УДК 327:623.8
EDN: LPIRAB
DOI: http://dx.doi.org/10.15211/vestnikieran320252836

АНАЛИЗ ДЕЯТЕЛЬНОСТИ США И НАТО ПО НЕЙТРАЛИЗАЦИИ «ТЕНЕВОГО ФЛОТА» РФ: ПОДХОДЫ И ТЕХНОЛОГИИ

Сергей Николаевич Гриняев

ИЕ РАН, Москва, Россия, e-mail: sgreen@csef.ru, ORCID: 0000-0001-6511-9553

Ссылка для цитирования: Гриняев С.Н. Анализ деятельности США и НАТО по нейтрализации «теневого флота» РФ: подходы и технологии // Научно-аналитический вестник ИЕ РАН. 2025. № 3. С. 28–36. DOI: 10.15211/vestnikieran320252836

Аннотация. *Исследование посвящено изучению комплекса мер США и НАТО по противодействию российскому «теневому флоту», используемому для обхода санкций в стратегически значимых морских регионах. Цель работы – анализ современных подходов и технологий, применяемых для отслеживания судов и защиты подводной инфраструктуры. Научная значимость определяется актуальностью темы в условиях геополитической конкуренции, а практическая – необходимостью совершенствования мер безопасности судоходства в новых геополитических условиях. Методология базируется на системном анализе технологических решений, включая методы искусственного интеллекта, и их интеграции в операции НАТО. Результаты показывают, что внедрение системы мониторинга, основанной на передовых алгоритмах, позволяет достаточно эффективно выявлять новые угрозы и прогнозировать возможные инциденты. Работа вносит вклад в понимание роли инноваций в обеспечении безопасности судоходства путём оценки эффективности и уязвимостей системы мониторинга. Практическая ценность заключается в предложенных рекомендациях для глобального применения подобных технологий в борьбе с экономическими и инфраструктурными вызовами.*

Ключевые слова: *Россия, «теневой флот», НАТО, США, Великобритания, Nordic Warden, искусственный интеллект, подводная инфраструктура, санкции, международное право, кибербезопасность, морская безопасность.*

Статья поступила: 29.03.2025; после доработки: 25.06.2025; принята к печати: 30.06.2025.

ANALYSIS OF US AND NATO EFFORTS TO NEUTRALIZE RUSSIA'S «SHADOW FLEET»: APPROACHES AND TECHNOLOGIES

Sergey N. Grinyaev

 Работа выполнена в рамках государственного задания Минобрнауки РФ (тема НИР № FMZS-2024-0013 «Системный анализ хозяйственно-политических рисков и возможностей Балтийско-Скандинавского макрорегиона»).

Institute of Europe, Russian Academy of Sciences, Moscow, Russia,
e-mail: sgreen@csef.ru, ORCID: 0000-0001-6511-9553

To cite this article: Grinyaev, S.N. (2025). Analysis of US and NATO efforts to neutralize Russia's «shadow fleet»: approaches and technologies. Nauchno-analiticheskij vestnik IE RAN 45(3): 28–36. (in Russian). DOI: 10.15211/vestnikieran320252836

Abstract. *The study examines the activities of the United States and NATO in countering the Russian «shadow fleet» used to circumvent sanctions in strategically important maritime regions. The purpose of the work is to analyze modern approaches and technologies used to track ships and protect underwater infrastructure. The scientific significance is determined by the relevance of the topic in the context of geopolitical competition, and the practical significance is determined by the need to improve navigation safety measures in new geopolitical conditions. The methodology is based on a systematic analysis of technological solutions, including artificial intelligence methods, and their integration into NATO operations. The results show that the implementation of a monitoring system based on advanced algorithms makes it possible to effectively identify new threats and predict possible incidents. The work contributes to understanding the role of innovation in ensuring the safety of navigation by assessing the effectiveness and vulnerabilities of the monitoring system. The practical value lies in offering recommendations for the global application of such technologies in the fight against economic and infrastructural challenges.*
Key words*: Russia, «shadow fleet», NATO, USA, Great Britain, Nordic Warden, artificial intelligence, underwater infrastructure, sanctions, international law, cybersecurity, maritime security.*

Article received: 29.03.2025; revised: 25.06.2025; accepted: 30.06.2025.

