления к передаваемому сообщению отрезков информации фиксированной длины,

называемых имитовставкой. В соответствии с работами [12; 13], в качестве имитовставки могут выступать различные криптографические преобразования, а также различные уникальные идентификаторы. Вместе с тем, криптографические преобразования могут потребовать распространения ключевой информации между удаленными объектами, а также могут быть сложны в реализации. В качестве альтернативы криптографическим преобразованиям в системах «свой-чужой» рассмотрим использование псевдослучайных последовательностей, являющихся примером уникальных идентификаторов [13].

Далее разработаем имитозащищенную систему, основанную на использовании АР. При разработке данной системы за основу возьмем систему, предложенную в работе [2]. С учетом работы [13], структурная схема имитозащищенной системы, основанной на использовании АР, выглядит следующим образом (рис.).

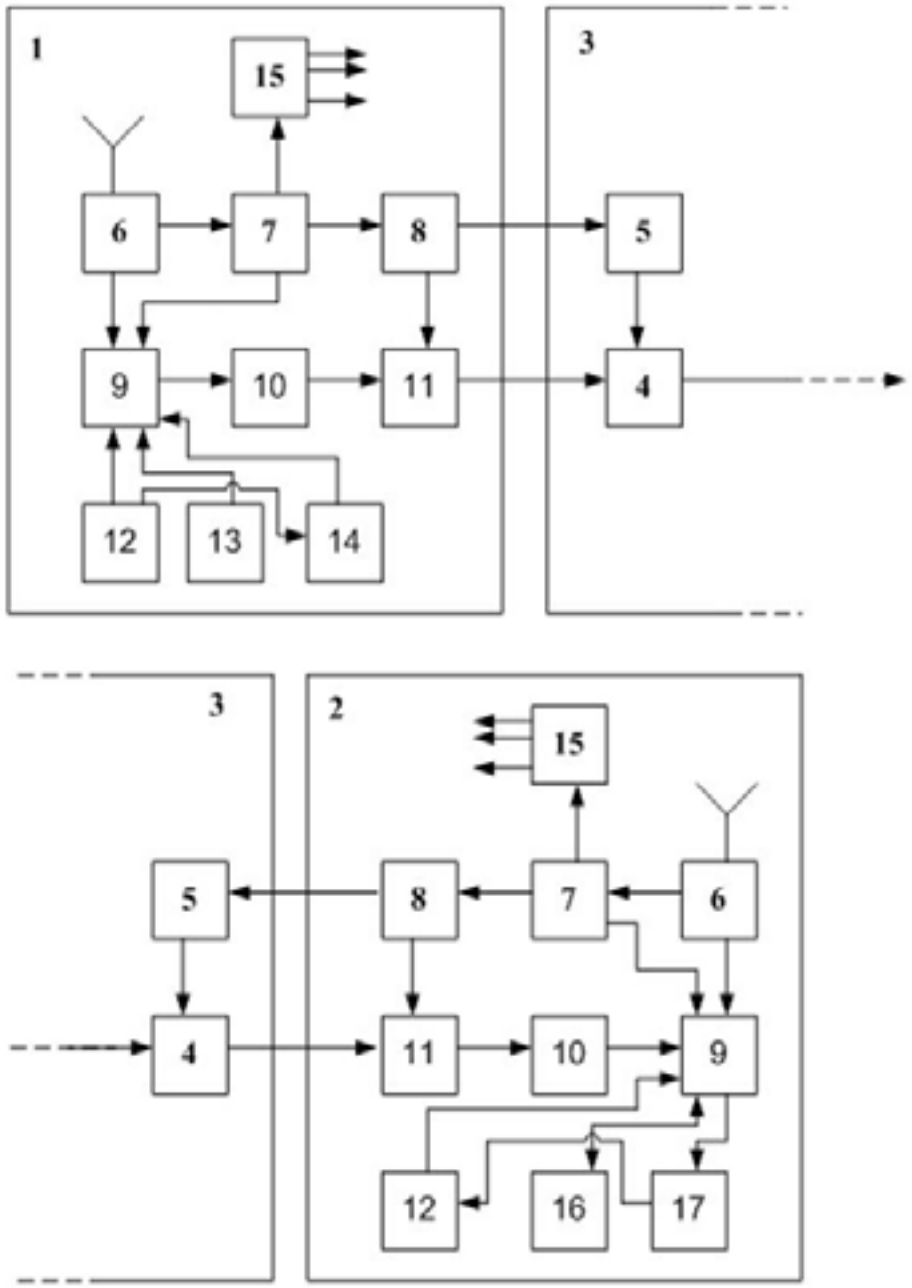

Рис. Структурная схема разработанной имитозащищенной системы, основанной на использовании АР

