Проблемы создания доверенной среды разработки и реализации интеллектуальных систем водного транспорта

Matters of trusted development framework creation and implementation of intelligent water transportation systems

Михалевич И.Ф.
Mikhalevich I.F.

Российский университет транспорта (МИИТ), Российская Федерация, Москва
Russian University of Transport (MIIT), Russian Federation, Moscow
mif-orel@mail.ru

Михалевич И.Ф.

Резюме. Цель. *На безопасность интеллектуальных транспортных систем (ИТС) существенное влияние оказывают угрозы нефизической природы. Они могут осуществляться незаконным вмешательством в разработку и реализацию ИТС. Создание доверенной среды разработки и реализации ИТС рассмотрено на примере интеллектуальных систем водного транспорта (ИСВТ).* **Проблемы.** *Указом Президента Российской Федерации ИТС, телекоммуникации и безопасность обработки информации включены в число приоритетных направлений научно-технологического развития. Технологии ИТС и технологии создания доверенного и защищенного системного и прикладного программного обеспечения отнесены к важнейшим наукоемким технологиям критического уровня. Функционирование ИТС связано с масштабным использованием компьютеризированных систем, реализующих новейшие информационные и телекоммуникационные технологии, технологии автоматизированного и автоматического управления, искусственного интеллекта, которые могут нести угрозы безопасности. Создание и функционирование ИТС должны осуществляться в условиях обеспечения доверенной среды их разработки и реализации.* **Методы.** *В работе были использованы методология обеспечения безопасности ИСВТ, разработки безопасных аппаратно-программных платформ автоматизированных систем в защищенном исполнении, методы системного анализа, теории надежности, защиты информации, права.* **Результаты.** *Сформулирована проблема создания доверенной среды разработки и реализации ИСВТ, разработана применимая к ней терминология. Исследовано влияние ИСВТ на безопасность критической информационной инфраструктуры (КИИ) и национальную безопасность, разработана модель отношений областей безопасности ИСВТ, учитывающая угрозы физического и нефизического происхождения. Приведены примеры компьютерных инцидентов в ИСВТ, повлекших последствия национального и межнационального уровня. Определен состав объектов ИСВТ, относимых к КИИ, приведены критические процессы, осуществляемые типовыми объектами КИИ в составе ИСВТ. Сформирован перечень концептуальных проблем обеспечения безопасности ИСВТ и сформулированы принципы создания доверенной среды разработки и реализации ИСВТ.* **Заключение.** *Обеспечение безопасности ИСВТ в условиях современных угроз требует решения проблем создания доверенной среды разработки и реализации ИСВТ. Для повышения оперативности и качества их решения предложена интуитивно понятная терминология, отражающая предметную область и позволяющая повысить уровень взаимопонимания проблем безопасности специалистов из различных сфер деятельности. Объекты ИСВТ оказывают влияние на безопасность КИИ и национальную безопасность в целом. Это учтено в модели отношений областей безопасности ИСВТ, показано на примерах компьютерных инцидентов в ИСВТ, повлекших последствия национального и межнационального уровня. С учетом вышеизложенного сформирован состав объектов ИСВТ, относимых к КИИ, и приведены примеры критических процессов, осуществляемых типовыми объектами КИИ в составе ИСВТ. Расширение ландшафта угроз безопасности ИСВТ небезопасными программным обеспечением, аппаратно-программными платформами, программно-аппаратными комплексами и новейшими технологиями учитывает сформированный перечень концептуальных проблем обеспечения безопасности ИСВТ При разработке принципов создания доверенной среды разработки и реализации ИСВТ учтен опыт успешного внедрения методологии создания национальных защищенных аппаратно-программных платформам объектов КИИ, обеспечившей создание автоматизированных систем в защищенном исполнении различного назначения на основе отечественных решений. Рассмотренные проблемы носят системный характер, что позволяет использо-*