Геополитическая ситуация в первой половине 2020-х гг. ознаменовалась новым этапом противостояния между Россией и странами Запада, вызванным событиями февраля 2022 г. и последующим введением беспрецедентных санкций против Москвы. Одним из ключевых инструментов, позволивших России сохранить экспорт энергоресурсов в условиях экономической изоляции, стал так называемый «теневой флот» – сеть судов, зарегистрированных в юрисдикциях с минимальным контролем, таких как Панама, Либерия или Маршалловы острова, и часто управляемых через подставные компании. К началу 2025 г. этот флот, по разным оценкам, насчитывал сотни танкеров и грузовых судов, перевозящих нефть, газ и другие ресурсы на рынки Азии, Африки и даже некоторых стран Европы, несмотря на санкции (Illuminating Russia's Shadow…).

Особую тревогу у НАТО и США вызывает активность «теневого флота» в североевропейских морях – Балтийском, Баренцевом и Северном, где сосредоточены важнейшие линии подводной инфраструктуры: кабели связи, трубопроводы и пр. Серия инцидентов в 2024 г., включая обрывы кабелей вблизи Финского залива и Датских проливов, усилила подозрения в преднамеренных действиях, хотя прямые доказательства так и не были представлены. События подтолкнули альянс к разработке новых подходов, среди которых выделяется система *Nordic Warden*, основанная на искусственном интеллекте и призванная усилить контроль над подозрительными судами.

Концепция и задачи системы *Nordic Warden*[1]

Разработка системы *Nordic Warden* была инициирована Великобританией в рамках Объединённых экспедиционных сил (ОЭС)[2] как ответ на нарастающие угрозы, связанные с «теневым флотом» и повреждением подводной инфраструктуры (Joint Expeditionary… 2024). Программа впервые была задействована в декабре 2023 г. после инцидента с обрывом кабеля в Северном море, который совпал с подозрительной активностью судна под флагом третьей страны. Этот случай стал катализатором для оперативного внедрения системы, а её возможности были доработаны в ходе учений *Joint Protector*, проведённых в Латвии в 2024 г. Координация *Nordic Warden* осуществляется из штаба ОЭС в Нортвуде, что подчёркивает её интеграцию в структуры совместных операций НАТО и союзников (Joint Expeditionary Force... 2025).

Зона ответственности системы охватывает обширный регион, включая Балтийское, Баренцево, Северное и Норвежское моря, а также ключевые проливы – Ла-Манш, Каттегат, Скагеррак, Датский и Балтийский. В неё также входят заливы Финский, Ботнический, Куршский, Рижский, Вислинский, Гданьский и Померанский, воды у побережья Эстонии, Латвии, Литвы, Польши, а также арктические районы Норвегии и России (U.K.-led… 2025). Такой широкий географический охват отражает стратегическую важность региона, где пересекаются торговые пути, энергетические сети и коммуникационные линии, соединяющие Европу с другими континентами (Felstead 2025).

Основная задача *Nordic Warden* заключается в мониторинге деятельности судов, представляющих потенциальную угрозу. Система ориентирована на три категории объектов: суда из государств «с высоким уровнем геополитической напряжённости» (к ним отнесены Россия, Иран и Китай); суда, демонстрирующие аномальное поведение, например, отключающие автоматические идентификационные системы (АИС), совершающие необъяснимые остановки вблизи кабелей или изменяющие курс без явных причин; суда с историей таких инцидентов, как столкновения или нарушения навигационных правил. Особое внимание уделяется российским судам «теневого флота», которые используются для транспортировки нефти в обход санкций, часто через сложные схемы перевалки в нейтральных водах.

Nordic Warden выполняет не только функцию наблюдения, но и собирает данные для подготовки новых санкционных мер и оперативного реагирования. Информация о маршрутах, экипажах и владельцах судов передаётся в штабы НАТО и национальные органы для анализа и принятия решений (Baltic nations… 2025). Это делает систему инструментом стратегического значения, направленным на предотвращение диверсий и поддержку политики альянса в условиях гибридных угроз. Программа также способствует координации между странами региона, укрепляя коллективный подход к решению проблемы.

