УДК 004.942:656.6:005.92
Оригинальная статья
https://doi.org/10.21683/1729-2646-2025-25-3-50-59

Цифровой испытательный стенд анализа безопасности объектов критической информационной инфраструктуры интеллектуальных систем водного транспорта

Digital testbench for security analysis of critical information infrastructure facilities of intelligent water transportation systems

Баранов Л.А.[1], Иванова Н.Д.[1], Михалевич И.Ф.[1]*
Baranov L.A.[1], Ivanova N.D.[1], Mikhalevich I.F.[1]*
[1]*Российский университет транспорта (МИИТ), Российская Федерация, Москва*
[1]*Russian University of Transport (MIIT), Russian Federation, Moscow*
**mif-orel@mail.ru*


Баранов Л.А.


Иванова Н.Д.


Михалевич И.Ф.

Резюме. Цель. *Использование новых технологий в интеллектуальных системах водного транспорта (ИСВТ), сопряжено с дополнительными рисками безопасности, которые обусловлены появлением новых типов угроз. Входящие в состав ИСВТ автоматизированные системы корпоративного и технологического управления являются объектами критической информационной инфраструктуры (КИИ). Это накладывает на ИСВТ повышенные требования безопасности. Программно-аппаратные комплексы, реализующие данные решения, в настоящее время находятся в состоянии активной разработки. Во многих случаях физическое макетирование объектов ИСВТ в разумные сроки затруднительно и экономически нецелесообразно. Эффективное решение данных вопросов обеспечивают современные методы имитационного моделирования. Они позволяют создавать цифровые прототипы объектов ИСВТ и ИСВТ в целом в безопасных виртуальных средах, на что было направлено исследование, результаты которого представлены в статье.* **Методы.** *Использованы методы системного анализа, исследования операций, имитационного моделирования, обеспечения безопасности ИСВТ.* **Результаты.** *Рассмотрена эволюция имитационного моделирования и приведена терминология в данной области. Определены типовые объекты КИИ в составе ИСВТ и объекты для цифрового моделирования. Проведен анализ средств создания цифрового испытательного стенда анализа безопасности объектов КИИ ИСВТ. Приведены описание цифрового испытательного стенда анализа безопасности объектов КИИ ИСВТ и примеры функционирования.* **Заключение.** *Представленный в работе цифровой испытательный стенд позволяет встраивать в свою среду как существующие, так и создаваемые отечественные защищенные программно-аппаратные комплексы, решать задачи по управлению рисками безопасности функционирования объектов ИСВТ. Это обеспечивает возможности применения стенда на различных этапах жизненного цикла объектов КИИ ИСВТ. Дальнейшее развитие стенда связано с разработками цифровых двойников акваторий внутренних водных путей, отечественных программно-аппаратных комплексов объектов КИИ ИСВТ, средств защиты объектов КИИ ИСВТ от компьютерных атак и методов гибридного управления их безопасностью.*

Abstract. Aim. *The application of novel technologies in intelligent water transportation systems (IWTS) is associated with additional security risks that are due to the emergence of new types of threats. The automated corporate and process management systems that are part of IWTS are critical information infrastructure (CII) facilities. That imposes increased safety requirements on IWTSs. Hardware and software systems that implement such solutions are undergoing active development. In many cases, physical prototyping of IWTS facilities within reasonable periods of time is difficult and economically unviable. Modern simulation methods efficiently solve the above problems. They allow creating digital prototypes of IWTSs and IWTSs proper within secure virtual environments. That represents the subject matter of this paper.* **Methods.** *The paper uses system analysis, operations research, simulation, and IWTS security.* **Results.** *The authors examine the evolution of simulation and provide subject-matter terminology. The paper defines standard CII facilities as part of IWTS and facilities to be digitally simulated. It analyses the tools that contribute to the creation of a digital testbench for analysing the IWTS CII security. It provides a description of the digital testbench for analysing IWTS CII security, as well as examples of its operation.* **Conclusion.** *The digital testbench presented in the paper allows incorporating both existing Russian secure software and hardware systems, and those under development. It also enables IWTS security risk management. That allows using the testbench at various lifecycle stages of IWTS CII facilities. Further development of the testbench*

is associated with the development of digital twins of inland waterways, Russian-made software and hardware systems of IWTS CII facilities, IWTS CII computer attack protection tools and methods for hybrid security management.

Ключевые слова: *автоматизированные системы корпоративного и технологического управления, имитационное моделирование, интеллектуальная система водного транспорта, компьютеризированные системы, критическая информационная инфраструктура, цифровая модель, цифровой двойник, цифровой испытательный стенд.*
Keywords: *automated corporate and process management systems, simulation, intelligent water transportation system, computerized systems, critical information infrastructure, digital model, digital twin, digital testbench.*

Для цитирования: *Баранов Л.А., Иванова Н.Д., Михалевич И.Ф. Цифровой испытательный стенд анализа безопасности объектов критической информационной инфраструктуры интеллектуальных систем водного транспорта // Надежность. 2025. №3. С. 50-59. https://doi.org/10.21683/1729-2646-2025-25-3-50-59*
For citation: *Baranov L.A., Ivanova N.D., Mikhalevich I.F. Digital testbench for security analysis of critical information infrastructure facilities of intelligent water transportation systems. Dependability 2025;3: 50-59. https://doi.org/10.21683/1729-2646-2025-25-3-50-59*

Поступила: *13.02.2025* / **После доработки:** *10.05.2025* / **К печати:** *25.07.2025*
Received on: *13.02.2025* / **Revised on:** *10.05.2025* / **For printing:** *25.07.2025*

Введение

Интеллектуальную основу морских и речных судов, портов, центров управления судами и объектами инфраструктуры водных путей, систем административного управления судоходством и иных объектов водного транспортного комплекса составляют компьютеризированные системы (КС). К ним относятся любые устройства или группы соединенных или взаимосвязанных устройств, одно или несколько из которых по команде компьютерной программы производит автоматическую обработку информации (данных). Под обработкой понимается выполнение любого действия (операции) или совокупности действий (операций) с информацией (данными), включая сбор, накопление, ввод, вывод, прием, передачу, запись, хранение, регистрацию, преобразование, отображение и т.п., совершаемых с заданной целью[1]. В интеллектуальных системах водного транспорта (ИСВТ) обработка информации и данных ведется в целях корпоративного и технологического управления [1, 2]. Посредством КС реализуются новейшие информационные, телематические и телекоммуникационные технологии [3-5], технологии искусственного интеллекта (ИИ) [6-8] и связи [9-11], обеспечивающие автоматизированный поиск и выработку максимально эффективных сценариев управления объектами ИСВТ для достижения заданной мобильности населения, максимизации показателей использования водных путей, повышения безопасности и эффективности транспортного процесса, комфортности для судоводителей и пользователей водного транспорта.

