

Научная статья

УДК 004.8:527.6:621.396.99

DOI: 10.26583/bit.2025.1.10

ОТЕЧЕСТВЕННАЯ НАВИГАЦИОННО-СВЯЗНАЯ ЭКОСИСТЕМА ДЛЯ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Виктор В. Юров¹, Захар К. Кондрашов², Евгений И. Старовойтов³

НИИ микроэлектронной аппаратуры «Прогресс», пр-д Черепановых, 54, Москва, 125183, Россия

¹*v.yurov@i-progress.tech, <https://orcid.org/0009-0002-9764-308X>*

²*z.kondrashov@i-progress.tech, <https://orcid.org/0009-0001-9839-0814>*

³*e.starovojtov@i-progress.tech, <https://orcid.org/0009-0002-5268-6174>*

Аннотация. В настоящей работе предлагается к реализации отечественная навигационно-связная экосистема для защиты критической информационной инфраструктуры (КИИ) Российской Федерации. Как показывает опыт, угрозы для КИИ возрастают при использовании на территории объекта персональных абонентских устройств для связи и обмена данными (мобильных телефонов, планшетов и т.д.). Целью статьи является создание такой экосистемы, которая должна обеспечить прозрачность обмена данными от абонента к абоненту, чтобы любой передаваемый пакет данных в своей посылке имел точное время и географическую привязку к координатам отправителя и получателя. Обязательным условием в этом случае является то, что местоположение абонента должно определяться независимо от доступности сигналов глобальных навигационных систем (ГНСС) – ГЛОНАСС, GPS и др., а навигационная аппаратура потребителей должна быть устойчивой к преднамеренному искажению передаваемой координатной информации (спуфингу). Поэтому в качестве основного источника навигационных данных в экосистеме КОНСУЛ должна быть локальная система навигации (ЛСН), обеспечивающая определение местоположения объектов в условиях плохого приема или полного отсутствия спутниковых сигналов ГНСС, а также в условиях подавления навигационного сигнала или его «спуфинга». Точное позиционирование объектов мониторинга с помощью ЛСН, предоставляет дополнительную информацию при комплексной обработке и сопоставлении из разнородных устройств сбора данных для формирования тревожных событий. Отслеживаются скопления объектов мониторинга и их динамика, местоположение взаимодействующих устройств, фиксируется появление новых объектов в пределах контролируемой территории. С целью широкого внедрения данной экосистемы предлагается реализовать ряд мер, к которым относятся стандартизация протокола для обмена данными на объектах КИИ и утверждение единых тактико-технических требований к навигационно-связной аппаратуре.

Ключевые слова: критическая информационная инфраструктура, защита, навигация, связь, обмен данными, местоположение, экосистема, локальная система навигации.

Для цитирования: Юров, Виктор В.; Кондрашов, Захар К.; Старовойтов, Евгений И. Отечественная навигационно-связная экосистема для защиты критической информационной инфраструктуры. *Безопасность информационных технологий, [S.l.], т. 32, № 1, с. 143–152, 2025. ISSN 2074-7136. URL: <https://bit.spels.ru/index.php/bit/article/view/1752>. DOI: <http://dx.doi.org/10.26583/bit.2025.1.10>.*

