Автоматизация и моделирование в проектировании и управлении. 2023. № 1 (19). С. 12-20.
ISSN 2658-3488 print, ISSN 2658-6436 online
Automation and modeling in design and management. 2023. № 1 (19). P. 12-20.

Научная статья
Статья в открытом доступе
УДК 531.391.1:532.5.011
doi: 10.30987/2658-6436-2023-1-12-20

МЕТОДЫ И СРЕДСТВА АВТОМАТИЗИРОВАННОГО ОБНАРУЖЕНИЯ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ НА ОБЪЕКТЕ ТРАНСПОРТНОЙ ИНФРАСТРУКТУРЫ (НА ПРИМЕРЕ МОРСКОГО ПОРТА)

Сергей Сергеевич Соколов [1]✉, Олег Николаевич Губернаторов [2], Татьяна Петровна Кныш [3]
[1, 2, 3] Государственный университет морского и речного флота имени адмирала С.О. Макарова, г. Санкт-Петербург, Россия
[1] sokolovss@gumrf.ru, http://orcid.org/0000-0002-4581-2518
[2] ovel82@mail.ru, http://orcid.org/0000-0002-7337-632X
[3] knyshtp@gumrf.ru, http://orcid.org/0000-0003-3745-4375

Аннотация. *В работе предлагаются методы и средства автоматизированного обнаружения нарушителя безопасности на объекте транспортной инфраструктуры. Рассматриваются возможности применения автономных технических средств в качестве инструмента для незаконного получения сведений об объекте транспортной инфраструктуры, которые необходимы для подготовки акта незаконного вмешательства. Проанализированы средства и системы обеспечения транспортной безопасности морского порта. Проведены исследования в области существующих средств и методов автоматизированного обнаружения таких автономных технических средств, как беспилотные летательные аппараты, с целью анализа достаточности или выявления необходимости в дальнейших исследованиях и разработках, а также определена возможность их использования в качестве технического средства обеспечения транспортной безопасности. Поставлена задача по разработке автоматизи-рованной системы, основанной на акустическом методе обнаружения с последующей видеоверификацией. В дальнейшем данная система может быть использована в качестве дополнительного модуля для систем обнаружения беспилотного воздушного судна, которые основаны на других методах обнаружения. Комплексная система позволяет минимизировать риск возникновения ошибок первого и второго рода, что позволяет ис-пользовать её в качестве технического средства обеспечения транспортной безопасности.*

Ключевые слова: методы, средства, автоматизация, обнаружение нарушителя, информационная безопасность, транспортная инфраструктура, транспортная безопасность, безопасность объекта транспортной инфраструктуры

Для цитирования: Соколов С.С., Губернаторов О.Н., Кныш Т.П. Методы и средства автоматизированного обнаружения нарушителя безопасности на объекте транспортной инфраструктуры (на примере морского порта) // Автоматизация и моделирование в проектировании и управлении. 2023. №1 (19). С. 12-20. doi: 10.30987/2658-6436-2023-1-12-20

Original article

Open Access Article

METHODS AND TOOLS FOR AUTOMATED DETECTION OF A SECURITY VIOLATOR AT THE TRANSPORT INFRASTRUCTURE FACILITY (BY THE EXAMPLE OF A SEAPORT)

Sergey S. Sokolov [1]✉, Oleg N. Gubernatorov [2], Tatyana P. Knysh [3]
[1, 2, 3] Admiral Makarov State University of Maritime and Inland Shipping, St. Petersburg, Russia
[1] sokolovss@gumrf.ru, http://orcid.org/0000-0002-4581-2518
[2] ovel82@mail.ru, http://orcid.org/0000-0002-7337-632X
[3] knyshtp@gumrf.ru, http://orcid.org/0000-0003-3745-4375

Abstract. *The paper proposes methods and tools for automated detection of a security violator at a transport infrastructure facility. The work considers the possibilities of using autonomous technical means as a tool for illegally obtaining information on a transport infrastructure facility, which is necessary for preparing an act of unlawful*

interference. The means and systems for ensuring the transport security of the seaport are analysed. Research is carried out in the field of existing means and methods for the automated detection of such autonomous technical resources as unmanned aerial vehicles, to analyse the sufficiency or identify the need for further research and development; also the possibility of their use as a technical means of ensuring transport security is determined. The objective was set to develop an automated system based on the acoustic detection method with the subsequent video verification. In the future, this system can be used as an additional module for unmanned aircraft detection systems that are based on other detection methods. The integrated system allows minimizing the risk of errors of the first and second kind, which makes it possible to use it as a technical means of ensuring transport security.