вать полученные результаты при разработке и реализации ИТС других видов транспорта.
Abstract. Aim. *Threats of a non-physical nature have a significant effect on the security of intelligent transportation systems (ITS). They may have the form of unlawful interference in the development and implementation of ITS. The creation of a trusted framework for the development and implementation of ITS is examined as in the case of intelligent water transportation systems (IWTS).* **Problems.** *By decree of the President of the Russian Federation, ITS, telecommunications and security of information processing are among the priority areas of scientific and technological development. ITS technologies, as well as those involved in the creation of trusted, secure system and application software are among the most important critical high technologies. The operation of ITS involves wide use of computerised systems that implement the latest information and telecommunication technologies, automated and automatic control technologies, artificial intelligence that can pose security threats. ITS are to be developed and operated in a trusted environment.* **Methods.** *The paper used the methodology for ensuring the security of IWTS, development of secure hardware and software platforms for secure automated systems, methods of system analysis, dependability theory, information protection, and law.* **Results.** *The paper defines the problem of creating a trusted framework for the development and implementation of IWTS, the applicable terminology is developed. The author examined the effect of IWTS on the security of critical information infrastructure (CII) and national security, developed a model of relationships between the IWTS security domains taking into account threats of physical and non-physical origin. Examples of computer incidents within IWTS that caused consequences at the national and international levels are given. The composition of the IWTS facilities attributed to CII is defined, critical processes implemented by standard CII facilities as part of the IWTS are set forth. The author lists conceptual problems of IWTS security, defines the principles of creating a trusted framework for the development and implementation of IWTS.* **Conclusion.** *Ensuring the security of IWTS against modern threats requires solving a number of problems associated with the creation of a trusted framework for the development and implementation of IWTS. For the purpose of improving the timeliness and quality of their solution, the paper proposes an intuitive terminology that reflects the subject area and helps finding a common understanding of the security domain by experts from various industries. IWTS facilities have an effect on CII security and national security in general. That is taken into account in the model of relationships between IWTS security domains, demonstrated using cases of computer incidents within IWTS that caused consequences at the national and international level. Given the above, the paper lists IWTS facilities attributed to CII and sets forth examples of critical processes implemented by standard CII facilities as part of the IWTS. The defined list of conceptual IWTS security problems take into account the growing landscape of IWTS security threats that includes insecure software, hardware and software platforms, software and hardware systems and emerging technologies. When developing the principles for the creation of a trusted IWTS development and implementation framework, the author took into account the best practice of implementing the methodology for creating national secure hardware and software platforms of CII facilities that enables the creation of secure automated systems for various applications that are based on domestically-developed solutions. The examined matters are of a systemic nature, which allows using the findings in the development and implementation of ITS in other modes of transportation.*

Ключевые слова: *безэкипажное (автономное) судно, искусственный интеллект, компьютерная атака, компьютерный инцидент, угроза.*
Keywords: *unmanned (autonomous) vessel, artificial intelligence, computer attack, computer incident, threat.*

Для цитирования: *Михалевич И.Ф. О 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*
For citation: *Mikhalevich I.F. Matters of trusted development framework creation and implementation of intelligent water transportation systems. Dependability 2025;2:39-47. https://doi.org/10.21683/1729-2646-2025-25-2-39-47*

Поступила: *24.11.2024* / **После доработки:** *10.12.2024* / **К печати:** *09.06.2025*
Received on: *24.11.2024* / **Revised on:** *10.12.2024* / **For printing:** *09.06.2025*

Введение

Указом Президента Российской Федерации от 18 июня 2024 года № 529[1] утверждены приоритетные направления научно-технологического развития страны и перечни важнейших наукоемких технологий. Интеллектуальные транспортные системы (ИТС) и телекоммуникации, безопасность получения, хранения, передачи и обработки информации включены в число приоритетных направлений научно-технологического развития. Транспортные технологии для различных сфер применения (море, земля, воздух), в том числе беспилотные и автономные системы, отнесены к важнейшим наукоемким технологиям критического уровня. К критическим наукоемким технологиям отнесены также технологии создания доверенного и защищенного системного и прикладного программного обеспечения (ПО).

Функционирование ИТС связано с масштабным использованием компьютеризированных систем, реализующих новейшие информационные и телекоммуникационные технологии, технологии автоматизированного и автоматического управления, искусственного интеллекта (ИИ) (далее – новейшие технологии), которые могут нести угрозы безопасности. В связи с этим создание и функционирование ИТС должны осуществляться в условиях обеспечения доверенной среды их разработки и реализации.

Проблемы создания доверенной среды разработки и реализации ИТС рассмотрим на примере интеллектуальных систем водного транспорта (ИСВТ).

