КОСМОНАВТИКА

УДК 629.7.051

**[1]С. П. Панько, [1]В. В. Сухотин, [1]А. В. Мишуров, [1]В. В. Евстратько, [1]А. А. Горчаковский, [1]Г. П. Килин, [2]С. А. Рябушкин, [2]А. И. Вильданов, [2] В. А. Шатров**

[1]*Сибирский федеральный университет, г. Красноярск, Россия*
[2]*АО «Информационные спутниковые системы» им. акад. М. Ф. Решетнёва», г. Железногорск, Красноярский край, Россия*

# ЗАЩИТА КОМАНДНОГО КАНАЛА СИСТЕМЫ УПРАВЛЕНИЯ КОСМИЧЕСКИМ АППАРАТОМ

*Рассматривается задача защиты канала передачи с наземного комплекса управления команд, управляющих подсистемами, узлами и блоками космического аппарата. Злоумышленное вмешательство в работу командной радиолинии может привести к тяжелым последствиям, вплоть до потери космического аппарата. Известные способы защиты не дают гарантии существенного уменьшения вероятности несанкционированного вмешательства в командный канал.*

*Ключевые слова: космический аппарат, команды управления, защита командной линии, координаты.*

**[1]S. P. Panko, [1]V. V. Sukhotin, [1]A. V. Mishurov, [1]V. V. Evstratko, [1]A. A. Gorchakovskii, [1]G. P. Kilin, [2]S. A. Ryabushkin, [2]A. I. Vildanov, [2]V. A. Shatrov**

[1]*Siberian Federal University, Krasnoyarsk, Russian Federation*
[2]*JCS «Academician M. F. Reshetnev» Information satellite systems», Zheleznogorsk, Russian Federation*

# PROTECTION OF THE COMMAND CHANNEL CONTROL SYSTEM OF A SPACECRAFT

*This paper considers the problem of protection of the transmission channel with Ground Control System commands that control the subsystems, components and blocks of the spacecraft. Malicious interference in the radio command link could lead to serious consequences, including the loss of the spacecraft. Known methods of protection do not guarantee significantly reduce the possibility of unauthorized interference in the command channel.*

*Key words: spacecraft, command, protection of command line, coordinates.*

Командно-измерительная система космического аппарата (КИС КА) обеспечивает прием от наземного комплекса управления (НКУ) командной информации, передачу на НКУ телеметрической информации о параметрах КА и поддерживает траекторные измерения. Составной частью КИС КА является двунаправленная радиолиния связи «Земля – космический аппарат», зона покрытия которой может занимать весьма значительную площадь. Наземная станция, с помощью которой нелегитимные пользователи умышленно или непреднамеренно имеют принципиальную возможность вмешательства, может быть рас-

положена в любой точке этой площади, в том числе вне пределов границ государственной территории. Поэтому защита КИС КА преследует цель снижения риска несанкционированного вмешательства, которое может быть осуществлено радиотехническими средствами злоумышленника и потенциально может привести к тяжелым последствиям, вплоть до утраты космического аппарата.

Один из наиболее распространенных способов защиты от несанкционированного вмешательства состоит в передаче пользователем уникальных пароля и логина, сопоставлении принятых пароля и логина с хранимыми в бортовой аппаратуре КИС КА и принятии решения на основании этого сопоставления о разрешении доступа пользователя к управленческим ресурсам бортовой аппаратуры КИС КА. Эта процедура широко распространена и называется процедурой аутентификации [1]. Недостаток этой процедуры состоит в том, что невозможно гарантированное исключение несанкционированного вмешательства в канал передачи команд управления КА.

В процессе передачи информации с криптозащитой по линии связи широко используются синхропоследовательности с большим периодом повторения (год и более). Шифрование синхропоследовательности производят с использованием заранее установленного ключа и перемножения по модулю 2 зашифрованной синхропоследовательности и исходного сообщения [2]. Недостаток способа состоит в принципиальной возможности вскрытия процедуры шифрования и нанесения вреда работе КА путем искажения командной информации. Кроме того, возможна постановка помех нелегитимным пользователем, в результате действия которых возможно деструктивное влияние на работу КА на фоне невозможности оперативного обнаружения факта постановки помех и определения координат постановщика помех.

В [3] описана спутниковая система, включающая в себя систему связи с использованием КА, в которой коммуникационная система (далее – командно-измерительная система) настроена для получения командной информации от наземного комплекса управления и передачи телеметрической информации от КА к наземному комплексу управления, и некоторое количество компьютеров, связанных с космическим аппаратом. Компьютеры настроены для определения блока информации и для шифрования инструкций в командной информации, генерирования ключа для части блока информации на основе инструкций, выполнения операции исключающее ИЛИ, на блоке информации с помощью ключа, чтобы сформировать и передать блок зашифрованных данных.

Кодирование (засекречивание) передаваемой информации производится с целью обеспечения скрытности содержательной её части. Но вскрытие кодированной (засекреченной) информации зачастую является принципиально возможным. Эти обстоятельства актуализируют задачу защиты канала передачи команд на КА от НКУ.

Защита командной линии управления КА может быть обеспечена блокированием команд, полученных от нелегитимного пользователя, на основе сопоставления координат источника принимаемого сигнала с координатами НКУ.

