ВЕСТНИК
ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
МОРСКОГО И РЕЧНОГО ФЛОТА ИМЕНИ АДМИРАЛА С. О. МАКАРОВА

DOI: 10.21821/2309-5180-2025-17-5-641-652 **EDN DKQYLH**

MODELS OF CYBERATTACKS ON THE AUTOMATIC IDENTIFICATION SYSTEM NETWORK

V. V. Volkov[1], E. O. Ol'khovik[2], Yu. S. Fedosenko[3]

[1] Scientific and Production Firm «Marinek» LLC, St. Petersburg, Russian Federation
[2] Admiral Makarov State University of Maritime and Inland Shipping, St. Petersburg, Russian Federation
[3] Volga State University of Water Transport, Nizhniy Novgorod, Russian Federation

The study examines cyber threats within the network of the maritime Automatic Identification System (AIS). A review of available data on identified AIS vulnerabilities has shown a lack of a well-structured formal description and classification of threats. At present, the existing scenario-based attack models do not encompass the full spectrum of possible threats, while most approaches to AIS cybersecurity — both organizational and technical — are limited to information-security measures implemented directly on board the vessel. Five independent models of external attacks on AIS are proposed, representing typical levels of cyber threats ranging from low (single-signal spoofing) to high (combined multistage attacks employing several methods). In addition to external threats, the study also considers internal threats related to unauthorized penetration into the ship's computer network followed by destructive actions. These cases are discussed separately, as they require specific methods of analysis and mitigation. New approaches and recommendations for AIS protection are proposed. Counteracting cyber threats requires a balanced combination of organizational and technical measures, conventionally divided into software-algorithmic and hardware-architectural categories. The former includes methods for improving the AIS protocol and software, such as message authentication and encryption, anomaly filtering, and intrusion detection systems. Another important direction involves the development of algorithms for detecting falsified AIS data. This requires the creation of additional monitoring systems capable of continuously analyzing incoming information for signs of anomalies, such as the absence of a previous route, illogical maneuvers, data duplication, or desynchronization with radar observations. Future AIS cybersecurity is expected to rely on more detailed regulations and guidelines issued by classification societies, as well as on enhanced software and hardware solutions implemented both on board vessels and in shore-based centers, such as Vessel Traffic Management Systems (VTMS).

Keywords: Automatic Identification System (AIS), cybersecurity, cyber threats, threat modeling, maritime safety, maritime terrorism, vessel identification, message encryption, cyber risks, spoofing.

For citation:
Volkov, Vasily V., E. O. Ol'khovik and Yu. S. Fedosenko. "Models of cyberattacks on the automatic identification system network." *Vestnik Gosudarstvennogo universiteta morskogo i rechnogo flota imeni admirala S. O. Makarova* 17.5 (2025): 641–652. DOI: 10.21821/2309-5180-2025-17-5-641-652.

УДК 656.61.052

МОДЕЛИ КИБЕРАТАК НА СЕТЬ АВТОМАТИЧЕСКОЙ ИДЕНТИФИКАЦИОННОЙ СИСТЕМЫ

В. В. Волков[1], Е. О. Ольховик[2], Ю. С. Федосенко[3]

[1] ОО «НПФ Маринэк», Санкт-Петербург, Российская Федерация
[2] ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова», Санкт-Петербург, Российская Федерация
[3] ГБОУ ВО «Волжский государственный университет водного транспорта», Нижний Новгород, Российская Федерация

В исследовании рассмотрены случаи киберугроз в сети морской автоматической идентификационной системы. Обзор данных о выявленных уязвимостях автоматической идентификационной системы показал отсутствие качественно формализованного описания и классификации угроз, так как в настоящее время предлагаемые сценарные модели атак не покрывают весь их возможный спектр, а подходы к обеспечению кибербезопасности АИС (организационные и технические меры) сводятся к сценариям

информационной безопасности непосредственно на судне. Предложено пять независимых моделей внешних атак на АИС — типовые уровни киберугрозы от низкого (единичная подделка сигнала) до высокого (комбинированная многоэтапная атака с использованием нескольких методов). Помимо внешних угроз в ходе исследования рассмотрены внутренние угрозы, связанные с проникновением в компьютерную сеть судна с последующим негативным воздействием. Эти результаты вынесены на отдельное обсуждение, поскольку требуют особого подхода и проработки. Предложены новые подходы и рекомендации к защите. Отмечается, что противодействие киберугрозам для АИС требует сочетания организационных и технических мер. Условно они разделены на программно-алгоритмические и аппаратно-архитектурные. К первым относятся методы, улучшающие протокол и программное обеспечение: аутентификация и шифрование АИС-сообщений, фильтрация аномалий, системы обнаружения атак. Обращается внимание на то, что альтернативным направлением является разработка алгоритмов выявления поддельных данных АИС, предусматривающая предварительное создание дополнительных систем мониторинга, которые могут непрерывно анализировать поступающие данные признаков аномалий: отсутствие предыдущего маршрута движения, нелогичные маневры, дублирование, рассинхронизацию с радиолокацией и т. п. Дан прогноз обеспечения кибербезопасности сетей АИС, предусматривающий создание более подробных правил и руководств классификационных обществ, а также разработку дополнительного программного обеспечения и технических средств как непосредственно на судне, так и в береговых центрах (например, в системах управления движением судов).

Ключевые слова: автоматическая идентификационная система, кибербезопасность, киберугрозы, модели угроз, безопасность судоходства, морской терроризм, идентификация судов, шифрование сообщений, киберриски, спуфинг.

Для цитирования:
Волков В. В. Определение долготы места судна по глубинам на основе нейронной сети / В. В. Волков, Е. О. Ольховик, Ю. С. Федосенко // Вестник Государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2025. — Т. 17. — № 5. — С. 641–652. DOI: 10.21821/2309-5180-2025-17-5-641-652. — EDN DKQYLH.

