

УДК 656.61.052.4:004.852

**СЛИЯНИЕ НАВИГАЦИОННЫХ ДАННЫХ В УСЛОВИЯХ
РАДИОЭЛЕКТРОННОГО ПРОТИВОДЕЙСТВИЯ:
КОНЦЕПЦИЯ И АЛГОРИТМЫ НЕЙРОСЕТЕВОГО КОМПЕЛИРОВАНИЯ**

Ермаков Никита Дмитриевич¹, аспирант
e-mail: ermakovnd@icloud.com

¹ Государственный морской университет имени адмирала Ф.Ф. Ушакова, Новороссийск, Россия

Аннотация. Предложена концепция нейросетевого компелирования навигационных данных, устойчивого к воздействию средств радиоэлектронного противодействия (РЭП) в акваториях с высокой навигационной нагрузкой. Разработана трёхуровневая архитектура слияния данных от ГНСС, АИС и РАДАР/САРП на основе энтропийного критерия аномалий, GRU-сети адаптивного перераспределения весов и синтеза навигационного решения с резервным переходом на инерциальную экстраполяцию. Результаты направлены на интеграцию в СППР морских автономных надводных судов уровня автономности 4.

Ключевые слова: радиоэлектронное противодействие, нейросетевое компелирование, слияние навигационных данных, спуфинг ГНСС, джаминг, доверительные коэффициенты, морские автономные надводные суда.

**NAVIGATION DATA FUSION UNDER ELECTRONIC WARFARE CONDITIONS:
CONCEPT AND ALGORITHMS OF NEURAL NETWORK-BASED
DATA COMPILING**

Nikita D. Ermakov¹, Doctoral Student
e-mail: ermakovnd@icloud.com

¹ Admiral F. F. Ushakov State Maritime University, Novorossiysk, Russia

Abstract. A concept of neural network-based navigation data compiling robust to electronic warfare (EW) in high-traffic maritime areas is proposed. A three-level data fusion architecture is developed for GNSS, AIS and RADAR/ARPA sources, comprising an entropy-based anomaly detection layer, a GRU network for adaptive confidence weight redistribution, and a navigation solution synthesis layer with fallback inertial extrapolation. The results are aimed at integration into the DSS of Maritime Autonomous Surface Ships at autonomy level 4.

Keywords: electronic warfare, neural network compiling, navigation data fusion, GNSS spoofing, jamming, confidence coefficients, maritime autonomous surface ships.

Введение

Нарастающее воздействие средств радиоэлектронного противодействия (РЭП) в акваториях с интенсивным судоходством формирует устойчивую угрозу достоверности навигационных данных судовых систем [1]. Особую актуальность проблема приобретает в стратегически значимых транзитных зонах — в частности, в акватории Керченского пролива: по данным EMSA, в Черноморско-Азовском регионе в 2022–2026 гг. зафиксировано свыше 10 000 аномальных событий с позиционными данными АИС, соответствующих признакам спуфинга ГНСС [2].

Для морских автономных надводных судов (МАНС) проблема РЭП приобретает критический характер: при отсутствии вахтенного офицера система поддержки принятия решений (СППР) обязана самостоятельно распознавать деградацию источника и формировать навигационное решение в условиях неполной или скомпрометированной информации [3, 4].

Цель работы — разработка концепции нейросетевого компелирования навигационных данных, устойчивого к воздействию РЭП, с формализацией моделей угроз и теоретическим анализом трёхуровневой архитектуры слияния данных. Научная новизна состоит в синтезе энтропийно-взвешенного критерия обнаружения аномалии с нейросетевым механизмом реконфигурации доверительных коэффициентов, адаптированным к специфике деградации навигационных данных при различных видах РЭП.

Методы и Материалы

Классификация угроз РЭП для судовых навигационных систем. Для корректного построения алгоритмов слияния данных необходимо формализовать модели угроз применительно к каждой из систем информационного контура СППР. ГНСС подвержена джамингу (потеря фиксирования, рост DOP) и спуфингу (плавный дрейф координат при сохранении фиксирования), причём последний не обнаруживается классической пороговой фильтрацией [5,6]. АИС уязвима к имитационной инъекции («суда-призраки») и подмене данных реального MMSI ввиду отсутствия криптоаутентификации в ITU-R M.1371 [7,8]. РАДАР/САРП подвержен активным помехам и пассивному маскированию; его деградация носит исключительно рецептивный характер [9]. Сводная классификация угроз представлена в таблице 1.