Scientific article

NATIONAL NAVIGATION-COMMUNICATION ECOSYSTEM FOR CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

Viktor V. Yurov¹, Zakhar K. Kondrashov², Evgenii I. Starovoirov³

JSC Progress MRI, Moscow, Cherepanovykh Passage, 54, Moscow, 125183, Russia

¹v.yurov@i-progress.tech, <https://orcid.org/0009-0002-9764-308X>

²z.kondrashov@i-progress.tech, <https://orcid.org/0009-0001-9839-0814>

³e.starovojtov@i-progress.tech, <https://orcid.org/0009-0002-5268-6174>

Abstract. This paper proposes to implement a domestic Navigation and Communication ecosystem to protect the critical information infrastructure (CII) of the Russian Federation. As experience shows, the threats of CII are increasing when using personal subscriber devices for communication and data exchange on the territory of the facility (mobile phones, tablets, etc.). The goal is to create an ecosystem that should ensure transparency of data exchange from subscriber to subscriber, so that any transmitted data packet in its parcel has an exact time and geographic reference to the coordinates of the sender and recipient. In this case a prerequisite is that the subscriber's location must be determined regardless of the availability of global navigation Satellite systems (GNSS) signals – GLONASS, GPS, etc., and consumer navigation equipment must be resistant to deliberate distortion of the transmitted coordinate information (spoofing). Therefore, the main source of navigation data in the CONSUL ecosystem should be a local navigation system (LNS), ensuring the determination of the location of objects in conditions of poor reception or complete absence of GNSS satellite signals, as well as in conditions of navigation signal suppression or «spoofing». Accurate positioning of monitoring objects using LNS provides additional information during complex processing and comparison of heterogeneous data collection devices to generate alarm events. Clusters of monitoring objects and their dynamics, the location of interacting devices are tracked, the appearance of new objects within the controlled territory is recorded. For the widespread implementation of this ecosystem, it is proposed to implement a number of measures, which include standardization of the protocol for data exchange at critical information infrastructure facilities and the approval of uniform tactical and technical requirements for navigation and communication equipment.

Keywords: *critical information infrastructure, protection, navigation, communication, data exchange, location, ecosystem, local navigation system.*

For citation: *Yurov, Viktor V.; Kondrashov, Zakhar K.; Starovojtov, Evgenii I. National telecommunications ecosystem for protecting critical information infrastructure. IT Security (Russia), [S.l.], v. 32, no. 1, p. 143–152, 2025. ISSN 2074-7136. URL: <https://bit.spels.ru/index.php/bit/article/view/1752>. DOI: <http://dx.doi.org/10.26583/bit.2025.1.10>.*

Введение

Сложившаяся к настоящему времени военно-политическая обстановка требует повышенного внимания к защищенности критической информационной инфраструктуры (КИИ) Российской Федерации от несанкционированного проникновения и противоправных действий. К критической информационной инфраструктуре¹ относятся объекты, от которых зависит функционирование органов власти, экономики, транспорта, связи, промышленности, энергетики, безопасность государства и т.д., автоматизированные системы управления этими объектами и обеспечивающие их взаимодействие сети электросвязи [1–3].

Действия, направленные на защиту критической информационной инфраструктуры, включают в себя меры оперативного реагирования и упреждающего воздействия. В первом случае реакция происходит после обнаружения факта нарушения – проникновения через периметр, физического или информационного воздействия на охраняемый объект. Во втором случае ответ следует уже при наличии подозрительной активности, к которой относятся отклонения от характерного для персонала и посетителей маршрута передвижения по объекту, изменения объема передаваемых и получаемых данных, находящимся на объекте абонентом.

¹Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

В большинстве случаев, угроза для критической информационной инфраструктуры государства возрастает из-за использования персоналом или находящимися на территории объекта присутствующими – личных абонентских устройств (мобильных телефонов, планшетов и иных умных персональных устройств) [2]. Различные деструктивные действия, направленные на нанесение максимального ущерба для оборудования и персонала, могут осуществляться в режиме «on-line» с использованием технологий беспроводной связи и средств определения позиционирования и навигации.

Существующие в настоящее время системы безопасности в основном позволяют проводить арбитраж уже после происшествия, при этом не всегда удается выявить сам деструктивный элемент, используемые им средства и его местонахождение.

Таким образом, является актуальным создание такой навигационно-связной экосистемы обмена данными с абонентами, которая обеспечит прозрачность обмена данными от абонента к абоненту, чтобы любой передаваемый пакет данных в своей посылке имел точное время и географическую привязку к координатам отправителя и получателя.

1. Основные принципы защиты критической информационной инфраструктуры

В случае компрометации защиты объектов критической информационной инфраструктуры крайне важно обеспечить быстрое реагирование для отражения угрозы и определить источник ее происхождения. В настоящее время потенциальную угрозу представляют телефонные звонки от абонентов, расположенных на территории недружественных по отношению к Российской Федерации государств. Если такой вызов приходит абоненту, находящемуся на объекте критической информационной инфраструктуры, то данная ситуация с высокой вероятностью относится к потенциальным угрозам, т.е. не исключено, что она может закончиться диверсией или террористическим актом.

