Оригинальная статья
https://doi.org/10.21683/1729-2646-2024-24-2-72-87

Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем

Conceptual problems of transportation security of intelligent water transportation systems

Михалевич И.Ф.
Mikhalevich I.F.

Российский университет транспорта (МИИТ), Москва, Российская Федерация
Russian University of Transport (MIIT), Moscow, Russian Federation

mif-orel@mail.ru

Михалевич И.Ф.

Резюме. Цель. *На водные пути выходят морские автономные и дистанционно-управляемые надводные суда (МАНС), безэкипажные суда внутреннего плавания (БЭС). Интеллектуальной становится инфраструктура водных путей. Повышается интеллектуальный уровень морских и речных портов, портовых терминалов и пристаней. Масштабное внедрение информационных технологий, технологий автоматизированного управления, автоматического управления и искусственного интеллекта существенно расширило ландшафт угроз транспортной безопасности водных интеллектуальных транспортных систем (ИТС) угрозами не физического происхождения. На изменение ландшафта угроз необходимо своевременно реагировать, чтобы не возникало разрыва между реально достигнутым уровнем интеллектуализации и совокупностью мер по обеспечению транспортной безопасности водных ИТС.* **Проблемы.** *Подмена или изменение показаний датчиков МАНС (БЭС) или сигналов, получаемых их исполнительными устройствами, может привести к изменению направления движения судов и вызвать их столкновения между собой или с объектами инфраструктуры, посадку на мель, а то и вовсе захват МАНС (БЭС) и находящихся на них пассажиров, грузов и сопровождающих их лиц. Несанкционированный доступ к информации в автоматизированных системах управления портовых терминалов может быть использован для злонамеренного шифрования информации. Это может вызвать блокировку погрузочно-разгрузочных работ в порту, срыв расписания движения судов, нарушение логистических операций в масштабах до национального уровня. Последствия национального уровня могут классифицироваться как нарушение безопасности критической информационной инфраструктуры страны, связанное с транспортной небезопасностью водной ИТС. Общей для различных ИТС является проблема цифрового неравенства автоматизированных систем технологического и корпоративного управления в сфере безопасности вышеназванных технологий.* **Методы.** *Обеспечение транспортной безопасности водных ИТС требует применения всего доступного комплекса методов, средств и мер защиты. Правовая база обеспечения транспортной безопасности должна учитывать весь спектр актуальных видов незаконного вмешательства в функционирование водных ИТС и обязывать к планированию и выполнению соответствующего ему комплекса защитных мероприятий. В статье применены методы системного анализа и обеспечения комплексной безопасности сложных систем.* **Результаты.** *Проведен анализ новых видов угроз транспортной безопасности водных транспортных систем и нормативной правовой базы обеспечения их транспортной безопасности. Выявлено, что новые виды угроз транспортной безопасности водных транспортных систем в них не учтены и, как следствие, в планах обеспечения транспортной безопасности отражения не находят. Рассмотрена архитектура водных ИТС в виде интегрированной автоматизированной системы корпоративного и технологического управления, применение которой направлено на динамичное согласование моделей водных ИТС с моделями актуальных угроз транспортной безопасности в информационной сфере.* **Заключение.** *Для обеспечения транспортной безопасности водных ИТС необходимо учитывать новые виды угроз, которые связаны с недекларированными возможностями и уязвимостями информационных технологий, технологий автоматизированного управления, автоматического управления и искусственного интеллекта. Рассмотренные проблемы носят системный характер, так как незаконное вмешательство в функционирование водных ИТС может негативно влиять на другие системы критической информационной инфраструктуры. Это следует учитывать при разработке нормативных правовых актов по обеспечению транспортной безопасности на водном и других видах транспорта.*

Abstract. Aim. *Autonomous and remote-controlled surface sea vessel (ASSV) and unmanned inland water vessels (UIWV) are entering the waterways. The infrastructure of waterways is becoming intelligent. The intellectual level of sea and river ports, port terminals, and harbours is improving. Large-scale deployment of information technologies, automated control, automatic control, and artificial intelligence has significantly expanded the landscape of transportation security threats to water intelligent transportation systems (ITS) and now includes non-physical threats. The evolving threat landscape requires timely response in order to avoid gaps between the current state of intellectual technology application and the set of measures to ensure the transportation security of water ITS.* **Problems.** *Spoofing or modifying sensors readings in ASSV (UIWV) or signals received by their executive units can cause vessels to lose direction and collide with each other or with infrastructure facilities, run aground, or even being hijacked along with the passengers, cargo, and attendants. Unauthorized access to information in automated control systems of port terminals can be used to maliciously encrypt information. That may block cargo handling operations in a port, disrupt ship traffic schedules and logistics operations up to the national level. National-level consequences can be classified as a disruption of the national information infrastructure security associated with the transportation insecurity in ITS. The various existing ITS have the common problem associated with the digital inequality of the automated systems employed by industrial enterprises and corporate governance in terms of the security of the above technologies.* **Methods.** *Ensuring the transportation security of water ITS requires the application of all available methods, means, and measures of protection. The legal framework of transportation security is to take into account the full range of relevant methods of illegal interference into the operation of water ITS and require planning and implementing a corresponding set of protective measures. The article uses methods of systems analysis and comprehensive security of complex systems.* **Results.** *The author analysed the new types of threats to the transportation security of water transportation systems and the corresponding regulatory framework. It was identified that the latter do not take into account the new types of threats to the transportation security of water transportation systems. Consequently, those are not covered by the transportation security planning. The paper examines the architecture of water ITS in the form of an integrated automated system of corporate and process management, whose application aims to dynamically coordinate water ITS models with those of current information-related threats to the transportation security.* **Conclusion.** *Ensuring the transportation security of water ITS requires taking into account the new types of threats associated with undocumented capabilities and vulnerabilities of information technologies, automated control, automatic control, and artificial intelligence technologies. The examined problems are of a systemic nature, since illegal interference in the operation of water ITS can negatively affect other systems of critical information infrastructure. That should be taken into account when developing regulations related to ensuring the transportation security of water and other modes of transportation.*

Ключевые слова: *Автоматизированная система корпоративного управления, автоматизированная система технологического управления, водный транспорт, интегрированная автоматизированная система корпоративного и технологического управления, интеллектуальная транспортная система, информационная безопасность, искусственный интеллект, недекларированные возможности, уязвимость, цифровая трансформация.*
Keywords: *automated corporate management system, automated process management system, water transportation, integrated automated corporate and process management system, intelligent transportation system, information security, artificial intelligence, undocumented capabilities, vulnerability, digital transformation.*

Для цитирования: *Михалевич И.Ф. Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем // Надежность. 2024. №2. С. 72-87. https://doi.org/10.21683/1729-2646-2024-24-2-72-87*
For citation: *Mikhalevich I.F. Conceptual problems of transportation security of intelligent water transportation systems. Dependability 2024;2:72-87. https://doi.org/10.21683/1729-2646-2024-24-2-72-87*

Поступила: *16.09.2023* / **После доработки:** *12.04.2024* / **К печати:** *10.06.2024*
Received on: *16.09.2023* / **Revised on:** *12.04.2024* / **For printing:** *10.06.2024*

Введение

Транспортная отрасль Российской Федерации находится в состоянии цифровой трансформации, в рамках которой осуществляется масштабное внедрение информационных технологий, технологий автоматизированного управления, автоматического управления и искусственного интеллекта. На основе этих технологий создаются и развиваются интеллектуальные транспортные системы (ИТС) всех видов транспорта, в том числе водного[1].

На водные просторы выходят морские автономные и дистанционно-управляемые надводные суда (МАНС) и безэкипажные суда внутреннего плавания (БЭС). Их поведение зависит от автоматически получаемой информации об окружающей навигационной обстановке и автоматически вырабатываемых решений о направлении, скорости и других параметрах движения судов, которая может быть злонамеренно подменена или изменена. Также возможна подмена или изменение показаний датчиков МАНС (БЭС), или сигналов, получаемых их исполнительными устройствами, что может привести к изменению направления движения и вызвать столкновения судов между собой или с объектами инфраструктуры, посадку на мель, а то и вовсе захват МАНС (БЭС) и находящихся на них пассажиров, грузов и сопровождающих их лиц.

Интеллектуальной становится инфраструктура водных путей. В 2021 году на подходном канале в Обской губе Карского моря для обеспечения безопасности судоходства были установлены 22 буя, оснащенные средствами автоматической идентификационной системы[2] (АИС). Такого рода интеллектуализированные знаки навигационного оборудования водных путей по радиосвязи передают информацию о типе знака и его координатах, состоянии навигационных огней, которая может быть злонамеренно подменена или изменена и негативно повлиять на поведение МАНС (БЭС).