Введение (Introduction)

Автоматическая идентификационная система (АИС, англ. AIS) — критически важная навигационная технология в судоходстве, служащая для идентификации судов, их габаритов, курса и других данных, которая предназначена для предотвращения столкновений судов и повышения ситуационной осведомленности на море. Согласно требованиям Международной конвенции СОЛАС (SOLAS[1]), использование АИС является обязательным для судов с валовой вместимостью более 300 рег. т. Применение АИС позволило значительно повысить безопасность через УКВ-радиоканал суда, береговые станции и спутники — суда обмениваются данными о своем местоположении (GPS-координаты), курсе, скорости, идентификаторах судов и другой информацией в реальном режиме времени. Однако изначально протокол передачи данных АИС был разработан без учета требований кибербезопасности. Так, в Стандарте[2] отсутствуют шифрование и аутентификация сообщений, приемники воспринимают любые данные, передаваемые на соответствующей частоте. Это означает, что злоумышленники способны подделывать АИС-трафик данных, передавая ложные данные в системы мониторинга и тем самым вводя в заблуждение экипажи судов. За последние два десятилетия исследования и инциденты показали широкий спектр кибератак на АИС: от относительно безобидных розыгрышей до опасных действий, близких к морскому терроризму.

Международная морская организация (IMO) признает проблему кибербезопасности АИС. В 2017 г. выпущена резолюция IMO MSC.428(98), обязавшая судоходные компании включить киберриски в системы управления безопасностью не позднее 2021 г. [1]. Профильные организации также издают соответствующие рекомендации. Например, Международная ассоциация маячных служб (IALA) опубликовала руководство по эксплуатации АИС [2]. Для защиты внутренних сетей судна разработаны новые технические стандарты (в частности, IEC 61162–450 и расширение IEC 61162–460), вводящие

[1] Международная конвенция по охране человеческой жизни на море 1974 года. СОЛАС 74. https://docs.cntd.ru/document/901765675.

[2] ITU-R. Recommendation ITU-R M.1371-5 (02/2014). Technical characteristics for an automatic identification system using time division multiple access in the VHF maritime mobile frequency band.

«электронный шлюз безопасности» для сегментации сети [3, 4]. Тем не менее внедрение этих мер происходит медленно, и гражданская АИС-сеть пока остается открытой для злоумышленников.

Актуальность проблемы подтверждена множеством публикаций. В 2013 г. специалисты Trend Micro[3] на конференции Hack In The Box[4] наглядно показали, что АИС «полностью уязвима для различных атак, которые можно реализовать с помощью недорогого оборудования [5]. Они классифицировали атаки на две категории: *1-я категория* — вмешательство через интернет-сервисы, собирающие АИС-данные; *2-я категория* — атаки на радиоэфир АИС [5]. Различные авторы описали конкретные сценарии: подделка координат судна, создание «кораблей-призраков», ложные аварийные сигналы, блокировка каналов и т. д. Так, С. А. Семёнов (2018 г.) опубликовал обзор уязвимостей АИС и указал, что без должной защиты судно может быть потеряно в результате кибератаки [6]. В 2019 г. А. Антипов детально проанализировал потенциальные угрозы от взлома АИС: фальсификацию координат, рассылку ложных навигационных предупреждений, имитацию аварийных маяков и др. [7]. Исследователи обратили внимание на «темные флоты» — группы судов, намеренно скрывающие передачу данных АИС. В результате G. Kessler с соавторами (2024 г.) разработал инструментарий для спуфинга АИС и мониторинга таких скрытых судов [8]. Академические работы фиксируют рост реальных инцидентов: в 2019–2021 гг. наблюдались случаи появления сотен фальшивых целей возле побережья (например, у о. Эльба), подделки треков военных кораблей в пропагандистских целях, взлома навигационных систем судов и др. Все эти данные свидетельствуют о том, что кибербезопасность АИС — крайне актуальная проблема международного судоходства.

Цель исследования — систематизировать и описать известные киберугрозы для систем АИС, предложить классификацию сценариев атак и оценить методы противодействия. Для достижения этой цели были поставлены следующие частные задачи:

– проанализировать опубликованные сведения об уязвимостях АИС, реальных кибератаках и предлагаемых мерах противодействия;

– разработать формальную модель (таксономию) классификации атак по источникам, целям, последствиям и другим признакам, а также описать типовые сценарии;

– сравнить предложенные сценарные модели с существующими классификациями в имеющихся публикациях и оценить полноту их охвата;

– рассмотреть подходы к обеспечению кибербезопасности АИС (организационные и технические меры), а также предложить направления дальнейших исследований.

Методы и материалы (Methods and Materials)

Исследование проведено методами аналитического и литературного обзора — таксономического анализа. В качестве материалов использованы открытые источники: научные статьи, технические отчеты компаний, отчеты об инцидентах и отраслевые стандарты, посвященные уязвимостям АИС и смежных систем. Вначале были отобраны сведения о выявленных уязвимостях протокола АИС и известных случаях кибератак (как экспериментальных, так и реальных). Затем эти данные были систематизированы и классифицированы по следующим основным критериям: *вектор атаки* (*внешний* — через радиоэфир или *внутренний* — через бортовую сеть судна); *уровень подготовки атакующего* (ресурсы и навыки, необходимые для реализации сценария); *масштаб и цель воздействия* (локальный сбой, дезинформация, выведение из строя и т. п.), а также *возможные последствия для судоходства*. Дополнительно учитывались мотивация злоумышленника и способ реализации (прямая радиопередача ложных данных, компрометация инфраструктуры, комбинированные методы).

На основе этих критериев была разработана *таксономия кибератак на АИС*. Все угрозы разделены на две большие группы: *внешние*, когда атакующий не проникает на судно, а воздействует

[3] Глобальная корпоративная платформа кибербезопасности на базе ИИ [Электронный ресурс]. Режим доступа: https://www.trendmicro.com/ru_ru/business.html.

[4] Hack In The Box Security Conference Hack in the box Security Conference // Hack in the Box Security Conference [Электронный ресурс]. Режим доступа: https://conference.hitb.org.