Keywords: methods, tools, automation, intruder detection, information security, transport infrastructure, transport security, transport infrastructure facility security

For citation: Sokolov S.S., Gubernatorov O.N., Knysh T.P. Methods and tools for automated detection of a security violator at the transport infrastructure facility (by the example of a seaport). Automation and modeling in design and management, 2023, no. 1 (19). pp. 12-20. doi: 10.30987/2658-6436-2023-1-12-20.

Введение

В наше время мы являемся свидетелями того, как экспоненциальными темпами осуществляется повсеместное массовое внедрение киберфизических и искусственных когнитивных систем. К ключевым технологическим тенденциям киберфизических систем можно отнести: большие данные, автономные роботы, моделирование и симуляторы, облачные вычисления, Интернет вещей, информационная безопасность, 3D-печать, дополненная реальность и т.д.

В рамках данной работы остановимся подробнее на тенденции автономности. Автономность, автономные роботы, автономные технические устройства открывают человечеству не только множество возможностей, но и целый ряд проблем.

Следом за сегодняшней технологической революцией (которая неминуема и не обратима) необходимо произвести реформы в различных областях.

Рассматривая область обеспечения транспортной безопасности, авторами поставлена проблема – появление возможности применения автономных технических средств в качестве инструмента для незаконного получения сведений об объекте транспортной инфраструктуры (в рамках темы исследования – морской порт), которые необходимы для подготовки акта незаконного вмешательства.

Морской порт как объект транспортной инфраструктуры имеет ряд особенностей, которые напрямую влияют на выбор методов и средств обеспечения его безопасного функционирования:

1. Локализованное размещение на территории страны, региона.

2. Существенно различающиеся вероятности по периметру реализации атаки с помощью беспилотных летательных аппаратов (БПЛА) (те части периметра, которые граничат с иными территориями государства/региона/с другими объектами транспортной инфраструктуры, имеют потенциально большую вероятность реализации атаки; те части периметра, которые граничат с морскими путями – имеют потенциально более низкую вероятность).

3. Плановость, предсказуемость, ритмичность основных процессов, включая процесс легального прохода и проезда на территорию морского порта различных видов транспортных средств и людей.

4. Преимущественно отрытое пространство перед главной проходной, свободное от помех в виде растительности, построек и т.д.

5. Иные особенности, продиктованные особенностью эксплуатации морского транспорта. [1]

Беспилотные летательные аппараты определены как автономные технические средства, которые обладают характеристиками, позволяющими использовать их в качестве инструмента для незаконного сбора информации. Более того БПЛА могут быть использованы и для уничтожения (воздействия) каких-либо целей.

Таким образом, БПЛА – это многоцелевое средство, которое может использоваться и для сбора данных, и для воздействия на объект транспортной инфраструктуры.

Встает вопрос об исследовании вопроса обнаружения и противодействия такому потенциальному нарушителю транспортной безопасности как БПЛА.

В связи с этим представляется актуальным проведение исследования в области существующих средств и методов автоматизированного обнаружения таких автономных технических средств как БПЛА с целью анализа достаточности или выявления необходимости в дальнейших исследованиях и разработках, а также определения возможности их использования в качестве технического средства обеспечения транспортной безопасности [2, 3].

Законодательство

Транспортная безопасность. В области обеспечения транспортной безопасности создание нормативно-правовой базы началось с принятия Государственной Думой Федерального закона «О транспортной безопасности» № 16-ФЗ от 09.02.2007 г. (далее – ФЗ-16).

ФЗ-16 определяет основное требование к техническим средствам обеспечения транспортной безопасности – согласно статье 12.2. технические средства обеспечения транспортной безопасности подлежат обязательной сертификации в соответствии с законодательством РФ.

