# РОЛЬ СПУТНИКОВОЙ НАВИГАЦИИ В СИСТЕМЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

***В.Н. Максименко,*** *к.т.н., доцент, Московский технический университет связи и информатики, vladmaks@yandex.ru;*
***К.Н. Елагина,*** *Московский технический университет связи и информатики, kristina.elagina@mail.ru.*

***УДК 004.056***

***Аннотация***. Навигация представляет собой особенный сервис, который может выполнять функцию базового информационного сервиса и вспомогательного сервиса информационной безопасности. Навигационно-информационные системы (НИС) представляют собой особый класс информационных систем, в которых функция навигации (определение местоположения мобильных пользователей) расширяет набор решаемых информационных задач и формирует отдельный класс задач. Однако, вместе с этим, НИС могут быть подвержены различным видам воздействий (угроз). Нарушения в работе навигационных сервисов могут привести к авариям и крупным катастрофам, что повлечет за собой значительные материальные и человеческие потери. Именно поэтому обеспечение информационной безопасности навигационных систем становится все более важным и требует серьезного внимания. Необходимо создание системы защиты от угроз и контроля ее работы, а также постоянное улучшение методов обнаружения и защиты от новых угроз.

***Ключевые слова:*** спутниковые системы; спуфинг-атака; цифровая подпись; технология *MIMO*; малоресурсная криптография.

# THE ROLE OF SATELLITE NAVIGATION IN THE INFORMATION SECURITY SYSTEM

***Maksimenko Vladimir,*** *Ph.D., Associate Professor, Moscow Technical University of Communications and Informatics.*
***Elagina Kristina,*** *Moscow Technical University of Communications and Informatics.*

***Annotation.*** Navigation is a special service that can perform the function of a basic information service and an auxiliary service of information security. Navigation and information systems (*NIS*) are a special class of information systems in which the navigation function (determining the location of mobile users) expands the set of information tasks to be solved and forms a separate class of tasks. However, at the same time, navigation and information systems can be subject to various types of impacts (threats). Disruptions in the operation of navigation services can lead to accidents and major disasters, which will entail significant material and human losses. That is why ensuring the information security of navigation systems is becoming more and more important and requires serious attention. It is necessary to create a system of protection against threats and control its operation, as well as to constantly improve the methods of detection and protection against new threats.

***Keywords:*** satellite systems; spoofing attack; digital signature; *MIMO* technology.

## Введение

Разработка систем связи и навигации с использованием искусственных спутников земли началась в 60-х гг. двадцатого века с разработки самой гуманной

деятельности человека: поисково-спасательных операций на море. Это, очевидно, одна из древнейших проблем, полностью реализовать которую еще предстоит.

С середины семидесятых годов прошлого века совместными усилиями многих стран были начаты работы по разработке системы «Инмарсат» – международной космической системы связи и навигации для морского флота. Аналогичную систему с более широкими возможностями по навигационному управлению по исследованию океанов и атмосферы разрабатывали под названием «Сарсат» (*Sarsat – Satellit aided rescue*) – спасение с помощью спутников.

В настоящее время навигация используются во многих сферах жизни. Она помогает не только определять местоположение объектов и рассчитывать безопасные маршруты движения, но и обеспечивать безопасность в процессе передвижения. Сочетание навигационных космических технологий и беспроводных радиотелефонных сетей позволило решать задачи поисково-спасательных операций на суше. В настоящее время функционируют четыре глобальные *GPS* (США), *GLONASS* (Россия), *BeiDou* (Китай), *GALILEO* (Европейский союз) и две региональные (Япония и Индия) спутниковые навигационные системы. Практическое применение российской системы ГЛОНАСС реализовано для решения социальных задач экстренного реагирования при дорожно-транспортных происшествиях в информационно-навигационной системе «ЭРА ГЛОНАСС», информационных и диспетчерско-навигационных системах автомобильного транспорта [1].