На рис. введены следующие обозначения: 1 – оборудование поисковой станции, 2 – оборудование радиобуя, 3 – цифровой радиоканал связи, 4 – модулятор-демодулятор, 5 – возбудитель-гетеродин, 6 – приемник спутниковой глобальной системы определения местоположения (ПСГСОМ), 7 – блок хранения регламента связи (ХРС), 8 – генератор псевдослучайной последовательности импульсов (ППИ), 9 – блок формирова-

ния сигнала запроса-принятия решения, 10 – блок временного и кодового уплотнения-восстановления, 11 – блок запоминания, 12 – генератор псевдослучайной последовательности (ПСП), 13 – постоянное запоминающее устройство (ПЗУ) уникального идентификатора поисковой станции, 14 – блок счетчика команд, 15 – блок аккумуляторного питания (АП), 16 – перезаписываемое постоянное запоминающее устройство (ППЗУ) уникальных идентификаторов поисковых станций, 17 – блок счетчика цикла псевдослучайной последовательности.

Работа представленной системы при передаче информации в одну сторону, с учетом работ [2, 13], осуществляется следующим образом. Блоки 7 ХРС на обеих сторонах радиоканала синхронизированы по сигналам точного времени, получаемым от 6 ПСГСОМ и, в соответствии с заранее заданным регламентом связи, хранящемся в указанных блоках 7, в определенное время автоматически запускают подачу питания от блоков 15 АП к ранее отключенным блокам приемного и передающего трактов, а также запускают процесс обмена данными [2]. Генератор 12 ПСП поисковой станции вырабатывает новое значение ПСП (первоначально в нем записано нулевое значение), которое передается в блок 14 счетчика команд, что приводит к увеличению значения счетчика на 1 (причем первоначально в нем установлено значение 1) [13]. После этого, в соответствии с [2], в оборудовании 1 поисковой станции сигнал от блока 9 формирования сигнала запроса, содержащий ИВИ поисковой станции (выработанная ПСП поисковой станции, значение счетчика команд и уникальный идентификатор поисковой станции, содержащийся в блоке 13), поступает в блок 10 временного и кодового уплотнения, в котором преобразуется в импульсный сигнал, «сжатый» во времени и записывается в блок 11 запоминания. Далее по сигналу от блока 7 ХРС запускается генератор 8 ППИ. Этот генератор 8 на своем стробирующем выходе в псевдослучайные моменты времени выдает стробирующие импульсы с одинаковой длительностью, которые поступают на стробирующий вход блока 11 запоминания и инициируют считывание записанного в нем сигнала. Полученный сигнал с выхода этого блока поступает на низкочастотный вход модулятора 4 радиоканала 3. На высокочастотный вход модулятора 4 поступает сигнал с выхода возбудителя 5, частота которого, в свою очередь, определяется сигналом от управляющего выхода генератора 8 ППИ. В результате, на выходе модулятора 4 радиоканала 3 формируются сложные радиосигналы, модулированные одинаковым, сжатым по длительности сигналом запроса, содержащим ИВИ поисковой станции (выработанная ПСП поисковой станции, значение счетчика команд и уникальный идентификатор поисковой станции) [2].

На другом конце радиоканала 3 в оборудовании 2 АР аналогичным образом синхронно происходит процесс демодуляции упомянутых радиосигналов с использованием демодулятора 4 и гетеродина 5, управляемого генератором 8 ППИ [2]. Генератор 8 управляется блоком 7 ХРС, синхронизируемым от 6 ПСГСОМ. Гетеродин 5 синхронно с возбудителем 5 на противоположной стороне радиоканала связи подает на гетеродинный вход демодулятора 4 известные частоты. В результате на выходе демодулятора 4 формируются импульсные сигналы, которые поступают на вход блока 11 запоминания и суммируются в нем. Полученный импульсный сигнал с выхода блока 11 запоминания на стороне приема после усиления и фильтрации поступает на вход блока 10 временного и кодового восстановления, где восстанавливается до исходной длительности и проходит далее на вход блока 9 принятия решения. Блок 9 принятия решения на основании дешифровки ИВИ поисковой станции (выработанная ПСП поисковой станции, значение счетчика команд и уникальный идентификатор поисковой станции) принимает решение о передаче или в отказе в передаче информации о местоположении аварийного радиобуя, получаемой от 6 ПСГСОМ, а так же иной важной информации (данные о государственной принадлежности объекта, его классе и индивидуальном номере, характере аварии и другие) на поисковую станцию. Для этого, блок 9 принятия решения осуществляет следующие действия [13]:

1. сравнивает уникальный идентификатор поисковой станции, пришедший по радиоканалу, с одним из уникальных идентификаторов поисковых станций, хранящимися в блоке 16 ППЗУ уникальных идентификаторов поисковых станций;
2. в случае верности пришедшего значения уникального идентификатора поисковой станции, блок 9 принятия решения переходит к сравнению пришедшей ПСП поисковой станции с ПСП, которая вырабатывается в АР; в случае неверности уникального идентификатора поисковой станции, пришедшего по радиоканалу – происходит отказ в передаче информации на поисковую станцию;

3. с помощью значения счетчика команд, пришедшего от поисковой станции, и блока 17 счетчика цикла ПСП происходит выработка ПСП АР (с учетом того, что генераторы ПСП поисковой станции и АР обладают одинаковым законом генерации ПСП, потенциально возможно проверить подлинность поисковой станции);
4. в случае верности пришедшего значения ПСП поисковой станции и выработанного ПСП в АР, блок 9 принятия решения принимает решение о передаче информации о местоположении АР, получаемой от 6 ПСГСОМ, а так же иной важной информации на поисковую станцию; в случае неверности ПСП поисковой станции, пришедшей по радиоканалу, и выработанной ПСП в АР – происходит отказ в передаче информации на поисковую станцию.

