КРАТКИЕ СООБЩЕНИЯ

ЛОКАЦИЯ И НАВИГАЦИЯ

УДК 629.78: 004.056.5

УЯЗВИМОСТЬ СПУТНИКОВЫХ ТЕХНОЛОГИЙ

А.В. МИШУРОВ, С.П. ПАНЬКО, С.А. РЯБУШКИН, В.В. СУХОТИН, В.А. ШАТРОВ

В статье рассмотрены возможные варианты уязвимости спутниковых технологий на современном уровне развития техники в результате действий злоумышленников. Обращается внимание на возможный международный характер деструктивной деятельности, способной нарушить работу спутниковых систем, вплоть до потери космического аппарата. Проводится анализ технической деятельности злоумышленников и рассматриваются методы противодействия.

Ключевые слова: спутниковые технологии, космический аппарат, кибератаки, защита информации, частотный ресурс ретранслятора, хакер.

ВВЕДЕНИЕ

Спутниковые технологии и системы давно стали неотъемлемой частью информационной структуры как отдельных стран, так и мирового сообщества в целом. Интеграция спутниковых коммуникаций в бизнес, образование, системы национальной безопасности и реагирования на чрезвычайные ситуации непрерывно развивается. Спутниковые технологии передачи информации и связи, наблюдения покровов Земли, контроля погоды, а также спутниковой навигации являются важнейшими компонентами современного информационного пространства.

Передача команд на исполнительные приборы и системы Космического Аппарата (КА), а также контроль состояния КА осуществляются персоналом Наземного Комплекса Управления (НКУ) в автоматическом, либо ручном режимах с помощью двух радиолиний: up link для передачи команд и полетных заданий на борт КА и down link для передачи телеметрии с борта КА в НКУ независимо от функционального назначения КА. Телеметрическая информация о состоянии бортовых систем и приборов и выполняемых ими функций являются единственным источником информации, позволяющим персоналу НКУ достаточно адекватно оценить работоспособность КА.

Большинство опубликованных исследований по Satellite Telemetry, Tracking and Control Subsystems [1..10] посвящено процедурам анализа потока телеметрических данных с позиций возможно более раннего распознавания аномального поведения узлов и систем КА. Наиболее распространенным способом прогноза является процедура Out-Of-Limits (OOL), при которой значение параметра сопоставляется с двумя порогами – верхним и нижним. Если значение параметра выходит за пределы, то это должно явиться поводом к пристальному вниманию персонала к этому событию. Нарушение деятельности КА возможно как в результате непреднамеренных помех, так и и в случае активных действий. Привлекательность мишени для кибератак со стороны хакеров – злоумышленников, преступников, террористов приводит к необходимости анализа уязвимости спутниковых технологий и систем. Поэтому необходима классификация помех естественного и умышленного происхождения спутниковым технологиям и разработка методов уменьшения их влияния на выполнение функциональной задачи КА.

Задача, так или иначе, рассматривалась в зарубежной и отечественной научно-технической литературе, начиная примерно с последней декады 20 века [2], однако это относилось исключительно к пиратскому захвату ресурсов телекоммуникационного КА. Проблема помехозащищенности и надежности командного управления, сбора и передачи телеметрической информации КА существует на протяжении всей эпохи становления и развития отрасли [6]. В настоящее время спектр возможных злоумышленных действий относительно КА значительно расширился. К ним можно отнести следующие.

ПИРАТСКИЙ ЗАХВАТ ЧАСТОТНОГО РЕСУРСА ТЕЛЕКОММУНИКАЦИОННОГО КОСМИЧЕСКОГО АППАРАТА

Пятно, покрываемое радиосигналом коммуникационного КА, зафиксированного на геостационарной орбите в точке стояния 80^0 вост. долготы, занимает площадь от Берлина до Камчатки и от Таймыра до Юго-Восточной Азии, включая Ближний Восток и Японию. Злоумышленники ориентируют свои Земные станции (ЗС) на те-

лекоммуникационный геостационарный КА и излучают свой сигнал, как правило, более мощный, чем легитимные пользователи, не обращая внимания на занятость частотного ресурса [12]. Владелец КА терпит двойные убытки, поскольку легитимный пользователь не имеет возможности воспользоваться телекоммуникационной услугой, а злоумышленник не оплачивает аренду ресурса КА, пользуясь безнаказанностью. Для такой деятельности хакеру необходимо соответствующее оборудование, но современные технические возможности делают эту задачу тривиальной. Одним из решений этой задачи является определение координат мешающей ЗС с целью принятия управленческих мер внутреннего, либо международного характера.