БПЛА. В отличии от области транспортной безопасности правовое регулирование в области создания и эксплуатации автономных технических средств только начинает зарождаться. Отсутствие чёткой системы ответственности создаёт проблему возможной безнаказанности, чем несомненно могут воспользоваться возможные злоумышленники. Законодательство в области БПЛА представлено привычной нормативной пирамидой, верхушка которой – это «Воздушный кодекс Российской Федерации» от 19.03.1997 №60-ФЗ (далее – 60-ФЗ). Данный кодекс меняет понятие БПЛА на «беспилотное воздушное судно» (БВС). Согласно документу БВС – это летательный аппарат, который поддерживается в атмосфере за счет взаимодействия с воздухом, отличным от взаимодействия с воздухом, который отражен от поверхности земли или воды, и при этом управляется и контролируется пилотом, который находится вне борта. Немаловажным фактом является то, что согласно 60-ФЗ учету подлежат БВС, превышающее взлетную массу в 0,25 килограмма, из чего следует, что БВС весом менее 250 грамм учету и контролю не подлежат. Отсутствие требований в учете, а следовательно, и должного контроля несёт за собой возможность использование таких БВС в качестве инструмента совершения преступлений (АНВ).

Следующим важным законодательным актом стало Постановление Правительства от 3 февраля 2020 года № 74, которое внесло правки в Постановление Правительства от 11.03.2010 № 138 – правки внесены касаемо правил использования БВС. Далее приведем ряд выписок из данного документа, которые являются наиболее важными в рамках данной работы:

«п. 47 б – пункты управления БВС, которые находятся в приграничной полосе, должны иметь систему наблюдения, которая позволит осуществлять контроль за полетом БВС»

«п. 49 – … полеты БВС выполняются при наличии у пользователей воздушного пространства разрешения соответствующего органа местного самоуправления, а в городах федерального значения (Москва, Санкт-Петербург и Севастополь) – разрешения соответствующих органов исполнительной власти указанных городов»

«п. 52(1) – план-полет воздушного судна не требуется в случае выполнения визуальных полетов БВС с максимальной взлетной массой до 30 кг, которые осуществляются в пределах прямой видимости в светлое время суток на высотах менее 150 метров от земной или водной поверхности: …»

Однако, все эти важные правила вновь определены для БВС за исключением использования БВС с максимальной взлетной массой менее 250 грамм. Можно сказать, что БВС с максимальной взлетной массой менее 250 грамм – это бесконтрольный инструмент для совершения АНВ.

Средства и системы обеспечения транспортной безопасности

Требования к функциональным свойствам технических средств ОТБ установлены Постановлением Правительства РФ №969 от 26.09.2016 г. [4]. Средства автоматизированного

обнаружения нарушителя безопасности на объекте транспортной инфраструктуры, по мнению авторов, должны обеспечивать:

– обнаружение незаконного проникновения (или попытки) на объект транспортной инфраструктуры;

– обнаружение совершения (или попытки) противоправных действий;

– выдачи информации на пульт централизованного наблюдения о попытках или совершении незаконного проникновения и (или) противоправных действий;

– контроль объектов охраны и прилегающих к ним территорий, в том числе визуальный и звуковой.

Таким образом, предполагается, что средство автоматизированного обнаружения нарушителя безопасности на объекте транспортной инфраструктуры – это техническое средство видеонаблюдения, обеспечивающее видеоверификацию тревог (раздел V Постановления Правительства № 969). Технические средства и системы, имеющие действующий сертификат соответствия данному разделу и в том числе п. 22 (а) можно условно разделить по используемым технологиям на следующие: с применением нейронных сетей (технические средства видеонаблюдения «Видеокомплексы «ИВК» АФЕТ.201219.100 ТУ, элементы системы видеонаблюдения «Тепловизионные комплексы ИТК» АФЕТ.201219.300 ТУ); автономный сервер видеоаналитики (расширенные алгоритмы искусственного интеллекта AI) (техническая система обеспечения транспортной безопасности «Система телевизионного наблюдения «BSVS», система охранная телевизионная «PROGMATIC» серии «PRO-M»); программно и аппаратно (М2Медиа.Видео – нейросети) (техническая система обеспечения транспортной безопасности «Система видеонаблюдения, аналитики, связи и оповещения на транспорте «М2Медиа.Видео+», система видеонаблюдения и регистрации на транспорте «М2Медиа.Видео» ТУ 4372-001-15086177-2020) и др.

Анализ представленных выше данных показывает, что к применяемым технологиям обнаружения «тревог/событий» можно отнести следующие понятия: машинное обучение, нейронные сети, искусственный интеллект, компьютерное зрение, видеосемантика, эффект Доплера [5].

