ИНТЕЛЛЕКТУАЛИЗАЦИЯ И НОВЫЕ ТИПЫ УГРОЗ БЕЗОПАСНОСТИ ВОДНОГО ТРАНСПОРТА


И.Ф. Михалевич


С.С. Соколов

Рассмотрены вопросы обеспечения безопасности интеллектуальных систем водного транспорта (ИСВТ), обусловленные угрозами нефизического характера, включая несовершенство нормативного регулирования разработки и эксплуатации ИСВТ, цифровое неравенство составных частей интегрированных автоматизированных систем корпоративного и технологического управления объектов ИСВТ, недостаточное развитие отечественных аппаратно-программных платформ ИСВТ.

Ключевые слова: акт незаконного вмешательства, интеллектуальная система водного транспорта, компьютерная атака, угроза

EDN: DOCNKB

Интеллектуализация транспорта предусматривает как повышение интеллектуального уровня отдельных транспортных средств, так и создание интеллектуальных транспортных систем (ИТС), что является мировым трендом. В России первые ИТС обеспечивали реализацию интеллектуальных функций отдельно внутри автомобиля и отдельно в объектах на обочине дороги или управления движением [1].

Термин ИТС имеет множество определений. В [2;3] ИТС определена как система управления, интегрирующая современные информационные и телематические технологии и предназначенная для автоматизированного поиска и принятия к реализации максимально эффективных сценариев управления транспортно-дорожным комплексом региона, конкретным транспортным средством или группой транспортных средств с целью обеспечения заданной мобильности населения, максимизации показателей использования дорожной сети, повышения безопасности и эффективности транспортного процесса, комфортности для водителей и пользователей транспорта. В [4] ИТС определяются как системы, использующие комбинацию компьютеров, коммуникаций, позиционирования и технологий автоматизации для повышения безопасности, управления и эффективности наземного транспорта.

Михалевич Игорь Феодосьевич, кандидат технических наук, старший научный сотрудник, доцент кафедры «Управление и защита информации» Российского университета транспорта (РУТ (МИИТ)), почетный радист, член-корреспондент Академии информатизации образования), награжден медалью ордена «За заслуги перед Отечеством II степени». Область научных интересов: связь и телекоммуникации, защита информации, информационная безопасность, информационные технологии, технологии автоматизированного, автоматического управления и искусственного интеллекта, автоматизированные системы, системы автоматического управления. Автор более 200 научных работ, в том числе двух монографий и шести учебных пособий. Имеет 11 авторских свидетельств и патентов на изобретения, свидетельства на программы для ЭВМ.

Соколов Сергей Сергеевич, доктор технических наук, доцент, проректор Российского университета транспорта (РУТ (МИИТ)), Почетный работник морского флота, действительный член Российской академии транспорта. Область научных интересов: теории систем, управления, графов, нечетких множеств, эвристических алгоритмов, интеллектуальные системы управления, системы принятия решений, информационные технологии, автоматизированные системы управления на транспорте, информационная и транспортная безопасность объектов транспортной инфраструктуры и транспортных средств морского и внутреннего водного транспорта, разработка средств автоматизации в рамках развития технологий автономного (безэкипажного) судовождения, цифровые двойники транспортных процессов, современные методы и технологии подготовки кадров для транспортной отрасли. Автор более 300 научных работ, в том числе восьми монографий. Имеет три патента на изобретения.

Развитие науки, техники и технологий позволило создавать ИТС различных видов транспорта [5]. Технологии водного, наземного и воздушного транспорта включены в приоритетные направления научно-технологического развития страны [6]. Технологии ИТС и автономных транспортных средств входят в перечень важнейших наукоемких технологий как критические [7], что вызвано возможностью влияния ИТС на безопасность критической информационной инфраструктуры страны и национальную безопасность в целом. Это в полной мере относится к интеллектуальным системам водного транспорта (ИСВТ) [8;9].

Угрозы безопасности ИСВТ

Технологии ИТС основаны на принципе V2X (Vehicle-to-Everytning). Его реализация предусматривает взаимодействие каждого транспортного средства ИТС со всеми другими объектами, способными повлиять на их поведение и внедрение в транспортные средства и объекты инфраструктуры ИТС технологий обработки больших объемов информации. Под обработкой информации понимаются любые действия по ее сбору, накоплению, вводу, выводу, приему, передаче, записи, хранению, регистрации, преобразованию, отображению и т.п., совершаемые с заданной целью [10;11]. В определенных случаях целью действий (или вследствие бездействия) может быть нарушение безопасности ИСВТ, что существенно расширяет ландшафт угроз.