Повышается интеллектуальный уровень морских и речных портов и терминалов, пристаней. В их составе функционируют информационные системы и автоматизированные системы управления, поведение которых также может быть изменено путем злонамеренных информационных воздействий. В частности, несанкционированный доступ к информации в автоматизированных системах управления портовыми терминалами может сопровождаться злонамеренным шифрованием информации и вызвать блокировку погрузочно-разгрузочных работ в порту, срыв расписания движения судов, нарушение логистических операций в масштабах вплоть до национального уровня. Последствия национального уровня могут классифицироваться как нарушение безопасности критической информационной инфраструктуры страны, вызванное транспортной небезопасностью водной ИТС.

Такого рода акты незаконного вмешательства в деятельность водных ИТС принято классифицировать по критериям безопасности информации. Она может быть нарушена в части конфиденциальности, доступности, целостности, аутентичности и достоверности, а также в совокупности отмеченных свойств информации.

1. Расширение ландшафта угроз транспортной безопасности водных транспортных систем

Согласно закону[3] и ГОСТ Р 56461-2015[4] транспортная безопасность определяется как состояние защищенности объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства, под которыми понимаются любые противоправные действия или бездействие, угрожающие безопасной деятельности транспортного комплекса, влекущие причинение или создающие угрозу причинения вреда жизни и здоровью людей или материальный ущерб. Следовательно, деятельность по обеспечению транспортной безопасности водных ИТС должна учитывать акты незаконного вмешательства как физического, так и не физического характера.

Информационные технологии, технологии автоматизированного управления, автоматического управления и искусственного интеллекта реализуются с использованием программных и аппаратных средств, программно-аппаратных комплексов, компьютеризированных и программируемых электронных систем, которые могут содержать программные закладки и уязвимости, позволяющие, в частности, осуществлять:

- несанкционированный доступ и несанкционированные воздействия на информацию, данные и информационные ресурсы водных ИТС;

- несанкционированный доступ и несанкционированные воздействия на объекты управления водных ИТС и их компоненты: датчики, исполнительные устройства, компьютеризированные и программируемые электронные системы управления судами, объектами инфраструктуры водных путей, портов и портовых терминалов, причалов, береговых центров управления безэкипажными судами и т.п., которые также должны быть защищены по требованиям безопасности информации[5].

[1] Транспортная стратегия Российской Федерации до 2030 года с прогнозом на период до 2035 года (утверждена распоряжением Правительства Российской Федерации от 27.11.2021 №3363-р).

[2] На Севморпути впервые установлены буи со станциями автоматической идентификационной системы // Российское судоходство, 21.10.2021. Отраслевой портал Российской палаты судоходства https://www.rus-shipping.ru/ru/service/news/?id=45658

[3] Федеральный закон от 09.02.2007 года № 16-ФЗ «О транспортной безопасности»

[4] ГОСТ Р 56461-2015 «Безопасность транспортная. Общие требования».

[5] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах,

Программными закладками являются внесенные в программное обеспечение водных ИТС вредоносные программы и/или программный код, которые инициируют выполнение не описанных в документации функций программного обеспечения[1], реализацию его недекларированных возможностей[2]. Это, например, вирусы, черви, трояны, программы-шифровальщики и др.

Уязвимость водных ИТС в общем случае можно определить как наличие слабых мест в их активах или элементах управления, которые могут быть использованы одной или несколькими угрозами[3]. Программной уязвимостью является недостаток (слабость) программного обеспечения, программно-технического средства или системы и сети в целом, который может быть использован для реализации угроз безопасности информации[4]. В водных ИТС они могут быть связаны, в частности, с уязвимостями программного кода, конфигурации, архитектуры или организации водной ИТС. Уязвимости могут быть также многофакторными.

Сложившийся исторически перечень видов актов незаконного вмешательства в функционирование объектов водных транспортных систем отражает действия, совершаемые исключительно путем физического доступа к объектам воздействия (транспортным средствам, инфраструктуре водных путей, портам, причалам, зданиям и т.п.) и с использованием исключительно физических средств воздействия (взрывчатки, газов, средств поджога и т.п.).

Для водных ИТС физический доступ к объектам воздействия не является обязательным и может осуществляться путем ближнего беспроводного доступа и удаленного доступа через сеть Интернет, что отражено на рис. 1.

Физический доступ предоставляет злоумышленнику полный перечень возможностей для незаконного вмешательства в функционирование МАНС (БЭС), интеллектуальных объектов инфраструктуры водных путей, причалов, информационных и автоматизированных систем управления портов и портовых терминалов. Но использоваться он может не только для совершения террористических, хулиганских и аналогичных актов, природа которых выявляется тут же по видимым следам и последствиям. Не менее опасными являются акты незаконного вмешательства, связанные с программными закладками и программными уязвимостями, приводящие к нарушению или прекращению функционирования объектов водных ИТС. При этом природа совершения таких актов не столь очевидна, а следы их подготовки и совершения могут быть надежно скрыты и даже удалены.

При нахождении вблизи вышеуказанных объектов водных ИТС злоумышленник может осуществить беспроводной доступ и вмешаться в функционирование встроенного в них интеллектуального оборудования (компьютеризированных и/или программируемых электронных систем) и вызвать нарушение (прекращение) функционирования объекта. Такое же вмешательство доступно злоумышленнику в отношении интеллектуального оборудования водных ИТС, подключенного к Интернету.

Рис. 1. Возможные пути доступа для совершения актов незаконного вмешательства в функционирование объектов водных ИТС

Для преднамеренного незаконного вмешательства могут быть задействованы все пути. Например, несанкционированный физический или беспроводной доступ может быть использован для подготовки канала для последующего удаленного вмешательства через Интернет с использованием средств искусственного интеллекта и иных вычислительно затратных средств.

На рис. 2 приведены результаты исследования рейтинга новых видов актов незаконного вмешательства в функционирование объектов авиационного, морского, железнодорожного и автомобильного транспорта ЕС в 2021-2022 годах [1]. Некоторые виды актов незаконного вмешательства вызвали комплексные последствия и были учтены в нескольких видах, вследствие чего общий процент учтенных актов превышает 100%.

Аналогичные результаты представлены Лабораторией Касперского в исследовательском отчете за первое полугодие 2023 года в отношении систем промышленной автоматики [2].

представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (утверждены приказом ФСТЭК от 14 марта 2014 г. № 31).

[1] Согласно ГОСТ Р 51624-2000. Автоматизированные информационные системы в защищенном исполнении. Общие положения.

[2] Согласно ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

[3] Согласно ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary.

[4] Согласно ГОСТ Р 56546-2015. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем.

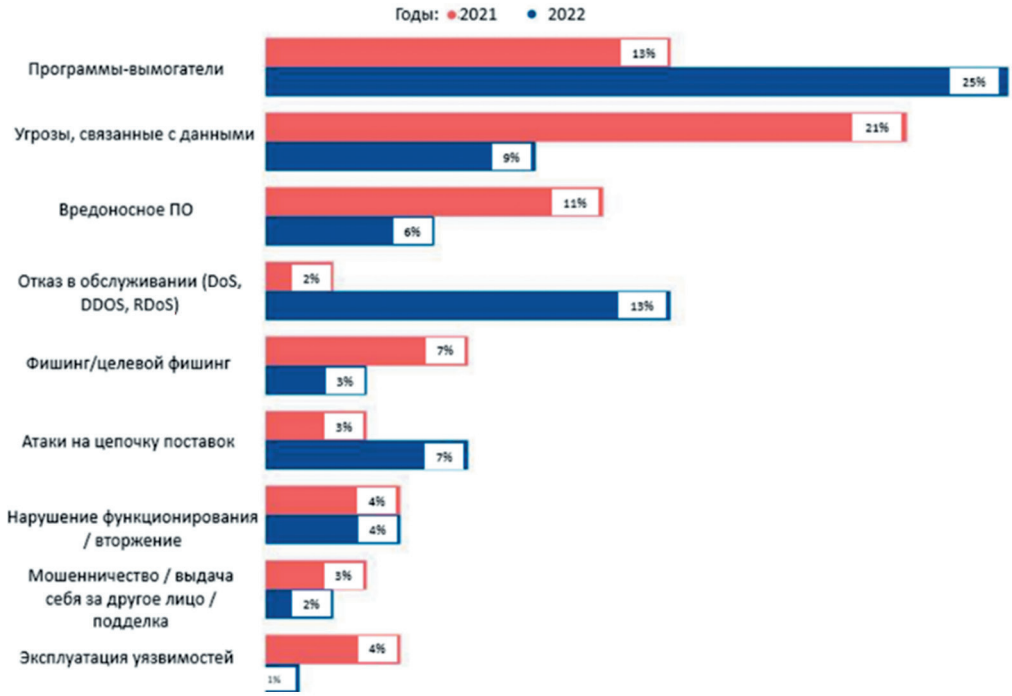


Рис. 2. Основные виды актов незаконного вмешательства в функционирование транспортного сектора ЕС в 2021-2022 годах (источник рисунка: [1])

В названных и других источниках обращено внимание на проблему неполноты отчетности о событиях нарушения информационной безопасности и на тот факт, что публично раскрытые сведения, использованные при подготовке исследовательских отчетов, являются лишь верхушкой айсберга. Это обстоятельство можно отнести к причинам, по которым опасность отраженных на рис. 2 видов воздействий на водные ИТС недооценивается, а проблематика информационной безопасности не находит должного отражения в действующей нормативной правовой базе обеспечения транспортной безопасности водных ИТС, что подтверждают приведенные далее результаты ее анализа.