на него извне (через радиосигналы АИС или внешние сервисы), и *внутренние*, связанные с проникновением во внутреннюю сеть или оборудование судна. В рамках внешних угроз выделено пять сценарных моделей атак, описывающих типичные ситуации — от простейшей до сложной многоэтапной диверсии. Такая классификация отражает градацию по сложности и опасности. Разработанные модели являются обобщением множества описанных в литературе сценариев. Для внутренней угрозы (атаки в корабельной сети) выполнен отдельный анализ, учитывающий специфику интегрированных мостиковых систем и стандартов (NMEA 0183, NMEA2000, IEC 61162–450/460 и др.).

Для построения предложенной классификации были учтены существующие подходы, включая модель, предложенную Trend Micro (2014), где атаки делятся на две категории: воздействие через интернет-сервисы и вмешательство в радиоканал АИС. Также рассматривались другие типологии — по целям атаки (навигация, связь, сенсоры) и по стадиям развития угрозы. Это позволило обеспечить полноту охвата и систематизировать известные сценарии. Надежность источников подтверждена использованием официальных инцидентных отчетов и рецензируемых публикаций.

Результаты (Results)

На основе исследования имеющихся данных выделено пять моделей внешних атак на АИС — типовые уровни киберугрозы от низкого (единичная подделка сигнала) до высокого (комбинированная многоэтапная атака с использованием нескольких методов). Рассмотрим формализованные сценарии каждой модели.

Модель 1 (M1) — простейшая атака минимальной сложности. Злоумышленник с базовыми техническими навыками способен выполнить ограниченную по масштабу имитацию АИС-сообщений. Имея в распоряжении недорогое оборудование (программно-определяемый радиопередатчик, УКВ-антенну и компьютер), он может передать в эфир ложное АИС-сообщение, которое будет принято ближайшими судами как настоящее. Например, атака M1 — это появление на экранах окружающих судов единственной фальшивой цели: несуществующего буя, «двойника» реального судна или неверных координат какого-либо судна. Радиус воздействия ограничен (несколько морских миль), и такая акция зачастую носит характер случайной или хулиганской. Тем не менее даже единичное ложное АИС-сообщение способно дезориентировать экипаж. Из-за отсутствия аутентификации приемники не отличают подделку от легитимного трафика. Подобные инциденты уже наблюдались на практике. Это подтверждает реальность даже низкоуровневых угроз. Отдельно следует отметить случаи злоупотребления АИС судовладельцами. Например, известны эпизоды, когда экипажи намеренно передавали фиктивные координаты, чтобы скрыть заход в запрещенный порт или иное нарушение. Технически это не «взлом» чужой системы, а неправомерное использование своей, однако реализуется оно теми же средствами (передача ложных данных в эфир) и попадает в общую категорию угроз типа M1.

Модель 2 (M2) — масштабная имитация целей (атака средней сложности). В этой модели предполагается более опытный нарушитель, обладающий достаточными знаниями и ресурсами для расширенной имитации обстановки. Такой атакующий способен сгенерировать одновременно множество разнообразных АИС-сообщений. Сценарий M2 — это создание целого «сюжета» в АИС-сети: злоумышленник транслирует несколько фальшивых судов с различными курсами и скоростями, дополняя их виртуальными навигационными опасностями (несуществующими буями, предупреждениями о шторме, дрейфующими минами и т. п.). В результате на экранах возникает правдоподобная, но полностью ложная картина, способная ввести в заблуждение операторов службы движения (VTS) и экипажи. В отличие от модели 1, данное воздействие не случайное, а целенаправленное: *нарушитель сознательно стремится дезинформировать и создать помехи*. Несмотря на то, что изначально можно предположить отсутствие злого умысла (например, энтузиаст экспериментирует «из любопытства»), последствия M2 могут быть серьезными. Ложные предупреждения о штормах вынуждают суда менять планы, что приводит к экономическим убыткам; десяток фантомных судов могут отвлечь диспетчеров и снизить эффективность контроля. Таким

образом, граница между несанкционированным экспериментом и целенаправленной атакой размывается: модель 2 представляет ощутимую угрозу для отрасли несмотря на то, что реализуется без использования сложных технологий.

Модель 3 (М3) — целенаправленная деструктивная атака (высокий уровень угрозы). Третья модель описывает намеренное нападение на судоходство с использованием АИС как инструмента. В данном случае предполагаются высокий уровень мотивации (преступный умысел нанести ущерб) и тщательная подготовка. Атакующий в сценарии М3 сочетает все ранее описанные приемы, чтобы достичь максимального эффекта. Возможная реализация: вокруг целевого судна создается множество ложных целей — десятки фальшивых судов внезапно появляются на экране, имитируя опасное сближение. Одновременно жертве рассылаются ложные предупреждения о столкновении от этих фантомных целей. Ситуация для экипажа выглядит как внезапное окружение быстро движущимися объектами. Вахтенные могут испытать стресс и совершить ошибочные действия, а система предотвращения столкновений (ARPA / ECDIS) способна самостоятельно выдать команду уклонения. В результате судно начинает маневрировать, пытаясь избежать несуществующую опасность. Подобная атака может привести к аварийному маневру (например, уходу с безопасного фарватера). Еще одним возможным вариантом сценария данной модели является *масштабная дезинформация*: злоумышленник транслирует радиоперехват АИС, чтобы скрыть реальные угрозы. Например, на экране появляются фальшивые «пиратские катера», отвлекающие охрану, или наоборот, при реальном нападении пиратов злоумышленник добавляет множество ложных целей, маскируя истинное число нападающих. Отличительной чертой данной модели является скоординированное применение различных средств с намерением спровоцировать чрезвычайную ситуацию (столкновение, посадка на мель, паника экипажа). Характер таких атак приближается к саботажу и требует от нарушителя серьезных технических навыков. Реализовать данную модель сложнее, чем модели 1 и 2, но и эффект несопоставимо опаснее. Этот сценарий можно также комбинировать с параллельными действиями. Например, для усиления эффекта можно одновременно осуществлять GPS-спуфинг (подмену сигналов навигации). В итоге модель 3 представляет собой полномасштабную кибератаку на судно или регион, потенциально способную вызвать аварии.