Теоретические основы определения координат месторасположения пиратской ЗС проработаны в [7] на основе методики фазовой пеленгации и основаны на использовании виртуальной антенной решетки. Это достигается при учете естественных признаков, поскольку геостационарный КА движется по эллиптической орбите с малой эллиптичностью и в плоскости, несколько смещенной относительно плоскости экватора.

АТАКА НА КОСМИЧЕСКИЙ АППАРАТ ИЛИ НАЗЕМНЫЙ КОМПЛЕКС УПРАВЛЕНИЯ

Цель — физическое уничтожение. В доступной печати подобные акты не описывались, кроме как случайное столкновение разных КА [13].

УПРАВЛЕНИЕ КОНФИГУРАЦИЕЙ И ФУНКЦИЯМИ КА

Осуществление возможно путем имитации хакером командной линии и передачи по ней ложных директив, направленных на изменение функций КА и/или его ориентации. Действия могут привести к катастрофическим последствиям, вплоть до потери КА. В настоящее время единственной методикой защиты командной и телеметрической линий является использование кодирующего (скрывающего) преобразования информации и использование процедуры аутентификации [9–11]. Очевидно, что эти методики обладают конечной глубиной защиты командного сигнала от постороннего вмешательства и необходим поиск других признаков, позволяющих повысить качество защиты. К таким может относиться упомянутое выше [7] определение координат источника сигнала средствами, размещенными на борту КА, и игнорирование сигнала, если координаты его источника отличны от разрешенных и хранимых в бортовой памяти КА.

ПЕРЕХВАТ И ДЕШИФРИРОВАНИЕ СИГНАЛА

Цель состоит во вскрытии функционального потока передаваемой информации, что особенно актуально при использовании спутникового сегмента в линиях передачи закрытой информации. Единственным средством защиты этого канала является использование специальных технологий закрывающего кодирования.

ИСКАЖЕНИЕ ТЕЛЕМЕТРИЧЕСКОГО СИГНАЛА

Данный вид злоумышленных действий производится с целью вызова неадекватной реакции обслуживающего персонала НКУ. Задача защиты телеметрического канала до настоящего времени не ставилась в опубликованных источниках, несмотря на ее важность, поскольку действия персонала, основанные на неадекватной информации, могут привести к серьезным последствиям. Постановка искажающих помех возможна при использовании многолучевого распространения путем ретрансляции телеметрического сигнала с помощью средств аэрокосмического базирования. В [4] рассмотрены вопросы борьбы с влиянием многолучевого распространения применительно к спутниковым технологиям.

Справедливости ради следует отметить, что на семинаре Стэнфордского университета в октябре 2007 г. [8] было предложено решение проблемы защиты спутниковых технологий от вмешательства путем многоуровневой группировки микроспутников, т.е. введения избыточности в слой передачи информации. В [11] предложено обеспечивать защиту путем анализа амплитудно-фазового спектра принимаемого сигнала, что при полной имитации сигнала не имеет смысла.

ЗАКЛЮЧЕНИЕ

Проблема защищенности спутниковых технологий, справедливо относимых к критическим [5], должна стать предметом специальных исследований с целью разработки методик, техники и технологий эффективной борьбы с деятельностью злоумышленников в этой сфере. Важно подчеркнуть необходимость международного сотрудничества в этой сфере.

Признание

Работа выполнена при финансовой поддержке Минобрнауки России в Сибирском федеральном университете и ОАО «Информационные спутниковые системы» имени академика М.Ф. Решетнёва» (Договор № 02.G25.31.0041

Литература

[1] *J. Heras, A. Donati.* Method and apparatus for monitoring an operational state of a system on the basis of telemetry data. ESA Patent 572, 2013.

[2] *В. Колюбакин В.* Конференция в Дубне. ТЕЛЕСпутник, май, 1999. – С.40

[3] *B. Lewis.* The Nature of Thread to Satellite Information Assurance. http://www.intelsatgeneral.com/blog. May 8, 2013.