Традиционно угрозы безопасности водного транспорта рассматриваются в контексте актов незаконного вмешательства (АНВ) в функционирование транспортных средств и объектов инфраструктуры физического характера, такие, как терроризм, хулиганство, аппаратные отказы оборудования, ошибки персонала и др. [12–15]. Это не соответствует ландшафту угроз безопасности ИСВТ, который содержит также АНВ нефизической природы, в том числе, компьютерные атаки, уязвимости и недекларированные возможности программного обеспечения (ПО) и технологий обработки данных, ошибки ПО и др. [8;9;16]. Компьютерной атакой в ИСВТ является целенаправленное воздействие программных и (или) программно-аппаратных средств на информационные системы, автоматизированные и (или) автоматические системы управления, системы искусственного интеллекта (ИИ), информационно-телекоммуникационные сети, сети связи морских и речных судов, портов и иных объектов ИСВТ в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, обрабатываемой такими объектами. Уязвимость ИСВТ можно определить как наличие слабых мест в активах или элементах управления ИСВТ, которые могут быть использованы одной или несколькими угрозами. Эти определения сформулированы на основе [17;18].

Функционирование ИСВТ обеспечивают сети радиосвязи, которые легко доступны для средств радиоэлектронной борьбы (РЭБ). Воздействие средств РЭБ приводит к уменьшению сетевых ресурсов, что снижает управляемость ИСВТ и может вызвать столкновения судов между собой, с объектами инфраструктуры, повлечь иные неблагоприятные последствия. Данные обстоятельства также существенно влияют на безопасность ИСВТ, что рассмотрено авторами в [8;9;12;16].

С учетом изложенного безопасность ИСВТ определим как состояние защищенности объектов инфраструктуры водных путей и судов, процессов их проектирования, производства, строительства и эксплуатации от АНВ. Под АНВ будем понимать любое противоправное действие (в том числе компьютерную атаку) или бездействие, угрожающее безопасности функционирования ИСВТ, повлекшее за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавшие угрозу наступления таких последствий.

Общемировым трендом является рост числа типов и частоты реализации угроз безопасности нефизического характера, основной состав и пример статистики реализации которых приведен в табл. 1.

В 2023–2024 годах наблюдались изменения частоты реализации при неизменном составе основных угроз безопасности, что установлено и российскими исследователями [20;21].

В ИСВТ АНВ нефизической природы могут быть реализованы с использованием физического, Интернет и беспроводного доступа к объектам, что иллюстрирует рис. 1.

В физической области угрозы возникают вследствие возможности прямого доступа злоумышленников (в том числе из числа легитимных лиц) к судовому оборудованию, оборудованию центров дистанционного управления, навигационных знаков и иных объектов инфраструктуры, причалов и портов. Посредством беспроводного доступа возможны атаки на указанные объекты при нахождении злоумышленников за пределами контролируемой зоны объекта, но в непосредственной близости с ними. Этим же угрозам подвержены объекты ИСВТ удаленно через Интернет.

Интеллектуализация водного транспорта, особенно в части безэкипажного (автономного) судовождения и использования ИИ, существенно влияет на безопасность ИСВТ. Безэкипажным является судно,

Таблица 1

Статистика реализации новых типов угроз безопасности функционирования транспортного комплекса Европейского Союза [19]

Типы актов незаконного вмешательства	Частота реализации	
	2021 год	2022 год
Программы-вымогатели	13%	25%
Атаки, связанные с данными	21%	9%
Вредоносное ПО	11%	6%
Атаки «отказ в обслуживании»	2%	13%
Фишинг	7%	3%
Атаки на цепочки поставок	3%	7%
Атаки нарушения функционирования	4%	4%
Подмена источника	3%	2%
Эксплуатация уязвимостей	4%	1%

управляемое внешним оператором или автономной бортовой программой [22;23]. Внешнее управление возможно лишь при наличии радиоканалов телемеханики, функционирование которых может быть нарушено, например, средствами радиоэлектронной борьбы и ошибками и/или недекларированными действиями ИИ. Под ИИ понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их [24]. Такой комплекс включает в себя информационно-коммуникационную инфраструктуру, ПО, процессы и сервисы по обработке данных и поиску решений [24], что опять-таки зависит от состояния каналов радиосвязи и ПО.