Таблица 1. Классификация угроз РЭП для судовых навигационных систем

Система	Вид угрозы	Механизм воздействия	Наблюдаемые признаки в данных
ГНСС	Джаминг	Широкополосная помеха в полосе ГНСС	Потеря фиксирования, резкое увеличение DOP
	Спуфинг	Инъекция структурно подобного сигнала	Плавный дрейф координат при сохранении фиксирования
АИС	Имитационная инъекция	Генерация УКВ-сообщений несуществующих судов	«Суда-призраки», аномальные скорости/курсы
	Подмена данных	Искажение параметров реального MMSI	Расхождение с РАДАР/САРП, аномальные ВР АИС
РАДАР/САРП	Активная помеха	Постановщик радиолокационных помех	Маскирование/ложные отметки, снижение СНО

Трёхуровневая архитектура компелирования. Под компелированием навигационных данных понимается активный процесс формирования целостного достоверного навигационного решения посредством последовательного отбора, оценки и интеграции разнородных источников, действующих в условиях деструктивного воздействия. Эта модель отличается от пассивного «слияния» (fusion). Предлагаемая архитектура включает три функционально изолированных уровня (рис. 1).

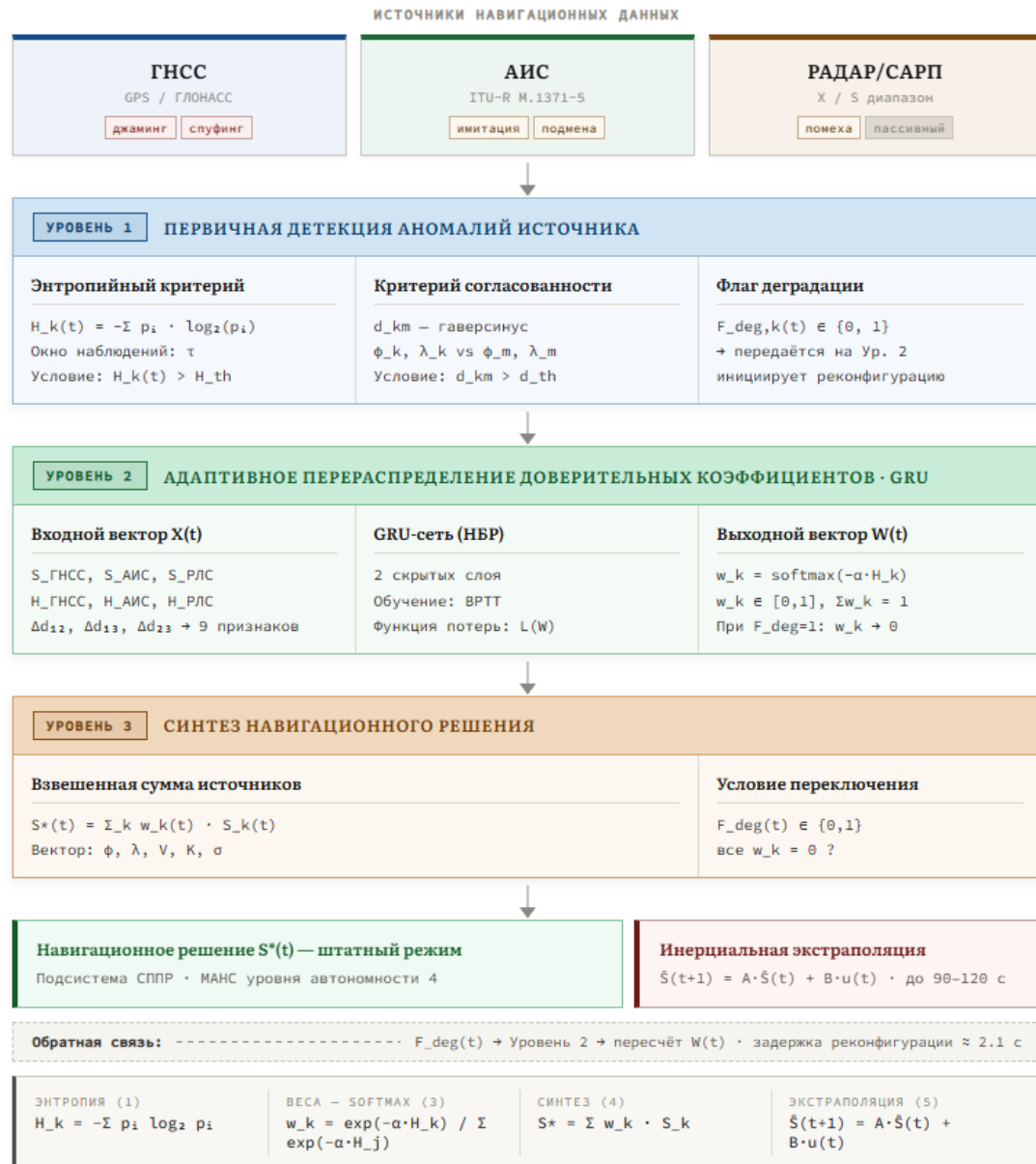


Рисунок 1 – Трёхуровневая архитектура компелирования

Уровень 1: функция первичной детекции аномалий. Описание источника $k \in \{\text{ГНСС}, \text{АИС}, \text{РАДАР}\}$ осуществляется векторным состоянием:

$$S_k(t) = \begin{bmatrix} \phi_k \\ \lambda_k \\ V_k \\ K_k \\ \sigma_k \end{bmatrix}, \quad (1)$$

где φ, λ — географические координаты;
 V — скорость;
 K — курс;
 σ — среднеквадратическое отклонение измерений.

Оценивание аномальности источника осуществляется с использованием энтропийного критерия неопределенности $H_k(t)$, вычисляемый на скользящем окне наблюдений длиной τ :

$$H_k(t) = - \sum_i p_i \log_2 p_i \quad (2)$$

где p_i — вероятностное распределение пространственно-временных отклонений Δr_k в окне τ .

При превышении порогового значения $H_k(t) > H_{th}$, источник классифицируется как потенциальный объект компрометации.