[4] *M.Z. Bhuiyan, E.S. Lohan.* Advanced Multipath Mitigation Techniques for Satellite-Based Positioning Applications. International Journal of Navigation and Observation. V.2010 (2010), Article ID 412393. Tampere University of Technology.

[5] Don Wilcoxson. Advanced Commercial Satellite Systems Technology for Protected Communications. The 2011 Military Communications Conference, Track 6. Department of Defense Programs.

[6] R.C. Jr, Chapman, G.F.; Critchlow, H. Mann. Command and Telemetry Systems. BSTJ 42: 4. July 1963.

[7] *С.П. Панько, В.В. Сухотин*. Определение координат земных передатчиков в спутниковой связи. Журнал «Радиотехника» № 10, 2005 г.

[8] http://cisac.stanford.edu/events

[9] C. J. Keesee. Satellite Telemetry, Tracking and Control Subsystems. Massachusetts Institute of Technology. 2003.

[10] D. Blanchard, et al. Selective Downlink Data Encryption System for Satellite. US Patent Appl. 20130077788, March, 2013.

[11] H. Rosen. Satellite command link protection system. US Pat 4612546, 1986.

[12] L. Francis, K.M. Sirett, K. Mayes, K Markantonakis. Countermeasures for Attacks on Satellite TV Cards using Open Receivers. In Proc. Third Australasian Information Security Workshop (AISW 2005), Newcastle, Australia. CRPIT, 44. Safavi-Naini, R., Montague, P. and Sheppard, N., Eds. ACS. 153-158.

[13] http://interfax.ru/news.asp?id=62662

Поступила в редколлегию 29.08.2013

Мишуров Андрей Валериевич, аспирант кафедры «Радиоэлектронные системы» Сибирского федерального университета. Научные интересы: телеметрические системы, телекоммуникации, спутниковые системы, приборостроение.

Панько Сергей Петрович, доктор технических наук, профессор кафедры «Радиоэлектронные системы» Сибирского федерального университета. Научные интересы: космические технологии, передача информации, медицинское приборостроение.

Рябушкин Станислав Анатольевич, начальник отдела проектирования и испытаний аппаратуры БКУ КА ОАО «Информационные спутниковые системы». Научные интересы: командно-измерительные системы, системы контроля и управления, спутниковые технологии.

Сухотин Виталий Владимирович, канд. техн. наук, доцент кафедры «Радиоэлектронные системы» Сибирского федерального университета. Научные интересы: радиодальнометрия, радиопеленгация, информационная безопасность, спутниковые системы.

Шатров Виталий Альбертович, инженер-конструктор, ОАО «Информационные спутниковые системы». Научные интересы: телекоммуникации, радиоэлектронные системы, повышение точности и помехоустойчивости передачи РТ сигналов.

УДК 629.78: 004.056.5

Уразливість супутникових технологій / А.В. Мішуров, С.П. Панько, С.А. Рябушкін, В.В. Сухотін, В.А. Шатров // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 3. – С. 471–473.

У статті розглянуто можливі варіанти уразливості супутникових технологій на сучасному рівні розвитку техніки в результаті дій зловмисників. Звертається увага на можливий міжнародний характер деструктивної діяльності, здатної порушити роботу супутникових систем, аж до втрати космічного апарату. Проводиться аналіз технічної діяльності зловмисників і розглядаються методи протидії.

Ключові слова: супутникові технології, космічний апарат, кібератаки, захист інформації, частотний ресурс ретранслятора, хакер.

Бібліогр.: 13 найм.

UDC 629.78: 004.056.5

Vulnerability of satellite technologies / A.V. Mishurov, S.P. Pan'ko, S.A. Ryabushkin, V.V. Suhotin, V.A. Shatrov // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 3 – P. 471–473.

The paper considers possible variants of vulnerability of satellite technologies at the modern level of technology as a result of intruders' actions. Attention is paid to a possible international character of destructive activities capable of disturbing the operation of satellite systems, up to the loss of a spacecraft. The analysis of the technical activities of criminals is done and methods of counteraction is done.

Keywords: satellite technologies, spacecraft, cyber attacks, information security, transponder frequency resource, attacker.

Ref.:13 items.