Применение новейших технологий сопряжено с дополнительными для транспортных систем рисками безопасности, обусловленными появлением новых типов угроз, что находит свое отражение в документах стратегического характера[2,3,4].

Основанные на КС автоматизированные системы корпоративного и технологического управления ИСВТ являются объектами критической информационной инфраструктуры (КИИ)[5]. Это обязывает осуществлять разработку и эксплуатацию объектов ИСВТ с соблюдением как общих [12-14], так и специальных требований безопасности КИИ[6]. Выполнение данных условий связано с использованием исключительно доверенных программно-аппаратных комплексов (ПАК)[7], находящихся в настоящее время в состоянии активной разработки [15].

Высокая стоимость объектов ИСВТ, многообразие и сложность КС, одновременные разработка ИСВТ, доверенных технологий и ПАК оказывают существенное влияние на выбор способов проверки безопасности. Во многих случаях физическое макетирование объектов ИСВТ в разумные сроки затруднительно и экономи-

[1] ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.

[2] Национальная стратегия развития искусственного интеллекта на период до 2030 года (утв. Указом Президента РФ от 10.10.2017 № 490, в редакции Указа Президента РФ от 15.02.2024 № 124).

[3] Приоритетные направления научно-технологического развития (утв. Указом Президента РФ от 18.06.2024 № 529.

[4] Перечень важнейших наукоемких технологий (утв. Указом Президента РФ от 18.06.2024 № 529).

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

[6] Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утв. приказом ФСТЭК России от 25.12.2017 № 239).

[7] Правила перехода субъектов критической информационной инфраструктуры Российской Федерации на преимущественное применение доверенных программно-аппаратных комплексов на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации (утв. постановлением Правительства РФ от 14.11.2023 № 1912).

чески нецелесообразно [16-17]. Решение данных вопросов, особенно на ранних этапах жизненного цикла, обеспечивают современные методы имитационного моделирования (ИМ), позволяющие создавать цифровые прототипы объектов ИСВТ и ИСВТ в целом в безопасных виртуальных средах при соблюдении ГОСТ[1] и требований регуляторов[2, 3].

1. Основные понятия

Замена физических макетов имитационными моделями [18, 19] является эффективным и хорошо зарекомендовавшим себя способом решения научно-технических задач высокого уровня сложности [20-22].

Термин «имитационное моделирование» имеет множество определений, формулировки которых уточнялись по мере развития компьютерной техники. Так, в [24] ИМ определено как метод исследования, при котором изучаемая система заменяется моделью, с достаточной точностью описывающей реальную систему, с которой проводятся эксперименты с целью получения информации о моделируемой системе. В [25] под ИМ понимается «соединение традиционного математического моделирования с новыми информационными технологиями, возникшими на базе ЭВМ. В [26] ИМ определено как метод исследования, основанный на том, что изучаемая динамическая система заменяется ее имитатором (подражателем), и с ним проводятся эксперименты с целью получения информации об изучаемой системе. В любом случае цель ИМ состоит в воспроизведении поведения исследуемой системы на основе результатов анализа наиболее существенных взаимосвязей между ее элементами. Результаты исследования имитационной модели, как правило, представляют собой оценки значений операционных (функциональных) характеристик системы, поведение которой имитируется [18].

Современные методы ИМ объединяют возможности оценки значений операционных (функциональных) характеристик системы с визуальным отображением исследуемых процессов и системы в целом. Сегодня имитационное (компьютерное) моделирование позволяет создавать «цифровых двойников» (ЦД) [27] систем, что распространяет ИМ на этапы внедрения и эксплуатации систем с использованием компьютерных моделей. Компьютерной (электронной) моделью является модель, выполненная в компьютерной (вычислительной) среде и представляющая собой совокупность данных и программного кода для работы с данными[4].

Концепция ЦД первоначально ориентировалась на отдельные изделия. В этом случае ЦД изделия определяется как система, состоящая из цифровой модели изделия и двусторонних информационных связей с изделием и (или) его составными частями[5]. Цифровой моделью (ЦМ) изделия является система математических и компьютерных моделей, а также электронных документов, описывающая структуру, функциональность и поведение изделия на различных стадиях жизненного цикла, для которой на основании результатов цифровых и (или) иных испытаний выполнена оценка соответствия предъявляемым к изделию требованиям[5].

В дальнейшем методология ЦД распространилась на большие системы. Например, для создания ЦД сетей мобильной связи [28], акватории, океана, Земли, метавселенной [29]. Как отмечается в [30], ЦД быстро перемещаются в неосязаемую сферу процессов и абстрактных идей. Прогнозируется, что их эволюция может стать интеллектуальной платформой, что позволит перейти из физического мира в виртуальный и окажет значительное влияние на эффективность и результативность различных сфер деятельности.

При этом методологические аспекты ЦД остаются неизменными. Это означает, что если речь идет о разрабатываемых или эксплуатируемых объектах ИСВТ (ИСВТ в целом), то их ЦМ должны описывать структуру, функциональность и поведение на соответствующих стадиях жизненного цикла, включая начальные. Таким образом, ЦД может быть создан в отсутствие физического объекта (системы) и далее развиваться на этапах его (ее) жизненного цикла с использованием цифрового (виртуального) испытательного стенда (ЦИС). В общем случае под ЦИС понимается система, состоящая из технических средств, программного, методического и организационного обеспечения и квалифицированного персонала, предназначенная для проведения стендовых испытаний по определению количественных и (или) качественных характеристик свойств объекта испытаний как результата исследования свойств ЦМ (или ЦД) этого объекта[5].

2. Типовые объекты критической информационной инфраструктуры в составе ИСВТ

Примерный состав типовых объектов КИИ ИСВТ приведен в табл. 1 (с учетом[6,7]).

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

[2] Требования по безопасности информации к средствам виртуализации (утв. приказом ФСТЭК России от 27.10.2022 № 187).

[3] Требования по безопасности информации к средствам контейнеризации (утв. приказом ФСТЭК России от 04.07.2022 № 118).

[4] ГОСТ Р 57412-2017 Компьютерные модели в процессах разработки, производства и эксплуатации изделий. Общие положения.

