

УДК 656.6

**БАЛАНС ИННОВАЦИЙ И БЕЗОПАСНОСТИ
В РАЗВИТИИ ВОДНОГО ТРАНСПОРТА****Верескун Ирина Александровна¹**, бакалавр*e-mail:* irinavereskun05@list.ru¹ Государственный морской университет имени адмирала Ф.Ф. Ушакова, Новороссийск, Россия

Аннотация. В статье рассматривается противоречие между активным внедрением инноваций (беспилотное судовождение, интеллектуальные порты, импортозамещение навигации) и необходимостью обеспечивать экономическую, информационную и физическую безопасность на водном транспорте России. Предлагается комплекс мер — нормативных, технических, экономических, организационных и кадровых, — позволяющих не выбирать между инновациями и безопасностью, а совмещать их. Сделан вывод о возможности достижения баланса при системном подходе.

Ключевые слова: водный транспорт, инновации, безопасность, беспилотное судовождение, кибербезопасность, баланс рисков, интеллектуальные порты, импортозамещение.

**BALANCE OF INNOVATION AND SAFETY
IN WATER TRANSPORT DEVELOPMENT****Irina A. Vereskun¹**, Bachelor's Degree Student*e-mail:* irinavereskun05@list.ru¹ Admiral Ushakov Maritime State University, Novorossiysk, Russia

Abstract. This article examines the tension between the active implementation of innovations (unmanned navigation, smart ports, import substitution for navigation) and the need to ensure economic, informational, and physical security water transport. A set of measures—regulatory, technical, economic, organizational, and personnel—is proposed to eliminate the need to choose between innovation and safety, rather than to combine them. A conclusion is drawn that a systemic approach can achieve this balance.

Keywords: water transport, innovation, safety, unmanned navigation, cybersecurity, risk balance, smart ports, import substitution.

Водный транспорт в России, непосредственно, соединяет жизнь огромных территорий. Северный завоз, доставка топлива в отдалённые посёлки, перевозка зерна по Волге, экспорт нефти из портов Балтики и Чёрного моря — всё это организовано за счет водного

транспорта, по средствам судов, портов, экипажей и береговых служб. Но в последние годы отрасль столкнулась с новым уровнем. С одной стороны, появление технологий: суда, которые могут ходить без капитана, системы, которые сами прокладывают маршрут и экономят топливо, порты, где краны работают без людей. А с другой стороны, эти же технологии принесли в нашу жизнь риски и связанные с ними последствия и проблемы такие как, кибератаки, подделка навигационных сигналов, утечка данных о грузах. Наше государство взяло курс на цифровую трансформацию.

В Транспортной стратегии до 2030 года чётко сказано: внедрять беспилотные технологии, создавать цифровые платформы, автоматизировать порты, а введенные санкции, подтверждают правильность этого решения. Многие западные компании ушли с рынка, и теперь приходится самим делать навигационное оборудование, системы управления. А когда что-то делается в спешке, безопасность часто отодвигается на второй план, или не продумывается вообще, из-за сжатых сроков. Все это подчеркивает актуальность выбранной темы.

Цель работы — предложить подходы к достижению баланса между внедрением инноваций и обеспечением безопасности на водном транспорте России.

Специфика водного транспорта колоссально отличается от других видов транспорта будь то автомобильный, железнодорожный или авиационный. Первая особенность — автономность и удалённость. Судно может находиться в море или на отдалённом речном участке неделями, а иногда и месяцами. Устойчивая связь есть далеко не всегда, и в такой ситуации, если что-то пошло не так (например, кибератака или сбой системы), быстро помочь судну не получится. Это значит, что системы управления должны быть максимально автономными и отказоустойчивыми. Но чем больше автономии, тем сложнее защита.

Вторая особенность — критическая инфраструктура. Порты, шлюзы, гидроузлы, причалы — это не просто здания и краны. Это объекты, от которых зависит работа целых регионов. А современные порты становятся всё более цифровыми: электронные очереди, автоматические ворота, системы управления движением судов. Один успешный взлом — и гигантский транспортный узел выходит из строя моментально, неся соответствующие ему огромные потери.

Это и есть следующая третья особенность - высокая стоимость последствий. Авария на водном транспорте может привести разливу нефти, человеческим жертвам (если это пассажирские суда, паромы). Это многомиллиардные штрафы и страховые выплаты. Четвёртая особенность — человеческий фактор. Когда на судне появляются сложные цифровые системы, риск ошибки возрастает. Существует вероятность случайно отключить защиту, загрузить вирус с флешки. Следовательно, даже самая совершенная техническая защита может быть сломана простым человеческим действием.

