АНАЛИЗ УЯЗВИМОСТЕЙ КАНАЛОВ СВЯЗИ СПУТНИКОВЫХ НАВИГАЦИОННЫХ СИСТЕМ LBS-УСЛУГИ

***В.Н. Максименко**, доцент кафедры ИБ МТУСИ, к.т.н., доцент, vladmaks@yandex.ru;*
***Д.А. Ухин,** магистрант МТУСИ, dmitri.Ukhin@gmail.com*

УДК 621.396

Аннотация. При разработке услуг на основе определения местоположения (*LBS*-услуг) с использованием глобальной навигационной спутниковой системы (ГНСС) необходимо учесть уязвимости информационной системы и возможные угрозы информационной безопасности. В качестве объекта исследования использована система «ЭРА-ГЛОНАСС» – федеральная государственная территориально-распределенная автоматизированная информационная система экстренного реагирования при авариях. Система *LBS*-услуг состоит из трех составляющих: космическая группировка глобальной навигационной спутниковой системы, терминала потребителя и центра услуг. Наибольший интерес с позиции информационной безопасности представляет взаимодействие спутниковой группировки с терминалом потребителя. Этот сегмент всех функционирующих на сегодняшний день спутниковых систем в той или иной мере подвержен двум основным уязвимостям: подавлению сигнала и спуфинг-атакам. Спуфинг-атаки (англ. spoofing – подмена) – вид атак, при которых с помощью специального устройства, работающего на частотах ГНСС, приемнику под видом истинных данных посылаются ложные с более высоким уровнем сигнала. Приемник начинает работать с более сильным сигналом и получает заведомо ложные данные. В статье приведены результаты анализа реализации спуфера, возможные способы предотвращения атак, алгоритмы обнаружения атак и предложения по внесения изменений в законодательную базу по защите навигационных каналов связи.

Ключевые слова: глобальная навигационная спутниковая система; сеть сотовой подвижной связи; уязвимость; угроза; атака; информационная безопасность; спуфинг-атака; подмена.

ANALYSIS OF THE VULNERABILITIES OF COMMUNICATION CHANNELS OF SATELLITE NAVIGATION SYSTEMS LBS-SERVICES

***Vladimir Maksimenko**, associate professor of «The information security» department MTUCI;*
***Dmitriy Ukhin,** master's student MTUCI.*

Annotation. When developing location-based services (*LBS* services) using the global navigation satellite system (*GNSS*) it is necessary to take into account the vulnerabilities of the information system and possible threats to information security. The *ERA-GLONASS* system the federal state geographically distributed automated information system for emergency response in case of accidents was used as an object of research. The *LBS* service system consists of three components: the space grouping of the global navigation satellite system, the consumer terminal and the service center. Of greatest interest from the position of information security is the interaction of the satellite constellation with the consumer terminal. This segment of all currently functioning satellite systems to one degree or another is subject to two main vulnerabilities: signal suppression and spoofing attacks. Spoofing attacks (English spoofing - substitution) a type of attack in which using a special device operating at GNSS frequencies, false signals with a higher signal level are sent to the receiver under the guise of true data. The receiver starts working with a stronger signal and receives false data. The article presents the results of the analysis of the implementation of the spoofer, possible ways to prevent attacks, attack detection algorithms and proposals for making changes to the legal framework for the protection of navigation communication channels.

Keywords: global navigation satellite system; cellular mobile network; vulnerability; threat; attack; information security; spoofing attack; substitution.

УДК 621.391

При создании *LBS*-услуги на базе определения местоположения с использованием спутниковой навигационной системы необходимо учесть угрозы информационной безопасности. Для этого рассмотрим структуру системы ЭРА-ГЛОНАСС и выявим ее уязвимые места [1, 2].

Государственная автоматизированная информационная система «ЭРА-ГЛОНАСС» – федеральная государственная территориально распределенная автоматизированная информационная система экстренного реагирования при авариях, обеспечивающая оперативное получение формируемой в некорректируемом виде на основе использования сигналов глобальной навигационной спутниковой системы (ГНСС) информации о дорожно-транспортных и об иных происшествиях на автомобильных дорогах в Российской Федерации, обработку этой информации, ее хранение и передачу в экстренные оперативные службы, а также доступ к этой информации государственных органов, органов местного самоуправления, должностных лиц, юридических лиц, физических лиц [3].