В качестве мер противодействия подобным атакам могут применяться алгоритмы с использованием искусственных нейронных сетей, на базе которых реализуются системы обнаружения вторжений (СОВ) и системы предотвращения вторжений (СПВ) [3].

СОВ отслеживает сеть на предмет недопустимых действий или нарушений политики безопасности, реагируя на них уведомлением системного администратора и регистрируя такие события. СПВ управляет процессом обнаружения вторжений и пытается предотвратить возможные инциденты, обеспечивая безопасность на всех уровнях системы от ядра сети такой системы до сетевых пакетов данных между абонентами.

СОВ и СПВ используют для обнаружения угроз два метода: по аномалиям, либо по сигнатурам. Этот подход по определению является ограниченным, так как не учитывает местоположение и динамику корреспондентов.

Предлагается дополнить существующие системы безопасности на основе искусственных нейронных сетей средствами контроля за перемещением абонентов в каждый конкретный момент: при приеме и передаче каждого пакета данных по беспроводным сетям связи должна фиксироваться информация, где эти данные генерируются, где и кем они принимаются и в какой точный момент времени происходит обмен данными. В этом случае на первый план выходит географическая привязка к координатам абонентов и отслеживание динамики их перемещения. Важно отметить, что географическое определение местоположения объекта должно быть обеспечено вне зависимости от того, находится этот абонент под открытым небом или внутри помещения, без прямой видимости сигналов глобальных навигационных спутниковых систем (ГНСС). Существующие технологии комплексирования позволяют обеспечить бесшовное

определение координат абонентов внутри сформированных частных сетей и с достаточной точностью (от 15 м до 3 м) узнавать местоположение абонентов.

Обязательным условием в этом случае является то, что местоположение абонента должно определяться независимо от доступности сигналов ГНСС типа ГЛОНАСС/GPS/SBAS/GALILEO и спутниковых группировок на низкой околоземной орбите типа Сфера/Starlink. Также навигационная аппаратура потребителей (НАП) должна быть устойчивой к преднамеренному искажению передаваемой координатной информации (т.н. спуфингу).

Кроме того, на объектах критической информационной инфраструктуры возникает необходимость обеспечить навигацию в различных сооружениях, конструкция которых экранирует сигналы ГНСС: складах, ангарах, шахтах и т.д.

В условиях отсутствия сигналов ГНСС используются локальные системы навигации (ЛСН), позволяющие определять координаты абонента в зоне покрытия радионавигационных опорных станций (РОС). Для навигации внутри помещений используются системы In-door навигации, использующие RFID-метки или различные технологии беспроводной связи (Bluetooth Low Energy, Wi-Fi, UWB, NFER, ZigBee, NanoLOC).

В полностью автономном режиме навигация абонента может обеспечиваться посредством счисления пути с помощью бесплатформенных инерциальных навигационных систем (БИНС) и одометров, а также за счет использования алгоритмов одновременной локализации и построения карты (англ. Simultaneous localization and mapping – SLAM) по видеоданным или «облакам точек», полученных лазерными локационными системами (лидарами). Основные характеристики датчиков для автономной навигации представлены в табл. 1.

Таблица 1. Основные характеристики датчиков для автономной навигации

Датчик	Погрешность определения координат	Накопление ошибки	Факторы, ограничивающие применение	Установка на транспортное средство	Установка на портативное носимое устройство
БИНС на базе МЭМС-гироскопов	–	100 м / 60 с без коррекции	–	+	–
Одометр	–	0,5...2,0 % от пройденного пути	–	+	–
Телекамеры *	1,0 м	–	Освещенность, погодные условия	+	+
Лидары *	1,0 м	–	Погодные условия	+	–
Bluetooth-модуль	1,0 м	–	Наличие внешних маяков	+	+
Wi-Fi-модуль	3,0 м	–		+	+
UWB-модуль	0,1 м	–		+	+
* Навигация осуществляется с использованием алгоритмов SLAM (погрешность определения местоположения движущегося объекта до 1 м)					

2. Отечественная навигационно-связная экосистема

для защиты критической информационной инфраструктуры

В АО «НИИМА «Прогресс» разработана система КОНСУЛ – комплексированная навигационно-связная система услуг локации, обеспечивающая определение местоположения абонента независимо от наличия сигналов ГНСС, в том числе в условиях, затрудняющих распространение радиосигналов [4].