Критерий пространственной согласованности определяется как: вычисляется взаимное гаверсиновое расстояние между треками источников k и m : $d_{km} = d_{hav}(k, m)$. При выполнении условия $d_{km} > d_{th}$, оба источника маркируются для последующей верификации уровня 2.

Уровень 2 — адаптивное перераспределение доверительных коэффициентов. Нейросетевой блок реконфигурации (НБР) реализован как рекуррентная нейронная сеть с вентилируемыми рекуррентными блоками (GRU — Gated Recurrent Unit) с двумя скрытыми слоями. Входной вектор НБР на шаге t объединяет векторы состояний источников, их энтропийные оценки и матрицу парных гаверсиновых расстояний:

$$X(t) = \begin{bmatrix} S_{ГНСС}(t) \\ S_{АИС}(t) \\ S_{РЛС}(t) \\ H_{ГНСС}(t) \\ H_{АИС}(t) \\ H_{РЛС}(t) \\ \Delta d_{12} \\ \Delta d_{13} \\ \Delta d_{23} \end{bmatrix} \quad (3)$$

Выходной вектор НБР — вектор доверительных коэффициентов:

$$W(t) = \begin{bmatrix} w_{ГНСС}(t) \\ w_{АИС}(t) \\ w_{РЛС}(t) \end{bmatrix}, w_k \in [0,1], \sum_k w_k = 1.$$

При обнаружении компрометации источника k соответствующий коэффициент w_k обнуляется, а оставшийся вес перераспределяется между активными источниками $A(t) \subseteq \{ГНСС, АИС, РАДАР\}$ с использованием softmax-нормализации:

$$w_k(t) = \frac{\exp(-\alpha \cdot H_k(t))}{\sum_{j \in A(t)} \exp(-\alpha \cdot H_j(t))} \quad (4)$$

где α — параметр чувствительности нормализации.

Уровень 3 — синтез навигационного решения. Итоговый вектор состояния формируется как взвешенная сумма:

$$S^*(t) = \sum_k w_k(t) S_k(t) \quad (5)$$

При $w_k = 0$ для всех источников, кроме одного, система переходит в режим автономной инерциальной экстраполяции по уравнению кинематической модели:

$$\hat{S}(t+1) = A \cdot \hat{S}(t) + B \cdot u(t) \quad (6)$$

где A — матрица перехода состояния (предполагается модель с постоянной скоростью и курсом);

B — матрица управляющего воздействия;

$u(t)$ — вектор угловой скорости изменения курса, полученный из предыстории наблюдений [5].