Модель 4 (М4) — компрометация береговой инфраструктуры АИС. Данный тип угроз направлен не на корабельные транспондеры, а на наземный сегмент АИС — береговые базовые станции и сетевые сервисы. Береговые станции АИС управляются портовыми властями и обладают расширенными функциями: они могут рассылать служебные команды (смена каналов, отключение передатчиков), передавать от имени береговых служб навигационные оповещения и т. д. В сценарии М4 злоумышленник либо имитирует базовую станцию, передавая сигнал с привилегиями береговой, либо взламывает реальную береговую систему / сервер. В обоих случаях он получает возможность влиять на множество судов одновременно, выступая как бы от имени «официального источника». Потенциальные атаки данной модели включают рассылку ложных команд и сообщений от имени властей. Например, злоумышленник может передать в эфир команду всем судам района переключиться на другую частоту, в результате чего часть судов потеряет связь на основном канале, или разослать навигационное предупреждение о несуществующей опасности, заставив суда изменить курс. Еще более опасным приемом является отключение АИС-транспондеров на судах.

Стандарт АИС допускает дистанционное выключение передатчика (функция для портовых служб). Если атакующий воспользуется этой командой, то он может заставить выбранное судно исчезнуть из сети АИС. Жертва перестает видеть окружающие суда и сама пропадает с их экранов. Особенно критично это при заходе в порт или в узкости: судно внезапно становится «слепым и невидимым». Реальный эксперимент показал, что злоумышленник через фальшивую базовую станцию сумел полностью погасить АИС-активность судна. Кроме того, компрометация береговых интернет-сервисов АИС, таких как публичные сайты отслеживания судов по АИС, также относится к модели 4. Атакующий, не вмешиваясь в радиоэфир, но посылая поддельные данные в базу данных сервиса, способен создать на онлайн-картах любые ложные перемещения судов, т. е. информационную атаку, которая не влияет напрямую на безопасность навигации (экипажи на мостике

не используют интернет для навигации), но способна ввести в заблуждение аналитиков, СМИ, военные и контролирующие органы. Так, в 2021 г. были подделаны публичные треки нескольких военных кораблей, в результате создана иллюзия их захода в чужие территориальные воды и эта ложная информация попала в средства массовой информации, т. е. стала официальной. Таким образом, данная модель является более технически сложной, чем три предыдущие (требует либо хакерского взлома ПО, либо инновационных способов радиопередачи с параметрами базовой станции), но ее последствия ее могут быть более масштабными, затрагивая сразу большие регионы и множество участников.

Модель 5 (M5) — комбинированная многоэтапная атака. Представляет комплексную атаку, в которой злоумышленники используют несколько каналов и методов одновременно. В реальных условиях организованные группы не ограничиваются одним приемом, а разрабатывают многоходовые операции для гарантированного достижения цели. Сценарий M5 можно описать на примере гипотетической, но основанной на реальных уязвимостях ситуации. Предположим, атакующая группа планирует захват или саботаж конкретного судна. В данном случае план действий злоумышленников может быть следующим:

1. *Проникновение во внутреннюю сеть судна.* Заблаговременно (до выхода судна в рейс) злоумышленники инфицируют бортовую систему судна вредоносным ПО либо устанавливают скрытое устройство в сеть с целью получения доступа к навигационным данным на мостике и подготовки плацдарма для атаки изнутри.

2. *Нарушение сигналов GPS.* Когда судно входит в нужный район, злоумышленники начинают глушить или подменять сигнал спутниковой навигации (GNSS). В результате у экипажа возникают проблемы с определением позиции по GPS и увеличивается зависимость от АИС и приборов.

3. *Введение ложных АИС-целей.* Параллельно злоумышленники через радиоэфир создают вокруг судна иллюзорные объекты (например, несколько быстро сближающихся «судов — призраков»), что представляет дополнительное давление на капитана и автоматику против столкновения.

4. *Дезактивация АИС-жертвы.* Используя возможности модели 4, атакующие отправляют от имени «береговой станции» команду, отключающую передатчик АИС на судне. В результате судно «не видит» чужих сигналов и само не отображается на приборах у других судов, становясь фактически невидимым в системе.

5. *Отвлекающие ложные тревоги.* Злоумышленники генерируют ложные сигналы бедствия поблизости (например, фальшивый сигнал «человек за бортом»). Это отвлекает внимание экипажа, и он вынужден реагировать на аварийную ситуацию, которой нет. Одновременно другие суда поблизости отвлекаются на помощь ложно терпящему бедствие судну.

6. *Инициирование аварии.* В кульминационный момент атакующие создают искусственную чрезвычайную ситуацию. Например, прямо по курсу судна внезапно возникает фантомное быстрое судно, направляющееся на таран. Система выдает немедленный сигнал уклонения, автопилот или напуганный рулевой в плохую видимость может резко переложить руль, в результате чего судно совершает опасный маневр — например, налетает на мель или попадает в засаду.

Этот сложный сценарий демонстрирует многогранную природу модели 5. Комбинация внутренних и внешних воздействий делает атаку крайне трудной для обнаружения. Даже если один из каналов будет выявлен, остальные все равно могут привести к успешной кибератаке. Данная ситуация является гипотетической, все ее элементы основаны на уязвимостях АИС, GPS и судовых сетей. В реальности аналогичной сложности инциденты уже происходили. Так, согласно данным баз кибератак на море (например, ADMIRAL), с 2019 по 2024 гг. были зафиксированы сотни таких инцидентов. Таким образом, модель 5 представляет собой наиболее опасный сценарий, характеризующийся высокой сложностью и требующий комплексных мер противодействия.

Помимо внешних угроз (M1–M5) в ходе исследования были рассмотрены внутренние угрозы, связанные с проникновением в компьютерную сеть судна. Результаты приведены в раздел «Обсуждение», поскольку требуют отдельного рассмотрения.