Применение ИИ является одним из перспективных направлений развития ИСВТ. Но его применение связано с новыми типами угроз, среди которых в [24] указаны:

- нехватка вычислительных мощностей, недостаточное развитие отечественных решений в области ИИ, включая программно-аппаратные комплексы и электронную компонентную базу;
- дефицит высококвалифицированных специалистов и инновационных разработок в области ИИ;
- низкий уровень внедрения технологий ИИ в государственном управлении;
- нормативные барьеры, препятствующие внедрению технологий ИИ в отдельных отраслях экономики, включая отсутствие методологической базы для обеспечения систем ИИ достоверными исходными данными;
- необходимость обеспечения безопасности при разработке и использовании технологий ИИ;
- необходимость обеспечения защиты персональных данных и иной информации ограниченного доступа, объектов интеллектуальных прав при создании и обучении моделей ИИ.

Более того, анализ отечественных нормативных правовых актов обеспечения безопасности объектов водного транспортного комплекса выявил разрыв

Рис. 1. Пути доступа для совершения АНВ в функционирование объектов ИСВТ

между физическими и нефизическими областями регулирования, а документов международных организаций – противоречия с российским законодательством в части терминологии и признаков классификации ИСВТ и судов как объектов критической информационной инфраструктуры [8;9;12;16]. Несовершенство нормативной правовой базы обеспечения безопасности ИСВТ может замедлить их создание и привести к неполному учету условий, влияющих на их безопасность.

Совместная реализация на объектах ИСВТ информационных технологий, технологий автоматизированного и автоматического управления привела к созданию интегрированных автоматизированных систем корпоративного и технологического управления объектов ИСВТ, составные части которых (АСКУ и АСТУ) неравно защищены от угроз нефизического характера. Цифровое неравенство АСТУ и АСКУ создает риски безопасности комплексного характера и содержать угрозу скрытного развития, что рассмотрено авторами в [8;9;16;25].

Для обеспечения безопасности ИСВТ необходимо в значительной степени повысить уровень их обеспеченности средствами защиты информации (СЗИ), адаптированными к особенностям функционирования АСТУ. Так, сертифицированные СЗИ содержат сотни наименований для АСКУ и только десятки для АСТУ.

Не менее важным является совершенствование методического обеспечения безопасности функционирования объектов ИСВТ. В отличие от банка данных угроз безопасности информации (БДУ БИ), созданного более десятка лет назад в интересах АСКУ. Банк данных угроз автоматизированных систем управления производственными технологическими процессами (БДУ АСУ ТП) был анонсирован только в декабре 2023 года.

Как указано на сайте ФСТЭК России, этот ресурс является первым в стране единым источником исходных данных об угрозах и уязвимостях, специфичных для АСУ ТП и промышленного интернета вещей в различных отраслях экономики, включая транспорт. Однако данный ресурс находится в начальном состоянии. В разделе «Транспорт» БДУ АСУ ТП на 16 сентября 2024 г. содержались только сведения о железнодорожном подвижном составе (рис. 2).

Отсутствие данных о других видах транспорта не означает отсутствие угроз. Это, скорее всего, проявление проблемы неполноты информации, поступающей от объектов транспортного комплекса, которая была рассмотрена авторами в [8;9;16]. О том, что такие угрозы есть несомненно, говорит перечень и характеристика угроз, характерных для АСТУ ИСВТ (АСУ ТП), которые приведены в табл. 2.