[1] Указ Президента РФ от 18.06.2024 № 529 «Об утверждении приоритетных направлений научно-технологического развития и перечня важнейших наукоемких технологий».

1. Терминология в области проблем создания доверенной среды разработки и реализации ИСВТ

Под ИСВТ (рис. 1) будем понимать систему управления, интегрирующую современные информационные, телематические, телекоммуникационные технологии, ИИ и предназначенную для автоматизированного поиска и принятия к реализации максимально эффективных сценариев управления водным транспортным комплексом, конкретным судном или группой судов, объектами водной инфраструктуры с целью обеспечения заданной мобильности населения, максимизации показателей использования водных путей, повышения безопасности и эффективности транспортного процесса, комфортности для судоводителей и пользователей водного транспорта (с учетом[2,3]).

При решении задач создания доверенной среды разработки и реализации ИСВТ предлагается использовать следующие определения терминов:

• обработка информации – любые действия по сбору, накоплению, вводу, выводу, приему, передаче, записи, хранению, регистрации, преобразованию, отображению информации, совершаемые с заданной целью (с учетом[4,5]). Отметим, что в определенных случаях

[2] ГОСТ Р 56829-2015. Интеллектуальные транспортные системы. Термины и определения.

[3] ПНСТ 555-2021. Интеллектуальные транспортные системы. Системы искусственного интеллекта для автоматизации управления автомобильными транспортными средствами. Классификация и общие технические требования.

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

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

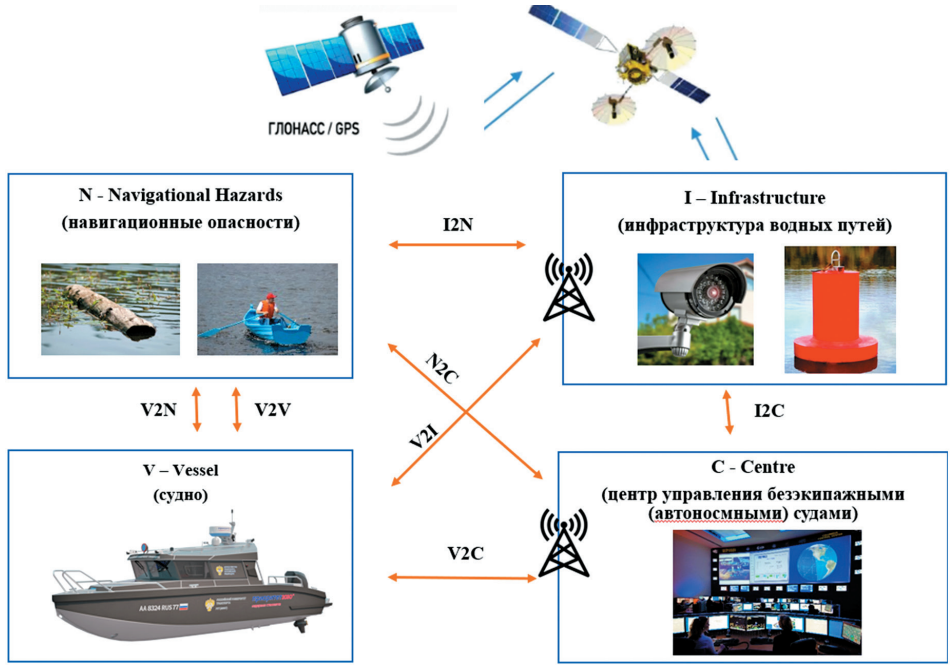

Рис. 1. Базовая конфигурация ИСВТ

Рис. 2. Связь областей безопасности компьютеризированных систем ИСВТ

целью таких действий или бездействия может быть нарушение безопасности ИСВТ;

• безопасность ИСВТ – состояние защищенности объектов инфраструктуры водных путей и судов, процессов их проектирования, производства, строительства и эксплуатации от актов незаконного вмешательства (АНВ) (с учетом[6,7]);

• акт незаконного вмешательства в ИСВТ – любое противоправное действие или бездействие, в том числе компьютерная атака, угрожающие безопасности ИСВТ, повлекшее за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавшие угрозу наступления таких последствий (с учетом[3,4]);