Комментируя рис. 2 и упреждая приведенные далее примеры, отметим следующее.

Водная отрасль все чаще сталкивается с угрозами транспортной безопасности типа «отказ в обслуживании»: DoS – отказ в обслуживании; RDoS – отказ в обслуживании с требованием выкупа; DDoS – распределенный отказ в обслуживании. В 2022 году реализация таких угроз в транспортном секторе ЕС выросла в шесть с половиной раз по сравнению с 2021 годом. В 2023 году тенденция роста сохранилась.

Эта угроза достаточно проста в реализации и осуществляется путем направления многочисленных запросов на сайты (или другие публичные информационные ресурсы) объектов водного транспортного комплекса. Это вызывает недоступность информационных ресурсов, влечет для их владельцев (операторов) материальный вред и потерю репутации. Для проведения атаки могут задействоваться десятки и сотни тысяч устройств (компьютеры, устройства интернета-вещей и т.п.), о чем их владельцы не подозревают, но непроизвольно этому способствуют.

Атакам типа «отказ в обслуживании» предшествует массированное сканирование Интернета и составление баз данных об устройствах, готовых к несанкционированному использованию («порабощению»). Эти базы могут использоваться самими составителями или продаваться другим злоумышленникам. В теневом Интернете существует услуга предоставления в аренду определенного количества «порабощенных» устройств. Возможности для пополнения «армии» «порабощенных» устройств обусловлены, в первую очередь, беспечностью легитимных владельцев (пользователей, администраторов) «порабощаемого» оборудования, которые игнорируют правила цифровой гигиены [3, 4]. Недопустимая беспечность заключается, например, в использовании устройств с предустановленными (заводскими) параметрами доступа: логином и паролем (admin/admin, root/root и т.п.). Эти параметры публично известны для каждой модели и модификации устройств, что открывает возможность для несанкционированного доступа к ним и несанкционированного использования.

Традиционно транспортной безопасности угрожают программы шифровальщики и похитители данных.

Использованию таких программ неизменно предшествует этап сбора информации об объекте будущего незаконного вмешательства. Делается это в крайне «деликатной» форме: путем посещения офиса, подслушивания или прослушки разговоров сотрудников с использованием технических средств, а также удаленно путем «невинных» электронных или голосовых запросов, направленных по адресам электронной почты или

высказанных голосом по публично известным адресам электронной почты и номерам телефонов планируемого объекта незаконного вмешательства. Однако за «деликатностью» кроется сбор (выманивание, выуживание) персонифицированной информации о легитимных пользователях (руководителях, администраторах, и т.п., адресах их электронной почты, номерах телефонов), назначении и архитектуре объекта, используемом в нем оборудовании и средствах защиты.

Наличие такой информации позволяет перейти к более сложным воздействиям, основанным на несанкционированном доступе к разведанному объекту, закреплению в нем и последующему перемещению по его архитектуре, пример которой будет рассмотрен далее (рис. 4). В зависимости от целей вмешательства (кража информации, получение выкупа, нарушение функционирования автоматизированной системы технологического управления и другие) злоумышленник может осуществлять горизонтальное перемещение по архитектуре водной ИТС, оставаясь на одном уровне, или углубляться внутрь архитектуры (вертикально), закрепляться на достигнутом уровне и далее осуществлять в нем горизонтальное перемещение.

Зная адреса электронной почты, не выходя за пределы уровня архитектуры, реализующего функции системы корпоративного (административного) управления, злоумышленники могут массово отправлять письма, содержащие «невинные» ссылки и предложения перейти по ним. После перехода по ссылке на компьютер сотрудника может быть удаленно загружена и инсталлирована программная закладка, открывающая каналы для вертикального перемещения по архитектуре вплоть до самого нижнего уровня, на котором находятся датчики и исполнительные устройства систем автоматического управления движением судна, например.

Также незаметно может быть установлена программа-шифровальщик. Ее активация приведет к шифрованию информации. Недоступность несанкционированно зашифрованной информации SCADA портового терминала приведет к невозможности выполнения погрузочно-разгрузочных работ. За расшифровку информации или передачу ключей шифрования злоумышленники, как правило, требуют крупный выкуп.

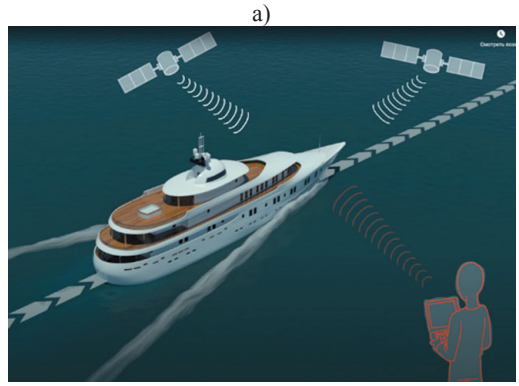
С применением программной закладки может быть получен несанкционированный доступ к персональным данным и иной конфиденциальной информации (служебной, коммерческой тайне и т.п.), обрабатываемой на объектах водного транспортного комплекса и ее раскрытие в публичных источниках или требование выкупа за нераскрытие информации.

И это только вершина айсберга новых видов актов незаконного вмешательства, расширяющих ландшафт угроз транспортной безопасности водных ИТС. Более того, ландшафт угроз водных ИТС расширяют также акты незаконного вмешательства непреднамеренного характера. Непреднамеренные акты незаконного вмешательства могут быть связаны с аппаратными сбоями и неисправностями средств вычислительной техники, не устраненными ошибками программного обеспечения, ошибочными действиями пользователей (операторов, администраторов) и т.п. событиями.

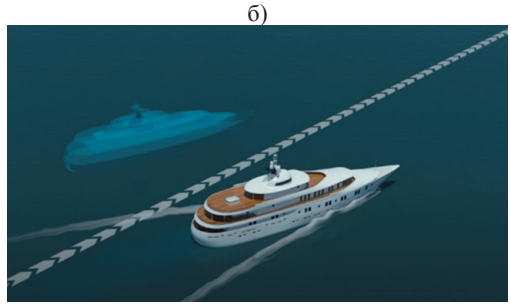
Некоторые из возможностей новых видов актов незаконного вмешательства в функционирование водных ИТС отражены в следующих примерах.

Без применения огнестрельного оружия или иных средств физического воздействия был изменен курс мегаяхты длиной 65 метров и стоимостью 80 миллионов долларов США (рис. 3) путем нефизического воздействия с использованием специализированного программно-аппаратного комплекса стоимостью2 тысячи долларов США [5, 6].

а)



б)



в)

Рис. 3. Изменение курса мегаяхты длиной 65 метров и стоимостью 80 миллионов долларов США путем подмены сигнала GPS (источники рисунков: а) – [5], б), в) – [6])

Вмешательство заключалось в подмене сигнала спутника GPS на сигнал, формируемый комплектом «псевдоспутникового» оборудования злоумышленника. Когда уровень сигнала «псевдоспутника» превысил уровень сигнала реального спутника GPS цифровой

приемник яхты переключился на более сильный сигнал «псевдоспутника», находящегося невдалеке (в сравнении с 10 000–20 000 км расстояния до спутников), судовое оборудование произвело расчет по ложным пространственным координатам спутника и курс яхты был изменен. Таким образом, нарушение достоверности навигационной информации о пространственных координатах, получаемой приемником глобальной навигационной спутниковой системы (ГНСС) яхты, создало для злоумышленника возможность повлиять на ее курс. Природа такого вмешательства обусловлена уязвимостями ГНСС, в которых не применены криптографические средства аутентификации источников сигналов (спутников), что создает условия для реализации описанной угрозы [7, 8]. Если такое воздействие будет произведено против МАНС или БЭС, не исключено, что судно сможет попасть в руки злоумышленников или погибнуть в столкновении с каким-либо препятствием. Проблема с уязвимостями ГНСС является общей для всех видов транспорта, включая авиа, что подтверждают последние (на момент написания статьи) события[1].