Система КОНСУЛ изначально создавалась для решения задач мониторинга и управления перемещаемыми объектами в пространстве и времени, в том числе определения местоположения высокоавтоматизированных транспортных средств (ВАТС).

В настоящее время основным источником навигационной информации в системах управления ВАТС и мобильными роботами являются данные ГНСС. При перемещении объекта с ГНСС-приемником в плотной городской застройке или промышленной зоне, как правило, происходит ухудшение условий приема и потеря сигнала из-за этого. А внутри сооружений с экранирующими стенами (ангаров, подземных парковок и т.д.) прием сигналов ГНСС невозможен в принципе.

Поэтому для навигации ВАТС и мобильных роботов в мегаполисах и на территории предприятий предлагается использовать систему КОНСУЛ, объединяющую возможности ЛСН (в зоне покрытия РОС) и In-door навигации (в экранирующих сооружениях). Таким образом, возможно обеспечить бесшовную навигацию подвижных объектов на открытой местности, в условиях городской застройки, в зонах с затрудненным приемом сигналов ГНСС, в промышленных сооружениях и объектах критической инфраструктуры, внутри помещений.

В системе КОНСУЛ осуществляется комплексирование нескольких источников навигационных данных, таких как ЛСН [5–7], система In-door навигации (на базе технологий Bluetooth Low Energy – BLE, Wi-Fi или UWB) [8, 9], телекамеры, лидары [10] и т.д. При условии доступности, могут быть использованы и сигналы ГНСС.

Таким образом, КОНСУЛ представляет собой целую экосистему, обобщенная схема которой представлена на рис. 1.



Рис. 1. Обобщенная схема экосистемы КОНСУЛ

Основные характеристики источников навигационных данных в экосистеме КОНСУЛ представлены в табл. 2.

Таблица 2. Основные характеристики источников навигационных данных системы КОНСУЛ

Тип источника навигационных данных	ГНСС	ЛСН	In-door навигация
Существующие системы и технологии	ГЛОНАСС, GPS, BeiDou, Galileo	GSM, 3G	Bluetooth, Wi-Fi, UWB
Принципы и методы навигации	Триангуляция	Гиперболическая, RTT	RSSI, AoA, TDoA, ToF
Диапазоны рабочих частот, МГц	1176...1602	450...470	2400...2500 / 3000...5000 / 4900...5500 / 5500...6100 / 6000...10000
Погрешность позиционирования, м	3,0...6,0 / 0,2...0,5*	1,5...15,0	0,1...3,0
Уровень сигнала, дБм	-125...-131	-87	-80
Помехозащищенность	Низкая	Высокая	Высокая**
Зона покрытия	Глобальная	10×10 км	В пределах помещения или сооружения
* В режиме дифференциальных поправок от контрольно-корректирующей станции			
** В сооружениях с экранирующими стенами			

Одним из основных источников навигационных данных является ЛСН, обеспечивающая определение местоположения объектов в условиях плохого приема или полного отсутствия спутниковых сигналов ГНСС, а также в условиях подавления навигационного сигнала или его «спуфинга» за счет следующих технических решений:

- изменение сигнала по сложному закону псевдослучайной последовательности, динамически изменяемой при работе;
- широкий диапазон рабочих частот, в котором возможна перестройка на другие частотные диапазоны;
- мощный, по сравнению с ГНСС, навигационный сигнал.

По своим характеристикам к ЛСН наиболее близка система LocataNet (Австралия), работающая на частоте 2400 МГц и использующая алгоритмы, аналогичные применяемым в ГНСС. LocataNet применяется для создания навигационного поля на промышленных объектах и местности со сложным рельефом [11]. Несмотря на высокую точность позиционирования (3...5 см) эта система имеет недостатки, связанные с невозможностью авторизации абонентов и сравнительно низкой помехоустойчивостью.

