РАСТУЩАЯ ПОТРЕБНОСТЬ В КИБЕРБЕЗОПАСНОСТИ В ГЛОБАЛЬНЫХ НАВИГАЦИОННЫХ СПУТНИКОВЫХ СИСТЕМАХ

***Б.В. Торгашев**, Московский технический университет связи и информатики, btorgashev@yandex.ru;*
***К.Н. Елагина**, Московский технический университет связи и информатики, kristina.elagina@mail.ru.*

УДК 004.056:629.056.8

Аннотация. Глобальные навигационные спутниковые системы (*GNSS*) стали частью нашей повседневной жизни, будь то использование систем навигации и локализации или синхронизация времени на ваших подключенных устройствах. Данная статья посвящена анализу достаточно фрагментированной экосистемы, связанной с *GNSS*, множества вариантов использования, которые позволяет эта технология, и связанных с ними киберрисков, которые создают новые возможности для защиты.

***Ключевые слова*:** ГНСС; безопасность; сегмент; технология; устройство; кибербезопасность; система.

THE GROWING NEED FOR CYBERSECURITY IN GLOBAL NAVIGATION SATELLITE SYSTEMS

***Boris Torgashev**, Moscow technical university of communications and informatics.*
***Kristina Elagina**, Moscow technical university of communications and informatics.*

Annotation. Global Navigation Satellite Systems (*GNSS*) have clearly become a part of our daily lives, whether it's using navigation and localization systems or synchronizing time on your connected devices. This article is devoted to the analysis of a rather fragmented ecosystem associated with *GNSS*, the many use cases that this technology allows, and the associated cyber risks that create new opportunities for protection.

Keywords: *GNSS*; security; segment; technology; device; cybersecurity; system.

Введение

Глобальные навигационные спутниковые системы (ГНСС или от английского *Global Navigation Satellite System, GNSS*) включают группировку спутников, вращающихся вокруг Земли, которые вычисляют наземные координаты путем трилатерации. ГНСС используются во всех видах транспорта: космических станциях, авиации, морском, железнодорожном, автомобильном и общественном транспорте. Позиционирование, навигация и синхронизация времени (*Positioning, navigation, and timing, PNT*) играют решающую роль в телекоммуникациях, геодезии, правоохранительных органах, реагировании на чрезвычайные ситуации (ЧС), горнодобывающей промышленности, финансах, научных исследованиях и так далее. Они используются для управления компьютерными сетями, воздушным движением, электросетями и многим другим.

Анализ рынка ГНСС

В настоящее время ГНСС включает в себя две полностью функционирующие глобальные системы: глобальную систему позиционирования (*Global Positioning System, GPS*) Соединенных Штатов Америки (США) и глобальную навигационную спутниковую систему Российской Федерации

(ГЛОНАСС). В ГНСС также входят разрабатываемые глобальные и региональные системы, а именно Европейская спутниковая навигационная система (*Galileo*), китайская (*Compass/Bei – Dou*), индийская региональная навигационная спутниковая система (*Indian Regional Navigation Satellite System, IRNSS*) и японская квазизенитная спутниковая система (*Quasi-Zenith Satellite System, QZSS*). Как только все эти глобальные и региональные системы станут полностью работоспособными, пользователь получит доступ к сигналам позиционирования, навигации и синхронизации с более чем 100 спутников.

В дополнение к ним существуют спутниковые системы функциональных дополнений, такие как глобальная система увеличения широкой площади США (*Wide Area Augmentation System, WAAS*), европейская геостационарная навигационная служба (*European Geostationary Navigation Overlay Service, EGNOS*), российская система дифференциальной коррекции и мониторинга (СДКМ), индийская *GPS*-навигация с дополненной геолокацией (*GPS Aided Geo Augmented Navigation, GAGAN*), японская многофункциональная транспортная спутниковая система (*Multifunctional Transport Satellites, MTSAT)* и спутниковые системы дополнения (*Multi-functional Satellite Augmentation System, MSAS*). Сочетание их с проверенными наземными технологиями, такими как инерциальная навигация, откроет двери для новых приложений с социально-экономическими преимуществами. Последние представляют собой приложения, требующие не только точности, но и, в частности, надежности или целостности. Критические для безопасности транспортные приложения, такие как посадка гражданского самолета, предъявляют строгие требования к точности и целостности.