Уязвимой является также АИС водных ИТС. В задачи АИС входит обеспечение навигационной информацией других систем МАНС и БЭС, включая ГНСС, систему радиолокационного наблюдения, электронную картографическую навигационно-информационную систему. Как и в случае с ГНСС, навигационная информация АИС может быть подменена или изменена, что обусловлено отсутствием средств, обеспечивающих надежную аутентификацию реальных объектов АИС (судов или оборудованных приборами АИС навигационных знаков инфраструктуры водных путей) и достоверность передаваемой ими навигационной информации. Например, информации о судне, его классе, техническом состоянии, направлении движения, грузе и так далее.

Используя такого рода уязвимости АИС [7, 9], злоумышленники могут посылать ложные сообщения о бедствиях для сближения с МАНС (БЭС) и последующего захвата судна, его пассажиров или груза, подменять идентификаторы судов для совершения любого рода противоправных деяний (контрабанды, перевозки нелегальных мигрантов, торговли людьми).

Как отмечалось ранее, высокой популярностью у злоумышленников пользуются угрозы типа «отказ в обслуживании». Так, в сентябре 2022 года была осуществлена DDoS-атака на сайт порта Нагоя, что привело к его недоступности около 40 минут. Последствия совершенного акта посчитали, по всей видимости, несущественными, что оказалось ошибочным.

В июле 2023 года порт Нагоя подвергся новым воздействиям, совершенным, по предположению автора, после первичного закрепления на уровне автоматизированной системы корпоративного управления порта и дальнейшего проникновения (вертикального перемещения по архитектуре) на уровни автоматизированной системы технологического управления порта. Злоумышленником был получен несанкционированный доступ в «Единую терминальную систему порта Нагоя», что позволило установить программу-шифровальщик, провести несанкционированное шифрование информации и нарушить работу порта[2]. Порт Нагоя является крупнейшим и самым оживленным морским портом в Японии, обеспечивает около 10% от общего объема торговли страны, имеет 21 причал и 290 стоянок, ежегодно обрабатывает более двух миллионов контейнеров и 165 миллионов тонн груза. В результате совершенного акта операции по погрузке и разгрузке контейнеров на терминалах порта с использованием прицепов были отменены. Это вызвало серьезные простои в процессе транспортировке товаров в национальном масштабе, затронуло многие крупные компании (Тойота и др.) и причинило огромные финансовые и репутационные потери порту.

В июне 2023 года в Нидерландах DDoS-атаке подверглись сайты четырех портов в Роттердаме, Амстердаме, Ден-Хелдере и Гронингене. Сайты трех портов были недоступны несколько часов, а на восстановление сайта порта Гронингена потребовалось около 10 дней[3]. О других способах воздействия не сообщалось, но дальнейшее проникновение «вглубь» портовых интегрированных автоматизированных систем корпоративного и технологического управления исключать нельзя, особенно после истории с портом Нагоя.

В июле 2023 года мишенью программы-вымогателя стала портовая и железнодорожная компания Transnet SOC Limited в ЮАР[4]. Воздействие привело к тому, что на контейнерных терминалах были вынуждены перейти к ручной обработке грузов, в том числе в порту Дурбане, который обрабатывает более половины грузов страны и является основными воротами для других экспортеров сырьевых товаров, включая Демократическую Республику Конго и Замбию.

В ноябре 2023 года австралийский оператор DP World, отвечающий за 40% морских перевозок Австралии, в результате установки и активации злоумышленником программы-шифровальщика был вынужден закрыть четыре порта в Сиднее, Мельбурне, Брисбене и Фримантле, ввести запрет на разгрузку судов и вывоз контейнеров из портов. За время устранения последствий воздействия

[1] Самолеты «заблудились» из-за хакеров. Frequent Flyers Ru, December 8, 2023. URL: https://www.frequentflyers.ru/2023/12/08/gps_spoof/ (дата обращения 12.12.2023).

[2] Nagoya Port Resumes Some Operations After Ransomware Attack. Bloomberg Businessweek, July 6, 2023. URL: https://www.bloomberg.com/news/articles/2023-07-06/nagoya-port-delays-restart-following-alleged-ransomware-attack (дата обращения 26.10.2023).

[3] Dutch ports' websites offline for hours, days due to pro-Russian cyber attacks. NL TIMES, June 14, 2023. URL: https://nltimes.nl/2023/06/14/dutch-ports-websites-offline-hours-days-due-pro-russian-cyber-attacks (дата обращения 18.11.2023).

[4] Cyber Pirates Prowling Ship Controls Threaten Another Big Shock. Bloomberg Businessweek, June 28, 2023. URL: https://www.bloomberg.com/news/articles/2022-06-28/cyber-pirates-prowling-ship-controls-threaten-another-big-shock (дата обращения 26.10.2023).

была задержана отправка 30 000 морских контейнеров, скопившихся в портах[1]. На правительственном уровне отмечалось, что Австралия столкнулась с инцидентом национального значения, который продолжался в течение нескольких дней и повлиял на движение товаров в страну и из нее.

Приведенные примеры показывают, что с увеличением степени интеллектуализации перечень актов незаконного вмешательства в функционирование объектов водного транспорта будет только расширяться. Это вызывает необходимость обеспечить полноту учета актов незаконного вмешательства и соответствия мероприятий по обеспечению транспортной безопасности реальному ландшафту угроз.

2. Анализ полноты учета видов актов незаконного вмешательства в нормативной правовой базе обеспечения транспортной безопасности водного транспортного комплекса

На обеспечение транспортной безопасности водного комплекса направлены, в частности, следующие нормативные правовые акты:

- Технический регламент о безопасности объектов внутреннего водного транспорта (утвержден постановлением Правительства Российской Федерации от 12.08.2010 № 623);

- Требования по обеспечению транспортной безопасности, учитывающие уровни безопасности для транспортных средств морского и внутреннего водного транспорта (утверждены Постановлением Правительства Российской Федерации от 08.10.2020 № 1637);

- Требования по обеспечению транспортной безопасности, в том числе требования к антитеррористической защищенности объектов (территорий), учитывающие уровни безопасности для различных категорий объектов транспортной инфраструктуры морского и речного транспорта (утверждены Постановлением Правительства Российской Федерации от 08.10.2020 № 1638);

- Требования по обеспечению транспортной безопасности, в том числе требования к антитеррористической защищенности объектов (территорий), учитывающие уровни безопасности для объектов транспортной инфраструктуры морского и речного транспорта, не подлежащих категорированию (утверждены постановлением Правительства Российской Федерации от 10.102020 № 1651).

Технический регламент о безопасности объектов внутреннего водного транспорта (далее – технический регламент, регламент) содержит требования по обеспечению транспортной безопасности как транспортных средств внутреннего водного транспорта, так и связанной с ним инфраструктуры. В связи с этим первичный анализ полноты учета актов незаконного вмешательства был проведен по нему.

Из анализа следует, что применение технического регламента направлено на достижение следующих целей:

- защиту жизни и здоровья граждан, имущества физических и юридических лиц, государственного или муниципального имущества от опасности, источником которой может стать деятельность внутреннего водного транспорта и связанная с ним инфраструктура;

- охрану окружающей среды, жизни и здоровья животных и растений;

- предупреждение действий, вводящих в заблуждение приобретателей в отношении объектов внутреннего водного транспорта и процессов, связанных с их проектированием, производством, строительством, монтажом, эксплуатацией и утилизацией (далее – объекты регулирования);

- обеспечение энергетической эффективности.

Учитывая приведенные выше примеры, функционирование водных транспортных средств и объектов инфраструктуры водных путей может быть нарушено актами незаконного вмешательства в информационной сфере. Следовательно, выполнение требований технического регламента должно быть направлено на обеспечение, в том числе, информационной безопасности.