До начала развития и повсеместного внедрения ГНСС для навигации летательных аппаратов и судов широко применялись низкочастотные (100 кГц) гиперболические радионавигационные системы LORAN-C (США) и Чайка, имеющие региональные зоны покрытия (дальность приема сигналов 1500...2000 км). Так как эти системы существенно уступали по точности ГНСС (100...700 м), то направлением их дальнейшего развития является переход на цифровую обработку сигналов и применение высокоскоростных алгоритмов обработки данных. Модернизированная система e-LORAN обладает соизмеримой с ГНСС точностью (8...20 м) при высокой помехоустойчивости и

возможностями работы внутри зданий и на местности со сложным рельефом благодаря низкочастотному сигналу [12].

Перечисленные выше аналоги, несмотря на большие зоны покрытия, не обеспечивают точность, необходимую для навигации ВАТС – 0,1 м [13]. Кроме того, отличительной особенностью ЛСН является наличие связного канала, позволяющего принимать служебную информацию от абонентов, в том числе об их местоположении.

ЛСН создает навигационное поле в зоне действия РОС, размещенных в точках с известными координатами. Группа из нескольких (от 3 до 6) РОС, установленных на одной территории, позволяет сформировать «соты» ЛСН с кодовым или частотным разделением сигналов, в которых создается навигационное поле.

Определение местоположения может осуществляться двумя методами – беззапросным или TDoA (Time Difference of Arrival) и запросным SDS-TWR (Symmetric Double Sided Two Way Ranging).

Если подразумевается широкое применение в портативных носимых устройствах, то в этом случае больше подходит беззапросный метод измерений, в котором РОС синхронизируются между собой и с абонентским терминалом для излучения радиосигнала в строго определенный момент времени. Дальность от абонента до РОС определяется по выражению

$$D = \Delta t \cdot c, \quad (1)$$

где Δt – задержка между импульсом метки времени и приходом радиосигнала; $c = 3 \cdot 10^8$ м/с – скорость света.

Погрешность измерений в этом случае равна

$$\Delta D = c \cdot (\Delta t_{изм} + \Delta t_{exp}), \quad (2)$$

где $\Delta t_{изм}$ – ошибка измерения времени прихода радиосигнала; Δt_{exp} – ошибка синхронизации РОС.

Координаты абонента определяются путем решения нескольких навигационных уравнений, число которых равно количеству РОС. Эти уравнения имеют вид

$$D_i = \sqrt{(x_{bi} - x)^2 + (y_{bi} - y)^2}, \quad (3)$$

где D_i – дальность до i -й РОС; x_{bi} , y_{bi} – координаты i -й РОС.

Принципиальной для работы ЛСН является проблема синхронизации РОС, от точности которой зависит погрешность определения координат абонентов. Таким образом, для функционирования ЛСН как составной части, так и для всей экосистемы КОНСУЛ, необходимо получение частотно-временной информации (ЧВИ), обеспечивающей синхронизацию приемопередатчиков, а также привязку к единому времени моментов передачи пакетов данных абонентами.

В настоящее время основным средством передачи ЧВИ является отечественная ГНСС ГЛОНАСС, а большая часть гражданских потребителей, в том числе элементы критической информационной инфраструктуры, получают ЧВИ от американской ГНСС GPS. Актуальные задачи и увеличение числа потребителей ЧВИ требует создания Единой системы координатно-временного обеспечения и Системы единого времени Российской Федерации (СЕВ РФ), обеспечивающих определение координат и временную синхронизацию для отечественных абонентов в любой момент времени, высокоточную взаимную синхронизацию средств глобальных и региональных навигационных систем [14, 15].

3. Практические аспекты применения

В ходе решения задач по обеспечению безопасности в экосистеме КОНСУЛ может использоваться единый программно-аппаратный комплекс, позволяющий обеспечить

обнаружение и идентификацию радиоизлучений, видеорегистрацию событий, и определение местоположения объектов мониторинга.

Анализ полученных данных, в том числе в режиме реального времени, позволяет определять:

- скопления объектов мониторинга и их динамику;
- места пребывания взаимодействующих устройств;
- фиксацию появления объекта мониторинга на территории.