Успешное завершение работы Международного комитета по глобальным навигационным системам (МКГ или от английского *International Committee on Global Navigation Satellite Systems, ICG*), в частности, по установлению функциональной совместимости между глобальными системами, позволит пользователю ГНСС использовать один инструмент для приема сигналов от нескольких спутниковых систем. Это позволит получить дополнительные данные, особенно в городских и горных районах, и повысить точность измерения времени или местоположения. Чтобы воспользоваться этими достижениями, пользователям ГНСС необходимо быть в курсе последних разработок в областях, связанных с ГНСС и наращивать потенциал для использования мульти-ГНСС-сигнала.

Таким образом, конкретные цели реализации приоритетной области ГНСС программы развития Организации Объединенных Наций (ПРООН или от английского *United Nations Development Programme, UNDP)* по применению космической техники заключаются в демонстрации и понимании сигналов ГНСС, кодов, погрешностей и практических применений, а также последствий предполагаемой модернизации.

Что касается начала 2022 г., установленная база устройств ГНСС должна превысит отметку в 10 млрд во всем мире, что составляет в среднем 1,3 устройства на душу населения. По данным Европейского агентства ГНСС (*General Services Administration, GSA*), уже в 2019 г. глобальные доходы от продажи чипсетов, приемников, устройств и услуг составили 150 млрд евро, и, по прогнозам, их рост продолжится со среднегодовым темпом роста 8%, достигнув таким образом 325 млрд в евро к 2029 г.

Рынок обычно разделен на оборудование и услуги, чтобы лучше понять эту экосистему, мы решили разбить ее по вертикали на три уровня, которые разделены на разные сегменты.

Глонасс

ГЛОНАСС – российская спутниковая система навигации. Система транслирует гражданские сигналы, доступные в любой точке земного шара, предоставляя навигационные услуги на безвозмездной основе и без ограничений.

На рис. 1 изображен логотип ГЛОНАСС.

Рисунок 1

Система ГЛОНАСС, имевшая изначально военное предназначение, была запущена одновременно с системой предупреждения о ракетном нападении (СПРН) в 1982 г. для оперативного навигационно-временного обеспечения неограниченного числа пользователей наземного, морского, воздушного и космического базирования.

Основой системы являются 24 спутника, движущихся над поверхностью Земли в трех орбитальных плоскостях с наклоном орбитальных плоскостей 64,8° и высотой орбит 19 100 км. Основное отличие от системы *Navstar* в том, что спутники ГЛОНАСС в своем орбитальном движении не имеют резонанса (синхронности) с вращением Земли, что обеспечивает им большую стабильность. Таким образом, группировка космических аппаратов (КА) ГЛОНАСС не требует дополнительных корректировок в течение всего срока активного существования.

Развитием проекта ГЛОНАСС занимаются «Роскосмос», АО «Информационные спутниковые системы имени академика М.Ф. Решетнева» и АО «Российские космические системы». Для обеспечения коммерциализации и массового внедрения технологий ГЛОНАСС в России и за рубежом постановлением Правительства РФ в июле 2009 г. был создан «Федеральный сетевой оператор в сфере навигационной деятельности», функции которого были возложены на ПАО «Навигационно-информационные системы». С 2012 г. эти функции были переданы некоммерческому партнерству «Содействие развитию и использованию навигационных технологий». На рис. 2 изображен один из первых приемников ГЛОНАСС.

Рисунок 2

Экосистема

Базовый уровень представляет собой строительные блоки технологии и разделен между операторами спутников, производителями наборов микросхем и приемников, без которых сигналы ГНСС не будут ни передаваться, ни приниматься.

Средний уровень, описываемый как устройства и платформы, разделен на два сегмента между производителями устройств и системными интеграторами, представляющими всю аппаратную и программную адаптацию технологии для конкретных отраслевых вариантов использования.

Наконец, верхний уровень представляет различные приложения технологии в каждой отрасли. Этот уровень разделен на пять хорошо известных сегментов ГНСС: транспорт и логистика, безопасность, потребительские решения, сельское хозяйство и геоматика и критическая инфраструктура.

Варианты использования кибербезопасности в ГНСС

На сегодняшний день ГНСС с ее многочисленными приложениями обеспечивает около 7% мирового внутреннего валового продукта (ВВП) и, таким образом, имеет решающее значение для многих отраслей и частных лиц. Учитывая эту высокую ценность, рынок в последнее время привлек повышенное внимание со стороны хакеров, осуществляющих кибератаки в форме глушения и спуфинга.