• компьютерная атака в ИСВТ – целенаправленное воздействие программных и (или) программно-аппаратных средств на информационные системы (ИС), автоматизированные системы управления (АСУ), системы автоматического управления (САУ), системы ИИ (СИИ), информационно-телекоммуникационные сети (ИТКС), сети электросвязи морских и речных судов, портов и иных объектов ИСВТ в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, обрабатываемой указанными объектами (с учетом[8]);

• компьютерный инцидент в ИСВТ – факт нарушения и (или) прекращения функционирования ИС, АСУ, САУ, СИИ, ИТКС, сети электросвязи морских и речных судов, портов и иных объектов ИСВТ и (или) нарушения безопасности информации, обрабатываемой объектом ИСВТ, в том числе произошедший в результате компьютерной атаки (с учетом[7]);

• доверие к ИСВТ – степень уверенности граждан, бизнеса, органов власти и других заинтересованных лиц в том, что ИСВТ будет выполнять свои функции так, как это предполагалось (с учетом[9]);

• доверенные ПО, аппаратно-программные платформы (АПП), программно-аппаратные комплексы (ПАК), технологии ИСВТ – ПО, АПП, ПАК, технологии ИСВТ, отвечающие стандартам безопасности ИСВТ, разработанные с учетом принципов объективности, недискриминации, этичности, исключающие при их использовании возможность причинения вреда человеку и нарушения его основополагающих прав и свобод, нанесение ущерба интересам общества и государства (с учетом[8]);

• доверие к безопасности ИСВТ – степень уверенности граждан, бизнеса, органов власти и других заинтересованных лиц в том, что безопасность ИСВТ будет обеспечена на заявленном уровне;

• доверенная среда разработки и реализации ИСВТ – среда, отвечающая принципам доверия к безопасности ИСВТ, требованиям по разработке безопасных ПО, АПП, ПАК, технологий ИСВТ (с учетом[10]).

[6] Федеральный закон от 09.02.2007 № 16-ФЗ «О транспортной безопасности».

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

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

[9] ГОСТ Р ИСО/МЭК 25010-2015. Информационные технологии (ИТ). Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (SQuaRE). Модели качества систем и программных продуктов

[10] ГОСТ Р 56939-2024. Защита информации. Разработка безопасного программного обеспечения. Общие требования

Табл. 1. Компьютерные инциденты на объектах ИСВТ (примеры, по сводкам [6])

Порт/ страна	Роль порта в экономике	Дата (период) / способ / цель атаки	Последствия	Сумма ущерба
Нагоя / Япония	10% от общего объема торговли Японии, в среднем 10 000 единиц грузов в день	05.07.2023 / шифрование информации АСУ грузовыми операциями / получение выкупа	2 суток простоя грузовых терминалов	Сведения отсутствуют, признается национальный уровень инцидента
Сидней, Мельбурн, Брисбен, Фримантле / Австралия	40% общего объема грузов Австралии	10.11.2023 / шифрование информации АСУ грузовыми операциями / получение выкупа	3 суток простоя грузовых терминалов	Сведения отсутствуют, признается национальный уровень инцидента
Дурбане/ ЮАР	более 60% грузооборота ЮАР, второй по величине контейнерный порт в южной Африке	22.07.2021 / шифрование информации АСУ грузовыми операциями / получение выкупа	7 суток простоя грузовых терминалов	Выкуп более 200 000 долларов США, признается межнациональный уровень инцидента
Роттердам / Нидерланды	Первое и второе место среди портов Европы по грузообороту в 2023г.	2011-2013 / подмена данных о контейнерах с наркотиками и оружием / контрабанда	Изменение местоположения и времени доставки контейнеров	200 000 евро на контрмеры
Антверпен / Бельгия				

2. Влияние ИСВТ на безопасность критической информационной инфраструктуры и национальную безопасность

В соответствии с федеральным законом о безопасности критической информационной инфраструктуры[8] (КИИ), ИСВТ входят в состав КИИ. В ИСВТ, следуя закону, объектами КИИ являются ИС, АСУ, САУ, СИИ, ИТКС, сети электросвязи, созданные (создаваемые) в целях обеспечения функционирования морских и речных судов, портов, пристаней, иных объектов инфраструктуры водных путей, технологических и административных центров управления и иных объектов ИСВТ, использующих компьютеризированные системы.

Модель отношений областей безопасности ИСВТ приведена на рис. 2.