Дальнейший анализ показал, что выполнение требований технического регламента должно обеспечить:

а) биологическую безопасность объектов регулирования;

б) взрывобезопасность объектов регулирования;

в) гидрометеорологическую безопасность объектов регулирования;

г) единство измерений;

д) механическую безопасность объектов регулирования;

е) пожарную безопасность объектов регулирования;

ж) термическую безопасность объектов регулирования;

з) химическую безопасность объектов регулирования;

и) электрическую безопасность объектов регулирования;

к) электромагнитную совместимость в части обеспечения работы приборов и оборудования, относящихся к объектам регулирования;

л) экологическую безопасность объектов регулирования;

м) энергетическую и экологическую эффективность объектов регулирования;

н) другие виды безопасности объектов регулирования.

Содержание регламента отражает его направленность, указанную в пунктах с а) по м) приведенного выше перечня. Из перечня следует, что выполнение требований технического регламента не направлено на обеспечение информационной безопасности объектов

[1] Australia locks down ports after «nationally significant cyberattack». The Independent, November 11, 2023. URL: https://www.independent.co.uk/news/world/australasia/australia-ports-cyber-attack-dp-world-b2445634.html (дата обращения 11.11.2023).

регулирования, в отличие от обеспечения пожарной, экологической, биологической безопасности и безопасности в иных областях угроз физического происхождения. Отметим, что регламент уточняет требования, обязательность выполнения которых установлена федеральным законодательством, например: о пожарной безопасности[1], об охране окружающей среды[2], о биологической безопасности[3]. Но такие же обязательные требования для объектов регулирования технического регламента установлены федеральным законодательством в сфере информационных технологий[4,5]. Таким образом, в техническом регламенте допущен разрыв между физическими и «не физическими» областями транспортной безопасности водных транспортных систем, что создает угрозу их транспортной безопасности при совершении актов незаконного вмешательства информационного характера.

Можно было бы предположить, что вопросы информационной безопасности водных транспортных систем рассматриваются в других нормативных правовых актах в соответствии с вышеуказанным подпунктом н) технического регламента. Но, как следует из [10–12], это не так. В частности, в [12] отмечается: «в области информационной безопасности в сфере водного транспорта отсутствует единый, системный и комплексный подход, унификация требований и правил. … В России отсутствует транспортный отраслевой центр компетенции по информационной безопасности. Ни в положении о Минтрансе России, ни в положении о Росморречфлоте нет ничего об информационной безопасности. То есть формирование единой отраслевой политики в области информационной безопасности не является задачей или обязанностью федеральных органов власти в сфере транспорта».

Отраженные выше нормативные правовые акты, устанавливающие требования по обеспечению транспортной безопасности транспортных средств морского и внутреннего водного транспорта и объектов транспортной инфраструктуры морского и речного транспорта, требований по обеспечению информационной безопасности также не содержат.

Неполнота учета видов актов незаконного вмешательства в функционирование водного транспорта и объектов инфраструктуры водных путей ИТС приводит к их неучету в планах обеспечения транспортной безопасности и, соответственно, не отражению в них мероприятий по обеспечению информационной безопасности [10-12].

В целом вышеизложенное можно отнести к проблемам цифровой трансформации, динамика которой в практической области существенно опережает развитие правовой сферы.

3. Проблемы цифровой трансформации водного транспорта

На ход цифровой трансформации водного транспорта значительно повлияла пандемия COVID-19, которая существенно обострила проблемы, характерные именно для ИТС [3, 13–15].

За пандемией COVID-19 последовали санкции, запрещающие экспорт в Российскую Федерацию высокотехнологичного оборудования и комплектующих, материалов и программного обеспечения, необходимых для водных ИТС. Однако это не стало полной неожиданностью, на что указывают предпринятые превентивные меры практического характера [16–20]. Они были направлены на создание отечественных аппаратно-программных платформ для объектов критической информационной инфраструктуры, частью которой, в соответствии с федеральным законодательством[6], является транспортная отрасль.

Однако проблемные вопросы создания и развития водных ИТС вышеизложенным не ограничиваются. Так, составляющая ИТС, реализующая информационные технологии, технологии автоматизированного управления, автоматического управления и искусственного интеллекта, оказалась недостаточно готовой к защите от актов незаконного вмешательства именно в информационной сфере. Эта сфера имеет важное значение при выполнении высокотехнологичных функций в интегрированных системах, реализующих одновременно функционал информационных систем, автоматизированных систем управления и систем автоматического управления.

Архитектура такого рода интегрированных систем, предложенная автором в [13, 14, 21, 22], представлена на рис. 4. При ее разработке было принято, что полностью развернутая ИТС представляет собой интегрированную систему, реализующую именно одновременно функционал информационных систем, автоматизированных систем управления и систем автоматического управления. В интегрированной автоматизированной системе функционирование любой из ее составных систем зависит от результатов функционирования других. Такой подход позволяет формировать модели водных ИТС, адаптированные к актуальным угрозам транспортной безопасности, не нарушая целостности модели водной ИТС как единой системы. Это согласуется с методологией обеспечения безопасности критической информационной инфраструктуры, объекты которой могут одновременно содержать в себе

[1] Федеральный закон «О пожарной безопасности» от 21.12.1994 N 69-ФЗ

[2] Федеральный закон «Об охране окружающей среды» от 10.01.2002 № 7-ФЗ

[3] Федеральный закон от 30.12.2020 № 492-ФЗ «О биологической безопасности в Российской Федерации»

[4] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ.

[5] Федеральный закон от 26.07.2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

[6] Федеральный закон от 26.07.2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Рис. 4. Архитектура интегрированной автоматизированной системы корпоративного и технологического управления водной ИТС (источник рисунка: [13, 21])

информационные системы, автоматизированные системы управления и системы автоматического управления или их фрагменты.

В целях исключения избыточной детализации описания систем при рассмотрении вопросов обеспечения транспортной безопасности все многообразие систем можно разделить на два базовых вида: автоматизированные системы корпоративного управления (АСКУ) и автоматизированные системы технологического управления (АСТУ). Совместно они образуют интегрированные автоматизированные системы корпоративного и технологического управления (ИАСКиТУ) представленной на рис. 4 архитектуры. Это позволяет при рассмотрении отношений между субъектами незаконного вмешательства (нарушителями безопасности) и защищаемыми объектами исключить факторы, в меньшей степени влияющие на транспортную безопасность.

При таком моделировании обеспечивается возможность по-разному формировать состав АСКУ и АСТУ, перераспределяя между ними соседние уровни архитектуры. Такая необходимость обусловлена различиями в основном назначении конкретных объектов водных ИТС, каждый из которых в конкретной ситуации в большей степени выполняет функции той или иной входящей в его состав системы: информационной, автоматизированного управления или автоматической, для каждой из которых формируется свой перечень актуальных угроз транспортной безопасности. Это позволяет распределить актуальные угрозы между уровнями ИАСКиТУ, обеспечивает детальное рассмотрение каждой угрозы, способов ее реализации и связанных с нею рисков, выработку адресных мер по устранению (нейтрализации) угроз в составе АСКУ и АСТУ, комплексное обеспечение транспортной безопасности водной ИТС как единой системы.

Приведенная на рис. 4 архитектура была апробирована при моделировании угроз безопасности информации системы автономного судовождения на внутренних водных путях, выполненном в рамках стратегического проекта «Электронная навигация и безэкипажное (автономное) судовождение»[1] по Программе стратегического академического лидерства «Приоритет – 2030». Применение интегрированной архитектуры позволило рассмотреть акты незаконного вмешательства в функционирование водной ИТС через призму их влияния на элементы, реализующие функции корпоративного

[1] Стратегический проект № 3. Электронная навигация и беспилотное (автономное) судовождение. https://www.miit.ru/page/178854

управления (например, в части взаимодействия с информационными ресурсами Единой государственной информационной системы обеспечения транспортной безопасности) и технологического управления (например, дистанционного управления БЭС) как для каждого элемента в отдельности, так и в их взаимной связи, определить негативные последствия, возможность наступления которых обусловлена, в том числе, наличием межуровневых связей в водной ИТС, имеющей интегрированную архитектуру.

В модели ИАСКиТУ водных ИТС рассматриваются две группы и четыре типа сущностей. В зависимости от решаемых задач транспортной безопасности сущность каждого типа может выполнять роль субъекта или объекта незаконного вмешательства.