Технологическая основа *Nordic Warden*

Создание *Nordic Warden* стало результатом масштабного сотрудничества между британскими компаниями и исследовательскими институтами, что подчёркивает её технологическую сложность (Russian Maritime… 2025). Ключевыми участниками проекта выступили *BAE Systems, Thales Group* и *Rolls-Royce Holdings plc*, обеспечившие инженерную базу и интеграцию систем. *QinetiQ* и Лаборатория оборонной науки и техники[3] провели испытания алгоритмов и оборудования в контролируемых условиях, моделируя сценарии угроз в Балтийском и

[1] *Nordic Warden* – «Северный страж».
[2] *The Joint Expeditionary Force, JEF.*
[3] *Defence Science and Technology Laboratory, DSTL*.

Северном морях. Специализированные компании (*Marine Systems Technology Ltd* и др.) сосредоточились на технологиях морской безопасности, *Sonardyne International Ltd* разработала гидролокационные системы и подводные датчики, *BMT Defence Services* предоставила инженерные решения для анализа данных, а *Ultra Electronics* обеспечила коммуникационные платформы. Этот консорциум создал систему, способную функционировать в динамичной и сложной морской среде.

Технологическая основа *Nordic Warden* базируется на методах искусственного интеллекта, который объединяет несколько передовых подходов для обработки данных и выявления угроз (Robinson 2025). Основу составляют алгоритмы машинного обучения (МО), такие как нейронные сети и деревья решений, которые анализируют поведение судов в реальном времени. Эти алгоритмы обучаются на исторических данных о маршрутах, инцидентах и аномалиях, что позволяет системе распознавать такие отклонения, как отключение АИС или необоснованные остановки вблизи кабелей. МО-модели способны выделить суда, чьи действия повторяют шаблоны, связанные с прошлыми случаями повреждения инфраструктуры (Tselentis et el. 2023). Обработка естественного языка[1] применяется для анализа текстовых данных, включая сообщения судов, отчёты портовых служб и разведывательные сводки, что помогает выявить подозрительные инструкции или запросы, такие как нестандартные разрешения на стоянку. Компьютерное зрение используется для интерпретации изображений с подводных дронов и спутников, позволяя обнаруживать физические следы активности (повреждения кабелей или присутствие посторонних объектов).

Прогнозная аналитика в *Nordic Warden* реализована через комбинацию методов временных рядов и байесовских сетей (Menon 2020). Анализ временны*х* рядов отслеживает динамику передвижения судов, прогнозируя вероятность их появления в зонах риска на основе прошлых траекторий и текущих условий, таких как погода или плотность трафика. Байесовские сети оценивают вероятность угроз, учитывая множественные факторы – от технического состояния судна до его принадлежности к «теневому флоту». Эти методы позволяют системе не только реагировать на текущие события, но и предсказывать потенциальные инциденты с точностью до нескольких часов, что было подтверждено в ходе испытаний в 2024 г. Прогнозная модель успешно спрогнозировала остановку танкера *Eagle S* вблизи кабеля *Estlink 2* за день до инцидента 25 декабря 2024 г., что дало время для подготовки ответа (Walker 2024).

Коммерческие продукты, интегрированные в *Nordic Warden*, включают платформы от ведущих разработчиков. *Microsoft Azure* предоставляет облачную инфраструктуру для хранения и обработки больших данных, обеспечивая масштабируемость системы. Программное обеспечение *MATLAB* от *MathWorks* используется для разработки и тестирования алгоритмов МО и прогнозной аналитики, позволяя моделировать сложные сценарии. *SAS Viya* применяется для анализа больши̇х массивов данных и визуализации результатов, что упрощает их интерпретацию операторами. Спутниковые данные поставляются через платформу *Maxar Technologies*, обеспечивая высокое разрешение изображений для компьютерного зрения. Гидролокационные системы от *Sonardyne*, такие как *Sentinel IDS*, интегрированы для мониторинга подводной среды, дополняя данные АИС и спутников. Эти продукты, объединённые в единую экосистему, обеспечивают высокую точность и надёжность *Nordic Warden*, хотя их использование увеличивает стоимость эксплуатации.