Навигация представляет собой особенный сервис, который может выполнять функцию базового информационного сервиса и вспомогательного сервиса информационной безопасности [2]. НИС представляют собой особый класс информационных систем, в которых функция навигации (определение местоположения мобильных пользователей) расширяет набор решаемых информационных задач и формирует отдельный класс задач. Однако, вместе с этим, НИС могут быть подвержены различным видам воздействий (угроз). Нарушения в работе навигационных систем могут привести к авариям и крупным катастрофам, что повлечет за собой значительные материальные и человеческие потери [3].

Именно поэтому обеспечение безопасности навигационных систем становится все более важным и требует серьезного внимания. Необходимо создание системы защиты от угроз и контроля ее работы, а также постоянное улучшение методов обнаружения и защиты от новых угроз [4, 5].

**Угрозы информационной безопасности спутниковым данным**

Актуальность исследований инженерных методов проектирования защищенных НИС обусловлена необходимостью обеспечения безопасности и надежности функционирования различных систем, которые используются во многих сферах деятельности, включая государственную безопасность, транспорт, энергетику, здравоохранение и другие. Сложность НИС, большой разнородный коллектив разработчиков, сокращение времени проектирования, ошибки проекта и неполное тестирование требуют ответственного выбора методов и средств для проектирования НИС.

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 [3].

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 [4].

Все ранее известные работы по данной теме, в основном, сосредоточены на простых атаках путем установки поддельного местоположения в целевом навигационном устройстве [5-7]. В других работах изучаются атаки *GPS* на системы в открытой среде (например, в небе/в воде) [8, 9], где простая подмена *GPS*-сигнала может незаметно управлять навигацией.

**Возможные способы предотвращения атак**

Рассмотрим возможные механизмы защиты, способные помочь защититься от спуфинг-атак. Всего можно выделить три таких механизма: шифрование спутниковых данных, цифровая подпись и использование алгоритмов обнаружения атак.

Известные сервисы информационной безопасности для компьютерных систем необходимо дополнить сервисом «навигация» при расширении информационных систем навигационной составляющей:

- Идентификация и аутентификация.
- Управление доступом.
- Протоколирование и аудит.
- Шифрование.
- Контроль целостности.
- Экранирование.
- Анализ защищенности.
- Обеспечение отказоустойчивости.
- Обеспечение безопасного восстановления.
- Туннелирование.
- Управление.
- Навигация.

Сервисы безопасности в общей архитектуре безопасности распределяются по следующим уровням мер защиты:

- Превентивные меры, препятствующие нарушениям информационной безопасности.
- Меры обнаружения нарушений.
- Локализующие меры, сужающие зону воздействия нарушений.
- Меры по выявлению нарушителя.
- Меры восстановления режима безопасности.

Классификация сервисов информационной безопасности по уровням мер защиты:

К превентивным мерам относятся:

- Идентификация и аутентификация.
- Управление доступом.
- Шифрование.
- Обеспечение отказоустойчивости.

- Обеспечение безопасного восстановления.
- Управление.
- Навигация.

К обнаружению нарушений относятся:
- Протоколирование и аудит.
- Контроль целостности.
- Анализ защищенности.
- Навигация.

К мерам локализации нарушений относятся:
- Экранирование.
- Обеспечение отказоустойчивости.
- Обеспечение безопасного восстановления.
- Туннелирование.

К мерам по выявлению нарушителя относятся:
- Протоколирование и аудит.
- Управление.
- Навигация.

К мерам восстановления режима безопасности относятся:
- Обеспечение отказоустойчивости.
- Обеспечение безопасного восстановления.

Сервис информационной безопасности «навигация» может быть использован на нескольких уровнях мер защиты.

**Распространение объектно-ориентированного подхода на информационную безопасность**

По мере эволюции компьютерных систем структура процесса проектирования претерпела несколько модификаций. ГОСТ 34.601-90 регламентирует блочно-иерархическое проектирование, при котором на каждой стадии детализируются блоки предыдущего уровня. В стандарте *ISO\IEC* 15288 предлагается рассматривать жизненный цикл информационной системы в виде набора циклически повторяющихся процессов. Недостатком перечисленных стандартов проектирования заключается в низком уровне автоматизации. Использование объектно-ориентированного подхода и использование компьютерных средств проектирования информационных систем и программных систем повышают уровень автоматизации и сокращают сроки разработки [5, 6].