Первую группу образуют такие сущности как информация (сущность 1) и данные (сущность 2). Под информацией понимаются все виды сообщений, сведений, команд и сигналов в их естественной физической форме, то есть в форме, воспринимаемой людьми непосредственно без применения программируемых технических средств. Под данными – все виды сообщений, сведений, команд и сигналов, представленных в цифровой форме. То есть подразумевается, что данные, как таковые, не существуют в физическом мире, а являются результатом преобразования информации в форму, пригодную для автоматической обработки, в том числе при возможном участии человека[1,2]. Таким образом учитывается, что информация и данные могут являться как объектом, на который направлено незаконное вмешательство, так и субъектом, которым незаконное вмешательство осуществляется. Например, подмена информации источника приведет к недостоверности данных, передаваемых от имени источника. Пусть их передача в сети осуществляется с соблюдением всех требований безопасности данных и при передаче данные не будут искажены. Пусть также они не будут искажены при преобразовании на стороне получателя в форму, воспринимаемую человеком. В этом случае измененная информация источника будет восприниматься ее получателем-человеком как истинная (достоверная), со всеми вытекающими для обеих сторон последствиями. В роли получателя может быть не только человек, но и техническое средство. В этом случае искаженная информация источника, которым может быть, например, физический (аналоговый) датчик, поступит в искаженном виде к физическому (аналоговому) исполнительному устройству, что вызовет реакцию, не соответствующую фактическому состоянию датчика.

Исходя из изложенного, вторую группу образуют такие сущности, как люди (сущность 3) и компьютеризированные и программируемые электронные системы и их компоненты (сущность 4). Таким образом учитывается, что человек (группа людей) и программное обеспечение со всеми своими производными (аппаратно-программные средства, сети, системы и т.п.) могут являться как объектом, на который направлено незаконное вмешательство, так и субъектом, которым незаконное вмешательство осуществляется.

Такое разделение на сущности позволяет перераспределять уровни АСКиТУ между АСКУ или АСТУ по признаку, определяющему, кто или что является объектом незаконного вмешательства. Принято, что любое незаконное вмешательство в информационной сфере, независимо от субъектности (человек, бот, устройство интернета вещей и т.п.), может повлечь неблагоприятные последствия для человека (группы людей, бизнеса, государства) непосредственно. Например, побудить человека к совершению действий, приводящих к нарушению безопасности данных. Такими действиями могут быть: ввод в систему недостоверной информации; изменение уставок средств автоматики и т.п. Или, применение легитимным пользователем незарегистрированных флэш-накопителей в контролируемой зоне, защищенной воздушным зазором, межсетевыми экранами, однонаправленными шлюзами (цифровыми диодами) и тому подобными средствами. Но указанное поведение человека способно свести на нет все предпринятые меры технической (в том числе криптографической) защиты информационных систем, автоматизированных систем управления и систем автоматического управления водных ИТС.

Также принято, что и любое нарушение безопасности данных способно повлечь неблагоприятные последствия для человека (группы людей, бизнеса, государства) опосредованно, вызвав нарушение или прекращение функционирования управляемого объекта, обеспечивающего информационные потребности людей, поддержку технологических и иных критически важных для них, бизнеса и государства процессов. В части водных ИТС нарушение безопасности данных, формируемых в ГНСС, АИС, системах управления движением МАНС и БЭС влекут крайне опасные последствия, описанные ранее.

Таким образом, АСКУ будут образовывать уровни ИАСКиТУ, которые содержат все виды систем (ERP, CRM, сайты, электронная почта и т.п.), выполняющих информационные и административные функции. В таких системах информация может контролироваться самими людьми непосредственно. Исходя из этого, в состав АСКУ будут включаться уровни ИАСКиТУ, в которых объектом незаконного воздействия, направленным на нарушение безопасности информации и/или данных, является человек.

Соответственно АСТУ будут образовывать уровни, содержащие все виды систем (ГНСС, АИС, автоматического сбора информации, управления движением и курсом судна, технологическими процессами производ-

[1] ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

[2] ГОСТ Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации.

ства продукции и оказания услуг, проведения денежных операций, технического обслуживания, экспериментов, функционирования IoT, IIoT и т.п.), предназначенные для управления объектами, функционирование которых осуществляется без прямого (непосредственного) контроля со стороны человека, которому для контроля необходимы специализированные средства работы с данными. Соответственно АСТУ являются системы, в которых объектом незаконного воздействия, направленным на нарушение безопасности данных и/или информации, являются датчики, исполнительные устройства, программируемые логические контроллеры и иные технические средства, способные изменять свое состояние без обязательного участия человека (без обращения к человеку за получением или подтверждением команды и т.п.).

Общей проблемой, характерной для различных ИТС, является цифровое неравенство в защищенности их АСТУ и АСКУ (OT- и IT-систем в зарубежной терминологии [23–26]) от актов незаконного вмешательства в сфере вышеуказанных технологий, что рассмотрено в [3, 14, 22]. Свидетельством такого неравенства является наличие в Государственном реестре сертифицированных средств защиты информации ФСТЭК России[1] и Перечне средств защиты информации, сертифицированных ФСБ России[2], сотен наименований средств защиты информации, разработанных для АСКУ, и только десятков наименований средств, разработанных для защиты информации и данных в АСТУ.

Такая ситуация сложилась исторически, так как внимание к информационной безопасности раньше было акцентировано в основном в отношении АСКУ, которые в большинстве своем имели распределенный характер, могли использовать открытое информационное пространство и их масштабная цифровизация началась задолго до цифровой трансформации АСТУ.

Прежние АСТУ функционировали, как правило, в своих замкнутых информационных пространствах, которые ограничивались производственными сетями передачи данных, соединяющими объекты на нулевом и первом уровнях архитектуры, представленной на рис. 4. С интеллектуализацией водного транспорта ситуация существенно меняется, затрагивая все вышеуказанные уровни управления и оказывая непосредственное влияние на транспортную безопасность.

Традиционный и, фактически, неизменный характер АСКУ позволил разработать для них нормативную правовую и методическую базу обеспечения безопасности, в том числе транспортной. Интеграция в составе водных ИТС АСКУ и АСТУ требует реагирования в правовой области обеспечения транспортной безопасности, нарушение которой может быть вызвано нарушением безопасности информации и данных, обрабатываемых в водных ИТС. Учитывается ли это обстоятельство, можно проверить на следующем примере.

4. Анализ проекта технического регламента обеспечения транспортной безопасности объектов внутреннего водного транспорта

В табл. представлены сведения о направленности требований действующего и проекта нового технического регламента обеспечения транспортной безопасности объектов внутреннего водного транспорта[3].

Табл. Направленность требований действующего и проекта нового технического регламента обеспечения транспортной безопасности объектов внутреннего водного транспорта

№ п/п	Требования Технического регламента о безопасности объектов внутреннего водного транспорта должны обеспечить:	
	Действующий регламент	Проект нового регламента
1	биологическую безопасность объектов регулирования	
2	взрывобезопасность объектов регулирования	
3	гидрометеорологическую безопасность объектов регулирования	
4	единство измерений	
5	механическую безопасность объектов регулирования	
6	пожарную безопасность объектов регулирования	
7	термическую безопасность объектов регулирования;	
8	химическую безопасность объектов регулирования	
9	электрическую безопасность объектов регулирования	
10	электромагнитную совместимость в части обеспечения работы приборов и оборудования, относящихся к объектам регулирования	
11	экологическую безопасность объектов регулирования	
12	энергетическую и экологическую эффективность объектов регулирования	безопасность судоходства при воздействии на объект регулирования.
13	другие виды безопасности объектов, указанные в целях применения настоящего технического регламента	-

Как видно из табл., проект нового регламента попрежнему не содержит требований, направленных на обеспечение безопасности информации и данных, нарушение которой в водных ИТС может повлечь гибель людей, привести к материальным и репутационным потерям, экологическим потрясениям.

[1] https://reestr.fstec.ru/reg3?ysclid=lpppmtjrme24662608
[2] http://clsz.fsb.ru/clsz/certification.htm

[3] Проект Постановления Правительства Российской Федерации «Об утверждении технического регламента о безопасности объектов внутреннего водного транспорта» (опубликован 30.08.2023 года). https://www.garant.ru/products/ipo/prime/doc/56867381/?ysclid=lmamarv7r6463806883 (доступ 08.10.2023).

5. Взаимосвязь областей безопасности водных ИТС

В ГОСТ Р 56461-2015 (пункт 3.20) отражено, что обеспечение транспортной безопасности осуществляется путем реализации определяемой государством системы правовых, экономических, организационных и иных мер в сфере транспортного комплекса, соответствующих угрозам совершения актов незаконного вмешательства.

Новые виды актов незаконного вмешательства в деятельность водного транспортного комплекса, связанные с угрозами информационной безопасности, многообразны и, частично, рассмотрены выше. Однако ситуация их неучета относима ко всем видам ИТС и является длящейся, несмотря на предпринимаемые инициативы по ее исправлению [10–12, 17–19, 27]. Применительно к водным ИТС информационная безопасность должна рассматриваться неразрывно с функциональной безопасностью [28], как это предусмотрено, например, ГОСТ Р 70732-2023[1].