[5] ГОСТ Р 57700.37-2021. Компьютерные модели и моделирование. Цифровые двойники изделий. Общие положения.

[6] Перечень типовых отраслевых объектов критической информационной инфраструктуры, функционирующих в сфере транспорта (утв. Минтрансом России 15.05.2024).

[7] Методические рекомендации по категорированию объектов критической информационной инфраструктуры, функционирующих в сфере транспорта (утв. Минтрансом России 24.01.2024).

Табл. 1. Типовые объекты КИИ в составе ИСВТ

Информационные системы	Автоматизированные системы управления	Интегрированные системы
обеспечения контроля деятельности морского пассажирского транспорта.	обеспечения управления деятельностью по навигационному обеспечению судоходства на морском и внутреннем водном транспорте	обеспечения комплексной автоматизации судна
обеспечения контроля деятельности морского и внутреннего грузового транспорта	обеспечения управление погрузочными станциями в портах	
обеспечения контроля судоходства в морских и прибрежных водах, включая лоцманскую проводку судов	обеспечения управления аварийно-спасательной и судоподъемной деятельностью на морском транспорте	
	обеспечения управления ледокольными судами	

3. Типовые объекты цифрового моделирования ИСВТ

Модель типового объекта для цифрового моделирования ИСВТ приведена на рис. 1.

Данная модель содержит КС глобальной навигационной спутниковой системы (ГНСС), автоматической идентификационной системы (АИС), радиолокационной системы (РЛС), систем технического зрения (СТЗ) и радиосвязи, электронной картографической навигационно-информационной системы (ЭКНИС), автоматизированной системы управления движением (АСУД) судов и соответствующие автоматизированные рабочие места (АРМ). Представленные на рис. 1 элементы создаются в составе безэкипажных (автономных) судов, а также береговых центров управления безэкипажными судами [2].

4. Анализ средств создания цифрового испытательного стенда анализа безопасности объектов КИИ ИСВТ

Целью анализа являлся выбор средства ИМ, обеспечивающего возможность одновременного запуска образов различных операционных систем (ОС) с установленным специальным программным обеспечением (СПО) реальных КС объектов ИСВТ. Результаты сравнительного анализа наиболее распространенных решений приведены в табл. 2.

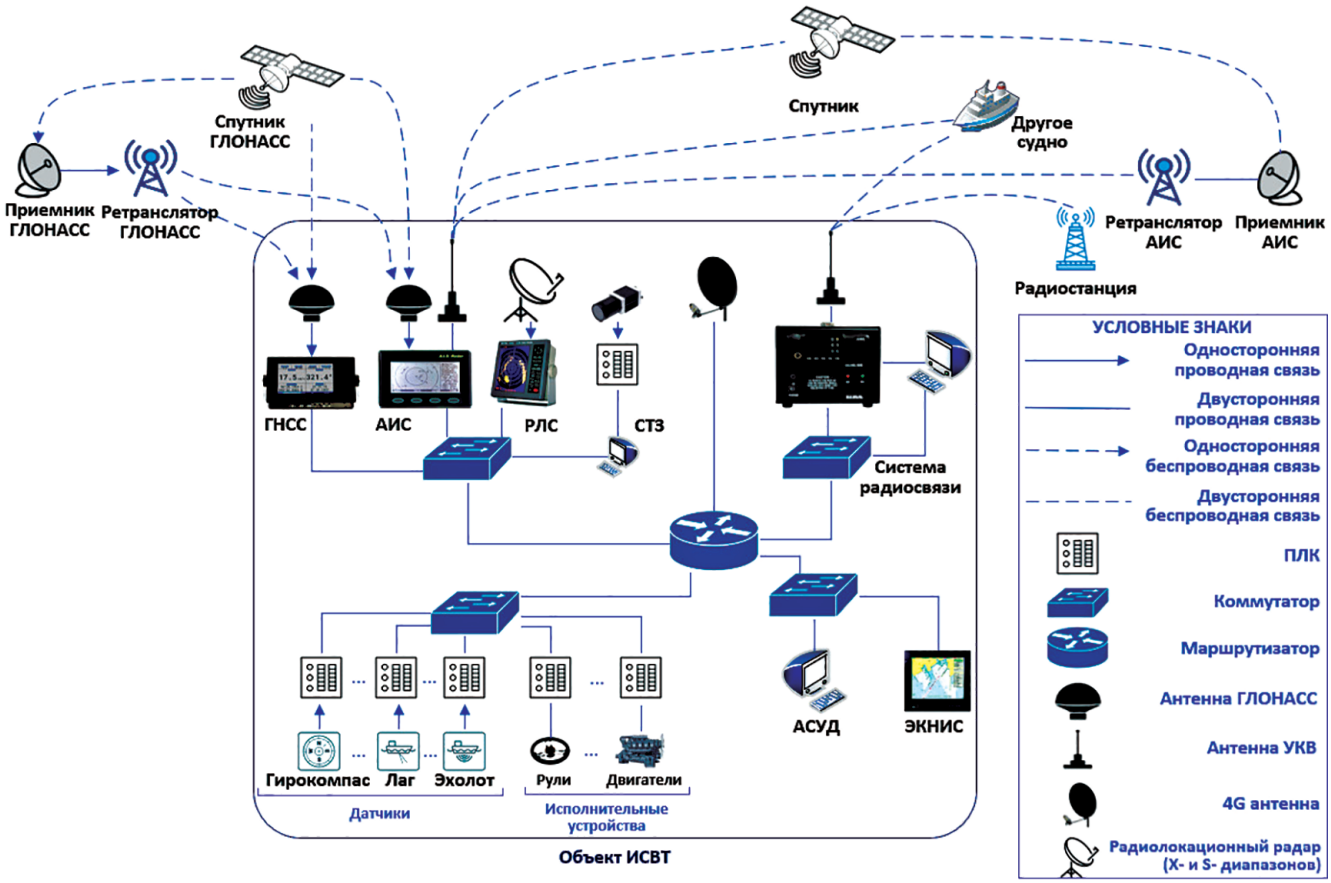

Рис. 1. Состав КС и схема информационных потоков объекта ИСВТ (пример)