Обсуждение (Discussion)

Предложенные пять моделей внешних атак охватывают весь спектр ранее описанных сценариев, которые в имеющихся на эту тему исследованиях либо рассматривались без четкой структуры, либо были разделены на большие категории. Например, в отчете компании Trend Micro (2014 г.) все атаки классифицированы по двум направлениям: вмешательство через интернет-сервисы, собирающие данные АИС, и воздействие на радиоканал передачи. Такой подход полезен для общего понимания, но он в недостаточной степени детализирует уровни угроз. В настоящем исследовании обе эти группы раскрыты через конкретные сценарные модели: *интернет-вектор* представлен моделью 4 (взлом береговых систем и онлайн-сервисов), *радиовектор* — моделями 1–3 (от одиночных подделок до координированных атак). Кроме того, модель 5 демонстрирует возможное сочетание сценарных моделей в рамках комплексной многоэтапной атаки, между тем как внимание других авторов работ сосредоточено лишь на частных случаях. Так, например, в публикации [7] описан случай подделки координат, ложных «мин» и штормовых предупреждений. Такие примеры относятся к предложенной в данном исследовании классификации (модели 1–2).

В работе [6] отмечается возможность «потери целых судов» из-за кибератак, что соотносится с моделью 5 (комплексная атака). Таким образом, предлагаемая таксономия не противоречит известным данным, а структурирует их. Ее преимуществом является полнота охвата: модели M1–M5 покрывают диапазон от низкоуровневых до самых сложных угроз, включая промежуточные ступени, что позволяет более ясно оценивать риски. Кроме того, рассмотрена внутренняя угроза — ранее ей уделялось меньше внимания, в исследованиях [9, 11]. указывается на уязвимости внутренних сетей мостика. В данном исследовании обращается внимание на то, что защита АИС должна учитывать также *внутренние атаки*, *когда злоумышленник уже проник на судно.*

Внутренние атаки отличаются от внешних тем, что злоумышленник минуя радиоэфир, напрямую воздействует на приборы или сеть судна. Современные навигационные системы интегрированы: данные АИС, радара, GPS, эхолота объединяются в ECDIS / INS и передаются по сети. Если хакер получит доступ к этой сети (например, через уязвимый спутниковый терминал, зараженную флешку или закладное устройство), то он будет способен подменять навигационные сообщения. Практически это реализуется методами «человек посередине» (MitM) или «подделка на конце» (POTs), когда между датчиком и дисплеем вставляется вредоносный узел, изменяющий данные. Экспериментально показано, что посредством утилит (BRAT и аналогичных) можно в реальном времени транслировать в сеть корабля ложные координаты как своего судна, так и чужих судов, смещать отметки на экране и т. д. При отсутствии внешней верификации экипаж будет видеть на приборах согласованно искаженную картину в течение длительного времени, не подозревая об обмане. Опасность усиливается, если одновременно атакованы две и более системы (например, АИС и GPS). В этом случае даже проверка по независимому источнику затруднена. Результаты обзора показывают, что внутренние атаки — уже не теория и подобного рода прецеденты имели место. Так, в 2014 г. был зафиксирован случай, когда преступная группа взломала офисную сеть судоходной компании и получила доступ к журналам АИС-переговоров с тем, чтобы выследить контейнер с ценным грузом. Получив информацию о маршруте, они совершили вооруженное нападение на судно. Несмотря на то, что в данном инциденте не произошло взлома оборудования корабля, он демонстрирует ценность компрометации АИС-данных для злоумышленников. В 2019 г. на танкере во внутренней сети распространился вирус-«выкуп», что привело к выводу из строя некоторых систем. Данные случаи являются подтверждением актуальности внутренних угроз. Таким образом, выполненный авторами настоящего исследования анализ согласуется с выводами зарубежных экспертов о том, что недостаточное внедрение стандарта IEC 61162–460 (*защитного шлюза*) оставляет судовые сети незащищенными, и до тех пор, пока ситуация не изменится, атаки типа «подмена данных на мостике» остаются возможными [9].

Противодействие киберугрозам для АИС требует сочетания организационных и технических мер. Условно их можно разделить на *программно-алгоритмические* и *аппаратно-архитектурные*. К первым относятся методы, улучшающие протокол и программное обеспечение: аутентификация

и шифрование АИС-сообщений, фильтрация аномалий, системы обнаружения атак. Исследователи предлагают внедрить в АИС криптографическую подпись сообщений, чтобы приемники проверяли источник (например, схема с идентификацией на основе открытых ключей) [11]. Пилотные реализации такого Secure АИС разрабатываются, однако их глобальное внедрение осложнено проблемами совместимости и распределения ключей. Альтернативным направлением является создание *алгоритмов выявления подделок*. Активно исследуются системы мониторинга, которые анализируют поступающие данные признаков аномалий: нелогичные маневры, дублирование MMSI, рассинхронизация с радиолокацией и т. п. Например, если координаты АИС судна существенно расходятся с данными радара, то система может выдать предупреждение. Такие решения типа IDS — Intrusion Detection System уже частично внедряются производителями оборудования. Что касается аппаратных мер, то здесь ключевое значение имеет *сегментация* и *защита бортовой сети*. Стандарт IEC 61162–460 рекомендует устанавливать между навигационной сетью и другими подсистемами специальный шлюз-файрвол, контролирующий трафик и доступ. Сертифицированные устройства такого типа появляются на рынке, и некоторые суда уже оснащены ими. Кроме того, важным является применение общих мер «кибергигиены»: изоляция критичных узлов, регулярное обновление ПО навигационных комплексов, обучение экипажа. Человеческий фактор служит последней *линией защиты и свидетельством того, что морякам нельзя полагаться безоговорочно на электронные данные*. Поэтому (IMO, BIMCO) выпускают руководства для судовладельцев по разработке процедур в случае инцидентов с киберугрозой, проводят тренинги и т. д.

В работе [12] выполнен обзор текущего массива работ по кибербезопасности в морской и судоходной отраслях. В частности, обращается внимание на то, что морская кибербезопасность является новой областью научных исследований с учетом актуальности и значимости этой проблемы.

