Введение

Автономное судоходство осуществляется на основе принципа V2X (Vehicle-to-Everytning), являющегося базовым для любых интеллектуальных транспортных систем [1]. В интеллектуальных системах водного транспорта (ИСВТ) реализация принципа V2X обеспечивает взаимодействие судов между собой, с инфраструктурой водных путей и центрами управления судоходством, а также с другими объектами, способными оказать влияние на поведение судов. Но, наряду с улучшениями, реализация принципа V2X влечет расширение перечня актов незаконного вмешательства в функционирование ИСВТ за счет угроз, обусловленных недекларированными возможностями и уязвимостями внедряемых технологий, являющихся конвергенцией информационных и телекоммуникационных технологий, технологий автоматизированного и автоматического управления и искусственного интеллекта. Особенностями указанных технологий является работа с большими объемами информации. Нарушение безопасности информации, обрабатываемой в ИСВТ: неправомерный доступ, подмена, шифрование, удаление, блокировка доступа и тому подобные несанкционированные воздействия, — вызывает нарушение транспортной безопасности (ТБ) и, как следствие, безопасности критической информационной инфраструктуры и критической инфраструктуры страны, национальной безопасности.

Указанные обстоятельства существенно изменяют представления об обеспечении ТБ судоходства как деятельности, связанной с использованием судов на внутренних водных путях [2, 3]. Однако действующая нормативная правовая база обеспечения ТБ не содержит требований, адаптированных к меняющимся условиям судоходства, а подразделения обеспечения ТБ не отражают в своих планах мероприятия по предупреждению актов незаконного вмешательства, влекущих указанные последствия [4–6]. Для снижения рисков их возникновения должны применяться научно обоснованные, закреплённые в нормативной правовой базе методы, модели, алгоритмы и механизмы обеспечения ТБ, отвечающие всему спектру угроз ТБ ИСВТ.

В ИСВТ важная роль принадлежит информационным системам и автоматизированным системам управления административного назначения, относимым к автоматизированным системам корпоративного управления, а также системам автоматического управления судами и объектами инфраструктуры, автоматизированным системам управления технологическими процессами и другим, относимым к автоматизированным системам технологического управления. В ИСВТ эти системы, как правило, образуют интегрированные автоматизированные системы корпоративного и технологического управления, между составными частями которых наблюдается цифровое неравенство [7]. В этих условиях вектор угроз может иметь комплексную направленность и вызывать множественные, но труднообнаруживаемые нарушения ТБ. Для снижения влияния цифрового неравенства на ТБ ИСВТ должны применяться научно обоснованные модели архитектуры ИСВТ, учитывающие весь спектр угроз ТБ ИСВТ.

Санкции, вызвавшие нарушение цепочек поставок технологий, оборудования и программных средств, обострили проблему зависимости от импорта. Для достижения технологического суверенитета ИСВТ необходимо применять отечественные защищенные аппаратно-программные платформы, обеспечивающие стабильность в течение всего срока жизни ИСВВТ и безопасное функционирование ИСВВТ в составе критической инфраструктуры [8, 9]. Для решения данной задачи необходима научно обоснованная и проверенная на практике методология создания отечественных защищенных аппаратно-программных платформ, способствующая повышению обоснованности выбора платформы и недопущению монополизации их рынка.

В пункте 9 перечня поручений Президента Российской Федерации от 19.12.2020 № Пр-2177 [10] Правительству Российской Федерации поручено обеспечить внесение изменений в законодательство Российской Федерации в части, касающейся регулирования правоотношений, возникающих при использовании безэкипажного (автономного) судовождения, проведение в период с 2021 по 2025 год эксперимента по опытной эксплуатации безэкипажных (автономных) судов, подготовку предложений по развитию инфраструктуры морской подвижной спутниковой системы связи в целях ее использования хозяйствующими субъектами, внедряющими средства безэкипажного (автономного) судовождения.

Распоряжением министра транспорта Российской Федерации от 15.02.2021 № ВС-23-р [11] решение ключевых задач в области

безэкипажного (автономного) судовождения поручено обеспечить Российскому университету транспорта (РУТ (МИИТ)).

На базе РУТ (МИИТ) создан консорциум «Электронная навигация и безэкипажное (автономное) судовождение», в состав которого вошли Московский физико-технический институт (национальный исследовательский университет, МФТИ), Государственный университет морского и речного флота имени адмирала С.О. Ушакова (ГУМРФ, АО «Ситроникс» и АО «Ситроникс КТ» [12].

РУТ (МИИТ) совместно с МФТИ в рамках программы стратегического академического лидерства «Приоритет-2030» выполняются работы по теме «Реализация проектов по разработке конструкторско-технологических решений и программных продуктов в области систем управления автономным судном на основе удаленного доступа (включая системы объективного контроля судна, системы обеспечения безопасности и живучести автономного судна)» (шифр СПЗ-19/РИД). Их целью является достижение технологического лидерства в области электронной навигации и безэкипажного (автономного) судовождения путём разработки и реализации пилотной модели эксплуатации безэкипажного (автономного) судна на основе проведения прикладных исследований, разработки специализированного программного обеспечения, разработки документов по техническому регулированию в области электронной навигации и безэкипажного (автономного) судовождения.

В монографии представлены результаты научного исследования проблем обеспечения транспортной безопасности ИСВТ, обусловленных их вышеуказанными особенностями.

Монография состоит из введения, шести частей, заключения и списка использованных источников.

В первой части исследована проблема неполноты учета угроз транспортной безопасности автономного судоходства, обусловленная появлением новых видов актов незаконного вмешательства нефизической природы, существенно расширяющих ландшафт угроз транспортной безопасности, реализация которых может вызывать нарушение безопасности критической инфраструктуры страны и национальной безопасности.

Во второй части рассмотрено автономное судовождение как сложный высокотехнологичный объект, для обеспечения транспортной безопасности которого необходимо защитить его по требованиям безопасности информации и обеспечить его информационную безопасность.

В третьей части представлены описательные модели системы автономного судоходства на внутренних водных путях, интеллектуальных систем внутреннего водного транспорта и их объектов, рассмотренные с позиций их уязвимости от актов незаконного вмешательства нефизической природы.

В четвертой части третьей рассмотрены безэкипажные и иные автономные надводные суда, их компьютеризированные и программируемые электронные системы, воздействие на которые может повлечь нарушение транспортной безопасности интеллектуальных систем внутреннего водного транспорта.

В пятой части рассмотрена проблема цифрового неравенства составных частей интегрированных автоматизированных систем корпоративного и технологического управления транспортной безопасностью интеллектуальных систем водного транспорта.

В шестой части исследована проблема недостаточного развития отечественных программно-аппаратных комплексов для интеллектуальных систем водного транспорта, представлена методология создания защищенных отечественных аппаратно-программных платформ, реализованная автором при создании автоматизированных систем в защищенном исполнении различного назначения.

В заключении изложены выводы и рекомендации по результатам части исследований, отраженных в монографии.