Табл. 2. Средства имитационного моделирования объектов КИИ ИСВТ

Характеристика	GNS3[1]	EVE-NG[2]	PNETLab[3]	VIRL[4]	eNSP[5]	CPT[6]
Поддержка ОС и оборудования различных производителей[7]	+	+	+	+/–	+/–	–
Производительность и масштабируемость[8]	+	+	+	+/–	–	+
Наличие свободной лицензии[9]	+	–	+	–	+	–
Поддержка сообщества пользователей[10]	+	+/–	+	–	–	+/–
Простота освоения	+/–	+/–	+	–	–	+
Возможность интеграции с реальной системой (сетью)	+	+	+	+	+	–

[1] GNS3 (Graphical Network Simulator). https://gns3.com/

[2] EVE-NG (Emulated Virtual Environment – Next Generation). https://www.eve-ng.net/ , https://eve-ng.ru/

[3] PNETLab (Packet Network Emulator Tool Lab). https://pnetlab.com/pages/main

[4] VIRL (Virtual Internet Routing Lab). https://learningnetwork.cisco.com/s/virl

[5] eNSP (Enterprise Network Simulation Platform). https://forum.huawei.com/enterprise/intl/en/thread/download-ensp-simulator-installation-software-here/667238396713648128?blogId=667238396713648128

[6] CPT (Cisco Packet Tracer). https://www.netacad.com/learning-collections/cisco-packet-tracer?courseLang=en-US

[7] Обозначения: «+» – поддержка широкого спектра образов ОС и сетевых устройств; «+/–» – ограниченная совместимость с мультивендорными ОС и сетевыми устройствами; «–» отсутствие поддержки работы с ОС

[8] Обозначения: «+» – высокая производительность при сравнительно малых затратах аппаратных ресурсов, моделирование сетей большого размера; «+/–» – высокая производительность при сравнительно больших затратах аппаратных ресурсов, моделирование сетей большого размера; «–» – моделирование сетей среднего и малого размеров (некоммерческая версия)

[9] Обозначения: «+» – свободная лицензия на полноценный функционал; «–» – коммерческие продукты с ограниченным функционалом в бесплатной версии

[10] «+» – имеются официальные форумы сообществ пользователей; «+/–» – имеются большие сообщества пользователей и/или обширные ресурсы для обучения; «–» – узкоспециализированные сообщества пользователей со сравнительно небольшой целевой аудиторией

Табл. 3. Состав компонентов ЦИС анализа безопасности объектов КИИ ИСВТ

Наименование компонента	Среда функционирования компонента	СПО компонента	Функционал компонента
АРМ ГНСС	Windows 7 Professional	GPS Simulator[1] NMEAsoft[2]	Генерация виртуальных данных GPS. СПО ГНСС позволяет настроить маршрут, определить скорость и курс судна. Сгенерированные данные GPS можно сохранять в локальный файл и передавать по COM-порту или по UDP в формате сигналов NMEA0183
АРМ АСУД судна	Windows 10 Professional	Advanced NMEA Monitor[3] GPS NMEA Emulator[4]	Мониторинг сигналов NMEA0183 от судовых навигационных устройств. СПО АСУД позволяет проводить анализ, хранение, передачу данных о движении судна в реальном времени, отображать положение ЦД судна на карте
АРМ ЭКНИС	Windows 7 Professional	Oziexplorer[5] gt-ozi[6]	Электронная картография и навигация. В рассматриваемом далее примере в АРМ ЭКНИС загружена электронная карта с рекой Волга
АРМ системы гибридного управления безопасностью (ГУБ) судна	Astra Linux	Сканер-ВС 6[7]	Сканирование ЛВС объекта ИСВТ и анализ состояния его КС (активов)
		Программа оценки рисков безопасности объектов КИИ ИСВТ	Оценка рисков безопасности объектов ИСВТ по методике [30]
Коммутатор	IOS	Cisco vIOS Switch[8]	Взаимодействие КС в составе ЛВС объекта ИСВТ
Маршрутизатор	IOS	Cisco vIOS Router[8]	Взаимодействие объекта с другими объектами КИИ ИСВТ
АРМ нарушителя ИБ	Kali Linux	Nmap	Несанкционированное сканирование ЛВС объекта ИСВТ и анализ состояния его КС (активов)

[1] GPS Simulator. https://download.cnet.com/gps-simulator/3000-20422_4-76475761.html

[2] NMEAsoft. https://download.cnet.com/developer/nmeasoft/i-10451367/

[3] Advanced NMEA Monitor. https://download.cnet.com/advanced-nmea-monitor/3000-2094_4-76570128.html