Наземная часть системы «ЭРА-ГЛОНАСС» состоит из устанавливаемых на транспортные средства автомобильных терминалов (система определения местоположения, тяжести аварии и автоматической отправки сообщения об аварии оператору экстренных оперативных служб) и территориально распределенных центров обработки данных и региональных коммутационных узлов.

Автоматизированная система «ЭРА-ГЛОНАСС» – это сложная техническая и организационная структура (рис. 1). Основные элементы АС «ЭРА-ГЛОНАСС»:

- космическая группировка спутниковой навигационной системы;
- автомобильный терминал;
- классическая сеть сотовой подвижной связи;
- виртуальная сеть сотовой подвижной связи;
- виртуальная частная сеть;
- контакт-центры служб экстренного реагирования, оснащенные средствами приема/передачи местоположения и тяжести аварии.

Наибольший интерес касательно рассматриваемого вопроса представляет взаимодействие спутниковой группировки с автомобильной системой. Этот сегмент всех функционирующих на сегодняшний день спутниковых систем в той или иной мере подвержен двум основным уязвимостям: подавлению сигнала и спуфинг-атакам [4-6].

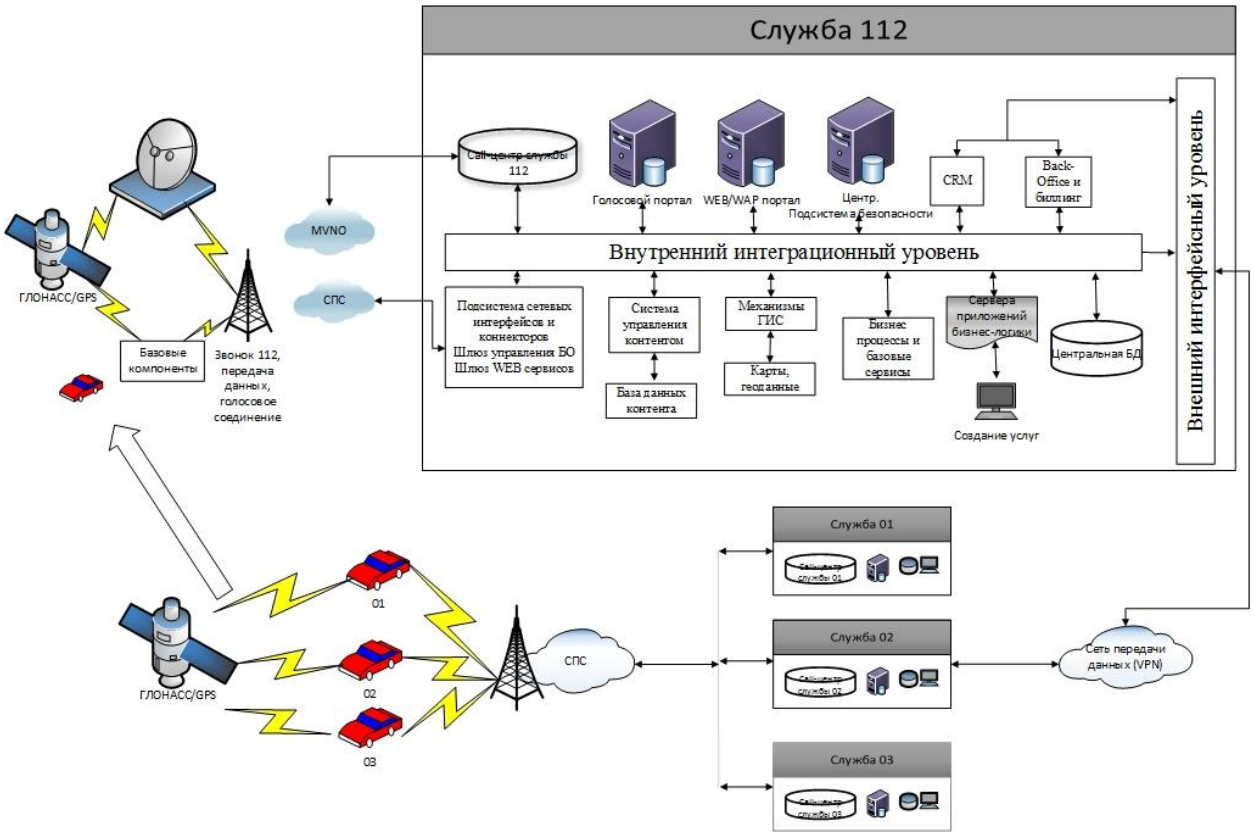

Рисунок 1

Подавление спутникового сигнала

Подавление спутникового сигнала – самая простая, очевидная и действенная атака на приемник спутникового сигнала. Принцип атаки заключается в генерации шумоподобного сигнала на частотах передачи спутникового сигнала (обычно ~1200-1600 МГц) с уровнем, превышающим реальный сигнал. Такая атака довольно проста в реализации, поскольку уровень спутникового сигнала обычно невысок (по причине большого расстояния и прохождения различных слоев атмосферы), а генерация «шума» не составляет большого труда.

