УДК 621.396

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В СПУТНИКОВОЙ СИСТЕМЕ СВЯЗИ

А.М. Ткачев, А.М. Носик, А.В. Ивашкин
(представил д.т.н., проф. Ю.В. Стасев)

Проводится анализ защищенности информации в спутниковой системе связи GLOBALSTAR. Разрабатываются рекомендации по созданию национального контура защиты информации.

Создание и применение систем спутниковой связи является одним из наиболее развитых направлений практического использования космического пространства. В настоящее время создан и десятки лет эксплуатируется ряд космических систем связи как коммерческого, так и военного назначения. Опыт эксплуатации этих систем показывает, что требуемое качество их функционирования в существенной мере зависит от решения проблемы безопасности передаваемой информации. Решение проблемы безопасности информации в этих системах связывают с решением проблемы помехозащищенности, конфиденциальности и аутентичности. Многочисленные исследования показывают, что в настоящее время эти проблемы решаются раздельно. Проблема помехозащищенности решается либо за счет увеличения энергетических ресурсов спутниковой радиолинии, либо за счет применения на физическом уровне сложных сигналов. Требуемая конфиденциальность и аутентичность обеспечивается посредством преобразования дискретной информации с использованием специальной аппаратуры.

Однако в такой концепции защиты информации не реализуются потенциальные возможности спутниковых систем связи. В качестве основной составляющей глобальной информационной инфраструктуры (ГИИ) в ближайшее время планируется использовать систему персональной спутниковой связи GLOBALSTAR.

В качестве абонентов сети GLOBALSTAR могут выступать пользователи различных структур и ведомств Украины, в том числе и силовых. Передаваемая этими пользователями информация требует дополнительной защиты и использованием национальных средств. Ниже на основе анализа особенностей функционирования системы GLOBALSTAR сформулированы основные предложения по решению этих задач.

Система GLOBALSTAR предназначена для обеспечения услуг подвижным абонентам по передаче в цифровой форме речи и данных. Основными услугами, предоставляемыми системой GLOBALSTAR, являются: цифровая телефония; чередующая передача речи и данных; одновременная передачи

речи и данных; асинхронная пакетная передача данных и цифровой речи со скоростью 2.4, 4.8, 9.6 Кбит/с; передача сообщений мобильному пользователю; передача сообщений от мобильного пользователя; чередующая передача речь/факс; автоматическая факсимильная связь; определение местоположения с высоким или низким разрешением.

Передача сообщений в системе реализована кадрами и использованием канального кодирования и перемежения с последующим расширением передаваемых в канале сигналов с помощью составных сложных сигналов, сформированных на основе 64 видов последовательностей Уолша и псевдослучайными последовательностями с количеством элементов 2^{15}-1 и 2^{42}-1. Безопасность связи обеспечивается также применением процедур аутентификации и шифрования сообщений. Процедура аутентификации реализована кадрами с использованием канального кодирования и перемежения с последующим расширением передаваемых в канале сигналов с помощью составных сложных сигналов, сформированных на основе 64 видов последовательностей Уолша и псевдослучайными последовательностями с количеством элементов 2^{15} - 1 и 2^{42} - 1. Безопасность связи обеспечивается также применением процедур аутентификации и шифрования сообщений.

Процедура аутентификации, реализованная в системе, соответствует стандартам аутентификации DAMPS, EIA/TIA/S-54B. В подвижной станции хранится один ключ Ф и набор общих секретных данных, которые используются при работе как в режиме с частотным разделением каналов, так и в режиме кодового разделения (CDMA). Подвижная станция передает цифровую подпись (ЦП) для аутентификации, состоящую из 18 бит. Эта информация передается в начале сообщения (в ответе подвижной станции на запрос сети при поиске станции), добавляется к регистрационному сообщению или пакету данных, передаваемых по каналу. В системе предусматривается возможность обновления общих конфиденциальных данных в подвижных станциях.

Шифрование сообщений, передаваемых по каналу связи, осуществляется на основе стандарта IS - 54B с использованием секретной маски в виде длинного кода. Следует отметить, что реализованные в системе алгоритмы обеспечения безопасности информации на дискретном уровне в ряде случаев не удовлетворяют пользователей системы. Реализация метода кодового разделения каналов в системе GLOBALSTAR позволяет решить задачи помехозащищенности радиоканала. В качестве расширяющих спектр, в этой системе нашли применение сложные сигналы, сформированные на основе функций Уолша с числом элементов **L = 64**. Причем каждому биту или 6 битам соответствует одна и та же форма функций Уолша. Применение сложных сигналов, сформированных на основе ортогональных функций Уолша, позволяет снизить внутрисистемные помехи.