Для работы системы требуется обширный поток данных. Аппаратура АИС предоставляет информацию о местоположении, скорости и курсе судов, формируя основу для монито-

[1] *Natural language processing, NLP.*

ринга в реальном времени. Гидролокационные данные, получаемые от подводных дронов и стационарных датчиков, обеспечивают контроль над глубоководной средой, позволяя обнаруживать такие действия, как сброс якорей вблизи кабелей. Спутниковые снимки фиксируют аномалии на поверхности (скопления судов в нестандартных зонах). Метеорологические данные – температура воды, сила ветра, течения – учитываются для оценки влияния внешних факторов на поведение судов. Записи о маршрутах, инцидентах и нарушениях служат базой для обучения алгоритмов, повышая точность прогнозов. Обобщённые текстовые отчёты о деятельности судов и их команд, а также показания подводных датчиков дополняют информационную картину события, обеспечивая возможность всестороннего и глубокого анализа его последствий.

Эффективность и уязвимости *Nordic Warden*

Эффективность *Nordic Warden* подтверждается её способностью оперативно выявлять подозрительные суда и прогнозировать угрозы. В ходе испытаний в 2024 г. система успешно зафиксировала несколько случаев отключения АИС российскими танкерами вблизи Финского залива, что позволило направить патрульные корабли для проверки. Анализ данных о 89 судах «теневого флота», внесённых в базу, показал, что система способна отслеживать смену экипажей и владельцев, выявляя попытки маскировки через сложные схемы перерегистрации. В Северном море *Nordic Warden* указала на потенциальный инцидент, обнаружив судно, остановившееся вблизи кабеля связи на несколько часов без видимой причины. Подобные примеры демонстрируют аналитический потенциал системы и её ценность для оперативного реагирования.

Однако эффективность *Nordic Warden* имеет пределы, обусловленные качеством и доступностью данных. В арктических водах, где доступ к АИС и спутниковым данным ограничен в силу недостаточного покрытия, точность прогнозов снижается. В Балтийском море высокая плотность судоходства усложняет выделение реальных угроз среди общего потока движения судов, что требует дополнительных ресурсов для фильтрации данных. Кроме того, система зависит от сотрудничества стран региона: если одно государство отказывается предоставлять информацию, это создаёт пробелы в мониторинге.

Уязвимости *Nordic Warden* связаны с её технологической природой. Кибербезопасность остаётся критическим аспектом: система подвержена риску атак со стороны государств с развитыми кибервозможностями (Кириленко, Алексеев 2022). Взлом алгоритмов, подмена данных или *DDoS*-атаки[1] могут вывести *Nordic Warden* из строя или привести к ложным выводам – классификации гражданских судов как угрозы (Cho et el. 2022). В 2024 г. в ходе учений была смоделирована такая атака, показавшая, что восстановление системы требует значительного времени. Зависимость от сложных технологий также означает высокую стоимость разработки и эксплуатации, что ограничивает её масштабирование на другие регионы без дополнительных инвестиций.

К недостаткам системы относится её ограниченная способность к прямому воздействию. *Nordic Warden* фиксирует нарушения и передаёт данные, но не имеет механизмов для физического перехвата судов или принуждения их к изменению курса. Это требует координации с военно-морскими силами, что замедляет реакцию и зависит от политической воли отдельных стран. Ещё одним недостатком является сложность интеграции с существующими системами НАТО, такими как командные центры операции «Балтийский часовой», из-за различий в форматах данных и уровнях доступа.

[1] *DDoS, distributed denial of service* – распределённый отказ в обслуживании.

Соответствие международным договорам и конвенциям

Деятельность *Nordic Warden* порождает вопросы о том, насколько она соответствует международному праву, прежде всего Конвенции ООН по морскому праву 1982 г. (КМП)[1] (United Nations Convention... 1982). Статья 87 КМП гарантирует свободу судоходства в международных водах, включая право судов передвигаться без необоснованного вмешательства. Мониторинг *Nordic Warden*, включая запросы страхования и сбор данных о маршрутах без согласия судов, может быть воспринят как нарушение этого принципа. Если система классифицирует судно как подозрительное и передаёт данные для санкций, это косвенно ограничивает его свободу, что противоречит духу конвенции, хотя формально не выходит за её рамки.