Негативное влияние такого вида атак довольно высока. В первую очередь, подавление спутникового сигнала делает невозможным отслеживание важных объектов. Например, злоумышленники могут использовать «глушилки» при хищении объектов или грузов, местоположение которых отслеживается с помощью ГНСС. Конечно, сам факт исчезновения объекта из поля зрения, скорее всего, будет быстро замечен, однако обнаружение его может стать затруднительным.

Другая опасность, хоть и являющаяся на сегодняшний день скорее потенциальной, вскоре может стать вполне реальной. Ни для кого не секрет, что беспилотный транспорт – одна из активно развивающихся отраслей технологий. В основе автопилотов для автомобилей лежит именно геопозиционирование. Подавление сигналов спутников может нарушить работу и вывести из строя такие системы, а в худших случаях – стать причиной автокатастроф.

Полностью победить атаки с использованием подавления навигационного сигнала невозможно, однако частично нивелировать вполне реально. Один из наиболее эффективных методов – дублирование приемников и сокрытие их местоположения. Поскольку простые, дешевые «глушилки», которыми, вероятнее всего будут пользоваться злоумышленники, обладают очень ограниченным радиусом действия, такой подход может быть эффективным.

Отдельно стоит заметить, что по законам РФ оборот и использование подавителей сигнала слабо регламентированы. Владение такими устройствами и продажа их вполне законна и требует регистрации в государственной комиссии по радиочастотам. Пользование

незарегистрированным устройством попадает под ст. 13.4 КоАП РФ, однако наказание для физических лиц крайне гуманное – штраф до 500 руб. и конфискация устройствах [5].

Спуфинг-атаки

Спуфинг-атаки (англ. spoofing – подмена) – вид атак, при которых с помощью специального устройства, работающего на частотах ГНСС, приемнику под видом истинных данных посылаются ложные с более высоким уровнем сигнала. Приемник начинает работать с более сильным сигналом и получает заведомо ложные данные.

Угроза от таких атак порой даже выше, чем от подавления сигнала. Помимо описанных ранее способов незаконного применения специальных технических средств, устройства для спуфинг-атак могут вносить искажения в реальные данные. Таким образом студентам Техасского университета в 2013 г. удалось внести искажения в маршрут яхты «Белая роза» ценой в 80.000.000 долларов. Для сравнения, стоимость оборудования, потребовавшегося для осуществления этих манипуляций – 3000 долларов [6].

Заметить такую атаку гораздо сложнее, чем подавление сигнала, что делает ее только опаснее. Российскими законами также не запрещается спуфинг зарегистрированными средствами, продажа и покупка оборудования для спуфинга [5, 6]. Защититься от этой атаки тяжело, не в последнюю очередь оттого, что атака довольно незаметная. Кроме того, возможность атаки обусловлена тем, что в системах ГЛОНАСС и *GPS* данные передаются открытым текстом. Из-за этого данные можно перехватить и подменить. Проблема может быть с высокой степенью эффективности решена, если в будущем структура ГНСС будет дополнена системой шифрования, но до этого придется изобретать алгоритмы обнаружения и отбрасывания ложных данных.

Новый вид спуфинг-атак

До недавнего времени оставался открытым вопрос, могут ли злоумышленники манипулировать системами дорожной навигации путем подделки входных данных *GPS*. Проблема является критической, учитывая, что навигационные системы активно используют миллионы водителей на дороге и играют ключевую роль в автономных транспортных средствах. В то же время, проблема является сложной, потому что большинство систем дорожной навигации используются (или тщательно контролируются) людьми-водителями. Кроме того, простые манипуляции с *GPS* вряд ли окажутся успешными прежде всего из-за физических дорожных ограничений. Например, случайные манипуляции *GPS* могут легко создать «физически невозможные» навигационные инструкции (например, поверните налево в середине шоссе). Так как о возможностях атак пока мало известно, большинство гражданских систем не имеют защитных механизмов.