[4] GPS NMEA Emulator. https://github.com/niclasankar/nmea-gps-emulator

[5] Oziexplorer 3.95.6f. https://www.oziexplorer4.com/eng/oziexplorer.html

[6] gt-ozi. https://github.com/nikolaybespalov/gt-ozi

[7] Сканер-ВС 6. https://scaner-vs.ru/

[8] ishare2. https://github.com/pnetlabrepo/ishare2

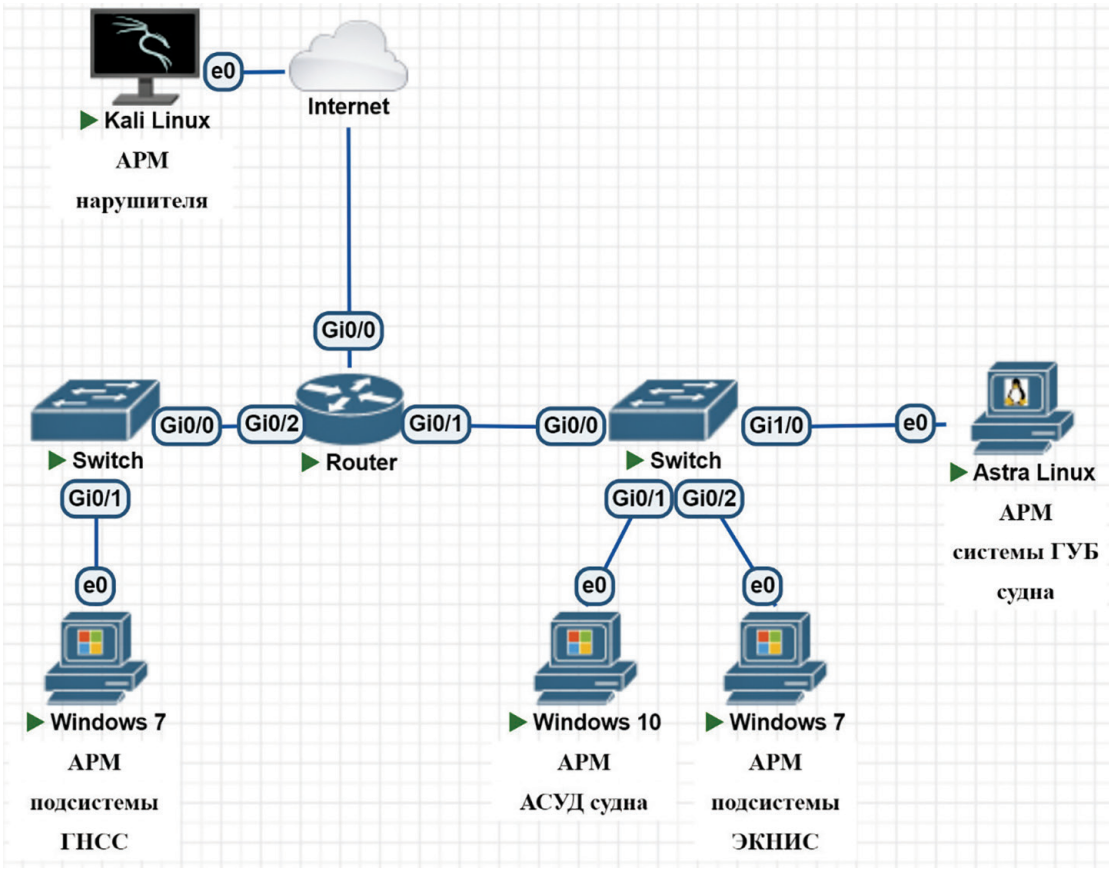

Рис. 2. Цифровой испытательный стенд анализа безопасности объекта ИСВТ (фрагмент)

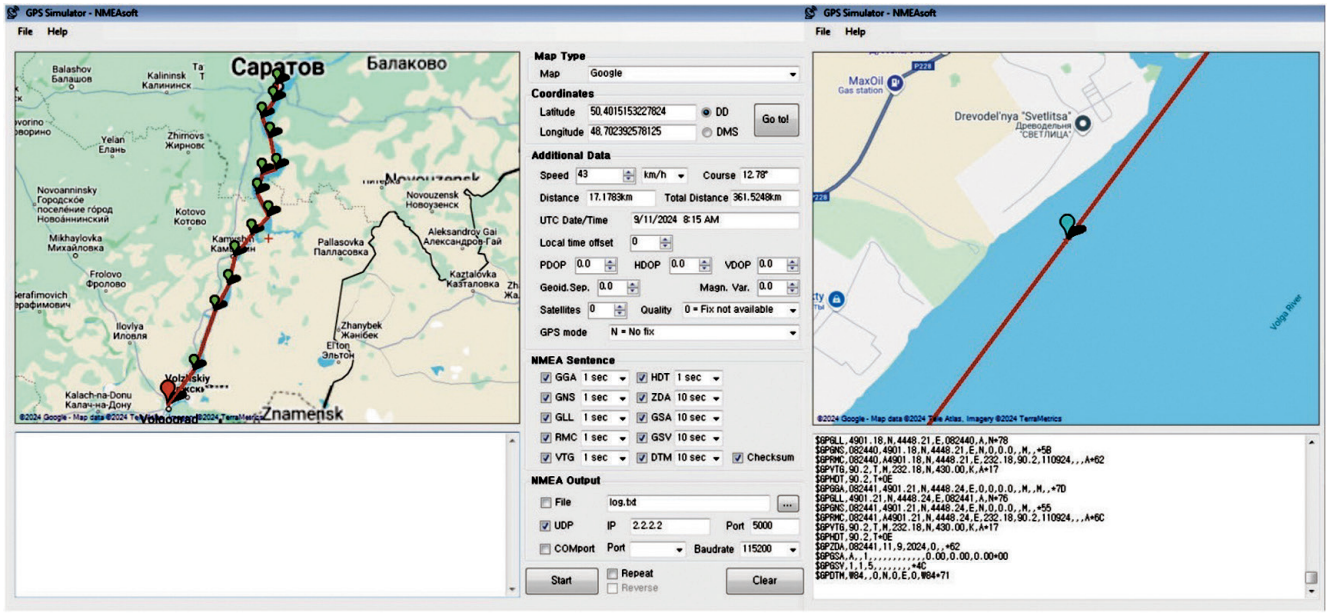

Рис. 3. Предварительная прокладка маршрута движения судна с использованием данных, генерируемых на АРМ ГНСС

Для ИМ объектов КИИИ ИСВТ выбрана сетевая лаборатория PNETLab (Packet Network Emulator Tool Lab). Она обеспечивает возможности по импортированию любых ОС и установки на АРМ СПО различных элементов ИСВТ, поддерживает сетевой режим обучения и разработки ЦМ.

5. Реализация цифрового испытательного стенда анализа безопасности объектов КИИ ИСВТ

Пример реализации ЦИС анализа безопасности объектов КИИ ИСВТ представлен на рис. 2.