Проектирование информационных услуг при использовании объектно-ориентированного подхода начинается с разработки модели вариантов использования (диаграммы прецедентов). Главный прецедент определяет основную цель информационной услуги. Вспомогательные прецеденты определяют требования, которые должны быть выполнены для достижения цели.

Обобщенная диаграмма прецедента услуги на основе определения местоположения приведена на рис. 1 [10]. Требования информационной безопасности на диаграмме представлены прецедентами авторизации и получение доступа к системе, реализующей информационную услугу. Предоставление услуги на базе определения местоположения связано отношением расширения между

базовым вариантом использования и другим вариантом использования, функциональное поведение которого задействуется базовым не всегда, а только при выполнении дополнительного условия – определения местоположения [10].

Расширение сервиса услуг определением местоположения пользователя формирует новый класс услуг, обязательным для которого является периодическое информирование приложения о местоположении.

Основную часть этих действий выполняет система мониторинга. Система мониторинга – это система, которая работает с большим количеством информации в реальном масштабе времени. Для снижения требований производительности системы мониторинга используют принцип декомпозиции по функциональному принципу, используя показатели: ресурсы, сервисы и услуги (приложения) [4, 5].

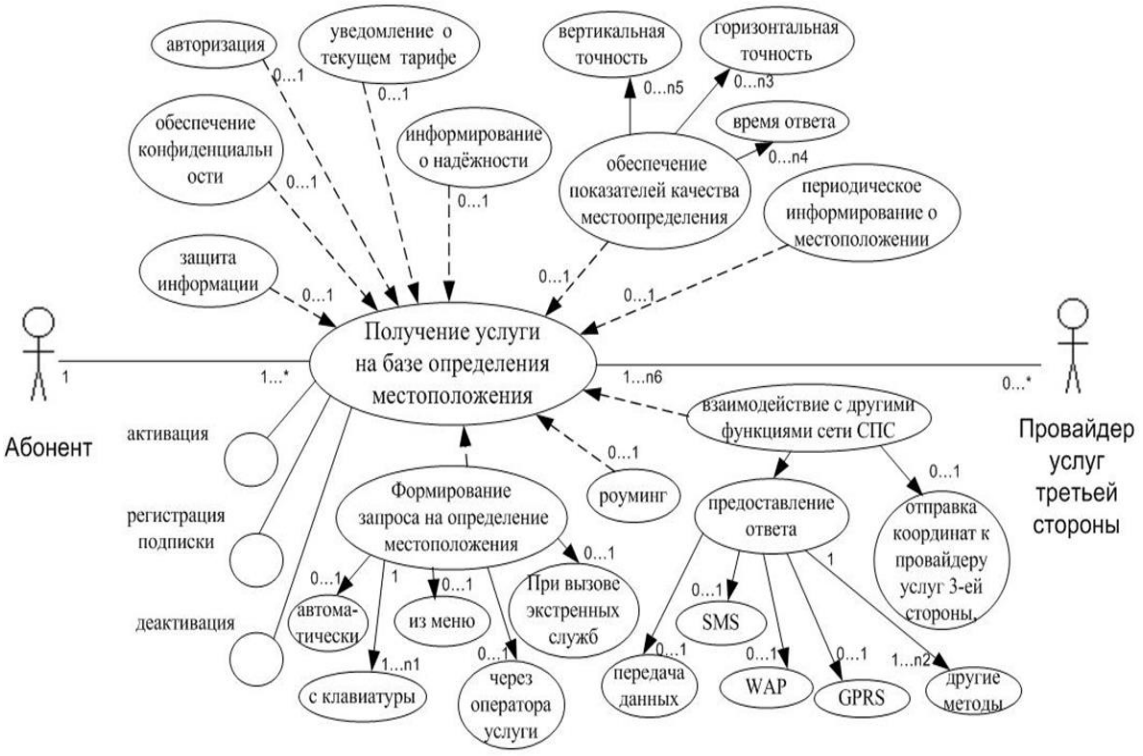


Рисунок 1

В рамках объектно-ориентированного подхода целью исследования является изучение моделей управления и качественных показателей навигационно-информационных систем. Предметом исследования являются инженерные методы проектирования навигационно-информационных систем [10].