Все ранее известные работы по данной теме в основном сосредоточены на простых атаках путем установки поддельного местоположения в целевом навигационном устройстве [7-9]. В других работах изучаются атаки *GPS* на системы в открытой среде (например, в небе/в воде) [10, 11], где простая подмена *GPS*-сигнала может незаметно управлять навигацией.

Однако все изменилось, когда летом 2018 г. группа исследователей, состоящая из сотрудников *Microsoft Research,* Политехнического университета Вирджинии и китайского Университета науки и технологий, представила доклад «*All Your GPS Are Belong To Us*», рассказывающий о новом методе применения спуфинг-атак [12].

При данной атаке жертва – водитель, который использует систему навигации *GPS* (например, мобильное приложение) во время движения по дороге. Жертвой также может быть человек, сидящий в беспилотном автомобиле с поддержкой *GPS*. Атакующий подделывает сигналы *GPS*-приемника жертвы для управления алгоритмом маршрутизации навигационной системы. Цель злоумышленника – незаметно направить жертву по неверному маршруту. Атака может быть реализована в трех целях:

- Для отклонения. Злоумышленник стремится направить жертву по неверному маршруту, но при этом не имеет определенного целевого назначения. На практике злоумышленник может сбить с маршрута машины скорой помощи или полиции и, например, зациклить их маршрут.
- Для направленного отклонения. Атакующий стремится направить жертву к заранее определенному целевому месту назначения, например, с целью грабежа или угона автомобиля.
- Чтобы поставить под угрозу. Злоумышленник стремится направить жертву в опасные ситуации, например, выставляя неправильный путь на шоссе.

В данной модели угроз злоумышленник не имеет доступа к внутреннему программному и аппаратное обеспечению целевого устройства *GPS* или его службам навигации. Злоумышленник также не может модифицировать навигационные сервисы или алгоритмы (например, на серверах *Google Maps*). Кроме того, мы предполагаем, что злоумышленник знает примерную область назначения жертвы (например, финансовый район, гостиничная зона) или контрольные точки, которые жертва будет проезжать (например, главные мосты, туннели, съезды с шоссе).

В докладе приведены результаты анализа реализации спуфера, возможные способы предотвращения атак, алгоритмы обнаружения атак и предложения по внесения изменений в законодательную базу по защите навигационных каналов связи.

Литература

1. Максименко В.Н. Методология модернизации услуг системы «ЭРА-ГЛОНАСС» // Технологии информационного общества. Материалы XII Международной отраслевой научно-технической конференции. 2018. – С. 355-356.
2. Максименко В.Н., Демчишин В.И., Чернявский Д.В. ГЛОНАСС – локомотив рынка диспетчерских навигационных систем // T-Comm: Телекоммуникации и транспорт, 2008. – № 52. – С. 10-13.
3. ГОСТ Р 54721-2011 Глобальная навигационная спутниковая система. Система экстренного реагирования при авариях. Общий порядок оказания системой базовой услуги.
4. Мухортов В.В., Королев И.Д., Шкуринский С.В. Защита систем спутниковой навигации от внешних программно-аппаратных воздействий // Инновации в науке: сб. ст. по матер. LV междунар. науч.-практ. конф. – № 3 (52). Часть II. – Новосибирск: СибАК, 2016. – С. 102-108.
5. КоАП РФ, Статья 13.4. Нарушение правил проектирования, строительства, установки, регистрации или эксплуатации радиоэлектронных средств и(или) высокочастотных устройств
6. https://xakep.ru/2013/07/30/60998/.
7. Huang L. and Yang Q. Low-Cost GPS Simulator GPS Spoofing by SDR. DEFCON, 2015.
8. Humphreys T. E., Ledvina B. M., Psiaki M. L., Ohanlon B. W. and Kintner jr P. M. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In ION GNSS (2008)
9. Wang K., Chen S. and Pan A. Time and Position Spoofing with Open Source Projects. Black- Hat, 2015.
10. Kerns A. J., Shepard D. P., Bhatti J. A. and Humphreys T. E. Unmanned aircraft capture and control via GPS spoofing. Journal of Field Robotics 31, 4 (2014), 617-636.
11. Psiaki M. L. and Humphreys, T. E. Protecting GPS From Spoofers Is Critical to the Future of Navigation. IEEE Spectrum, 2016.
12. https://www.microsoft.com/en-us/research/uploads/prod/2018/06/security18gps.pdf.