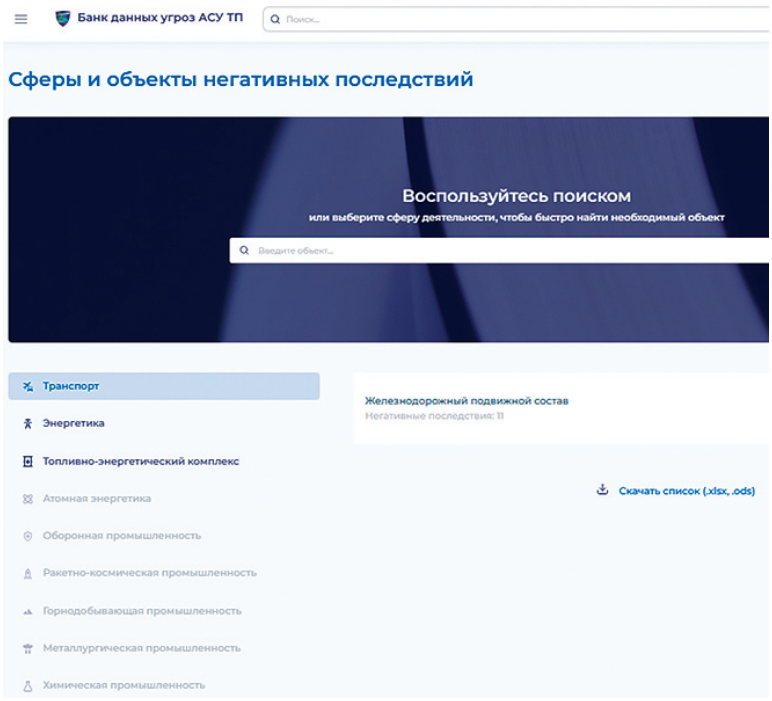

Рис. 2. Раздел «Транспорт» БДУ АСУ ТП

Таблица 2

Угрозы безопасности АСУ ТП [24]

Код	Наименование	Характеристика
1	*2*	*3*
УТП:01	Угроза утечки информации	Угроза заключается в возможности противоправного получения либо передачи информации (конфиденциальной, конфигурационной, аутентификационной, управляющей, измерительной и др.). Например, утечка значений параметров технологического процесса с АРМ оператора технологическим процессом.
УТП:02	Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника	Угроза заключается в возможности нарушения функционирования АСУ ТП и (или) внедрения в ее состав вредоносных программных или программно-аппаратных средств в результате получения компонентов программного обеспечения или его обновлений из недоверенных или скомпрометированных источников. Например, загрузка обновлений, содержащих программные закладки.
УТП:03	Угроза удаленного несанкционированного подключения к компонентам АСУ ТП	Угроза заключается в возможности получения удаленного доступа к информационным ресурсам АСУ ТП с использованием штатных средств удаленного доступа, предоставляемых компонентами АСУ ТП, и (или) проведения сетевой атаки. Например, использование сервисов и ресурсов корпоративной сети предприятия для получения доступа к компонентам АСУ ТП.
УТП:04	Угроза несанкционированного доступа	Угроза заключается в возможности получения доступа к информационным ресурсам, нарушающего установленные в АСУ ТП правила разграничения доступа, с использованием штатных средств, предоставляемых компонентами АСУ ТП. Например, несанкционированный доступ к информации, хранимой на файловом хранилище.
УТП:05	Угроза несанкционированной модификации (искажения)	Угроза заключается в возможности изменения содержания или формы представления обрабатываемой в АСУ ТП информации (конфигурационной, аутентификационной, управляющей, измерительной и др.), нарушающего установленный в АСУ ТП порядок обработки информации и правила разграничения доступа. Например, искажение отображаемой средствами человеко-машинного интерфейса информации.
УТП:06	Угроза несанкционированной подмены	Угроза заключается в возможности внедрения ложного или подмены существующего компонента АСУ ТП и (или) обрабатываемой с его использованием информации. Например, несанкционированная загрузка в ПЛК некорректных значений переменных.
УТП:07	Угроза удаления информационных ресурсов	Угроза заключается в возможности удаления обрабатываемой в АСУ ТП (конфиденциальной, конфигурационной, аутентификационной, управляющей, измерительной и др.), нарушающего установленные в АСУ ТП правила разграничения доступа. Например, удаление файлов проектов управления и контроля.

Табл. 2. Окончание

1	2	3
УТП:08	Угроза отказа в обслуживании	Угроза заключается в недоступности АСУ ТП или ее компонентов и (или) приостановлении оказания услуг или предоставления сервисов для авторизованных пользователей (в том числе до перезагрузки или проведения восстановительных работ). Например, вывод из строя (отказ в обслуживании) модуля ввода-вывода.
УТП:09	Угроза нарушения функционирования (работоспособности)	Угроза заключается в возможности нарушения штатного функционирования компонентов АСУ ТП и (или) задержке (замедлении) времени обработки информации. Например, выключение или перезагрузка ПЛК за счет несанкционированной отправки специального сетевого пакета.
УТП:10	Угроза несанкционированного сбора данных об автоматизированной системе управления	Угроза заключается в возможности сбора нарушителем данных о конфигурации АСУ ТП, учетных записях пользователей, применяемом программных и программно-аппаратных средствах, перечнях открытых портов и запущенных сервисов, возможных уязвимостей программного обеспечения, используемых протоколах передачи данных и другой информации, необходимой для реализации компьютерной атаки. Например, сканирование технологической сети для определения доступных хостов.

