М. Ю. Сенаторов, Р. Б. Сятковский

О БЕЗОПАСНОСТИ ГЛОБАЛЬНОЙ НАВИГАЦИОННОЙ СПУТНИКОВОЙ СИСТЕМЫ ГЛОНАСС

Постановлением Правительства РФ от 12 сентября 2008 г. № 680 утверждена новая редакция Федеральной целевой программы «Глобальная навигационная система», основными целями которой являются:

- дальнейшее развитие и эффективное использование глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития страны, обеспечения национальной безопасности;
- сохранение Россией лидирующих позиций в области спутниковой навигации за счет гарантированного предоставления навигационных сигналов отечественным и зарубежным потребителям [1].

В результате осуществления программы был выполнен комплекс мер по развитию системы ГЛОНАСС и, в частности, по восполнению орбитальной группировки: по данным Федерального космического агентства, по состоянию на 13.10.2010 в орбитальной группировке ГЛОНАСС находилось 26 спутников: 21 космический аппарат использовался по целевому назначению; 3 временно выведены на техобслуживание; 2 — в орбитальном резерве. Такая группировка обеспечивает 100-процентную доступность услуг системы на всей территории России и практически на всей поверхности Земли ((PDOP1)<6, максимальный перерыв в навигации — 0,2 часа) [2]. В данном случае доступность оценивается как вероятность получения потребителем навигационной информации в заданный интервал времени с требуемой точностью.

До конца нынешнего года планируется вывести на орбиту еще четыре навигационных спутника: три типа «ГЛОНАСС-М» и один — нового поколения типа «ГЛОНАСС-К» [2].

Таким образом, будет обеспечена 100-процентная доступность услуг системы ГЛОНАСС по всей поверхности Земли и достигнуты условия для конкуренции с американской GPS.

Но, кроме доступности системы, не менее важной характеристикой является достоверность передаваемой навигационной информации, определяемая целостностью системы, т. е. способностью выдавать потребителю своевременное и достоверное предупреждение в тех случаях, когда какие-либо сигналы нельзя использовать по целевому назначению в полном объеме. Очевидно, что, по сути, это является идентификацией угрозы нарушения информационной безопасности глобальной навигационной спутниковой системы (ГНСС). Несвоевременное исключение неверной информации, излучаемой спутником, может привести к значительному снижению точности навигационных определений потребителя вплоть до неверного определения местоположения.

В настоящее время требованиям по целостности не соответствует ни одна из существующих глобальных навигационных спутниковых систем — ни ГЛОНАСС (Россия), ни GPS (США), так как время обнаружения неисправного космического аппарата в системе ГЛОНАСС может достигать 16 часов (обусловлено размещением наземных станций слежения только на территории Российской Федерации), а в системе GPS — около 1—4 часов.

Ключевыми угрозами безопасности для ГЛОНАСС являются программные угрозы, так как они влияют на закладываемую в бортовую аппаратуру (БА) спутников и впоследствии излучаемую ими навигационную информацию.

Удаленное воздействие на закладываемые эфемериды практически исключено, это обусловлено повышенными организационными мерами.

При локальном доступе на программном уровне к программному обеспечению, формирующему и закладывающему навигационную информацию в БА спутников, нарушитель может осуществить

угрозу только на ресурс, при этом на ресурсе располагаются следующие компоненты: операционная система, прикладное программное обеспечение, а также сама ценная информация, хранящаяся и обрабатываемая на ресурсе. Нарушение функционирования, целостности или конфиденциальности любого из этих элементов может привести к потере ценной информации — навигационной информации.

Для контроля программных угроз от локального нарушителя предлагается использовать метод орбитального мониторинга инцидентов по вине оператора системы ГЛОНАСС.

Суть предлагаемого метода орбитального мониторинга заключается в следующем: на борту каждого космического аппарата ГЛОНАСС устанавливается комплект навигационной аппаратуры потребителей (НАП). Она принимает сигналы от других спутников системы, в область диаграммы направленности которых попадает данный космический аппарат. Принимая штатный сигнал, на борту аппарата с помощью НАП можно измерить псевдодальность до источника излучения по временной задержке прохождения сигнала. Кроме того, в состав штатного сигнала входит информация о координатах излучившего его спутника (эфемериды). По принятым и известным собственным координатам космического аппарата можно рассчитать еще одно значение псевдодальности до источника сигналов. Определив разность между измеренным и рассчитанным значениями псевдодальности и сравнив ее со значением предельно допустимой погрешности, можно сделать вывод о достоверности излучаемой информации.

Для реализации данного метода необходима некоторая модификация передающего и антенного устройства бортовой аппаратуры всех спутников системы, а также установка на борту каждого космического аппарата многоканальной НАП, что возможно осуществить при дальнейшем развитии космических аппаратов «ГЛОНАСС». Необходимо отметить, что данная модификация БА навигационных спутников имеет также положительный «побочный эффект» — навигационное поле ГНСС «ГЛОНАСС» станет доступным низкоорбитальным космическим аппаратам, в том числе и пилотируемым, что будет неоспоримым конкурентным преимуществом перед американской GPS.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральная целевая программа. ГЛОНАСС/ГНСС-Форум. URL: http://aggf.ru/proekt/zakon/doc.php?zakID=2.
2. Федеральное космическое агентство. Информационно-аналитический центр. URL: http://www.federalspace.ru/main.php?id=3&nid=13077.

Е. С. Степанова, И. В. Кансафаров

ПРОГРАММНЫЙ МОДУЛЬ РЕАЛИЗАЦИИ АЛГОРИТМА ЧИСЛЕННОЙ ОЦЕНКИ РИСКА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Повышение эффективности систем защиты информации (СЗИ) обусловливает необходимость разработки методического обеспечения, затрагивающего вопросы анализа рисков нарушения информационной безопасности.

На основе модели угроз в виде нечеткой когнитивной карты [1] разработаны метод и алгоритм оценивания риска нарушения ИБ, сущность которого сводится к следующему:

1. На основе политики безопасности, принятой в организации, с учетом категорирования информационных ресурсов, обрабатываемых в сегментах сети организации, строится матрица разграничения прав доступа;