Эти особенности подтверждают, что водный транспорт — это среда повышенной чувствительности. Внедрять здесь инновации, не думая о безопасности, нельзя. Но и отказываться от инноваций, ссылаясь на риски, тоже нельзя — отрасль отстанет, станет неконкурентоспособной. Нужен баланс. И чем точнее он будет найден, тем лучше.

Существует направления, которые уже начинают тестировать на судах:

Беспилотное и автономное судовождение. Это самая обсуждаемая тема и разные уровни делегирования: от автоматизации отдельных операций (например, удержание курса) до полностью автономного судна, которое может выйти из порта, пройти по маршруту и пришвартоваться без участия человека. В России реализуются проекты «Пилот» на Волге, беспилотные буксиры в порту Усть-Луга, ведутся эксперименты на Северном морском пути. Плюсы очевидны: снижение расходов на экипаж (а это большая статья затрат), уменьшение влияния человеческого фактора (усталость, ошибки), возможность



оптимизировать маршруты в реальном времени. Однако риски тоже серьёзные. Во-первых, кибервзлом. Если хакер получит доступ к системе управления судном, он сможет направить его куда захочет — на мель, на встречное судно, в запретную зону. Во-вторых, спуфинг GNSS — подделка сигналов спутниковой навигации. Судно думает, что идёт по фарватеру, а на самом деле его уведут в сторону. В-третьих, потеря связи с береговым центром. В 2020 году исследователи из Университета Техаса удалённо захватили управление яхтой через уязвимости в автопилоте. В 2023 году в Чёрном море фиксировались случаи спуфинга GPS, из-за которых несколько судов чуть не сели на мель.

Интеллектуальные порты (Smart Port). Современный порт — это уже не просто причалы и склады. Это автоматизированные краны, которые работают без крановщиков, электронные очереди для грузовиков, системы распознавания номеров, единая операционная система. Плюсы: рост пропускной способности, снижение очередей, меньше ошибок при учёте грузов. Минусы: единая точка отказа. Если хакеры атакуют операционную систему порта, работа может встать полностью. Краны не будут двигаться, ворота не откроются, грузы потеряются. Кроме того, через удалённый доступ можно физически саботировать оборудование: разогнать кран, перегрузить конвейер.

Импортозамещение навигационного оборудования. После ухода западных компаний Россия вынуждена создавать свои приёмники ГЛОНАСС, авторулевые, эхолоты, системы автоматической идентификации. Это важнейшая задача для технологического суверенитета. Но на начальном этапе отечественные системы уступают импортным по надёжности и защищённости. Выявлены следующие риски: недостаточная отработка криптозащиты, сбои ПО, проблемы совместимости со старыми судовыми системами.

И чтобы инновации не превращались в катастрофу, нужны определенные правила. Транспортная стратегия РФ до 2030 года — главный документ отрасли. В ней много сказано о цифровизации, об инновациях, о безопасности. Но эти понятия идут отдельно. Нет раздела, который бы назывался «Безопасность инноваций». Существует серьёзный пробел, ведь нет требования оценивать риски до того, как внедрять новую технологию.

Правила Российского морского регистра судоходства — технический документ, по которому строят и классифицируют суда. В последние годы в него начали включать требования по киберзащите. Но пока они носят рекомендательный характер. То есть судовладелец может их выполнять, а может и нет. Для автономных судов обязательных требований вообще нет — их просто не существует в правилах. Федеральный закон №187-ФЗ «О безопасности критической информационной инфраструктуры» распространяется на порты, железные дороги, аэропорты и атомные ледоколы. Но на обычные суда, такие как танкер или сухогруз — нет.

Ведомственные приказы Минтранса по транспортной безопасности в основном касаются физической защиты (пропускной режим, досмотр) и антитеррора. Кибербезопасность судовых систем в них почти не прописана. В итоге получается картина: нормативная база сильно отстаёт от технологий. Есть отдельные хорошие начинания (проект ГОСТ Р 59355-2025 по защите судовых автоматизированных систем), но они ещё не утверждены. Нет обязательной оценки влияния инноваций на безопасность. Нет стандартов для беспилотных судов. Нет ответственности за кибератаки на суда. Это зоны, которые требуют срочного вмешательства.

Механизмы достижения баланса, рассмотрение системного подхода. Опираясь на анализ специфики, рисков и пробелов в законах, был сформулирован рекомендательный комплекс мер.