В [1, 2] рассмотрены концептуальные проблемы обеспечения безопасности ИСВТ, состав которых представим следующим перечнем:

• расширение ландшафта угроз безопасности ИСВТ за счет АНВ нефизического характера [3–5]. Невыявленные (или) неустраненные уязвимости ИСВТ приводят к компьютерным инцидентам, последствия которых могут достигать национальных и межнациональных масштабов (табл. 1) [6];

• несовершенство нормативной правовой базы обеспечения безопасности ИСВТ, создающее правовой разрыв между физическими и нефизическими областями регулирования, вследствие чего в планах обеспечения безопасности объектов ИСВТ могут быть пропущены актуальные угрозы [7];

• наличие противоречий в международных документах по обеспечению безопасности морского транспорта с российским законодательством о безопасности КИИ, что затрудняет процессы исполнения;

• запутанность кибертерминологии, затрудняющая понимание причин компьютерных инцидентов в ИСВТ [8];

• низкий уровень публичного раскрытия информации о имевших место компьютерных инцидентах в ИСВТ [9–11];

• несоблюдение на объектах ИСВТ цифровой гигиены;

• цифровое неравенство в защищенности автоматизированных систем технологического и корпоративного управления ИСВТ, повышающее в интегрированных системах управления риски реализации угроз комплексного характера, в том числе со стороны ИИ [12-14].

Критические процессы, осуществляемые типовыми объектами КИИ в составе ИСВТ, приведены в табл. 2 (с учетом[11,12]).

В связи с вышеизложенным перечень концептуальных проблем обеспечения безопасности ИСВТ дополняет проблемы создания доверенной среды разработки и реализации ИСВТ. Для их решения сформулированы приведенные ниже принципы.

3. Принципы создания доверенной среды разработки и реализации ИСВТ

В соответствии с ГОСТ Р 51624-2000[13] объекты ИСВТ относятся к автоматизированным системам в защищенном исполнении (АСЗИ) и должны создаваться в

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

[12] Методические рекомендации по категорированию объектов критической информационной инфраструктуры, функционирующих в сфере транспорта (утв. Минтрансом России 24.01.2024). URL: https://mintrans.gov.ru/documents/10/13201?ysclid=lu2cx9gfse525544140. (дата обращения 10.03.2024).

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

Табл. 2. Типовые объекты КИИ в составе ИСВТ

№ п/п	Типовые объекты КИИ в составе ИСВТ	Критические процессы, осуществляемые типовым объектом КИИ в составе ИСВТ
1	Информационные системы, предназначенные для контроля деятельности морского пассажирского транспорта.	Контроль за деятельностью морского и внутреннего водного пассажирского транспорта. Контроль перевозки пассажиров в морских и прибрежных водах, осуществляемой по расписанию либо вне расписания. Контроль за деятельностью экскурсионных, круизных или прогулочных судов. Контроль за перевозкой пассажиров на паромах, водных такси. Контроль за перевозкой пассажиров по морским трассам на судах смешанного (река – море) плавания.
2	Информационные системы, обеспечивающие контроль деятельности морского и внутреннего грузового транспорта	Контроль за деятельностью морского и внутреннего грузового транспорта. Контроль за перевозкой грузов в морских и прибрежных водах, осуществляемой по расписанию либо не по расписанию. Контроль за деятельностью судов заграничного плавания. Контроль за деятельностью судов каботажного плавания. Контроль за деятельностью судов речного плавания.
3	Информационные системы, предназначенные для обеспечения судоходства в морских и прибрежных водах, включая лоцманскую проводку судов	Обеспечение безопасного судоходства в морских и прибрежных водах. Обеспечение лоцманской проводки судов.
4	Автоматизированные системы, предназначенные для управления деятельностью по навигационному обеспечению судоходства на морском и внутреннем водном транспорте	Предоставление картографической информации. Определение местоположения судов морского и внутреннего водного плавания. Контроль маршрута вне зоны покрытия GSM-связи.
5	Автоматизированные системы, обеспечивающие управление погрузочными станциями в портах	Сбор и обработка информации о состоянии технологических параметров. Обнаружение, сигнализация и регистрация аварийных ситуаций. Контроль доступа в основные складские помещения. Архивирование истории изменения параметров. Формирование и выдача оперативных и архивных данных персоналу. Дистанционное управление запорно-регулирующей арматурой (задвижки). Дистанционное управление насосными агрегатами. Управление процессом слива/налива нефтепродуктов: автоматическое открытие/закрытие задвижек с целью обеспечения требуемого маршрута слива/налива. Диагностика состояния программно-технических средств управления.
6	Автоматизированные системы, предназначенные для управления аварийно-спасательной и судоподъемной деятельностью на морском транспорте	Контроль сигналов о бедствии от судов морского и внутреннего водного плавания. Автоматизация управления аварийно-спасательной деятельности. Осуществление работ по подъему судов морского плавания.
7	Автоматизированные системы, обеспечивающие управление ледокольными судами	Контроль параметров ледокольных судов. Отображение информации о контролируемых параметров ледокольных судов операторам. Обеспечение проводки судов во льдах. Обеспечение прокладки маршрутов во льдах. Обеспечение спасательных работ во льдах. Управление распределением электроэнергии между потребителями. Управление техническими средствами и системами обитаемости и жизнеобеспечения. Управление техническими средствами и системами борьбы с пожарами. Управление техническими средствами и системами грузовых и балластных систем.