В ГОСТ Р 56461-2015 (пункт 3.14) также указано, что транспортная безопасность является составной частью национальной безопасности. Связь составных частей комплексной безопасности водных ИТС, влияния информационной безопасности водных ИТС на иные области безопасности, включая транспортную, отражает рис. 5.

Представленная на рис. 5 система отношений отражает особенности правового регулирования Российской Федерации в областях информационной безопасности и безопасности критической информационной инфраструктуры, в том числе в виртуальных средах, включая сеть Интернет[2,3].

Заключение

Транспортную безопасность водных ИТС следует рассматривать всесторонне, учитывая не только традиционные для водного транспорта акты незаконного вмешательства физического характера, но и специфические для ИТС события, связанные с ненаблюдаемыми физически, но при этом потенциально опасными недекларированными возможностями и уязвимостями информационных технологий, технологий автоматизированного управления, автоматического управления и искусственного интеллекта, обеспечивающих функционирование водных ИТС.

Проведенный анализ показывает, что аспекты безопасности, связанные с указанными технологиями, не находят своего отражения в нормативных правовых актах по транспортной безопасности водного транспорта и, как следствие, в планах ее обеспечения, что создает дополнительные риски.

Водные ИТС функционируют в сложном окружении и взаимодействуют с ИТС других видов транспорта и иными объектами критической информационной инфраструктуры. По результатам упомянутого в статье моделирования угроз безопасности информации системы автономного судовождения на внутренних водных путях водные ИТС могут взаимодействовать с Единой государственной системой обеспечения транспортной безопасности, ведомственной информацион-

[1] ГОСТ Р 70732-2023. Автоматизированные системы управления технологическими процессами и техническими средствами железнодорожного транспорта. Требования к функциональной и информационной безопасности программного обеспечения и методы контроля.

[2] ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения.

[3] ГОСТ Р ИСО/МЭК 27033- 5-2021. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 5. Обеспечение безопасности межсетевого взаимодействия с помощью виртуальных частных сетей (ВЧС).

Рис. 5. Области влияния информационной безопасности ИТС на транспортную и национальную безопасность

ной системой Росморречфлота, речными и морскими информационными службами, информационными службами МЧС России и другими системами. Это требует решения проблемы исключения возможного негативного влияния водных ИТС на функционирование взаимодействующих систем.

Рассмотренные в статье проблемы носят системный характер и относимы к ИТС других видов транспорта, так как обусловлены общими факторами. В условиях бурного развития вышеназванных высоких технологий возникает разрыв между сферами технического и технологического характера обеспечения транспортной безопасности, с одной стороны, и правовой сферой – с другой. Возможность реализации достижений в первой сфере может сдерживаться отставанием второй.

Существует насущная потребность отражения в нормативных правовых актах по обеспечению транспортной безопасности водных ИТС вопросов их информационной безопасности, что справедливо и для ИТС других видов транспорта [13, 14].

Благодарности

Автор благодарен доктору технических наук, доценту Сабанову А.Г. за ценные комментарии и рекомендации, которые помогли акцентировать материал статьи на целевой аудитории (исследователи транспортной безопасности водных ИТС, разработчики нормативной правовой базы по ее обеспечению и лица, участвующие в обеспечении транспортной безопасности водных ИТС), исходя из чего была изменена структура изложение и дополнен материал статьи.

Библиографический список

1. Threat Landscape of Transport Sector. ENISA, March 21, 2023. URL: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape (дата обращения 15.09.2023).

2. Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2023. URL: https://ics-cert.kaspersky.ru/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023 (дата обращения 15.09.2023).

3. Михалевич И.Ф. Цифровая трансформация систем управления в условиях пандемии COVID-19 // REDS: Телекоммуникационные устройства и системы. 2021. Т. 11. № 4. С. 25-31.

4. Михалевич И.Ф. Цифровая гигиена информационного общества: влияние пандемии COVID-19 // REDS: Телекоммуникационные устройства и системы. 2022. № 3. С. 10-17.

5. University of Texas team takes control of a yacht by spoofing its GPS. URL: https://newatlas.com/gps-spoofing-yacht-control/28644 (дата обращения 15.09.2023).

6. Spoofing on the High Seas. URL: https://youtu.be/ctw9ECgJ8L0 (дата обращения 15.09.2023).

7. INTERTANKO (2019). Jamming and Spoofing of Global Navigation Satellite Systems (GNSS). URL: https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf (дата обращения 15.09.2023).

8. Androjna A. Perkovic M. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. September 2021. Transactions on Maritime Science 10(2). DOI: 10.7225/toms.v10.n02.w08

9. Balduzzi M., Pasta A., Wilhoit K. A security evaluation of AIS automated identification system / In: Proceedings of the 30th annual computer security applications conference. 2014. Pp. 436-445. DOI:10.1145/2664243.2664257

10. Семенов С.А. Кибербезопасность морского и речного транспорта // Транспорт Российской Федерации. 2018. №1 (74). С. 43-46.

11. Семенов С. Морская кибербезопасность: оценка состояния и пути решения // Морские вести России. 2020. № 1. URL: https://morvesti.ru/analitika/1692/82776/?ysclid=lmc8mqcng3762121902 (дата обращения 15.09.2023).

12. Семенов С. Морская кибербезопасность – ситуация, проблемы и риски. Экспертная колонка Российского совета по международным делам (РСМД), 8 сентября 2020 года. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/?ysclid=ll572kfohg283787912 (дата обращения 15.09.2023).

13. Mikhalevich I.F. Problemic Issues of Deploying Cooperative Intelligent Transport Systems During of Digital Transformation // 2021 International Conference “Systems of Signals Generating and Processing in the Field of on Board Communications”. IEEE, 2021. DOI: 10.1109/IEEECONF51389.2021.9415999

14. Mikhalevich I.F. Priority Ways to Ensure Cybersecurity of Cooperative Intelligent Transport Systems” // 2022 International Conference “Systems of Signals Generating and Processing in the Field of on Board Communications”. IEEE, 2022. DOI: 10.1109/IEEECONF53456.2022.9744337

15. Radhakrishnan Subramaniam, Satya P. Singh, Parasuraman Padmanabhan, Balázs Gulyás, Prashobhan Palakkeel, Raja Sreedharan. Positive and Negative Impacts of COVID-19 in Digital Transformation // Sustainability 13(16):9470, August 2021. DOI: 10.3390/su13169470/

16. Mikhalevich I.F. Transformation of transport under conditions of digital inequality of control systems // International scientific conference International transport scientific innovation: ITSI-2021. P. 1-7. DOI: 10.1063/5.0105275.

17. Михалевич И.Ф. Проблемы создания доверенной среды функционирования автоматизированных систем управления в защищенном исполнении / Труды XII Всероссийского совещания по проблемам управления (ВСПУ-2014, Москва). М.: Институт проблем управления им. В.А.Трапезникова РАН, 2014. С. 9201-9207.

18. Mikhalevich I.F. Methodological foundations of creation of national protected hardware-software platforms

for critical information infrastructures // T-Comm. 2018. Vol. 12. No. 3. Pp. 75-81.

19. Mikhalevich I.F. Methodology development and implementation of protected hardware and software platform based on the existing // 2018 International Conference “Systems of Signals Generating and Processing in the Field of on Board Communications”. DOI: 10.1109/SOSG.2018.8350623

20. Михалевич И.Ф. Требования, принципы, практика создания отечественных аппаратно-программных платформ для автоматизированных систем в защищенном исполнении критической информационной инфраструктуры Российской Федерации // Интеллектуальные системы. Теория и приложения. 2018. Том. 22. Вып. 4. С. 11-30.

21. Михалевич И.Ф. Гармонизация требований безопасности цифровых систем корпоративного и технологического управления // В сборнике: Управление развитием крупномасштабных систем (MLSD’2020). Труды Тринадцатой международной конференции. 2020. С. 426-436. DOI: 10.25728/mlsd.2020.0426

22. Михалевич И.Ф. Проблема цифрового неравенства автоматизированных систем корпоративного и технологического управления // REDS: Телекоммуникационные устройства и системы. 2020. № 3. С. 43-47.

23. Andy Koronios, Abrar Haider, Kristian Steenstrup. Information and Operational Technologies Nexus for Asset Lifecycle Management // Proceedings of the 4th World Congress on Engineering Asset Management Athens, Greece, 28–30 September 2009 “Engineering Asset Lifecycle”. P. 112-119. URL: https://link.springer.com/chapter/10.1007/978-0-85729-320-6_13 (дата обращения 15.09.2023).