Спуферы подавляют относительно слабые сигналы *GNSS* радиосигналами, несущими ложную информацию о местоположении. Существует два способа подделки:

1) Ретрансляция сигналов *GNSS*, записанных в другом месте или в другое время.

2) Генерация и передача модифицированных спутниковых сигналов.

Это, конечно, началось с незначительных атак, таких как, использование дешевого спуфинга или программно-определяемых радиостанций, чтобы, например, скрыть свое местоположение от кого-то, обмануть в *Pokemon GO* или совершить другие неопасные атаки.

Совсем недавно события такого рода приняли совершенно другую точку зрения и привлекли внимание правительств. Например, США объявили о необходимости усиления безопасности в морской и логистической отраслях, Федеральная авиационная ассоциация (*Federal Aviation Association, FAA*) продемонстрировала большое количество глушения и спуфинга, полученных авиалайнерами или даже недавний взлом серверов *Garmin* в июле 2020 г., когда поставщик технологий и услуг *GPS* был вынужден заплатить выкуп в размере 10 млн долл. США, чтобы снова получить доступ к своим системам.

Это всего лишь несколько примеров, подчеркивающих растущую потребность в надежных решениях в области кибербезопасности, чтобы обеспечить защиту сигналов ГНСС во всех приложениях.

Стратегическое обоснование применения ГНСС

Для отрасли транспорта и логистики преимущества безопасности ГНСС будут включать более точную и безопасную разработку автономных транспортных средств, более точное отслеживание (пассажиров или грузов), а также лучшее планирование и синхронизация подключенных транспортных средств, благодаря предотвращению ложных сигналов и кибератаки, в том числе.

Само собой разумеется, что любая компания в сфере обороны и безопасности нуждается в серьезной киберзащите, в том числе в решениях против

глушения и спуфинга атак, которые пока представляют собой в основном дорогие аппаратные решения, требующие дорогостоящего обслуживания и не всегда исправные.

На отрасль потребительских решений приходится примерно 38% мирового рынка ГНСС, что обусловлено продажами смартфонов, приложений, дополненной реальности и других подключенных носимых устройств. С ростом числа подключенных устройств, что приводит к увеличению объема персональных данных, собираемых в рамках бизнес-моделей, включая *PNT*, адекватная защита является вполне логичной.

Помимо отраслей транспорта, логистики и потребительских решений, отрасль сельского хозяйства и геоматики является третьей отраслью экосистемы, приносящей наибольший доход, при этом текущие предложения по обеспечению безопасности крайне ограничены, если вообще отсутствуют. С ростом использования автономных транспортных средств и техники в сельском хозяйстве, добыче ресурсов и строительстве безопасность ГНСС станет необходимой для обеспечения эффективности и безопасности операторов машин.

Что касается отрасли критически важной инфраструктуры, некоторые решения в сфере кибербезопасности уже используются для обеспечения синхронизации и точности нескольких систем, например, в финансовой отрасли или в телекоммуникациях. Поскольку технологию становится довольно легко взломать, улучшение этих решений обеспечит точность данных *PNT*, тем самым защитив точность и надежность этих критически важных инфраструктурных сетей.

Аутентификация *GNSS* на уровне сигнала

Система *Galileo* будет предлагать коммерческую службу аутентификации (*Commercial Authentication Service, CAS)* для сигнала *E*6 с высочайшим уровнем безопасности для критически важных приложений, таких как автономные транспортные средства. Шифрование уровня сигнала будет основано на тех же методах, что и военные сигналы *GPS*. Только получатели, у которых есть секретный ключ, могут отслеживать такие зашифрованные сигналы. Секретный ключ также необходим для генерации сигнала, что делает невозможным подделку. Методы аутентификации *CAS* в настоящее время тестируются в *Septentrio* в сотрудничестве с Европейским космическим агентством.

Заключение

Подводя итог, можно сказать, что с растущим использованием технологий ГНСС в различных отраслях, к сожалению, ожидается, что все больше и больше компаний и частных лиц будут страдать в финансовом и, в худшем случае, физическом плане, например, в автомобильной аварии, которая случилась в результате спуфинга и глушения атак. Внедрение эффективного программного обеспечения (ПО) для кибербезопасности является ключом к обеспечению точной и синхронизированной передачи сигнала по всей экосистеме ГНСС. Здесь как устоявшиеся, так и новые игроки в области кибербезопасности, могут помочь в дальнейшем развитии и коммерциализации этой важной технологии с нулевым риском.