В работе [13] авторами впервые рассмотрен вопрос использования АИС для морских автономных надводных судов (МАНС). Отмечается, что ретроспективные данные АИС могут быть использованы для прогнозирования траектории движения судов, что, с одной стороны, является релевантным подходом, а с другой, соответствует моделям угроз М2–М3. При этом авторы предлагают использовать инфраструктуру АИС для передачи маршрутной информации, что при соответствующей формализации протоколов обмена может обеспечить устойчивость к киберугрозам класса подмены существующего траффика движения, например, на ранее записанный, но с деформированными временными метками.

В работе [14] авторы приводят результаты масштабного анализа данных АИС в Балтийском море с целью выявления опасностей, а также изучения практических действий экипажей судов при расхождении или при наличии навигационных опасностей. Данные результаты были заложены в основу тестирования и оценки эффективности действий МАНС путем сравнения их с реальными действиями (маневрами) экипажа судов. При этом такой анализ может быть использован также при создании киберугроз, а именно создании заведомо опасной ситуации в сети АИС или создании условий для побуждения экипажа к определенным маневрам, которые в конечном итоге могут быть опасными.

Примером масштабной атаки на сеть АИС (Модель М5) могут быть данные, приведенные в работе [15], где на основе анализа трафика движения судов выделены области с максимальным транспортным потоком судов с высокой интенсивностью и плотностью движения. Скорее всего, злоумышленники будут использовать такие географические кластеры для планирования атак, поскольку высокая плотность потока судов не оставляет достаточного времени на анализ угроз и их предупреждение.

Нерешенным остается вопрос о применение методов формальной оценки безопасности IMO [16] для выявления самих угроз и их возможных последствий. Анализ имеющихся источников информации показал, что подобные исследования для АИС-сетей практически не проводятся, скорее всего, в силу сложности работы с большими объемами данных и недостаточной формализации возможных рисков. Необходимо также отдельно рассмотреть вопрос «теневого режима» АИС и «закрытых групп обмена данными». Парадоксально, но одним из способов защиты от внешних угроз

является отключение или ограничение АИС в опасных районах. Согласно требованиям международных правил капитанам судов разрешено отключать транспондер АИС, если сохранность судна находится под угрозой (например, при опасности нападения пиратов) [1, 2]. Таким образом, судно *уходит в тень*, становится невидимым для общего трафика. Широкое использование такого режима ведет к появлению закрытых групп судов, не обменивающихся данными с остальными.

В настоящее время существует феномен «темных флотов»: группы коммерческих судов (например, участвующие в нелегальных перевозках нефти) по договоренности отключают АИС, создавая параллельную невидимую сеть [8]. С одной стороны, отсутствие сигнала затрудняет для злоумышленников слежение и атаки через подделку: «*нет сигнала, нет подделки*». С другой стороны, отказ от АИС снижает общую безопасность судоходства, так как окружающие суда не видят «погасшие» объекты. Кроме того, преступные группы могут использовать закрытые каналы обмена навигационными данными, недоступные властям. Обсуждается идея создания защищенных кластеров АИС, когда, например, военные корабли или конвои могут обмениваться координатами только внутри зашифрованной группы. По сути, это аналог *теневого режима*, но в контролируемом формате. Пока такие решения не стандартизированы, но в перспективе могут появиться. В целом тенденция такова: либо АИС-сеть станет безопаснее для всех, либо все большее количество судов будут уходить «в тень», что чревато потерей основной ценности АИС, а именно прозрачности и открытости информации о движении.

Заключение (Discussion)

АИС из важнейшего инструмента обеспечения безопасности мореплавания превратилась в потенциальный вектор кибератаки. Выполненный анализ показал, что АИС имеют фундаментальные уязвимости, позволяющие злоумышленникам фальсифицировать координаты и параметры судов, создавать несуществующие цели, рассылать дезинформацию (ложные штормовые или аварийные сигналы) и даже выводить из строя оборудование. Эти атаки могут исходить как извне (через радиоэфир), причем порог их реализации сравнительно низок, так и изнутри (через взломанные бортовые системы), что порой представляет еще большую опасность. Реальные случаи, произошедшие в течение последних 20 лет, подтвердили нетеоретический характер угроз — от экспериментальных демонстраций исследователей (Trend Micro, UT Austin и др.) до инцидентов с сотнями «кораблей-призраков» у побережий и целенаправленных кибератак в преступных целях. Все они свидетельствуют о том, что кибербезопасность на море требует не меньшего внимания, чем традиционные меры безопасности.

Международное сообщество предпринимает шаги для решения проблемы. В частности, принятие Резолюции IMO MSC.428(98) позволило учесть киберриски в рамках системы управления безопасностью судоходства [1]. Разрабатываются новые стандарты и рекомендации (например, стандарт IEC 61162–460 [4], руководства BIMCO), выходят обновления протоколов. Тем не менее, как отмечают аналитики, инерция отрасли велика: внедрение мер происходит медленно, многие предлагаемые решения являются сложными и требуют значительных финансовых затрат для практического применения [10]. Тем не менее можно предположить, что при активизации киберугроз в судоходстве на национальном уровне возникнет необходимость доработки Руководств [17] и Правил РС [18].

В настоящее время гражданская АИС-сеть остается открытой, и все суда транслируют данные в эфир без защиты. Поэтому особую роль играет *мониторинг и подготовка*: необходимо фиксировать все необычные инциденты (создание баз данных морских кибератак типа MCAD, ADMIRAL), распространять информацию о методах злоумышленников и вырабатывать стандарты реагирования. Экипажи должны понимать, что «видимое на экране не всегда соответствует истине», и отрабатывать навыки перехода на резервные средства. Производителям оборудования рекомендовано встраивать средства индикации аномалий и недостоверности данных.

Результатом данного исследования является формализация пяти типовых моделей кибератак на сеть АИС и систематизация ранее разрозненных сведений. Предложенная классификация может служить основой для оценки рисков и разработки учебных сценариев для экипажей. Кроме того,

проанализирована внутренняя угроза и отмечается необходимость защиты не только радиоканала, но и бортовых интегрированных систем. Следующим шагом планируется практическая отработка описанных сценариев на симуляторах и тестовых стендах для оценки эффективности существующих средств защиты. Также необходимо дальнейшее исследование методов аутентификации АИС-сообщений и разработка прототипов защищенных приемопередатчиков. В целом сочетание технологических решений (шифрование, шлюзы безопасности) и организационных мер (политики кибербезопасности, обучение персонала) должно обеспечить существенное снижение рисков.