Точное позиционирование объектов мониторинга с помощью ЛСН дает дополнительную информацию при комплексной обработке и сопоставлении из разнородных устройств сбора данных для формирования тревожных событий.

Синергетический эффект экосистемы КОНСУЛ достигается путем выявления аномалий на основе определения отсутствия корреляций данных идентификаторов и местоположения объектов. В этом случае управление разнородными подсистемами осуществляется путем генерации управляющих воздействий в автоматическом и автоматизированном режимах.

Отказоустойчивое масштабируемое решение на региональном и объектовом уровне кластеризации обеспечивается с использованием защищенных средств виртуализации.

Выявление угроз нанесения преднамеренного ущерба и документирование данных для оценки работы служб в области обеспечения безопасности, ликвидации происшествий и чрезвычайных ситуаций, должны обеспечить возможность оперативного упреждения или предиктивного анализа для предотвращения такого рода ситуаций.

Учитывая реалии настоящего времени, крайне важно подойти к осмыслению задачи взаимодействия навигационно-связных полей, которые со временем будут охватывать все важные объекты критической информационной инфраструктуры на территории Российской Федерации, а в перспективе и за её пределами.

Такое масштабирование позволяет существенно снизить риски компрометации любых объектов, находящихся и перемещающихся в зоне покрытия экосистемы КОНСУЛ.

Операторы систем смогут обеспечивать арбитраж любых данных по инцидентам, реагировать на обнаружение, предотвращение и задержание злоумышленников в виртуальной среде с выявлением координат реального места происшествия, в том числе и работать на упреждение с помощью средств прогностики и искусственного интеллекта по ранее накопленным знаниям нарушений и поведенческой модели объектов в системе.

Заключение

Представленная в настоящей работе навигационно-связная экосистема предназначена для упреждения угроз для критической информационной инфраструктуры Российской Федерации. Основой этой экосистемы является разработанная в АО «НИИМА «Прогресс» система КОНСУЛ, позволяющая определять местоположение абонентов (персонала и транспортных средств) независимо от доступности сигналов ГНСС и наличия помех. основополагающий принцип функционирования экосистемы заключается в том, что в каждый момент точного времени при обмене данными между абонентами происходит фиксация, где и кем эти данные генерируются, а также где и кем они принимаются.

Широкое внедрение данной экосистемы потребует реализации следующих мер:

1. Разработать протокол КОНСУЛ и подготовить его к утверждению в качестве стандарта обмена данными при перемещении объектов в пространстве и времени на территории Российской Федерации в зонах критической информационной инфраструктуры;

2. Утвердить тактико-технические требования к единой системе навигационно-связного обеспечения и ее составным частям, в том числе используемой электронной компонентной базе;

4. Выпустить единые тактико-технические требования к навигационной аппаратуре потребителей и руководствоваться ими на межведомственном уровне, в том числе ввести категории НАП по помехоустойчивости;

5. Разработать стандарты по методам комплексирования и обеспечения помехоустойчивости НАП;

6. Развернуть тестовые полигоны по отработке технических решений и пилотных проектов составных частей единой навигационно-связной системы КОНСУЛ.

СПИСОК ЛИТЕРАТУРЫ:

1. Фадеев В.В. О критически важных объектах и защите критических инфраструктур. Воздушно-космические силы. Теория и практика. 2017, № 1, с. 29–33. – EDN: QICURV.
2. Ромашкина Н.П. Вооружения без контроля: современные угрозы международной информационной безопасности. Пути к миру и безопасности. 2018, № 2(55), с.64–83. DOI: 10.20542/2307-1494-2018-2-64-83. – EDN: VPJXEN.
3. Бугорский М.А., Каплин М.А., Остроцкий С.В., Казакова О.В., Селин В.И. Особенности использования объектов критической информационной инфраструктуры с современной системой обнаружения вторжений. Sciences of Europe. 2021, № 66, с. 42–46. DOI: 10.24412/3162-2364-2021-66-1-42-46. – EDN: SXGMNB.
4. Корнеев И.Л., Кузнецов А.С., Королев В.С. Режимы работы локальной системы навигации в проекте «КОНСУЛ». Потребители системы «КОНСУЛ». Наноиндустрия. Спецвыпуск. 2021, № S7(107), с. 57–59. DOI: 10.22184/1993-8578.2021.14.7s.57.59.
5. Корнеев И.Л., Егоров В.В. Вопросы построения локальных систем навигации. Перспективы применения и потенциальные возможности проектируемых технических модулей. Наноиндустрия. Спецвыпуск. 2019, № S(189), с. 37–41. DOI: 10.22184/NanoRus.2019.12.89.37.41.
6. Корнеев И.Л., Егоров В.В. Задачи практического применения локальных систем навигации. Наноиндустрия. Спецвыпуск. 2020, № S96-1, с.12–17. DOI: 10.22184/1993-8578.2020.13.3s.12.17.
7. Корнеев И.Л., Прасолов В.Ф. Развертывание локальной системы навигации в условиях подавления сигналов ГНСС. Моделирование работы системы в различных конфигурациях. Наноиндустрия. Спецвыпуск. 2024, т.1, № S10-1(128), с.10–15. DOI: 10.22184/1993-8578.2024.17.10s.10.15.
8. Скиба Е. Пилотный проект навигации по выставке на форуме «Микроэлектроника 2023». Электроника: наука, технология, бизнес. 2023, № 10(231), с. 16–19. DOI: 10.22184/1992-4178.2023.231.10.16.19.
9. Скиба Е., Старовойтов Е. Непрерывная навигация персонала внутри и снаружи помещений. Электроника: наука, технология, бизнес. 2024, № 6(237), с. 108–114. DOI: 10.22184/1992-4178.2024.237.6.108.114.
10. Старовойтов Е.И. Технология интеллектуальной навигации на основе комплексирования ЛСН проекта «КОНСУЛ» и данных лазерной локации. Наноиндустрия. Спецвыпуск. 2024, т. 17, № S10-1(128), с. 31–38. DOI: 10.22184/1993-8578.2024.17.10s.31.38.
11. Брагин А.С. Сравнительный анализ систем глобального и локального позиционирования. Экономика и качество систем связи. 2021, № 3, с. 71–77. – EDN: SZUXXU.
12. Пешехонов В.Г. Высокоточная навигация без использования информации глобальных навигационных спутниковых систем. Гироскопия и навигация. 2022, т. 30, № 1(116), с. 3–11. DOI: 10.17285/0869-7035.0084.
13. Чикрин Д.Е., Савинков П.А., Кокунин П.А., Шагиев Р.И. Интегрированные системы высокоточной спутниково-локально-инерциальной навигации в задачах беспилотного управления транспортными средствами. Наноиндустрия. 2019, № S(89), с. 49–56. DOI: 10.22184/NanoRus.2019.12.89.49.56. – EDN: NRXOQI.
14. Блинов И.Ю., Бандура А.С., Батура А.С., Белов Л.Я., Дружин В.Е., Крупская А.В., Скобелин А.А., Тюляков А.Е. Система единого времени Российской Федерации – преодоление новых вызовов. Радионавигация и время: Труды СЗРЦ Концерна ВКО «Алмаз – Антей». 2022, № 10(18), с. 8–20. – EDN: DJCMWY.
15. Тюлин А.Е., Шпак В.В., Михайлов Ю.М., Карутин С.Н., Донченко С.И., Дворкин В.В., Климов В.Н. Технологии координатно-временного обеспечения – неотъемлемая часть цифровой экономики России. Научный вестник оборонно-промышленного комплекса России. 2024, № 3, с. 5–13. – EDN: AODVCK.

REFERENCES:

- [1] Fadeev V.V. About critical Objects and critical Infrastructure protection. Aerospace forces. Theory and practice. 2017, no. 1, p. 29–33. – EDN: QICURV (in Russian).
- [2] Romashkina N. Uncontrolled weapons: modern threats to international informational security. Pathways to Peace and Security. 2018, no. 2(55), p.64–83. DOI: 10.20542/2307-1494-2018-2-64-83. – EDN: VPJXEN (in Russian).
- [3] Bugorsky M., Kaplin M., Ostrotsky S., Kazakova O., Selin V. Features of Using critical Information Infrastructure Facilities with a modern Intrusion detection System. Sciences of Europe. 2021, no. 66, p. 42–46. DOI: 10.24412/3162-2364-2021-66-1-42-46. – EDN: SXGMHB (in Russian).
- [4] Korneyev I.L., Kuznetsov A.S., Korolev V.S Modes of the Local Navigation System Operation in the CONSUL Project. Consumers of the CONSUL System. Nanoindustry. 2021, no. S7(107), p. 57–59. DOI: 10.22184/1993-8578.2021.14.7s.57.59 (in Russian).
- [5] Korneev I.L., Egorov V.V. Issues of Building Local Navigation Systems. Application Prospects and Potential of Designed Technical Modules. Nanoindustry. 2019, no. S(189), p. 37–41. DOI: 10.22184/NanoRus.2019.12.89.37.41 (in Russian).
- [6] Korneev I.L., Egorov V.V. Tasks of Practical Implementation of Local Navigation Systems. Nanoindustry. 2020, no. S96-1, p.12–17. DOI: 10.22184/1993-8578.2020.13.3s.12.17 (in Russian).
- [7] Korneyev I., Prasolov V. Deployment of a Local Navigation System in Conditions of GNSS Signal Suppression. Simulation of the System Operation in Various Configurations. Nanoindustry. 2024, v. 17, no. S10-1(128), p. 10–15. DOI: 10.22184/1993-8578.2024.17.10s.10.15 (in Russian).
- [8] Skiba E. Pilot Project for Exhibition Area Navigation 16 at the "Microelectronics 2023" Forum. Electronics: Science, Technology, Business. 2023, no.10(231), p. 16–19. DOI: 10.22184/1992-4178.2023.231.10.16.19 (in Russian).
- [9] Skiba E., Starovoitov E. Continuous Navigation of Personnel Indoors and Outdoors. Science, Technology, Business. 2024, no. 6(237), p. 108–114. DOI: 10.22184/1992-4178.2024.237.6.108.114 (in Russian).
- [10] Starovoitov E.I. Intelligent Navigation Technology based on the Integration of the Local Navigation System (CONSUL Project) and LIDAR Data. Nanoindustry. 2024, v. 17, no. S10-1(128), p. 31–38. DOI: 10.22184/1993-8578.2024.17.10s.31.38 (in Russian).
- [11] Bragin A.S. Comparative Analysis of Global and Local Positioning Systems. Economics and quality of communication systems. 2021, no. 3, p. 71–77. – EDN: SZUXXU (in Russian).
- [12] Peshekhonov V.G. High-Precision Navigation Independently of Global Navigation Satellite Systems Data. Gyroscopy and Navigation. 2022, v. 13, no. 1, p.1–6. DOI: 10.1134/S2075108722010059 (in Russian).
- [13] Chickrin D.E., Savinkov P.A., Kokunin P.A., Shagiev R.I. Integrated Systems of High-Precision Satellite-Local-Inertial Navigation in Unmanned Vehicle Control. Nanoindustry. 2019, no. S(89), p. 49–56. DOI: 10.22184/NanoRus.2019.12.89.49.56. – EDN: NRXOQI (in Russian).
- [14] Blinov I.Yu., Bandura A.S., Batura A.S., Belov L.Ya., Druzhin V.E., Krupskaya A.V., Skobelin A.A., Tyulyakov A.E. Unified Time System of the Russian Federation - new Challenges Overcoming. Radio Navigation and Time: Proceedings of the NWRC of the Almaz-Antey Concern. 2022, no. 10(18), p. 8–20. – EDN: DJCMWY (in Russian).
- [15] Tyulin A.E., Shpak V.V., Mikhailov Yu.M., Karutin S.N., Donchenko S.I., Dvorkin V.V., Klimov V.N. Position and Timing Technologies is it Essential part of Russia Digital Economy. Scientific Bulletin of the Military-Industrial Complex of Russia. 2024, no. 3, p. 5–13. – EDN: AODVCK (in Russian).

*Статья поступила в редакцию 04.11.2024; одобрена после рецензирования 10.12.2024;
принята к публикации 10.01.2025
The article was submitted 04.11.2024; approved after reviewing 10.12.2024;
accepted for publication 10.01.2025*