Литература

1. Глобальная навигационная спутниковая система ГЛОНАСС. Интерфейсный контрольный документ // Российский институт космического приборостроения. Ред. 5.1. 2008.

2. IS-GPS-200G 5-SEP-2012. Global Positioning Systems Directorate Systems Engineering & Integration. Interface Specifications IS-GPS-200. NavS- tar GPS Space Segment / Navigation User Interfaces. Вступил в действие 31-01-2013.
3. Шебшаевич В.С. Сетевые спутниковые радионавигационные системы. Под ред. П.П. Дмитриева и В.С. Шебшаевича. – М.: Радио и связь, 1982. – 272 с.
4. Шебшаевич В.С. Сетевые спутниковые радионавигационные системы. Под ред. В.С. Шебшаевича. - 2-е изд., перераб. и доп. – М.: Радио и связь, 1993. – 408 с.
5. Дмитриев С.П. Высокоточная морская навигация. – СПб.: Судостроение, 1991. – 224 с.
6. Кудрявцев И.В. Бортовые устройства спутниковой радионавигации. – М.: Транспорт, 1988.
7. Харисов В.Н. Глобальная спутниковая радионавигационная система ГЛОНАСС / Под. ред. В.Н Харисова. – М.: ИПРЖР, 1998.
8. ГЛОНАСС. Принципы построения и функционирования. Под ред. А.И. Перова, ВН. Харисова. – 4-е изд., перераб. и доп. – М.: Радиотехника, 2010. – 800 с.
9. Перов А.И. Методы и алгоритмы оптимального приема сигналов в аппаратуре потребителей спутниковых радионавигационных систем: учеб, пособие для вузов. – М.: Радиотехника, 2012. – 240 с.
10. Перов АИ. Основы построения спутниковых радионавигационных систем: учеб, пособие для вузов. – М.: Радиотехника, 2012. – 240 с.
11. Соловьев Ю.А. Системы спутниковой навигации. – М.: Эко-трендз, 2000.
12. Соловьев Ю.А. Спутниковая навигация и ее приложения. – М.: Эко-трендз, 2003. – 326 с.
13. Поваляев А.А. Спутниковые радионавигационные системы: время, показания часов, формирование измерений и определение относительных координат. – М.: Радиотехника, 2008. – 328 с.
14. Антонович К.М. Использование спутниковых радионавигационных систем в геодезии: монография: в 2 т. Т.1 / К.М. Антонович.
15. Антонович К.М. Использование спутниковых радионавигационных систем в геодезии: монография: в 2 т. Т.2 / К.М. Антонович; ГОУ ВПО «Сибирская государственная геодезическая академия». – М.: ФГУП «Картгеоцентр», 2006. – 360 с.
16. Волков Н.М. Глобальная спутниковая радионавигационная система ГЛОНАСС // Успехи современной радиоэлектроники, 1997. – № 1.
17. Решетнев М.Ф. Развитие спутниковых навигационных систем // Информационный бюллетень НТЦ «Интернавигация», 1992. – № Г-С. 6-10.
18. Анучин О. Н. Интегрированные системы ориентации и навигации для морских подвижных объектов. Под общ. ред. чл.-кор. РАН В. Г. Пешехонова. – СПб.: ЦНИИ «Электроприбор», 1999. – 357 с.
19. Стрельцова А. Методологические вопросы применения норм, правил и принципов ответственного поведения государств, призванных способствовать обеспечению открытой, безопасной, стабильной, доступной и мирной икт-среды. Исследовательский проект Международного исследовательского консорциума информационной безопасности, 2020. – 34 с.
20. Загорский А.В., Ромашкина Н.П. Проблемы информационной безопасности в международных военно-политических отношениях. – М.: ИМЭМО РАН, 2016. – 183 с.
21. Градостроительный кодекс Российской Федерации от 24.12.2004 № 190-ФЗ (С изменениями и дополнениями) // Собрание законодательства Российской Федерации, 2004. – № 1.

22. Федеральный закон «О саморегулируемых организациях» от 01.12.2007 № 315-ФЗ (С изменениями и дополнениями) // Собрание законодательства Российской Федерации, 2007. – № 21.
23. Дроздова И.В. Проблемы саморегулируемых организаций (СРО) в строительстве // Проблемы современной экономики, 2012. – № 1. – С. 235-236.