СПИСОК ЛИТЕРАТУРЫ

1. IMO. Resolution MSC.428(98). Maritime Cyber Risk Management in Safety Management Systems. 2017. [Электронный ресурс]. — Режим доступа: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (дата обращения: 27.08.2025).

2. IALA. Guideline 1082 — An Overview of АИС, Ed. 2.0. Saint-Germain-en-Laye, France: IALA, June 2016. [Электронный ресурс]. — Режим доступа: https://navcen.uscg.gov/sites/default/files/pdf/IALA_Guideline_1082_An_Overview_of_АИС.pdf (дата обращения: 27.08.2025).

3. IEC. International Standard IEC 61162–450:2018. Maritime navigation and radiocommunication equipment and systems — Digital interfaces — Part 450: Multiple talkers and multiple listeners — Ethernet interconnection (Lightweight Ethernet). — Geneva: IEC, 2018. — 84 p.

4. IEC. International Standard IEC 61162–460:2015. Maritime navigation and radiocommunication equipment and systems — Digital interfaces — Part 460: Multiple talkers and multiple listeners — Ethernet interconnection — Safety and Security (Security gateway). — Geneva: IEC, 2015. — 62 p.

5. *Storm D.* Hack in the Box: Researchers attack ship tracking systems for fun and profit [Электронный ресурс]. — Режим доступа: https://www.computerworld.com/article/2500102/hack-in-the-box — researchers-attack-ship-tracking-systems-for-fun-and-profit.html (дата обращения: 27.08.2025).

6. *Семёнов С. А.* Сетевая угроза: как защитить морские суда от кибератак? // Транспортная безопасность и технологии. — 2018. — № 2(53). — С. 86–91.

7. *Антипов А.* Возможные угрозы для морского судоходства, исходящие от взломанной системы АИС SecurityLab. [Электронный ресурс]. — Режим доступа: https://www.securitylab.ru/analytics/497745.php (дата обращения: 27.08.2025).

8. *Kessler G. C.* AIS Spoofing: A Tutorial for Researchers / G. C. Kessler, D. M. Zorri // 2024 IEEE 49th Conference on Local Computer Networks (LCN) — 2024. — С. 1–7. DOI: 10.1109/LCN60385.2024.10639747.

9. *Oruc A.* Perspectives on the Cybersecurity of the Integrated Navigation System / A. Oruc, G. Kavallieratos, V. Gkioulos, S. Katsikas // Journal of Marine Science and Engineering. — 2025. — Vol. 13. — Is. 6. — P. 1087. DOI: 10.3390/jmse13061087.

10. *Munro K.* Ships can't be hacked. Wrong. Pen Test Partners Blog. [Электронный ресурс]. Режим доступа: https://www.pentestpartners.com/security-blog/ships-cant-be-hacked-wrong/ (дата обращения: 27.08.2025).

11. *Hemminghaus C.* BRAT: a BRIDGe attack tool for cyber security assessments of maritime systems / C. Hemminghaus, J. Bauer, E. Padilla // TransNav the International Journal on Marine Navigation and Safety of Sea Transportation. — 2021. — Т. 15. — № 1. — С. 35–44. DOI: 10.12716/1001.15.01.02.

12. *Harish A. V.* Literature review of maritime cyber security: The first decade / A. V. Harish, K. Tam, K. Jones // Maritime Technology and Research. — 2024. — Vol. 7. — Is. 2. — Pp. 273805. DOI: 10.33175/mtr.2025.273805.

13. *Смоленцев С. В.* Проблемы использования сообщений автоматической идентификационной системы в задаче прогнозирования траекторий движения судов / С. В. Смоленцев, Д. В. Исаков, М. Б. Солодовниченко // Вестник государственного университета морского и речного флота имени адмирала С. О. Макарова. — 2025. — Т. 17. — № 2. — С. 163–174. DOI: 10.21821/2309-5180-2025-17-2-163-174. — EDN AYBTLM.

14. *Smolentsev S. V.* Algorithm for analyzing the automatic identification system data to identify typical scenarios for vessel divergence and testing the systems of autonomous shipping / S. V. Smolentsev, A. A. Butsanets, S. F. Shakhnov, A. P. Nyrkov, E. O. Ol'khovik // T-Comm. — 2024. — Vol. 18. — Is. 3. — Pp. 50–59. DOI: 10.36724/2072-8735-2024-18-3-50-59.

15. *Ol'khovik E.* Assessment of the Possibility of Using a Waterway for Operation of Autonomous Ships / E. Ol'khovik, A. Butsanets, A. Zhidkova // Transportation Research Procedia. — 2023. — Vol. 68. — Pp. 383–388. DOI: 10.1016/j.trpro.2023.02.051.

16. The Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process. London: IMO, 2018 — 71 p.

17. Руководство по обеспечению кибербезопасности. НД № 2–030101–040. — Санкт-Петербург: ФАУ «Российский морской регистр судоходства», 2021. — 46 с.

18. Правила классификации и постройки морских судов, часть XXI: Киберустойчивость. НД № 2–020101–174. — Санкт-Петербург: ФАУ «Российский морской регистр судоходства», 2025. — 74 с.

REFERENCES

1. IMO. Resolution MSC.428(98). Maritime Cyber Risk Management in Safety Management Systems. 2017. Web. 27 Aug. 2025 <https://wwwcdn.imo.org/localresources/en/ OurWork/Security/Documents/Resolution%20MSC.428(98).pdf>.

2. IALA. Guideline 1082 — An Overview of АИС, Ed. 2.0. Saint-Germain-en-Laye, France: IALA, June 2016. Web. 27 Aug. 2025 <https://navcen.uscg.gov/sites/default/files/pdf /IALA_Guideline_1082_An_Overview_of_АИС.pdf>.