На рис. 1 приведен один из вариантов структурной схемы устройства для реализации предлагаемого способа защиты командного сигнала и, как следствие, КИС КА [4].

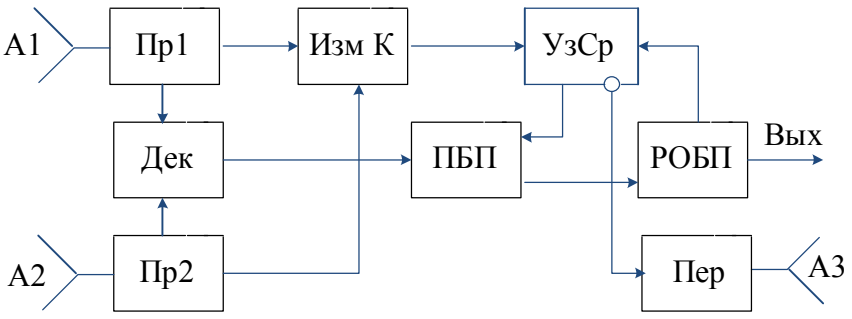


Рис. 1. Структурная схема устройства защиты командного канала

Прием сигналов любого (легитимного или нелегитимного) пользователя обеспечивается с помощью двух приемных антенн А1, А2 и двух приемников Пр1, Пр2. Сигналы с выходов приемников поступают на блок измерения координат Изм К и на декодер Дек командно-программной информации. На основе разности фаз между принимаемыми сигналами в блоке измерения координат определяются координаты источника сигналов. Фронт волны, поступающий на приемные антенны, несет информацию о координатах источника сигнала. В первом приближении для двух приемных антенн линией положения на поверхности Земли явится кривая, образованная сечением поверхности Земли вертикальной плоскостью, делящей пополам базовое расстояние между приемными антеннами, и к которой принадлежит радиус-вектор КА, направленный в центр Земли. Поэтому для передающего средства (источника сигнала), расположенного в любой точке этой кривой на поверхности Земли, разность фаз между принятыми антеннами сигналами будет близка к нулю. Для всех других расположений источника сигналов разность фаз между сигналами, принимаемыми антеннами, будет отличной от нуля. Это является основой отличия координат нелегитимного пользователя от координат НКУ, которые закладываются в рабочую область бортовой памяти РОБП в процессе предстартовой подготовки. Сопоставление измеренных и координат НКУ обеспечивается в узле сравнения УзСр. В это же время выделенные команды с выхода декодера командно-программной информации Дек поступают в промежуточную бортовую память ПБП. После того, как сравнение координат источника и НКУ оказалось успешным (т.е. источник является легитимным), принимается решение о переносе выделенных команд из промежуточной бортовой памяти ПБП в рабочую область бортовой памяти РОБП с целью последующего исполнения. В случае несовпадения координат на вход передатчика Пер поступает сигнал информационной атаки на КА, который через передающую антенну А3 передается в НКУ совместно с координатами нелегитимного пользователя.

Таким образом, нелегитимный пользователь существенно ограничен в выборе места для размещения станции – постановщика помех, что существенно снижает вероятность несанкционированного вмешательства в работу командно-измерительной системы КА.

Возможна реализация описанной технологии с тремя приемными антеннами. При этом третья приемная антенна образует с одной из первых двух приемных антенн вторую базу, размещенную под прямым углом относительно базы, образованной антеннами А1 и А2. Такая конфигурация антенн позволит измерять две координаты источника сигнала, расположенного в любой точке освещаемого пространства с КА. Если использовать еще одну приемную антенну, расположенную в плоскости, перпендикулярной плоскости расположения первых двух баз, образованных тремя антеннами, то конфигурация антенн позволит измерять три координаты нелегитимного источника (в том числе высоту), если он расположен на борту другого летательного аппарата или другого КА.

Отсюда следует, что факт атаки на КА будет обнаружен при расположении передатчика нелегитимного пользователя в любой точке окружающего пространства. Таким образом, путем оценки координат источника сигнала и принятия решения о легитимности пользователя (при близком совпадении координат источника сигнала с хранимыми в рабочей области бортовой памяти космического аппарата) и блокирования команд, полученных от нелегитимного пользователя, решается задача защиты командной линии космического аппарата, в частности, исключения несанкционированного доступа нелегитимных пользователей к командно-измерительной системе КА.

## Библиографические ссылки

1. The Consultative Committee for Space Data System. Draft Recommendation for Space Data System Standards. Space data link security protocol. Draft recommended standard CCSDS 355.0-R-2. Красная книга, февраль 2012.
2. http://library.tuit.uz/skanir_knigi/book/telekommunikacionnie_sistemi/glava_2.htm.
3. Blanchard D. L. Selective Downlink Data Encryption System for Satellites. US 20130077788. March 28, 2013.
4. Способ защиты командно-измерительной системы космического аппарата : пат. № 2554090 Рос. Федерация / Панько С. П., Сухотин В. В., Мишуров А. В., Евстратько В. В., Горчаковский А. А., Килин Г. П., Рябушкин С. А., Вильданов А. И., Шатров В. А. Опубл. 27.06.2015.

*Статья поступила в редакцию 16.10.2015 г.*