Табл. 2. Типовые объекты КИИ в составе ИСВТ (окончание)

№ п/п	Типовые объекты КИИ в составе ИСВТ	Критические процессы, осуществляемые типовым объектом КИИ в составе ИСВТ
8	Интегрированные системы, обеспечивающие комплексную автоматизацию судна	Обеспечение безопасного судовождения речных и морских судов. Управление динамическим позиционированием речных и морских судов. Управление дизельными и электрическими установками речных и морских судов. Управление распределением электроэнергии между потребителями. Управление техническими средствами и системами обитаемости и жизнеобеспечения. Управление техническими средствами и системами борьбы с пожарами. Управление техническими средствами и системами грузовых и балластных систем. Управление техническими средствами и системами обеспечения экологической чистоты и экологической безопасности судна.

Табл. 3. Принципы создания доверенной среды разработки и реализации ИСВТ

Наименование	Описание
Безопасность	недопустимость использования АПП, создающих угрозы безопасности информации ИСВТ или угрозы нарушения (прекращения) функционирования ИСВТ вследствие применения информации, безопасность которой была нарушена
Защищенность	безопасность и правовая охрана решений в области АПП для ИСВТ, разграничение ответственности организаций – разработчиков АПП и пользователей АПП, а также защита указанных пользователей от негативного влияния АПП на функционирование и безопасность ИСВТ и взаимодействующих с ними иных объектов КИИ
Контролируемость	наличие полного комплекта документации на АПП, в том числе о соответствии всех компонентов АПП и процессов достижения результатов их работы по отдельности и совместно в составе вычислительных систем (ПАК) требованиям по безопасности
Технологический суверенитет	преимущественное использование отечественных решений в области АПП, независимость от импорта и технологическая независимость: обеспечение полноценности, способности сохранять заявленные характеристики, развиваться и поддерживаться независимо от внешнеполитических и внешнеэкономических факторов, без применения импортных компонентов, без иностранного участия, принудительного обновления компонентов и управления из-за рубежа, передачи информации, в том числе технологической, за пределы РФ
Полноценность	обеспечение полноты состава АПП, необходимого для функционирования ИСВТ различного назначения, разных классов защищенности, уровней топологической и архитектурной сложности
Промышленный уровень	обеспечение необходимого уровня производительности, отказоустойчивости и других заявленных характеристик ИСВТ сложных топологии и архитектуры, при высоких нагрузках и больших объемах данных в течение всего срока эксплуатации
Универсальность	обеспечение на основе собственных базовых компонентов создание (модернизацию) ИСВТ различного назначения, разных классов защиты и уровней топологической и архитектурной сложности
Гарантии развития и поддержки	обеспечение развития, эксплуатации, обслуживания и модернизации ИСВТ, созданных на основе АПП
Совместимость	обеспечение необходимого уровня аппаратной и программной совместимости компонентов АПП, включенных в вычислительную систему (ПАК), возможность создания на их основе интегрированной программной среды (экосистемы)
Гибкость	обеспечение возможности создания разнообразных архитектур вычислительных систем (ПАК) на основе компонентов АПП
Оперативность	обеспечение сокращения сроков перехода от научного или прикладного исследования к созданию вычислительных систем (ПАК)
Преемственность (наследование)	обеспечение постепенного перехода на отечественное специальное программное обеспечение (СПО) путем последовательного замещения СПО, функционирующего под управлением операционных систем (ОС) из недружественных стран (унаследованное ПО)
Целостность инновационного цикла	обеспечение тесного взаимодействия научных исследований и разработок в области АПП с реальными потребностями ИСВТ
Поддержка конкуренции	развитие рыночных отношений и недопустимость действий, направленных на монополизацию и ограничение конкуренции между российскими организациями, осуществляющими деятельность в области АПП