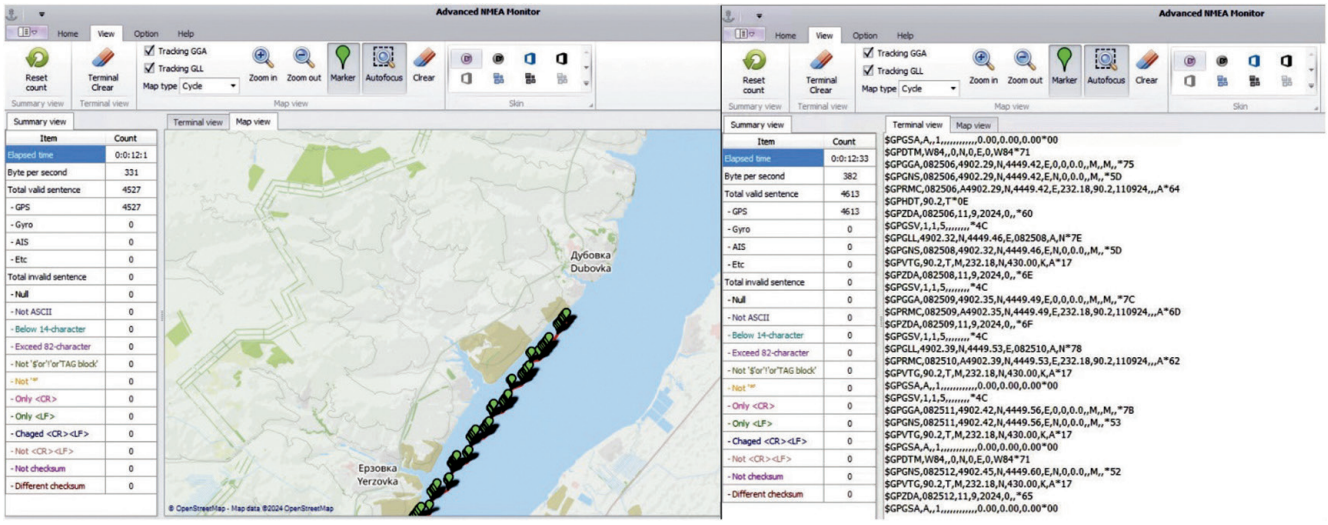

Рис. 4. Отображение информации о фактическом маршруте судна на АРМ АСУД

В состав ЦИС включены цифровые модели АСУД судна, подсистем ГНСС, ЭКНИС, системы гибридного управления безопасностью (ГУБ) судна [30] и оборудования ЛВС, ЦМ нарушителя информационной безопасности объекта ИСВТ. Работа с навигационной информацией реализована в формате протокола NMEA0183[1], обеспечивающего совместимость информации от приемников ГНСС, сонаров, радаров, компасов, барометров и других навигационных источников.

Описание и характеристика основных программных компонентов ЦИС приведены в табл. 3.

Генерируемые ЦИС данные о маршруте движения судна приведены на рис. 3. Для примера был выбран маршрут от г. Волгограда до г. Саратова вверх по реке Волга.

Генерируемая АРМ ГНСС навигационная информация передается в подсистемы ЭКНИС и АСУД судна, обрабатывается соответствующим СПО и отображается на ЦД постов управления судном (рис. 4).

На АРМ системы ГУБ судна реализована методика оценка рисков безопасности объекта КИИ ИСВТ [30], обеспечивающая автоматизированный поиск эффективных решений и интеллектуальных алгоритмов защиты объектов КИИ ИСВТ от компьютерных атак и внутренних угроз.

Заключение

Автоматизированные системы корпоративного и технологического управления ИСВТ относятся к объектам КИИ, что требует обеспечения высокого уровня безопасности и дополнительных проверок.

Представленный в работе ЦИС позволяет встраивать в свою среду как существующие, так и создаваемые отечественные защищенные программно-аппаратные комплексы, решать задачи по управлению рисками безопасности функционирования объектов ИСВТ. Это создает возможности применения стенда на различных этапах жизненного цикла объектов КИИ ИСВТ.

Дальнейшее развитие стенда связано с разработками ЦД акваторий внутренних водных путей [28], отечественных ПАК КИИ ИСВТ, средств защиты объектов КИИ ИСВТ от компьютерных атак и методов гибридного управления их безопасностью [30].

Список литературы

1. Михалевич И.Ф. Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем // Надежность. 2024. № 2. С. 72-87. DOI: 10.21683/1729-2646-2024-24-2-72-87

2. Михалевич И.Ф. Проблемы обеспечения безопасности автономного судоходства на внутренних водных путях. М.: Научно-техническое издательство «Горячая линия – Телеком», 2024. 336 с.

3. Розенберг И.Н., Беляков С.Л., Боженюк А.В. и др. Методы и алгоритмы создания интеллектуальных геоинформационных систем для управления транспортными процессами. М.: ВИНИТИ РАН, 2019. 292 с.

4. Amit Pundir, Sanjeev Singh, Sanjeev Singh, Manish ShailaniManish, Geetika Jain Saxena. Cyber-Physical Systems Enabled Transport Networks in Smart Cities: Challenges and Enabling Technologies of the New Mobility Era. January 2022. IEEE Access 10:1-1. DOI: 10.1109/ACCESS.2022.3147323

5. Kul'ba V.V., Mikrin E.A., Pavlov B.V., Somov S.K. A Comprehensive Software Verification Technology for Onboard Control Systems of Spacecraft // Automation and Remote Control. 2023. Vol. 84. No. 10. Pp. 1047–1054. DOI: 10.1134/S0005117923100065

6. Kurek Wiktor, Pawlicki Marek, Pawlicka Aleksandra et al. Explainable Artificial Intelligence 101: Techniques, Applications and Challenges // ICIC 2023: Advanced

[1] National Marine Electronics Association. The NMEA 0183 Protocol. https://web.archive.org/web/20070322070358/http://www.tronico.fi/OH6NT/docs/NMEA0183.pdf

Intelligent Computing Technology and Applications. Pp 310–318. DOI: 10.1007/978-981-99-4752-26

7. Walter M. J., Barrett A., Tam K. A Red Teaming Framework for Securing AI in Maritime Autonomous Systems // Applied Artificial Intelligence. 2024. Vol. 38(1). DOI: 10.1080/08839514.2024.2395750

8. Sai S, Yashvardhan U., Chamola V. et al. Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E, and Other Models for Enhancing the Security Space // In: IEEE Access. 2024. Vol. 12. Pp. 53497-53516. DOI: 10.1109/ACCESS.2024.3385107

9. Moya D.P. Osorio et al. Towards 6G-Enabled Internet of Vehicles: Security and Privacy // IEEE Open Journal of the Communications Society. 2022. Vol. 3. Pp. 82-105. DOI: 10.1109/OJCOMS.2022.3143098

10. Shrestha R., Bajracharya R., Kim S. 6G Enabled Unmanned Aerial Vehicle Traffic Management: A Perspective // In: IEEE Access. 2021. Vol. 9. Pp. 91119-91136. DOI: 10.1109/ACCESS.2021.3092039

11. Khan S.K., Shiwakoti N., Stasinopoulos P. et al. Security assessment in Vehicle-to-Everything communications with the integration of 5G and 6G networks // 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC), Rome, Italy, 2021. Pp. 154-158. DOI: 10.1109/ISCSIC54682.2021.00037

12. Попов П.А., Розенберг Е.Н., Сабанов А.Г. и др. Комплексная безопасность АСУ ТП объектов КИИ железнодорожного транспорта // Надежность. 2024. № 24(4). С. 48-57. DOI: 10.21683/1729-2646-2024-24-4-48-57

13. Шубинский И.Б. Надежность, риски, безопасность систем управления на железнодорожном транспорте : монография / И.Б. Шубинский, Е.Н. Розенберг, А.В. Бочков. Москва; Вологда: Инфра-Инженерия, 2024. 416 с.