Задачи, поставленные в работе:

1. Анализ навигационных технологий для проектирования навигационно-информационных систем.

2. Исследование формальных методов анализа расширенной модели управления инфотелекоммуникационной системой.

3. Исследование качественных показателей информационной безопасности на разных этапах жизненного цикла навигационно-информационных систем.

4. Разработка технологии проектирования защищенных навигационно-информационных систем с использованием компьютерных средств (CASE-технологии).

Для целей данного исследования воспользуемся следующим определением понятия «информационная безопасность» как защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных

воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Из данного определения следует, что существует два вида воздействий (угроз), первое – это случайные и естественные воздействия и второе – это преднамеренные и искусственные воздействия. Первые можно отнести к природным, не зависящим от человека воздействиям, а вторые – это угрозы, создаваемые человеком (злоумышленником). Защита от первого вида угроз может быть предусмотрена на ранних этапах жизненного цикла навигационно-информационной системы, а реагирование на угрозы злоумышленников возникают в основном на этапе эксплуатации жизненного цикла навигационно-информационной системы и решения по защите от данного вида угроз.

Был проведен сравнительный анализ трех наиболее распространённых технологий определения местоположения ГНСС, СПС и *WI-FI* и на основе показателей глобальности, точности и времени определения места положения была выбрана технология ГНСС для проектирования навигационно-информационных систем [1].

В настоящее время предпочтительным методом управления информационно-телекоммуникационными системами является ситуационный метод [3], базирующийся на непрерывном мониторинге информационной системы и оперативной реакции на нестандартные и непредвиденные ситуации. Ситуационный метод позволяет обеспечить защиту от искусственных и преднамеренных угроз, то есть от угроз, создаваемых злоумышленником. Это требует высокой квалификации оперативного персонала, что не всегда возможно. Поэтому предлагается разработать набор сценариев, которые позволили бы снизить требования к управляющему.

На этапе проектирования можем заложить сервисы безопасности ИБ от случайных и естественных угроз, такие как надежность, качество и устойчивость. Необходимо разрабатывать сервисы безопасности для этапа эксплуатации от преднамеренных воздействий искусственного характера. От второго типа угроз, которые создаются злоумышленниками, следует защищаться сервисами ИБ.

Выбор технологий для проектирования информационных систем с использованием компьютерных средств (*CASE*-технологии) имеет множество преимуществ:

*Увеличение производительности. CASE*-технологии сокращают время, затрачиваемое на разработку различных проектов, поскольку в них содержатся встроенные функции, которые значительно упрощают разработку и отладку кода.

*Снижение затрат.* Применение *CASE*-технологий снижает затраты на разработку информационных систем, за счет сокращения трудозатрат и скорости выполнения проектов.

*Улучшение качества разработки.* С помощью *CASE*-технологий можно разрабатывать сложные проекты с меньшим числом ошибок. Это достигается благодаря использованию готовых шаблонов, согласованных методик и процедур разработки, которые используются в *CASE*-средствах.

*Улучшение коммуникации. CASE*-технологии позволяют улучшить коммуникацию между разработчиками, дизайнерами, пользовательскими группами и другими членами команды, благодаря возможности создания единой документации проекта и облегчению взаимодействия между ними.

*Увеличение гибкости и масштабируемости. CASE*-технологии предоставляют гибкость и масштабируемость проектирования информационных

систем. Это позволяет быстро отвечать на изменения на рынке и в технических требованиях заказчика.

В целом, *CASE*-технологии являются существенным инструментом для разработки информационных систем и могут улучшить процесс проектирования и разработки, а также увеличить конечное качество продукта [4, 5, 10].