порядке, установленном ГОСТ Р 51583-2014[14], с учетом ГОСТ 56939-2024.

В [15] приведена методология создания национальных защищенных аппаратно-программных платформ объектов КИИ, основанная на Концепции создания доверенной среды функционирования АСЗИ [16], реализованной с учетом [17, 18] при создании и внедрении АПП типовых технических решений построения АСЗИ. Концепция и методология были успешно реализованы при создании АСЗИ различного назначения. На их основе разработаны принципы создания доверенной среды разработки и реализации ИСВТ, описание которых приведено в табл. 3.

Заключение

Обеспечение безопасности ИСВТ в условиях современных угроз требует решения проблем создания доверенной среды разработки и реализации ИСВТ. Для повышения оперативности и качества их решения предложена интуитивно понятная терминология, отражающая предметную область и позволяющая повысить уровень взаимопонимания проблем безопасности специалистов из различных сфер деятельности.

Объекты ИСВТ оказывают влияние на безопасность КИИ и национальную безопасность в целом. Это учтено в модели отношений областей безопасности ИСВТ, показано на примерах компьютерных инцидентов в ИСВТ, повлекших последствия национального и межнационального уровня. С учетом вышеизложенного сформирован состав объектов ИСВТ, относимых к КИИ, и приведены примеры критических процессов, осуществляемых типовыми объектами КИИ в составе ИСВТ.

Расширение ландшафта угроз безопасности ИСВТ небезопасными ПО, АПП, ПАК и новейшими технологиями учитывает сформированный перечень концептуальных проблем обеспечения безопасности ИСВТ.

При разработке принципов создания доверенной среды разработки и реализации ИСВТ учтен опыт успешного внедрения методологии создания национальных защищенных АПП объектов КИИ, обеспечившей создание АСЗИ различного назначения на основе отечественных решений.

Рассмотренные проблемы носят системный характер, что позволяет использовать полученные результаты при разработке и реализации ИТС других видов транспорта.

Библиографический список

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.: Горячая линия – Телеком, 2024. 336 с.

3. 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

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

5. Шубинский И.Б. Функциональная безопасность систем управления на железнодорожном транспорте / И.Б. Шубинский, Е.Н. Розенберг. М.; Вологда: Инфра-Инженерия, 2023. 360 с.

6. Maritime Cyber Attack Database (MCAD). URL: https://maritimecybersecurity.nl/ (дата обращения 30.03.2025).

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

8. 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.

9. Annual Threat Assessment 2024. The Nordic Maritime Cyber Resilience Centre. URL: https://static1.squarespace.com/static/5fae4682cc2b52123f436f99/t/6614e6a60fbde93c9dfdc4e3/1712645824622/Norma+Cyber+Annual+Threat+Assessment+-+Spreads.pdf (дата обращения 30.03.2025).

10. Q2 2024 – a brief overview of the main incidents in industrial cybersecurity. Kaspersky ICS CERT Analytical Report/. URL: https://ics-cert.kaspersky.com/publications/reports/2024/11/08/q2-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity/ (дата обращения 30.03.2025).

11. Threat landscape for industrial automation systems. Q2 2024. Kaspersky ICS CERT Analytical Report/ URL: https://ics-cert.kaspersky.com/publications/reports/2024/09/26/threat-landscape-for-industrial-automation-systems-q2-2024/ (дата обращения 30.03.2025).

12. Намиот Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность // International Journal of Open Information Technologies. 2022. Vol. 10. No. 9. Pp. 135-147.