Выводы

В качестве выводов отметим следующее.

1. Создание ИСВТ сопровождается появлением новых типов угроз, обусловленных обработкой больших объемов информации, сложностью, уязвимостями и недекларированными возможностями используемых новейших технологий (информационных, телекоммуникационных, автоматизированного и автоматического управления, ИИ и др.), реализуемых путем компьютерных атак, неустранения ошибок ПО, загрузки ПО из недоверенных источников, инициирования недекларированного поведения ИИ и др. способами.

2. Новыми для ИСВТ угрозами безопасности являются также:

• несовершенство нормативной правовой базы разработки и реализации ИСВТ, отставание которой от состояния готовых к внедрению и, возможно, используемых технологий создает условия для неучета актов незаконного вмешательства нефизического происхождения в функционирования объектов ИСВТ;

• цифровое неравенство автоматизированных систем технологического и корпоративного управления в обеспеченности средствами защиты и персоналом, способными обеспечить комплексную защиту объектов ИСВТ от актов незаконного вмешательства физической и нефизической природы происхождения.

3. Решение задач обеспечения безопасности ИСВТ должно носить комплексный характер. Меры безопасности должны охватывать все этапы жизненного цикла ИСВТ, а их реализация начинаться заблаговременно.

Исследование выполнено в рамках стратегического проекта № 3 «Электронная навигация и беспилотное (автономное) судовождение» по программе стратегического академического лидерства «Приоритет-2030» по теме «Реализация проектов по разработке конструкторско-технологических решений и программных продуктов в области систем управления автономным судном на основе удаленного доступа (включая системы объективного контроля, обеспечения безопасности и живучести).

Литература

1. Козлов, Л. Н. О концептуальных подходах формирования и развития интеллектуальных транспортных систем в России / Л. Н. Козлов, Ю. М. Урличич, Б. Е. Циклис. - Текст : непосредственный // Транспорт Российской Федерации. - 2009. - № 3-4 (22-23). - С. 30-35.
2. ГОСТ Р 56829-2015. Интеллектуальные транспортные системы. Термины и определения = Intelligent transport systems. Terms and definitions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 10 декабря 2015 г. № 2150-ст : дата введения 2016-06-01. - URL: https://docs.cntd.ru/document/1200128315?ysclid=m4gn8yqc7j399550789 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.
3. ПНСТ 555-2021. Интеллектуальные транспортные системы. Системы искусственного интеллекта для автоматизации управления автомобильными транспортными средствами. Классификация и общие технические требования. = Intelligent transport systems. Artificial intelligent systems for automatization of motor vehicle driving. Classification and general technical requirements : предварительный национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 26 ноября 2021 г. № 48-пнст : срок действия с 2022-03-01 до 2023-03-01. - URL: https://docs.cntd.ru/document/1200181919?ysclid=m4gnna7k6x853460858 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.
4. Intelligent transport systems. Handbook on Land Mobile (including Wireless Access). International Telecommunication Union Radiocommunication Sector. Volume 4, 2021 edition. - URL: https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-49-2021-PDF-E.pdf (дата обращения: 25.08.2024). - Текст: электронный.
5. 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). - URL: http://static.government.ru/media/files/7enYF2uL5kFZlOOpQhLl0nUT91RjCbeR.pdf (дата обращения: 25.08.2024). - Текст : электронный.
6. Приоритетные направления научно-технологического развития Российской Федерации (утверждены Указом Президента Российской Федерации от 18.06.2024 № 529). - URL: https://docs.cntd.ru/document/1306389112?ysclid=m4go7fjnvk639317311 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.
7. Перечень важнейших наукоемких технологий Российской Федерации (утвержден Указом Президента Российской Федерации от 18.06.2024 № 529). - URL: https://docs.cntd.ru/document/1306389112?ysclid=m4goatbeh9215270477 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.
8. Михалевич, И. Ф. Концептуальные проблемы транспортной безопасности водных интеллектуальных транспортных систем / И. Ф. Михалевич. - Текст : непосредственный // Надежность. - 2024. - № 2. - С. 72-87. - https://doi.org/10.21683/1729-2646-2024-24-2-72-87.
9. Михалевич, И. Ф. Проблемы обеспечения безопасности автономного судоходства на внутренних водных путях / И. Ф. Михалевич / Москва : Горячая линия - Телеком, 2024. - 335 с. - Текст : непосредственный.
10. ГОСТ Р 51624-2000. Автоматизированные информационные системы в защищенном исполнении. Общие требования : национальный стандарт Российской Федерации : издание официальное : принят и введен в действие Постановлением Госстандарта России от 30 июня 2000 г. № 175-ст.: введен впервые. - URL: https://гостайна.рф/gost-r-51624-00-zi-as-v-zashchishchennom-ispolnenii-obshchie-trebovaniya?ysclid=m4gq25ol2e18078858 (дата обращения: 09.12.2024). - Режим доступа : Центр новых технологий Импульс. - Текст : электронный.
11. ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения = Information protection. Sequence of protected operational system formation. General provisions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 января 2014 г. № 3-ст.: переиздание. Октябрь 2018 г. - URL: https://docs.cntd.ru/