Концептуальная модель подсистемы информационной безопасности разработана на основе моделей *eTOM* и *SID*. Концептуальная модель подсистемы информационной безопасности приведена на рис. 2 и представлена в виде диаграммы классов в нотациях языка визуального моделирования *UML*. На диаграмме показаны классы и связи между ними. По диаграмме можно определить путь (сценарий) выбора контрмеры по угрозе и уязвимости.

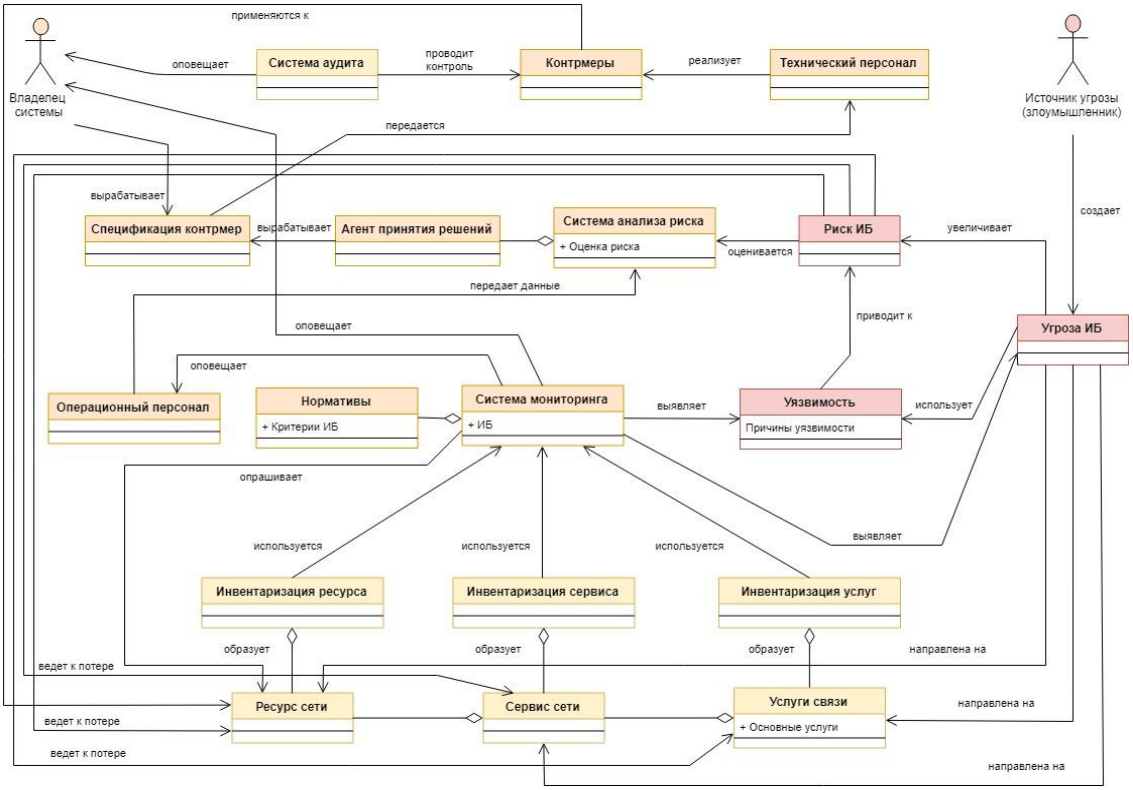


Рисунок 2

На концептуальной модели подсистемы информационной безопасности выделено три плоскости: угроз, уязвимостей и контрмер. Связи между тремя плоскостями составляют сценарий купирования от преднамеренных воздействий искусственного характера.

Архитектура безопасности должна обеспечивать защиту от угроз, будь то преднамеренные или случайные, такие как искажение или изменение информации, воровство, утечки, потери информации и других ресурсов, а также разглашение конфиденциальной информации.

Модель угроз может быть представлена при помощи диаграммы прецедентов. При помощи данной диаграммы можно определить на какую составляющую информационной безопасности направлена угроза: доступности, целостности, конфиденциальности или их сочетании.