13. Yamin M.M. et al. Weaponized AI for cyber attacks // Journal of Information Security and Applications. 2021. Vol. 57. P. 102722. DOI: 10.1016/j.jisa.2020.102722

14. Nwakanma C.I., Ahakonye L.A.C., Njoku J.N. et al. Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review // Appl. Sci. 2023. Vol. 13. P. 1252. DOI: 10.3390/app13031252

15. 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.

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

17. Зегжда Д.П., Ивашко А.М. К созданию защищенных систем обработки информации // Проблемы информаци-

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

онной безопасности. Компьютерные системы. 1999. № 1. С. 99-107.

18. Зегжда Д.П., Ивашко А.М. Технология создания безопасных систем обработки информации на основе отечественной защищенной операционной системы // Проблемы информационной безопасности. Компьютерные системы. 1999. № 2. С. 59-66.

References

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

2. Mikhalevich I.F. [Challenges in ensuring safe autonomous navigation on inland waterways]. Moscow: Goriachaya liniya – Telekom; 2024. (in Russ.)

3. 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. (in Russ.) DOI: 10.21683/1729-2646-2023-23-3-38-45.

4. 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.)

5. Shubinsky I.B., Rozenberg E.N. [Functional safety of control systems in railway transportation]. Moscow; Vologda: Infra-Inzheneria; 2023. (in Russ.)

6. Maritime Cyber Attack Database (MCAD). (accessed 30.03.2025). Available at: https://maritimecybersecurity.nl/.

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

8. 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).

9. Annual Threat Assessment 2024. The Nordic Maritime Cyber Resilience Centre. (accessed 30.03.2025). Available at: https://static1.squarespace.com/static/5fae4682cc2b52123f436f99/t/6614e6a60fbde93c9dfdc4e3/1712645824622/Norma+Cyber+Annual+Threat+Assessment+-+Spreads.pdf.

10. Q2 2024 – a brief overview of the main incidents in industrial cybersecurity. Kaspersky ICS CERT Analytical Report. (accessed 30.03.2025). Available at: https://ics-cert.kaspersky.com/publications/reports/2024/11/08/q2-2024-a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity.

11. Threat landscape for industrial automation systems. Q2 2024. Kaspersky ICS CERT Analytical Report/ (accessed 30.03.2025). Available at: https://ics-cert.kaspersky.com/publications/reports/2024/09/26/threat-landscape-for-industrial-automation-systems-q2-2024.

12. Namiot D., Ilyushin E., Chizov I. Artificial intelligence and cybersecurity. *International Journal of Open Information Technologies* 2022;10(9):135-147. (in Russ.)

13. Yamin M.M. et al. Weaponized AI for cyber attacks. *Journal of Information Security and Applications* 2021;57:102722. DOI: 10.1016/j.jisa.2020.102722.

14. Nwakanma C.I., Ahakonye L.A.C., Njoku J.N. et al. Explainable Artificial Intelligence (XAI) for Intrusion Detection and Mitigation in Intelligent Connected Vehicles: A Review. *Appl. Sci.* 2023;13:1252. DOI: 10.3390/app13031252.

15. 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.).

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

17. Zegzhda D.P., Ivashko A.M. [Towards the creation of secure information processing systems]. *Information Security Problems. Computer Systems* 1999;1:99-107. (in Russ.)

18. Zegzhda D.P., Ivashko A.M. [Process of creating secure information processing systems using a domestically-developed secure operating system]. *Information Security Problems. Computer Systems* 1999;2:59-66. (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, 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, bldg. 9 Obraztsova str., Moscow, Russian Federation, e-mail: mif-orel@mail.ru

Вклад автора в статью

Автором сформулирована проблема создания доверенной среды разработки и реализации ИСВТ и разработана применимая к ней терминология. Исследовано влияние ИСВТ на безопасность критической информационной инфраструктуры и национальную безопасность, разработана модель отношений областей безопасности ИСВТ, учитывающая угрозы физического и нефизического происхождения. Приведены примеры компьютерных инцидентов в ИСВТ, повлекших последствия национального и межнационального уровня. Определен состав объектов ИСВТ, относимых к критической информационной инфраструктуре, приведены критические процессы, осуществляемые типовыми объектами КИИ в составе ИСВТ. Сформирован перечень концептуальных проблем обеспечения безопасности ИСВТ и сформулированы принципы создания доверенной среды разработки и реализации ИСВТ. Предложено распространить полученные результаты на ИТС других видов транспорта.

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.