Таким образом, с помощью указанных действий возможно провести идентификацию и верификацию поисковой станции и передать или отказать в передаче на нее информации. Процесс передачи в обратном направлении (от АР на поисковую станцию) осуществляет аналогично процессу, описанному выше.

Заключение

Таким образом, в данной работе, с учетом трудов [2, 13], разработана имитозащищенная система, основанная на использовании АР, в основу которой положено использовании псевдослучайных последовательностей. С помощью разработанной системы, в отличие от большинства известных систем, в частности [1; 4; 5], возможно провести идентификацию и верификацию поисковой станции для целей передачи или отказа в передаче на нее информации о местоположении АР, получаемой от 6 ПСГСОМ, а так же иной важной информации. В условиях поисково-спасательных операций, ликвидации чрезвычайных ситуаций, решения иных специальных задач это будет способствовать повышению имитозащищенности систем, основанных на использовании АР, от деструктивных воздействий со стороны посторонних наблюдателей.

Дальнейшие исследования в данной области авторы связывают с использование в качестве шумоподобных сигналов для систем, основанных на использовании АР, хаотических сигналов, которые по различным показателям скрытности кратно превосходят известные шумоподобные сигналы [14; 15].

Литература

1. Баранов Э.В. Анализ эффективности использования шумоподобных сигналов в канале связи системы поиска и спасения // Научный вестник МГТУ ГА. Сер. Радиофизика и радиотехника. 2007. № 117. С. 71-75.
2. Гордон О.И., Пряхин Е.В. Система обеспечения информацией о местоположении // Патент РФ на полезную модель № 84655 от 10.07.2009.
3. Архангельский В.А., Белоглазова Н.Ю. Точность определения координат аварийных радиобуев по измерениям частот и времен прихода сигналов этих буев на космические аппараты среднеорбитального сегмента системы КОСПАС-САРСАТ // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10. №1. С. 62-67.
4. Заренков В.А., Заренков Д.В., Дикарев В.И., Койнаш Б.В. Аварийно-сигнальная система // Патент РФ на изобретение № 2355603 от 20.05.2009.
5. Заренков В.А., Заренков Д.В., Дикарев В.И., Койнаш Б.В. Аварийный радиобуй // Патент РФ на изобретение № 2282870 от 27.08.2006.
6. Сухарев Е.М. Общесистемные вопросы защиты информации. Коллективная монография. Кн. 1. М.: Радиотехника, 2003. 292 с.
7. Гавришев А.А. Повышение защищенности беспроводных систем безопасности: аналитический обзор публикаций // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2017. Т. 15. № 1. С. 5-14.
8. Брауде-Золотарев Ю. Алгоритмы безопасности радиоканалов//Алгоритм безопасности. 2013. № 1. С. 64-66.
9. Дворников С.В., Погорелов А.А., Вознюк М.А., Иванов Р.В. Оценка имитостойкости каналов управления с частотной модуляцией // Информация и Космос. 2016. № 1. С. 32-35.

10. Дворников С.В., Иванов Р.В. Предложения по оценке защищенности радиоканалов от структурных помех // Труды учебных заведений связи. 2016. № 2. С. 44-48.
11. Кокконен П., Мухонен Я., Игнатиус Я., Крауфвелин С. Способ обеспечения информацией о местоположении // Патент РФ на изобретение № 2316152 от 27.01.2008.
12. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии: учебный курс. 3-е изд. М: Горячая линия-Телеком, 2011. 175 с.
13. Петренко В.И., Жук А.П., Осипов Д.Л., Гавришев А.А., Некрасова Е.А. Радиоуправляемый замок с имитозащищенным обменом командами // Патент РФ на изобретение № 2710471 от 26.12.2019.
14. Сиващенко С.И. Скрытность радиосистем со сложными и хаотическими сигналами // Системи управління, навігації та зв'язку. 2009. № 3(11). С. 56-58.
15. Гавришев А.А. Сравнительный анализ хаотических сигналов и известных шумоподобных сигналов по критерию скрытности // Материалы IV МНПК, посвященной Всемирному дню гражданской обороны: Гражданская оборона на страже мира и безопасности. В 3-х частях. 2020. М.: АГПС МЧС России. С. 470-475.