Машинное обучение – класс искусственного интеллекта, основанный на обучении за счет применения решений множества сходных задач (используемые средства: математическая статистика, численные методы, математический анализ, методы оптимизации, теория вероятностей, теория графов и т.д.). Нейронная сеть – математическая модель, которая построена по принципу организации и функционирования сетей нервных клеток живого организма. Характеризуется способностью к обучению. Решает задачи адаптивного управления, распознавания образов, дискриминантного анализа и т.д. Искусственный интеллект – технология создания интеллектуальных машин. Компьютерное зрение – технология создания машин. Производящих обнаружение, отслеживание и классификацию объектов. Видеосемантика – направление видеоаналитики, основанное на изложении видеоинформации на семантические единицы. Эффект Доплера – изменение частоты и длины волны излучения, которое воспринимается приёмником, вследствие движения источника излучения.

Эффективность использования представленных на рынке технических средств видеонаблюдения в качестве инструмента, который решает задачу автоматизированного обнаружения такого нарушителя безопасности, как БВС на объекте транспортной инфраструктуры, потенциально мала. Объясняется это тем, что:

– при использовании простых механизмов, например, датчиков движения существует высокий риск ложного срабатывания;

– при использовании сложной видеоаналитики, существует проблема потери времени для срабатывания (прохождение трафика на сервер и его обработка занимает от 1 до 15 минут);

– при осуществлении видеоверификации человеком существует, так называемый, человеческий фактор.

Для решения данной проблемы проанализируем методы, которые используют совре-

менные системы обнаружения БВС. Цель данного анализа – определить какой метод в сочетании со средством видеонаблюдения гипотетически будет максимально эффективным в решении задачи обнаружения БВС.

Системы обнаружения БВС. Различают следующие системы автоматического обнаружения БВС в заданном секторе:

– оптические (состоит как минимум из одного из базовых оптических элементов);

– радиолокационные (использует метод, который основан на излучении радиоволн и регистрации их отражений от объектов);

– акустические (использование звука для определения расстояния и направления его источника или отражателя);

– радиочастотные (принцип передачи и приема радиоволн для определения расстояния, скорости и относительного угла движения объектов, которые находятся в поле обнаружения);

– по температурной аномалии (использование тепловизоров);

– лидар (технология обнаружения и определения дальности с помощью света);

– комбинированные.

Радиолокационное обнаружение. Эффективность и качество обнаружения с использованием радиолокационных станций характеризуются следующими параметрами:

– зона радиолокационного обзора – область произведения облучения и приема/обработки отраженных сигналов. Прием сигналов происходит в условиях естественных или искусственных помех случайного характера. Соответственно прием сигналов – это случайное явление, изучаемое теорией вероятности;

– разрешающая способность – характеристика, которая определяет возможность разделять близко расположенные цели;

– точность радиолокационных измерений – это характеристика, которая зависит от допущения грубых, систематических или случайных ошибок. Грубая ошибка – это результат грубого просчета оператора или неисправности аппаратуры. Систематическая ошибка – это результат действия факторов на протяжении длительного времени (возмещается калибровкой аппаратуры). Случайные ошибки – это результат случайно произошедших событий (невозможно учесть заранее);

– помехозащищенность – это совокупность помехоустойчивости и скрытности. Помехоустойчивость – это способность противостоять помехам. Скрытность – это способность противостоять разведке;

– пропускная способность – это характеристика, выражающая способность обеспечивать одновременную работу с рядом объектов;

– надежность – это способность непрерывной работы в течение необходимого времени;

– степень автоматизации съема и обработки информации (автоматизированная если получатель информации – это вычислительное устройство; полуавтоматическая – если получатель – человек).

Системы обнаружения, основанные на применении радиолокационных станций, не обеспечивают стабильной эффективности, так как многое зависит от влияния помех. Следовательно, существуют значительные ограничения для производительной работы, например: сложности работы на загруженных участках (на которых используется несколько радиолокационных станций одновременно) – возникает вероятность совпадения частотных диапазонов; ограничения работы при наличии крупных отражающих объектов в радиусе работы радиолокационной станции – вероятность возникновения эффекта мнимого изображения (на экране появляется объект, который расположен в другом месте); наличие большого количества близких объектов – вероятность возникновения эффекта многократного отражения (на экране видны несколько ложных объектов).