На основе диаграмм прецедентов можно разработать сценарий ситуационного управления информационной безопасности информационной системы по одному объекту из классов (угроза, уязвимость, контрмера). Сценарий

позволяет по одной составляющей (угроза) разработать последовательность действий, которые могут привести к уязвимостям, связанным с данной угрозой, и выбрать соответствующую контрмеру.

Результаты данной работы имеют важное практическое значение. Исследование различных технологий позиционирования позволило выбрать оптимальную технологию ГНСС для использования в навигационно-информационных системах. Анализ формальных методов анализа расширенной модели управления инфотелекоммуникационной системой позволил определить подход, который будет эффективно применяться для управления системой. Исследование качественных показателей информационной безопасности на разных этапах жизненного цикла системы обеспечило понимание необходимых мер для защиты от угроз.

**Заключение**

Обобщая результаты работы, можно сделать вывод, что обеспечение безопасности навигационно-информационных систем является важной задачей, требующей комплексного подхода и постоянного совершенствования. Навигация представляет собой особенный сервис, который может выполнять функцию базового информационного сервиса и вспомогательного сервиса информационной безопасности [2]. Исследования и разработки, проведенные в рамках данной работы, позволяют принять меры по защите от угроз и обеспечить безопасность и надежность функционирования систем в различных областях навигационной деятельности.

Дальнейшие исследования в области НИС должны быть направлены на разработку новых методов и технологий, а также на адаптацию существующих подходов для эффективной борьбы с новыми угрозами. Также необходимо уделять внимание разработке и внедрению стандартов и нормативных документов, регулирующих безопасность навигационных систем. Это позволит обеспечить единый и стандартизованный подход к защите и управлению безопасностью в этой области.

**Литература**

1. Громаков Ю.А., Северин А.В., Шевцов В.А. «Технологии определения местоположения в GSM и UMTS». – М.: «Эко Трендз», 2005.
2. Максименко В.Н. Услуга определения местоположения абонента как средство защиты в сети сотовой подвижной связи // Известия ЮФУ, Технические науки. 2007. – № 4 (76). – С. 151-155.
3. Максименко В.Н., Ухин Д.А. Анализ уязвимостей каналов связи спутниковых навигационных систем LBS-услуги // Экономика и качество систем связи, 2019. – № 1 (11). – С. 18-22. – С. 37-41.
4. Максименко В.Н. Категорный подход к исследованию аспектов защиты информации и управления качеством сервисов и услуг в сетях сотовой подвижной связи // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 9. – С. 41-49.
5. Максименко В.Н. Конвергенция сервисов качества и защиты информации в сетях сотовой подвижной связи на этапах проектирования // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 11. – С. 57-64.
6. Крейнделин В.Б., Смирнов А.Э., Бен Режеб Т.Б.К. Эффективность методов обработки сигналов в системах MU-MIMO высоких порядков // T-Comm: телекоммуникации и транспорт, 2016. – Т. 10. – № 12. – С. 24-30.

7. Максименко В.Н., Васильев М.А. Методика расчета стандартных показателей качества дополнительных услуг на сетях подвижной связи // T-Comm: Телекоммуникации и транспорт, 2011. – Т. 5. – № 4. – С. 26-28.
8. Максименко В.Н., Васильев М.А. Методика системного проектирования инфокоммуникационных услуг сетей 3G // Электросвязь, 2011. – № 6.
9. Максименко В.Н., Соколов А.В. Цифровая подпись для защиты сигнала в структуре ГНСС // В книге: Мобильный бизнес: Перспективы развития и реализации систем радиосвязи в России и за рубежом. Сборник материалов (тезисов) 45-й международной конференции. Москва, 2020. – С. 28-31.
10. Леоненков А.В. Объектно-ориентированный анализ и проектирование с использованием UML и IBM Rational Rose: Учебное пособие / А.В. Леоненков. – М. Интернет-Университет Информационных Технологий, БИНОМ, Лаборатория знаний, 2010. – 320 с.