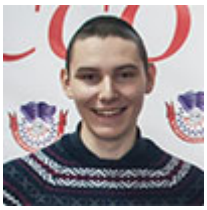
Молодые учёные СФУ разработали защищённую систему передачи данных для спутников

Группа учёных Института космических и информационных технологий СФУ предложила нестандартное решение задачи, связанной с обеспечением безопасности космических объектов. Разработаны защищённая система передачи данных по спутниковому каналу связи и собственное программное обеспечение.

Предложенное программное обеспечение поможет отражать атаки злоумышленника, нацеленные на подмену сведений о времени и геолокации, и будет в дальнейшем использоваться организациями, которые получат соответствующую лицензию. Система разработана в рамках производственной практики на базе ведущего предприятия России по созданию космических аппаратов связи, телевещания, ретрансляции, навигации, геодезии «Информационные спутниковые системы имени академика М. Ф. Решетнёва».

Основными типами атак на спутниковую связь являются глушение и спуфинг (*Spoofing — подмена объекта или субъекта с целью получения несанкционированных преимуществ*) — в последнем случае происходит опасная подмена данных о текущем времени и геолокации. Учёные разрабатывают всё новые методы борьбы с этим типом атак, выполняя определённый набор действий.

Анализируется режим функционирования действующей системы; выбирается наиболее подходящий метод защиты, учитывая специфику системы; разрабатывается промышленный образец и программное обеспечение для него, а после характеристики получившегося программного обеспечения сравниваются с ожидаемыми. Собственно, если новый метод получится пригодным к применению, то этап внедрения продолжится, будут анализироваться и устраняться недостатки полученного метода.



> *«Разработка ПО для бортового цифрового вычислительного комплекса космического аппарата достаточно трудоёмкая задача. Во–первых, используются достаточно низкоуровневые языки программирования (ассемблер или язык СИ). Другая особенность возникает из–за использования специфичного центрального процессора — приходится обеспечивать высокий уровень распараллеливания. Ко всем этим нюансам добавляется ещё один: программы имеют в своём распоряжении малый объём памяти, поэтому требуется составлять программный код с высокой степенью искусности»,* — отметил один из разработчиков, ассистент кафедры информационных систем **Евгений Халтурин**.

Поскольку спуфинг в навигации — подмена легитимных навигационных данных злоумышленником с целью предоставления ложных сведений о геолокации и текущем времени, была поставлена следующая цель — разработать защищенную от спуфинга систему передачи навигационных данных по спутниковому каналу связи. Для этого учёные провели анализ того, как функционирует глобальная навигационная спутниковая система (ГНСС ГЛОНАСС) и как реализуются типовые сценарии спуфинг атак на неё. Также исследователи рассмотрели методы защиты данных, которые

используются на практике или являются перспективными. Требовалось модифицировать эти методы, чтобы «подстроить» их для нужд спутниковой связи. Важнейшей задачей стало создание программного обеспечения, которое сможет обеспечить функционал для модифицированных методов защиты.

> *«Объект подмены спуфинг атаки на ГНСС ГЛОНАСС, это навигационное сообщение. Объектом атаки, то есть жертвой, является наземная аппаратура пользователя – приёмник, улавливающий и декодирующий навигационный сигнал. Спуфинг атака обычно состоит из 4 этапов: разведки, установки вспомогательных средств (например, незаметная установка усилителя сигнала в непосредственной близости от транспорта жертвы). Третий этап — это подмена сигнала, а четвёртый — контроль объекта. На финальной ступени происходит небольшое изменение навигационных данных на нужные. Мы предложили свои методы защиты на каждом из этих этапов»,* — сообщил **Евгений Халтурин**.

В основном, предложенные методы защиты основывались на электронной подписи. Разработчики рассмотрели 5 различных алгоритмов выработки и предложили квантовые алгоритмы обеспечения защиты. Что касается разработанного программного обеспечения, то оно доказало свою состоятельность при прохождении 248 тестов, что свидетельствует о корректности применённых функций в программном коде. Было написано порядка 3 тысяч строк программного кода. Для разработки не использовался общедоступный код, так как его применение создаёт уязвимость системы.

По словам разработчиков, наиболее сложным этапом разработки ПО стало создание библиотеки для работы с большими числами. Грамотная реализация библиотеки обеспечивает скачок производительности. Была предложена авторская модернизация алгоритма Бурникеля–Циглера, при помощи которой можно сократить число процессорных операций.

Исследователи уточняют, что на основании Постановления Правительства РФ от 16 апреля 2012 года N 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств», созданный ими программный код не может быть использован в реальной спутниковой системе. Однако предложенное ПО может стать базой для дальнейших разработок другими организациями, получившими соответствующую лицензию, а алгоритм целочисленного деления можно ускорить, если реализовать его в виде ассемблерного кода.

Пресс-служба СФУ, 31 мая 2021 г.