document/1200108858?ysclid=m4gqcv18s9579104562 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.

12. Технический регламент о безопасности объектов внутреннего водного транспорта (утвержден Постановлением Правительства Российской Федерации от 12.08.2010 № 623). - URL: https://docs.cntd.ru/document/902231454?ysclid=m4gql0ilmc135551877 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.

13. Требования по обеспечению транспортной безопасности, учитывающие уровни безопасности для транспортных средств морского и внутреннего водного транспорта (утв. Постановлением Правительства Российской Федерации от 08.10.2020 № 1637). - URL: https://docs.cntd.ru/document/565983839?ysclid=m4gqmwvlqz509256631 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.

14. 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 (утв. Постановлением Правительства Российской Федерации от 08.10.2020 № 1638). - URL: https://docs.cntd.ru/document/565983835?ysclid=m4gqq4argq346819313 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.

15. 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 10.10 2020 № 1651). - URL: https://docs.cntd.ru/document/565995417?ysclid=m4gqts8s3c713642424. - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.

16. Информационная безопасность системы автономного судовождения в контексте специфических для интеллектуальных транспортных систем угроз / Л. А. Баранов, И. Ф. Михалевич, Н. Д. Иванова, С. С. Соколов. - Текст : непосредственный // Проблемы управления безопасностью сложных систем : материалы XXXI международной конференции, Москва, 13 декабря 2023 года. - Москва : Институт проблем управления им. В. А. Трапезникова РАН, 2023. - С. 249-256. - DOI: 10.25728/iccss.2023.53.91.033.

17. Российская Федерация. Законы. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. - URL: https://docs.cntd.ru/document/436752114?ysclid=m4grgngr58397410000 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.

18. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения = Protection of information. Object of informatisation. Factors influencing the information. General : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст.: переиздание : Декабрь 2018 г. - URL: https://docs.cntd.ru/document/1200057516?ysclid=m4grjf72of81237717 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.

19. Threat Landscape Transport Sector. ENISA, March 21, 2023. - URL: https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape (дата обращения: 16.09.2024). - Текст : электронный.

20. Аналитический отчёт: Ландшафт киберугроз для России и СНГ 2024. Лаборатория «Касперского». - URL: https://go.kaspersky.com/rs/802-IJN-240/images/Report_Threat_Landscape_RU.pdf (дата обращения: 22.05.2024). - Текст : электронный.

21. Кибербезопасность на бескрайних морях. Блог компании Positive Technologies. - URL: https://habr.com/ru/companies/pt/articles/303198/ (дата обращения: 04.07.2023). - Текст : электронный.

22. ГОСТ Р 59298-2021. Суда безэкипажные внутреннего плавания. Термины и определения = Unmanned inland navigation vessels. Terms and definitions : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 января 2021 г. № 29-ст.: введен впервые: дата введения 2021-04-01. - URL: https://docs.cntd.ru/document/1200177819?ysclid=m4gugpvgr3786113598 (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.

23. ГОСТ Р 59284-2020. Суда безэкипажные технического флота. Общие требования = Unmanned vessels of technical fleet. General requirements: национальный стандарт Российской Федерации : издание официальное : введен впервые утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2020 г. № 1429-ст Приказом Федерального агентства по техническому регулированию и метрологии от 29 декабря 2020 г. № 1429-ст (дата обращения: 09.12.2024). -Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.

24. Национальная стратегия развития искусственного интеллекта на период до 2030 года (утв. Указом Президента Российской Федерации от 10.10.2019 г. № 490, в редакции Указа от 15.02.2024 № 124). - URL: https://docs.cntd.ru/document/563441794?marker=65C0IR (дата обращения: 09.12.2024). - Режим доступа : Электронный фонд правовых и нормативно-технических документов. - Текст : электронный.

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