14. 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

15. Михалевич И.Ф Проблемы создания доверенной среды разработки и реализации интеллектуальных систем водного транспорта. Надежность. 2025. № 2. С. 39-47. https://doi.org/10.21683/1729-2646-2025-25-2-39-47

16. Вишневский В.М., Рыков В.В., Козырев Д.В. и др. Моделирование надежности привязных высотных беспилотных телекоммуникационных платформ. М.: Техносфера, 2022. 194 с.

17. Willbold Johannes, Schloege Moritz, Vogele Manuel et al. Space Odyssey: An Experimental Software Security Analysis of Satellites. URL: https://jwillbold.com/paper/willbold2023spaceodyssey.pdf (дата обращения: 24.06.2025). DOI: 10.1109/SP46215.2023.10351029

18. Таха Х. Глава 17. Имитационное моделирование // Введение в исследование операций: В 2-х книгах. Кн. 2. Пер. с англ. М.: Мир, 1985. 496 с.

19. Советов Б.Я., Яковлев С.А. Моделирование систем. М.: ГУП «Издательство «Высшая школа», 2001. 343 с.

20. Tam K., Jones K. MaCRA: a model-based framework for maritime cyber-risk assessment // WMU J Marit Affairs. 2019. Vol. 18. Pp. 129–163. DOI: 10.1007/s13437-019-00162-2

21. Kharchenko V., Illiashenko O., Fesenko H. et al. AI Cybersecurity Assurance for Autonomous Transport Systems: Scenario, Model, and IMECA-Based Analysis // In: Dziech, A., Mees, W., Niemiec, M. (eds). Multimedia Communications, Services and Security. MCSS 2022. Communications in Computer and Information Science. Vol 1689. Pp 66–79. Springer, Cham, 2022. DOI: 10.1007/978-3-031-20215-5_6

22. Amro A., Gkioulos V. Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth // Int. J. Inf. Secur. 2023. Vol. 22. Pp. 249–288. DOI: 10.1007/s10207-022-00638-y

23. Национальное общество имитационного моделирования России – начало пути. Интервью чл.-корр. РАН Р.М. Юсупова, директора СПИИРАН. // CAD/CAM/CAE Observer. 2012. Vol. 2(70) Pp. 10-18. URL: http://www.cadcamcae.lv/hot/Interview_Yusupov_n70_p10.pdf (дата обращения 12.06.2025).

24. Павловский Ю.Н. Имитационные модели и системы. М.: Изд-во Фазис, ВЦ РАН, 2000. 144 с.

25. Киндлер Е. Языки программирования. М.: Энергоиздат, 1985. 288 с.

26. Прохоров А., Лысачев М. Цифровой двойник. Анализ, тренды, мировой опыт: Издание первое, исправленное и дополненное / Научный редактор профессор Боровков А. М.: ООО «АльянсПринт», 2020. 401 с.

27. Jingjing Guo, Zhiquan Liu, Siyi Tian et al. TFL-DT: A Trust Evaluation Scheme for Federated Learning in Digital Twin for Mobile Networks // IEEE Journal on Selected Areas in Communications, 30 August 2023. DOI: 10.1109/JSAC.2023.3310094

28. Розенберг И.Н., Соколов С.С., Дубчак И.А. Методы формирования цифрового двойника акватории для навигации беспилотных судов. Мир транспорта. 2023. № 21(6). С. 6-13. DOI: 10.30932/1992-3252-2023-21-6-1

29. Grieves M.W. Digital Twins: Past, Present, and Future // In: The Digital Twin. Springer International Publishing, Cham, 2023. Pp. 97–121. DOI: 10.1007/978-3-031-21343-4

30. Баранов Л.А. Нечеткая система оценки рисков информационной безопасности интеллектуальных систем водного транспорта / Л.А. Баранов, Н.Д. Иванова, И.Ф. Михалевич // Автоматика на транспорте. 2024. Т. 10. № 1. С. 7-17. DOI: 10.20295/2412-9186-2024-10-01-7-17

References

1. Mikhalevich I.F. Conceptual problems of transportation security of intelligent water transportation systems. *Dependability* 2024;24(2):72-87. (in Russ.) https://doi.org/10.21683/1729-2646-2024-24-2-72-87.

2. Mikhalevich I.F. [Matters of safety of autonomous navigation on inland waterways]. Moscow: Nauchno-tekhnicheskoe izdatelstvo «Goryachaya liniya – Telekom»; 2024. (in Russ.)

3. Rozenberg I.N., Belyakov S.L., Bozhenyuk A.V. et al. [Methods and algorithms for creating intelligent geoinformation systems for managing transportation processes]. Moscow: VINITI RAS; 2019. (in Russ.)

4. Pundir A., Singh S., Shailani M., Bafila A., Saxena G.J. Cyber-Physical Systems Enabled Transport Networks in Smart Cities: Challenges and Enabling Technologies of the New Mobility Era. January 2022. *IEEE Access* 10:1-1. DOI: 10.1109/ACCESS.2022.3147323.

5. Kul'ba V.V., Mikrin E.A., Pavlov B.V., Somov S.K. A Comprehensive Software Verification Technology for Onboard Control Systems of Spacecraft. *Automation and Remote Control* 2023;84(10):1047-1054. DOI: 10.1134/S0005117923100065.

6. Kurek W., Pawlicki M., Pawlicka A. et al. Explainable Artificial Intelligence 101: Techniques, Applications and Challenges. In: Proceedings of ICIC 2023: Advanced Intelligent Computing Technology and Applications. Pp 310-318. DOI: 10.1007/978-981-99-4752-26.

7. Walter M.J., Barrett A., Tam K. A Red Teaming Framework for Securing AI in Maritime Autonomous Systems. *Applied Artificial Intelligence* 2024;38(1). DOI: 10.1080/08839514.2024.2395750.

8. Sai S., Yashvardhan U., Chamola V. et al. Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E, and Other Models for Enhancing the Security Space. *IEEE Access* 2024;12:53497-53516. DOI: 10.1109/ACCESS.2024.3385107.

9. Moya D.P., Osorio et al. Towards 6G-Enabled Internet of Vehicles: Security and Privacy. *IEEE Open Journal of the Communications Society* 2022;3:82-105. DOI: 10.1109/OJCOMS.2022.3143098.

10. Shrestha R., Bajracharya R., Kim S. 6G Enabled Unmanned Aerial Vehicle Traffic Management: A Perspective. *IEEE Access* 2021;9:91119-91136. DOI: 10.1109/ACCESS.2021.3092039.