Переключение между режимами (5) и (6) выполняется автоматически по флагу деградации $Fdeg(t) \in \{0, 1\}$.

Результаты и обсуждения

Отказ от статических весовых коэффициентов представляет преимущество трехуровневой архитектуры. В отличие от EKF, предполагающего стационарность шумовых источников, при скачкообразной (джаминг) или постепенной (спуфинг) деградации оценочная модель не перераспределяет доверие оперативно, что повышает уязвимость оценок. В GRU-архитектуре НБР весовые коэффициенты динамически обновляются с учетом временного контекста через последовательное интегрирование скрытых состояний. Обеспечивается адаптация доверия и устранение единой точки отказа классических СППР.

Энтропийный критерий проявляет агностичность к типу деградации. Реагирование на джаминг, спуфинг и имитационную инъекцию обеспечивается оценкой распределения неопределенности. Совместное применение с критерием пространственной согласованности формирует двухуровневую защиту. Первый уровень обеспечивает обнаружение временных аномалий посредством изменения локальной энтропии. Второй уровень выявляет пространственные несоответствия через корреляцию сигналов. При полной потере внешних источников инерциальная экстраполяция обеспечивает непрерывность навигационного решения на горизонте 90–120 с. Указанный горизонт соответствует требованиям ИМО по точности прибрежного плавания.

Ограничением подхода является чувствительность порога N_{th} к гидрометеорологическим факторам и навигационным условиям: при волнении от 5 баллов и выше естественные флуктуации повышают $N_k(t)$, что может вызывать ложные срабатывания. Адаптивное управление длиной окна τ и интеграция ИНС в качестве четвертого независимого источника составляют предмет дальнейших исследований.

Заключение

В работе предложена концепция нейросетевого компелирования навигационных данных, устойчивого к РЭП. Проведена формализованная классификация угроз применительно к ГНСС, АИС и РАДАР/САРП. Разработана трёхуровневая архитектура:

детекция аномалий на основе энтропийного критерия (1); адаптивное перераспределение доверительных коэффициентов посредством GRU-сети (2); синтез навигационного решения с переключением на инерциальную экстраполяцию (3–4). Теоретический анализ подтвердил концептуальное превосходство подхода над ЕКФ в сценариях одновременного воздействия нескольких видов РЭП. Практическая значимость — интеграция в подсистему СППР МАНС уровня автономности 4.

Список литературы:

1. Androjna A., Perković M., Pavic I., Mišković J. AIS data vulnerability indicated by a spoofing case-study // Applied Sciences. — 2021. — Vol. 11, No. 11. — P. 5015. — DOI: 10.3390/app11115015.
2. European Maritime Safety Agency (EMSA). Annual Overview of Marine Casualties and Incidents 2023. — Lisbon: EMSA, 2023. — 108 p.
3. IMO. Maritime Cyber Risk Management in Safety Management Systems. MSC-FAL.1/Circ.3. — London: IMO, 2017.
4. IMO. Code of Safety for Autonomous and Semi-autonomous Ships (MASS Code). MSC 108/26/Add.1. — London: IMO, 2024.
5. Фокин А.П., Фокина Н.Н. Влияние GPS-спуфинга на навигационные приёмники ГНСС // Труды ИПА РАН. — 2023. — Вып. 67. — С. 38–44.
6. ITU-R. Recommendation ITU-R M.1371-5. Technical Characteristics for AIS Using TDMA. — Geneva: ITU, 2014.
7. Balduzzi M., Pasta A., Wilhoit K. A Security Evaluation of AIS // Proc. ACSAC 2014. — P. 436–445. — DOI: 10.1145/2664243.2664257.
8. Katsilieris F., Braca P., Coraluppi S. Detection of Malicious AIS Position Spoofing by Exploiting Radar Information // Proc. FUSION 2013. — P. 1196–1203.
9. Uncovering the Security Landscape of Maritime Software-Defined Radios: A Threat Modeling Perspective // Applied Sciences. — 2026. — Vol. 16, No. 2. — Art. 813. — DOI: 10.3390/app16020813.