Опыт разработки и эксплуатации систем с кодовым разделением сигналов показывает [2], что качество функционирования таких систем зависит от возможностей злоумышленника по формированию структурных, имитацион-

ных и ретранслированных помех. Учитывая тот факт, что формы сложных сигналов, используемых для передачи информационных символов не изменяются во времени, злоумышленник обладает реальной возможностью сформировать структурную помеху, максимально коррелированную с полезным сигналом. Это приводит к снижению отношения энергии сигнала к спектральной плотности помехи, определяемое отношением

$$\frac{E_c}{N_0} = \left(\frac{P_c}{P_n}\right)_{вх} B(1 - R_{\delta\ max}), \qquad (1)$$

где $\left(\frac{P_c}{P_n}\right)_{вх}$ - отношение мощности сигнала к мощности помехи на входе приемного устройства;

B – база сигнала;

$R_{\delta max}$ - степень корреляции между полезным сигналом и структурной помехой и, как следствие, к снижению помехозащищенности радиоканала.

Проведенные исследования в этой области показали, что для сигналов, построенных на основе функций Уолша, существуют помеховые сигналы с $R_{\delta max}$. Подставив значение $R_{\delta max}$ в выражение (1), получим, что злоумышленник при применении стратегии подавления имеет реальную возможность подавить систему связи.

При применении стратегии имитации злоумышленник, перехватив одну из форм используемого сложного сигнала, формирует ложные сообщения и передает их в радиоканал. Даже если эти сообщения не будут восприниматься приемником как истинные, то приемные устройства сложных сигналов будут задействованы на обработку имитационных сигналов, и тем самым информационный канал будет заблокирован. Аналогичная ситуация возникает и при применении злоумышленником ретранслированных помех.

Следовательно, система GLOBALSTAR оказывается незащищенной от преднамеренных помех злоумышленников на уровне сложных сигналов.

Обеспечить требуемые значения помехозащищенности, имитостойкости и криптостойкости, как показали исследования, возможно при реализации в радиоканале режима динамической смены форм сложных сигналов, при котором соответствие “информационный символ - сложный сигнал” изменяется во времени по псевдослучайному закону [3].

Эффективность применения режима динамической смены форм сложных сигналов зависит от форм используемых сложных сигналов. Проведенные авторами исследования показали, что в системе GLOBALSTAR предпочтительнее использовать производные ортогональные сигналы, а в качестве задающих сигналов использовать функции Уолша. Такой подход к построению сложных сигналов позволит с одной стороны обеспечить совместимость защищенных абонентов с обычными абонентами системы, а с другой стороны

повысить помехозащищенность и имитостойкость системы, так как производные системы сигналов, сохраняя ортогональность в точке, имеют гораздо меньший уровень боковых лепестков функции взаимной корреляции. [4]

Таким образом, создаваемый национальный контур защиты информации обеспечивает: подлинность и целостность информации и сообщений, циркулирующих в системе; конфиденциальность информации и сообщений; идентификацию абонентов и субъектов системы, и от НСД со стороны как санкционированных, так и несанкционированных пользователей; управление ключевыми структурами в национальном контуре защиты информации.

Анализ структуры и особенностей функционирования системы GLOBALSTAR показал, что применяемые в системе методы обеспечения безопасности информации в ряде случаев не удовлетворяют некоторых пользователей системы.

С целью обеспечения национальных интересов в части информационной безопасности в системе GLOBALSTAR предлагается создание дополнительного контура защиты информации. Создаваемый национальный контур защиты информации должен прозрачно интегрироваться в систему спутниковой связи и не ухудшать основные характеристики системы.

Реализация режима динамической смены форм позволяет на уровне сложных сигналов решить проблему защиты от несанкционированного доступа к каналам, а также обеспечить скрытие смыслового содержания передаваемых сообщений. Кроме того, реализация режима динамической смены форм сигналов обеспечивает активную имитозащиту и помехозащиту системы – защиту, при которой имитационные сигналы воспринимаются получателем информации как внутрисистемные помехи.

ЛИТЕРАТУРА

1. Горбенко И.Д., Стасев Ю.В. //Радиотехника.-1989.-№9.-С.16-18.

2. Варакин Л.Е. Теория систем сигналов. - М.: Сов. Радио, 1978. – 304 с.

3. Горбенко И.Д., Стасев Ю.В. Безопасность информации в космических системах связи и управления .// Космічна наука і технологія.-1996.-Т2. - № 5 - 6.-С.64 - 68.

4. Стасев Ю.В., Пастухов Н.В. Алгоритм синтеза и свойства ортогональніх систем сигналов // Космічна наука і технологія. -1996.- Т2. - №5 - 6.-С.69 - 73.