Многовековой договор о свободе судоходства, уходящий корнями в эпоху торговых соглашений XVII в., также ограничивает возможности прямого вмешательства. Запросы страхования, согласованные в Таллине, находятся в «серой зоне»: они не являются обязательными, но отказ судна предоставить информацию усиливает подозрения и может привести к экономическим последствиям. Международные правила предотвращения столкновений судов в море 1972 г. (МППСС-72)[2] (Convention on the…1972), регулирующие навигацию, не адаптированы к автоматизированным системам контроля, что создаёт правовую неопределённость. *Nordic Warden* не управляет судами напрямую, но её влияние на их поведение требует пересмотра этих норм.

С другой стороны, защита подводной инфраструктуры может быть оправдана ст. 301 КМП, запрещающей действия, угрожающие миру и безопасности. Повреждение кабелей, даже непреднамеренное, наносит ущерб экономике и коммуникациям, что даёт НАТО основание для мониторинга. Однако отсутствие чётких международных стандартов для таких систем подчёркивает необходимость новых договорённостей. Для полного соответствия нормам требуется согласование на уровне ООН или Международной морской организации, что до настоящего времени остаётся нереализованным.

Региональные меры контроля

Региональные усилия НАТО и США дополняют *Nordic Warden* более традиционными мерами. В декабре 2024 г. в Таллине представители 12 стран – Великобритании, Дании, Эстонии, Финляндии, Германии, Исландии, Латвии, Литвы, Нидерландов, Норвегии, Польши и Швеции – договорились о запросах доказательств страхования у подозрительных судов, проходящих через Ла-Манш, Датские проливы (Большой Бельт и Зунд) и Финский залив (12 European… 2024). Эта инициатива, хотя и ограничена рамками международного права, направлена на сбор данных для системы мониторинга. Судно, отказывающееся предоставить информацию, может быть отмечено как потенциально опасное, что усиливает базу для последующих действий.

В систему *Nordic Warden* внесены данные о десятках российских судов «теневого флота», включая их технические характеристики, маршруты и персональные сведения об экипажах (Barnard 2025). Это позволяет отслеживать аномалии в деятельности (появление одних и тех же моряков на разных судах), что часто указывает на попытки скрыть принадлежность к операциям по обходу санкций. В Балтийском море усилия сосредоточены на контроле подходов к портам Санкт-Петербурга и Калининграда, где «теневой флот» активно использует мелководные зоны для перевалки грузов. В Баренцевом море акцент сделан на арктических

[1] *United Nations Convention on the Law of the Sea, UNCLOS.*
[2] *Convention on the International Regulations for Preventing Collisions at Sea, COLREGs.*

маршрутах, связанных с проектами добычи газа, а в Северном море — на путях к портам Западной Европы, через которые Россия пытается сохранить экспорт (Willett 2025).

США дополняют эти меры усилением санкционного давления. В 2025 г. Вашингтон планирует ввести новые ограничения против операторов «теневого флота», зарегистрированных в третьих странах, таких как Панама и Либерия. Эти санкции затронут не только суда, но и страховые компании, поддерживающие их деятельность, что должно повысить стоимость операций и снизить их рентабельность. Комбинация мониторинга и экономических мер создаёт синергетический эффект, постепенно сужая пространство для манёвра российского экспорта.

Стратегическое значение и перспективы

Стратегическое значение *Nordic Warden* выходит за рамки текущих задач в североевропейском регионе. Система демонстрирует потенциал для применения в других акваториях, таких как Чёрное море, где используются схожие схемы для обхода санкций, или Персидский залив, где контроль над поставками энергоресурсов остаётся ключевым фактором глобальной конкуренции. Её алгоритмы и методы анализа могут быть адаптированы для мониторинга поставок вооружений, редкоземельных металлов или других стратегических ресурсов, что расширяет сферу применения технологий.

Перспективы включают интеграцию *Nordic Warden* с другими инициативами НАТО (операцией «Балтийский часовой», запущенной в 2025 г. для защиты подводной инфраструктуры Балтийского моря и др.) (NATO launches… 2025). Совместное использование данных этими программами может повысить эффективность обнаружения угроз и координации действий, создавая многоуровневую систему безопасности. Кроме того, технологии *Nordic Warden* могут быть распространены на воздушные и наземные логистические цепочки. Анализ спутниковых данных и сетевых связей применим для отслеживания грузовых авиаперевозок или железнодорожных маршрутов, используемых для обхода санкций.