11. Khan S.K., Shiwakoti N., Stasinopoulos P. et al. Security assessment in Vehicle-to-Everything communications with the integration of 5G and 6G networks. In: Proceedings of the 2021 International Symposium on Computer Science and Intelligent Controls (ISCSIC), Rome, Italy, 2021. Pp. 154-158. DOI: 10.1109/ISCSIC54682.2021.00037.

12. Popov P.A., Rozenberg E.N., Sabanov A.G., Shubinsky I.B. Integrated Safety of ACS of Railway CII Facilities. *Dependability* 2024;24(4):48-57. (in Russ.) https://doi.org/10.21683/1729-2646-2024-24-4-48-57.

13. Shubinsky I.B., Rozenberg E.N, Bochkov A.V. [Dependability, risks, safety of control systems in railway transportation]. Moscow; Vologda: Infra-Engineering; 2024. (in Russ.)

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

15. Mikhalevich I.F. Matters of trusted development framework creation and implementation of intelligent water transportation systems. *Dependability* 2025;25(2):39-47. (in Russ.) https://doi.org/10.21683/1729-2646-2025-25-2-39-47.

16. Vishnevsky V.M., Rykov V.V., Kozyrev D.V. et al. [Simulating the dependability of tethered high-altitude unmanned telecommunication platforms]. Moscow: Tekhnosfera; 2022. (in Russ.)

17. Willbold J., Schloege M., Vogele M. et al. Space Odyssey: An Experimental Software Security Analysis of Satellites. (accessed 24.06.2025). Available at: https://jwillbold.com/paper/willbold2023spaceodyssey.pdf DOI: 10.1109/SP46215.2023.10351029.

18. Taha H. [Chapter 17. Simulation]. In: [Operations Research. An introduction: In 2 books. Book 2]. Moscow: Mir; 1985.

19. Sovietov B.Ya., Yakovlev S.A. [System simulation]. Moscow: GUP Izdatelstvo Vysshya shkola; 2001. (in Russ.)

20. Tam K., Jones K. MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU J Marit Affairs* 2019;18:129-163. DOI: 10.1007/s13437-019-00162-2.

21. Kharchenko V., Illiashenko O., Fesenko H. et al. AI Cybersecurity Assurance for Autonomous Transport Systems: Scenario, Model, and IMECA-Based Analysis. In: Dziech A., Mees W., Niemiec M., editors. Multimedia Communications, Services and Security. MCSS 2022. Communications in Computer and Information Science. Vol 1689. Pp 66–79. Springer, Cham; 2022. DOI: 10.1007/978-3-031-20215-5_6.

22. Amro A., Gkioulos V. Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. *Int. J. Inf. Secur.* 2023;22:249-288. DOI: 10.1007/s10207-022-00638-y.

23. [The National Society of Simulation of Russia. The Journey Begins. Interview with R.M. Yusupov, corresponding member, RAS, Director, SPIIRAS]. *CAD/CAM/CAE Observer* 2012;2(70):10-18. (accessed 12.06.2025). Available at: http://www.cadcamcae.lv/hot/Interview_Yusupov_n70_p10.pdf.

24. Pavlovsky Yu.N. [Simulation models and systems]. Moscow: Izdatelstvo Fazis, CC RAS; 2000. (in Russ.)

25. Kindler E. [Programming languages]. Moscow: Energoizdat; 1985. (in Russ.)

26. Prokhorov A., Lysachev M., prof. Borovkov A.M., editor. [Digital twin. Analysis, trends, global experience: First edition, revised and expanded]. Moscow: OOO AliansPrint; 2020. (in Russ.)

27. Guo J., Liu Z., Tian S. et al. TFL-DT: A Trust Evaluation Scheme for Federated Learning in Digital Twin for Mobile Networks. *IEEE Journal on Selected Areas in Communications* 2023. DOI: 10.1109/JSAC.2023.3310094.

28. Rosenberg I.N., Sokolov S.S., Dubchak I.A. Methods for Development of a Digital Twin of the Water Area for Navigation of Unmanned Vessels. *World of Trans-*

port and Transportation 2023;21(6):6-13. https://doi.org/10.30932/1992-3252-2023-21-6-1.

29. Grieves M.W. Digital Twins: Past, Present, and Future. In: The Digital Twin. Springer International Publishing, Cham; 2023. Pp. 97-121. DOI: 10.1007/978-3-031-21343-4.

30. Baranov L.A., Ivanova N.D., Mihalevich I.F. Fuzzy system for assessing the information security risk of intelligent water transport systems. *Transport automation research* 2024;1:7-17. (in Russ.) DOI: https://doi.org/10.20295/2412-9186-2024-10-01-7-17.

Сведения об авторах

Баранов Леонид Аврамович – доктор технических наук, профессор, Российский университет транспорта (МИИТ), заведующий кафедрой «Управление и защита информации», ул. Образцова, д. 9, стр. 9, Москва, Российская Федерация, e-mail: baranov.miit@gmail.com

Иванова Нина Дмитриевна – Российский университет транспорта (МИИТ), аспирант кафедры «Управление и защита информации», ул. Образцова, д. 9, стр. 9, Москва, Российская Федерация, e-mail: ivanovand.nina@yandex.ru

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

About the authors

Leonid A. Baranov, Doctor of Engineering, Professor, Russian University of Transport (MIIT), Head of Department, Management and Protection of Information, 9, bldg 9 Obraztsova st., Moscow, Russian Federation, e-mail: baranov.miit@gmail.com

Nina D. Ivanova, Russian University of Transport (MIIT), Post-graduate Student, Department of Management and Protection of Information, 9, bldg 9 Obraztsova st., Moscow, Russian Federation, e-mail: ivanovand.nina@yandex.ru

Igor F. Mikhalevich, Doctor of Engineering, Senior Researcher, Russian University of Transport (MIIT), Professor, Department of Management and Protection of Information, 9, bldg 9 Obraztsova st., Moscow, Russian Federation, e-mail: mif-orel@mail.ru

Вклад авторов

Баранов Л.А. – постановка задачи, общее руководство.

Иванова Н.Д. – реализация ЦИС анализа рисков информационной безопасности объектов КИИ ИСВТ.

Михалевич И.Ф. – теоретические основы и прикладные методы обеспечения безопасности ИСВТ, разработка и реализация ЦИС объектов КИИ ИСВТ.

Конфликт интересов

Авторы заявляют об отсутствии конфликта интересов.