3. IEC. *International Standard IEC 61162–450:2018. Maritime navigation and radiocommunication equipment and systems* — Digital interfaces — Part 450: Multiple talkers and multiple listeners — Ethernet interconnection (Lightweight Ethernet). Geneva: IEC, 2018.

4. IEC. *International Standard IEC 61162–460:2015. Maritime navigation and radiocommunication equipment and systems* — Digital interfaces — Part 460: Multiple talkers and multiple listeners — Ethernet interconnection — Safety and Security (Security gateway). Geneva: IEC, 2015.

5. Storm D. Hack in the Box: Researchers attack ship tracking systems for fun and profit Web. 27 Aug. 2025 <https://www.computerworld.com/article/2500102/hack-in-the-box — researchers-attack-ship-tracking-systems-for-fun-and-profit.html>.

6. Semyonov, S.A. “Setevaya ugroza: kak zashchitit’ morskie suda ot kiberatak? “ *Transportnaya bezopasnost’ i tekhnologii* 2(53). (2018): 86–91.

7. Antipov A. Vozmozhnye ugrozy dlya morskogo sudohodstva, iskhodyashchie ot vzlomannoj sistemy AIS. SecurityLab. Web. 27 Aug. 2025 <https://www.securitylab.ru/analytics/497745.php>.

8. Kessler, G. C. and D. M. Zorri. “AIS Spoofing: A Tutorial for Researchers.” *2024 IEEE 49th Conference on Local Computer Networks (LCN)* — 2024: 1–7. DOI: 10.1109/LCN60385.2024.10639747.

9. Oruc, A., G. Kavallieratos, V. Gkioulos and S. Katsikas. “Perspectives on the Cybersecurity of the Integrated Navigation System.” Journal of Marine Science and Engineering 13.6 (2025): 1087. DOI: 10.3390/jmse13061087.

10. Munro K. Ships can’t be hacked. Wrong. Pen Test Partners Blog. Web. 27 Aug. 2025 <https://www.pentestpartners.com/security-blog/ships-cant-be-hacked-wrong/>.

11. Hemminghaus, C., J. Bauer and E. Padilla. “BRAT: a BRIDGe attack tool for cyber security assessments of maritime systems.” *TransNav the International Journal on Marine Navigation and Safety of Sea Transportation* 15.1 (2021): 35–44. DOI: 10.12716/1001.15.01.02.

12. Harish, A. V., K. Tam and K. Jones. “Literature review of maritime cyber security: The first decade.” *Maritime Technology and Research* 7.2 (2024): 273805. DOI: 10.33175/mtr.2025.273805.

13. Smolentsev, S. V., D. V. Isakov and M. B. Solodovnichenko. “Problems of using automatic identification system messages in the task of forecasting vessel movement trajectories.” *Vestnik gosudarstvennogo universiteta morskogo i rechnogo flota im. admirala S. O. Makarova* 17.2 (2025): 163–174. DOI: 10.21821/2309-5180-2025-17-2-163-174.

14. Smolentsev, S. V., E. O. Ol’khovik, et al. “ Algorithm for analyzing the automatic identification system data to identify typical scenarios for vessel divergence and testing the systems of autonomous shipping.” *T-Comm* 18.3 (2024): 50–59. DOI: 10.36724/2072-8735-2024-18-3-50-59.

15. Ol’khovik, E., A. Butsanets and A. Zhidkova. “Assessment of the Possibility of Using a Waterway for Operation of Autonomous Ships.” *Transportation Research Procedia* 68 (2023): 383–388. DOI: 10.1016/j.trpro.2023.02.051.

16. The Guidelines for Formal Safety Assessment (FSA) for use in the IMO rule-making process. London: IMO, 2018.

17. Rukovodstvo po obespecheniyu kiberbezopasnosti. ND № 2–030101–040. Saint-Petersburg: FAU «Rossijskij morskoj registr sudohodstva», 2021.

18. Pravila klassifikacii i postrojki morskih sudov, chast’ XXI «Kiberustojchivost’». ND № 2–020101–174. Saint-Petersburg: FAU «Rossijskij morskoj registr sudohodstva», 2025.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Волков Василий Владимирович —
ведущий инженер-разработчик,
ООО «НПФ Маринэк»
198035, Российская Федерация, Санкт-Петербург, ул. Двинская, д. 12
e-mail: *vasekama160599@yandex.ru*

Ольховик Евгений Олегович —
доктор технических наук, профессор
ФГБОУ ВО «ГУМРФ имени адмирала С. О. Макарова»
198035, Российская Федерация, Санкт-Петербург, ул. Двинская, 5/7
e-mail: *olhovikeo@gumrf.ru*

Федосенко Юрий Семенович —
доктор технических наук, профессор,
заведующий кафедрой «Систем информационной безопасности, управления и телекоммуникаций»
ФГБОУ ВО «Волжский государственный университет водного транспорта»
603950, Нижний Новгород, ул. Нестерова, 5а
e-mail: *fds1707@mail.ru*

INFORMATION ABOUT THE AUTHORS

Volkov, Vasily V —
Lead Design Engineer, Scientific and Production Firm “Marinek” LLC
12 Dvinskaya Str., St. Petersburg 198035, Russian Federation
e-mail: *vasekama160599@yandex.ru*

Ol’khovik, Evgeniy O. —
Grand PhD in Technical Sciences, professor
Admiral Makarov State University of Maritime and Inland Shipping
5/7 Dvinskaya Str., St. Petersburg 198035, Russian Federation
e-mail: *olhovikeo@gumrf.ru*

Fedosenko, Yuriy S. —
Grand PhD in Technical Sciences, Professor,
Head of the Department «Systems of Information Security Systems, Control and Telecommunications»”
Volga State University of Water Transport
Nesterova St., 5a, Nizhniy Novgorod, 603950, Russian Federation,
e-mail: *fds1707@mail.ru*

Статья поступила в редакцию: 01 сентября 2025 г.
Received: Sep. 1, 2025.