Однако реализация подобных перспектив требует устранения уязвимостей. Кибербезопасность системы нуждается в усилении путём внедрения многоуровневого шифрования и резервных каналов связи. Снижение стоимости эксплуатации возможно за счёт стандартизации компонентов и привлечения дополнительных партнёров, таких как страны ЕС или Япония. Правовая адаптация предполагает разработку международных стандартов для автоматизированных систем мониторинга, что потребует переговоров в рамках ООН или Международной морской организации. Без этих шагов масштабирование *Nordic Warden* останется ограниченным в своих возможностях.

* * *

Многогранная деятельность США и НАТО по нейтрализации российского «теневого флота» сочетает передовые технологии, региональное сотрудничество и экономическое давление. Система *Nordic Warden*, в основу которой положены алгоритмы искусственного интеллекта, стала важным инструментом в этом процессе, демонстрируя способность эффективно выявлять угрозы и собирать данные для подготовки оперативных и стратегических решений. Её эффективность в обнаружении подозрительных судов в Балтийском и Северном морях подчёркивает потенциал инноваций в обеспечении нового уровня контроля морских путей и акваторий. Однако уязвимости системы, включая риски кибератак, высокую стоимость и зависимость от качества данных, указывают на необходимость дальнейшего её совершенствования. Правовая неоднозначность применения подобных систем в рамках международных

норм (в частности, в рамках КМП и МППСС-72) требует разработки новых стандартов, обеспечивающих легитимность подобных действий и способствующих предотвращению дипломатических конфликтов.

Обобщая результаты анализа, можно отметить, что *Nordic Warden* и сопутствующие меры формируют новую парадигму борьбы с гибридными угрозами в морской сфере. Они не только ограничивают возможности «теневого флота», но и создают прецедент для использования технологий в решении глобальных вызовов. Прогнозные оценки указывают на вероятное расширение применения *Nordic Warden* в ближайшие годы. Если текущие усилия по устранению уязвимостей окажутся успешными, система может стать основой для глобальной сети мониторинга, охватывающей не только морские, но и воздушные и наземные маршруты. В перспективе до 2030 г. возможно создание унифицированной платформы под эгидой НАТО, интегрирующей данные от союзников и партнёров, таких как Япония, Австралия или страны ЕС. Это усилит контроль над потоками ресурсов и вооружений, минимизируя влияние государств, использующих скрытые схемы для обхода международных ограничений. Однако такой сценарий потребует значительных инвестиций – как финансовых, так и политических – для согласования интересов участников и преодоления правовых барьеров.

В краткосрочной перспективе, до конца 2025 г., ожидается усиление санкций США и расширение зоны действия *Nordic Warden* на Чёрное море. Долгосрочный результат зависит от способности альянса адаптировать технологии к новым угрозам, включая развитие автономных судов и дронов, которые могут быть использованы для диверсий. Системы, подобные *Nordic Warden*, представляют серьёзную угрозу интересам Российской Федерации в Мировом океане, что требует повышенного внимания к их деятельности и оценки влияния на безопасность судоходства.

Список источников / References

12 European Countries Crack Down on Russia's 'Shadow Fleet'. Embassy of Estonia in Helsinki. 31.12.2024. Available at: https://helsinki.mfa.ee/en/12-european-countries-crack-down-on-russias-shadow-fleet/ (accessed 28.03.2025).

Baltic nations using AI + AIS to track Russian shadow fleet. The Digitalship. 08.01.2025. Available at: https://thedigitalship.com/news/electronics-navigation/north-sea-baltic-nations-using-ai-ais-to-track-russian-shadow-fleet/ (accessed 28.03.2025).

Barnard, S. (2025). The Baltic: A 'strategic sea'. ESD. 17.02.2025. Available at: https://euro-sd.com/2025/02/articles/42619/the-baltic-a-strategic-sea/ (accessed 28.03.2025).

Cho S., Orye, E., Visky, G., Prates, V. (2022). Cybersecurity Considerations in Autonomous Ships. CCDCOE. Available at: ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf (accessed 28.03.2025).

Convention on the International Regulations for Preventing Collisions at Sea (COLREGs) 1972. London: International Maritime Organization, 1972.