24. Cyber Attacks on Maritime OT Systems Increased 900% in Last Three Years. 2020. URL: https://safety4sea.com/cyber-attacks-on-maritime-ot-systems-increased-900-in-last-three-years/#:~:text=Cyber%2Dattacks%20on%20the%20maritime,security%20firm%20Naval%20Dome%20reveals (дата обращения 15.09.2023).

25. The guidelines on Cyber security onboard ships. URL: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (дата обращения 15.09.2023).

26. Complete Guide to OT Threat Detection and Response By Sectrio | November 20th, 2023. URL: https://sectrio.com/ot-threat-detection-and-response/#what-is-threat-detection-investigation-and-response (дата обращения 15.09.2023).

27. Легуша С.Ф. Киберпроблемы на водном транспорте – усилия основных игроков морской индустрии и классификационных обществ на примере Российского морского регистра судоходства // Транспортное право и безопасность. 2022. № 4(44). С. 183-194.

28. Шубинский И.Б., Розенберг Е.Н. Общие положения обоснования функциональной безопасности интеллектуальных систем на железнодорожном транспорте // Надежность. 2023. №3. С. 38-45. DOI: 10.21683/1729-2646-2023-23-3-38-45

References

1. Threat Landscape of Transport Sector. ENISA; 2023. (accessed 15.09.2023). Available at: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape.

2. [Threat landscape for industrial automation systems. First half of 2023]. (accessed 15.09.2023). Available at: https://ics-cert.kaspersky.ru/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023. (in Russ.).

3. Mikhalevich I.F. [Digital transformation of control systems in the context of the COVID-19 pandemic]. *REDS: Telecommunication devices and systems* 2021;11(4):25-31. (in Russ).

4. Mikhalevich I.F. [Digital hygiene of the information society: the impact of the COVID-19 pandemic]. *REDS: Telecommunication devices and systems* 2022;3:10-17. (in Russ).

5. University of Texas team takes control of a yacht by spoofing its GPS. (accessed 15.09.2023). Available at: https://newatlas.com/gps-spoofing-yacht-control/28644.

6. Spoofing on the High Seas. (accessed 15.09.2023). Available at: https://youtu.be/ctw9ECgJ8L0.

7. INTERTANKO (2019). Jamming and Spoofing of Global Navigation Satellite Systems (GNSS). (accessed 15.09.2023). Available at: https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf.

8. Androjna A., Perkovic M. Impact of Spoofing of Navigation Systems on Maritime Situational Awareness. *Transactions on Maritime Science* 2021:10(2). DOI: 10.7225/toms.v10.n02.w08.

9. Balduzzi M., Pasta A., Wilhoit K. A security evaluation of AIS automated identification system. In: Proceedings of the 30th annual computer security applications conference; 2014. Pp. 436-445. DOI:10.1145/2664243.2664257.

10. Semenov S.A. [Cybersecurity of sea and river transport]. *Transport Rossiyskoy Federatsii* 2018;1(74):43-46. (in Russ).

11. Semenov S. [Maritime cybersecurity: assessment of the state and solutions]. (accessed 15.09.2023). *Morskiye vesti Rossii* 2020;1. Available at: https://morvesti.ru/analitika/1692/82776/?ysclid=lmc8mqcng3762121902. (in Russ).

12. Semenov S. [Maritime cybersecurity – situation, problems, and risks]. (accessed 15.09.2023). Available at: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/?ysclid=ll572kfohg283787912. (in Russ).

13. Mikhalevich I.F. Problemic Issues of Deploying Cooperative Intelligent Transport Systems During of Digital Transformation. 2021 International Conference “Systems of Signals Generating and Processing in the Field of on Board Communications”. IEEE; 2021. DOI: 10.1109/IEEECONF51389.2021.9415999.

14. Mikhalevich I.F. Priority Ways to Ensure Cybersecurity of Cooperative Intelligent Transport Systems”. In: proceedings of the 2022 International Conference “Systems of Signals Generating and Processing in the Field of

on Board Communications". IEEE; 2022. DOI: 10.1109/IEEECONF53456.2022.9744337.

15. Subramaniam R., Singh S.P., Padmanabhan P., Gulyás B., Palakkeel P., Sreedharan R. Positive and Negative Impacts of COVID-19 in Digital Transformation. *Sustainability* 2021;13(16):9470. DOI: 10.3390/su13169470.

16. Mikhalevich I.F. Transformation of transport under conditions of digital inequality of control systems. In: proceedings of the International scientific conference International transport scientific innovation: ITSI-2021. Pp. 1-7. DOI: 10.1063/5.0105275.

17. Mikhalevich I.F. [Problems of creating a trusted environment for the functioning of automated control systems in a secure design]. In: Proceedings of the XII All-Russian Meeting on Control Problems (VSPU-2014, Moscow). Moscow: V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences; 2014. Pp. 9201-9207. (in Russ).

18. Mikhalevich I.F. Methodological foundations of creation of national protected hardware-software platforms for critical information infrastructures. *T-Comm* 2018;12(3):75-81. (in Russ.).

19. Mikhalevich I.F. Methodology development and implementation of protected hardware and software platform based on the existing. In: proceedings of the 2018 International Conference "Systems of Signals Generating and Processing in the Field of on Board Communications". DOI: 10.1109/SOSG.2018.8350623.

20. Mikhalevich I.F. [Requirements, principles, practice of creating domestic hardware and software platforms for automated systems in a secure design for the critical information infrastructure of the Russian Federation]. *Intellektualnye sistemy. Teoriya i primeneniya* 2018;22(4):11-30. (in Russ).

21. Mikhalevich I.F. [Harmonization of security requirements for digital systems of corporate and technological management]. In: [Management of the development of large-scale systems (MLSD'2020). Proceedings of the Thirteenth International Conference]; 2020. Pp. 426-436. https://DOI: 10.25728/mlsd.2020.0426. (in Russ).

22. Mikhalevich I.F. [The problem of digital inequality in automated corporate and technological management systems]. *REDS: Telecommunication devices and systems* 2020;3:43-47. (in Russ).

23. Koronios A., Haider A., Steenstrup K. Information and Operational Technologies Nexus for Asset Lifecycle Management. In: Proceedings of the 4th World Congress on Engineering Asset Management. Athens (Greece), 28–30 September 2009 "Engineering Asset Lifecycle". (accessed 15.09.2023). P. 112-119. Available at: https://link.springer.com/chapter/10.1007/978-0-85729-320-6_13.

24. Cyber Attacks on Maritime OT Systems Increased 900% in Last Three Years. (accessed 15.09.2023). Available at: https://safety4sea.com/cyber-attacks-on-maritime-ot-systems-increased-900-in-last-three-years/#:~:text=Cyber%2Dattacks%20on%20the%20maritime,security%20firm%20Naval%20Dome%20reveals.

25. The guidelines on Cyber security onboard ships. (accessed 15.09.2023). Available at: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf.

26. Complete Guide to OT Threat Detection and Response By Sectrio. November 20th; 2023. (accessed 15.09.2023). Available at: https://sectrio.com/ot-threat-detection-and-response/#what-is-threat-detection-investigation-and-response.

27. Legusha S.F. Cyber problems in water transport concerning the efforts of the main players in the maritime industry and classification societies on the example of the Russian Maritime Shipping Register. Transport law and security 2022;4(44):183-194. (in Russ).

28. Shubinsky I.B., Rozenberg E.N. General provisions of the substantiation of functional safety of intelligent systems in railway transportation. *Dependability* 2023;3:38-45. DOI: 10.21683/1729-2646-2023-23-3-38-45 (in Russ.)

Сведения об авторе

Михалевич Игорь Феодосьевич – кандидат технических наук, старший научный сотрудник, Российский университет транспорта (МИИТ), доцент кафедры «Управление и защита информации», ул. Образцова, д. 9, стр. 9, Москва, Российская Федерация, 127994, e-mail: mif-orel@mail.ru

About the author

Igor F. Mikhalevich, Candidate of Engineering, Senior Researcher, Russian University of Transport (MIIT), Senior Lecturer, Department of Management and Protection of Information, 9/9 Obraztsova St., Moscow, 127994, Russian Federation, e-mail: mif-orel@mail.ru.

Вклад автора

Автором проведен анализ новых видов угроз транспортной безопасности водных транспортных систем и нормативной правовой базы обеспечения их транспортной безопасности. Рассмотрена архитектура водных ИТС в виде интегрированной автоматизированной системы корпоративного и технологического управления, применение которой направлено на динамичное согласование моделей водных ИТС с моделями актуальных угроз транспортной безопасности в информационной сфере.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.