Нормативные механизмы. Первое — закрепить в Транспортной стратегии принцип, что любой инновационный проект с самого начала должен включать требования к защите. Второе — разработать и утвердить ГОСТы для судовых автоматизированных систем



управления с обязательными криптографическими требованиями. Третье — ввести обязательную сертификацию кибербезопасности для судов, работающих в автономном или дистанционно-управляемом режиме. Четвёртое — создать процедуру оценки влияния на безопасность для всех инновационных проектов на водном транспорте, претендующих на господдержку.

Технические механизмы. Действия на уровне судна и береговой инфраструктуры. Многофакторная аутентификация для удалённого доступа к судовым системам (пароль + токен + биометрия). Физическая и логическая изоляция сетей управления от сетей общего доступа (WiFi для экипажа не должен пересекаться с системой управления двигателем). Системы обнаружения вторжений на судовой сети, которые сигнализируют о подозрительной активности.

Экономические механизмы. Безопасность стоит денег. Но её можно стимулировать. Субсидии и налоговые льготы для судоходных компаний, которые внедряют сертифицированные защищённые системы. Дифференциация страховых тарифов — если судно защищено хорошо, ставка по каско должна быть ниже. За рубежом такие практики уже есть. В России можно создать фонд компенсации убытков от киберинцидентов на водном транспорте — по аналогии с фондами на случай разлива нефти.

Организационные и кадровые механизмы. Технологии бесполезны без людей. Предлагается создать Отраслевой центр кибербезопасности водного транспорта. Этот центр будет разрабатывать стандарты, анализировать инциденты и, что самое важное, готовить специалистов. В учебные планы транспортных вузов необходимо ввести дисциплины: «Информационная безопасность судовых систем», «Киберриски в управлении флотом», «Правовые аспекты инноваций».

Водный транспорт — сложнейшая система, где любая ошибка или сбой могут привести к катастрофе. Внедрение инноваций в такую систему требует особой осторожности. Нельзя просто взять и поставить беспилотное судно на линию. Слишком серьезные могут быть последствия: жизни людей, экология, финансовые потери. Было показано, что специфика водного транспорта многократно усиливает риски, связанные с инновациями. Автономность судов (они неделями в море без быстрой помощи), критический характер портовой инфраструктуры (один сбой — и вся цепочка встаёт), высокая стоимость последствий (разлив нефти или столкновение пассажирского лайнера — это миллиарды рублей), технологическая зависимость от импорта (до 80% навигации — чужое) и низкая цифровая грамотность экипажей — всё это делает отрасль уязвимой.

Инновации и безопасность на водном транспорте не должны противопоставляться. Ключевые риски сосредоточены в этих зонах: беспилотное судовождение, интеллектуальные порты, импортозависимость. Баланс достигается комплексом мер — нормативных, технических, экономических, кадровых, организационных. Роль вузов и молодёжной науки — не только генерировать инновационные идеи, но и с самого начала оценивать их безопасность. Перспектива — переход от простого баланса к синергии, когда меры безопасности сами становятся инновациями. Россия может занять лидирующие позиции в безопасном автономном судоходстве.

Список литературы:

1. Гарнов А.П., Краснова Л.Н. Экономическая безопасность предприятия: современные вызовы и цифровые решения. — М.: ИНФРА-М, 2024. — 215 с.



2. ГОСТ Р 59355-2025. Безопасность информационных технологий. Защита судовых автоматизированных систем. Общие требования (проект). — М.: Стандартинформ, 2025. — 34 с.
3. Иванов А.Н. Кибербезопасность в морской отрасли: практическое руководство / Под ред. А.Н. Иванова. — СПб.: Морской вестник, 2024. — 210 с.
4. Кузьмичев И.К., Лукачева К.Е. Цифровая трансформация водного транспорта: вызовы и решения // Вестник ВГУВТ. — 2025. — № 2. — С. 34–41.
5. Транспортная стратегия Российской Федерации на период до 2030 года с прогнозом до 2035 года: официальный текст. — М.: Кодекс, 2022. — 87 с.
6. Безопасность судовых информационных систем: рекомендации BIMCO [Электронный ресурс]. — Режим доступа: <https://www.bimco.org/cybersecurity> (дата обращения: 10.04.2026).
7. Единая государственная система информации об обстановке в Мировом океане (ЕСИМО). Раздел «Кибербезопасность на флоте» [Электронный ресурс]. — Режим доступа: <https://esimo.ru/cyber> (дата обращения: 10.04.2026).