Tselentis D., Papadimitriou E., van Gelder P. (2023). The usefulness of artificial intelligence for safety assessment of different transport modes. Accident Analysis & Prevention Vol. 186: 107034. DOI: 10.1016/j.aap.2023.107034

Felstead, P. (2025). UK steps up efforts to head off Russian interference with critical undersea infrastructure. ESD. 24.01.2025. Available at: https://euro-sd.com/2025/01/major-news/42222/rn-monitors-russian-spy-ship/ (accessed 28.03.2025).

Johnson R., Brown T. (2023). Cybersecurity Challenges in Autonomous Maritime Operations. New York: Wiley.

Joint Expeditionary Force activates UK-led reaction system to track threats to undersea infrastructure and monitor Russian shadow fleet. UK Parliament. 06.01.2025. Available at: https://www.gov.uk/government/news/joint-expeditionary-force-activates-uk-led-reaction-system-to-track-threats-to-undersea-infrastructure-and-monitor-russian-shadow-fleet (accessed 28.03.2025).

Joint Expeditionary Force trains protecting critical undersea infrastructure. NATO. 06.06.2024. Available at: https://ac.nato.int/archive/2024/JEF_nordic_warden_24.aspx (accessed 28.03.2025).

Illuminating Russia's Shadow Fleet. Windward's Maritime AI™ Insights & Resources. Available at: https://windward.ai/knowledge-base/illuminating-russias-shadow-fleet/ (accessed 28.03.2025).

Laird, R. (2025). Nordic Warden Tests AI-Enabled Tracking System for Undersea Cable Protection. DefenseInfo. 01.09.2025. Available at: https://defense.info/partners-corner/2025/01/nordic-warden-tests-ai-enabled-tracking-system-for-undersea-cable-protection/ (accessed 28.03.2025).

Menon, A. (2020). Time Series Analysis in SAP Predictive Analytics (August 19, 2020). DOI: 10.2139/ssrn.3677420

NATO launches «Baltic Sentry» to increase critical infrastructure security. NATO. 14.01.2025. Available at: https://www.nato.int/cps/en/natohq/news_232122.htm (accessed 28.03.2025).

Robinson, R. (2025). AI-Driven Security: Nordic Warden and Northern Europe's Maritime Infrastructure Protection. ComplexDiscovery. 11.01.2025. Available at: https://complexdiscovery.com/ai-driven-security-nordic-warden-and-northern-europes-maritime-infrastructure-protection/ (accessed 28.03.2025).

Russian Maritime Activity and UK Response. UK Parliament. 22.01.2025. Available at: https://hansard.parliament.uk/commons/2025-01-22/debates/7DB30945-1C23-48E1-A629-B113C53CD9E2/RussianMaritimeActivityAndUKResponse (accessed 28.03.2025).

U.K.-led Nordic Warden System Activated Following Black Sea Cable Damage. DefenseMirror. 08.01.2025. Available at: https://www.defensemirror.com/news/38562 (accessed 28.03.2025).

United Nations Convention on the Law of the Sea (UNCLOS) 1982. Montego Bay: UN. 1982.

Walker, S. (2024). Sixty-mile drag mark found near damaged Baltic Sea cable, says Finland. The Guardian. 30.12.2024. Available at: https://www.theguardian.com/world/2024/dec/30/finnish-investigators-into-suspected-sabotage-find-100km-trail-on-baltic-sea-bed (accessed 28.03.2025).

Willett, L. (2025). Turning the tide: NATO, national, and multinational efforts build Baltic CUI security. ESD. 27.03.2025. Available at: https://euro-sd.com/2025/03/articles/43355/turning-the-tide-nato-national-and-multinational-efforts-build-baltic-cui-security/ (accessed 28.03.2025).

Кириленко, В.П., Алексеев, Г.В. (2022). Роль цифровой трансформации в борьбе с преступностью на море. Евразийская интеграция: экономика, право, политика (4): 68–81. [Kirilenko, V., Alekseev, G. (2022). The Role of the Digital Transformation in the Fight against Crime at Sea. Eurasian integration: economics, law, politics (4): 68–81. (In Russian)]. DOI: 10.22394/2073-2929-2022-04-68-81