Радиочастотное обнаружение. Радиоволна – распространяющееся в пространстве возмущение электромагнитного поля с частотами до 3 ТГц, которая распространяется в пространстве без искусственного волновода.

Радиоволны широко применяются для обнаружения объектов и определения координат, что обусловлено такими свойствами, как:

– распространение со скоростью света, вне зависимости от времени суток и метеорологических условий;

– отражение от любых объектов, встречающихся на пути распространения;

– прямолинейное распространение в однородной среде;

– поглощение энергии сопровождает процесс распространения в среде отличной от воздуха;

– дифракция наиболее сильна в случае, когда препятствия по размеру сравнимы с длиной волны;

– интерференция;

– способность прохождения через некоторые неметаллические материалы, при минимальном их отражении.

Не все свойства имеют исключительно положительный характер, с точки зрения обеспечения эффективности обнаружения интерференция играет обратную роль, в случае, когда на пути встречаются плоские металлические предметы (дорожные знаки, рекламные щиты и т.д.).

Оптическое (видео) обнаружение. Оптическое обнаружение – это применение систем видеонаблюдения в качестве средств обнаружения. Видеонаблюдение – это процесс, который осуществляется оптико-электронными устройствами, которые в свою очередь предназначены для визуального контроля/автоматического анализа. Система видеонаблюдения – это программно-аппаратный комплекс, в который входят видеорегистраторы, видеокамеры, мониторы, объективы, усилители и прочие устройства. Система видеонаблюдения, охватывающая большую зону, должна включать в себя устройства, обладающие наивысшими характеристиками, что делает её, в первую очередь, достаточно дорогостоящей.

Основным недостатком данного метода является сильная зависимость от факторов окружающей среды. Также присутствует проблема зависимости увеличения дальности обнаружения от сужения зоны поиска. Помимо этого, системы обнаружения, использующие данный метод обнаружения, подразумевают под собой применение видеоаналитики – особенности данных технологий уже были рассмотрены ранее в этой работе.

Акустическое обнаружение. Акустические датчики работают по схеме:

– прослушивание – распознание уникальных звуковых сигнатур различных типов БВС;

– анализ – сравнение распознанных образцов с базой данных (совпадение есть – запись идентифицирующей информации);

– идентификация – обнаружение акустических сигнатур БВС (уровень ложных срабатываний зависит от имеющейся базы данных);

– оповещение.

К преимуществам данных систем относятся: возможность интеграции; доступность по цене; возможность обнаружения БВС малого веса; обнаружение БВС с отсутствием радиочастотной связи.

Обнаружение по температурной аномалии. Тепловидение – это метод, позволяющий обнаруживать объекты в полной темноте и различных погодных условиях. Тепловизор – это устройство для наблюдения за распределением температуры, которое может быть использовано и для гражданских объектов без каких-либо ограничений. Принцип действия заключается в регистрации и анализе температур поверхности объектов, которые находятся в радиусе действия устройства. Результатом является картина распределения температур.

Радиус действия тепловизора – это характеристика, определяющая дальность видимости цели, и которая определяется дальностью обнаружения, распознавания и идентификации. Обнаружение – это выявление некого объекта без возможности определить какой именно. Распознавание – очертание объекта четкие, тип определяется безошибочно. Идентификация – возможность охарактеризовать объект.

Данный принцип сложно применять для обнаружения малогабаритных БВЗ, велика вероятность возникновения ошибок первого и второго рода.

Обнаружение с помощью света (лидар) [6]. Лидар – технология дистанционного зондирования, использующая лазерный импульс для сбора измерений. В сочетании с системами GPS, лидар – это инструмент для обеспечения точных геопространственных измерений. Принцип работы лидара заключается в распространении световой волны для дальнейшего считывания отражения от объекта. В результате работы лидара получается некая карта местности [7, 8].

Данная система также имеет ряд преимуществ и недостатков. К преимуществам относятся: высокая скорость сбора данных; высокая точность сбора данных; высокое проникновение; возможность использования в любое время суток (ночью, в солнечный день) без потери свойств; высокое разрешение полученного изображения; отсутствие геометрических искажений; не зависит от человеческого фактора; высокая степень интеграции.

К недостаткам применения систем лидара относятся: стоимость; зависимость от метеорологических условий (дождь, туман, снег); большой трафик данных, требующий либо больших вычислительных ресурсов, либо времени для обработки; существуют ограничения по высоте.

В табл. 1 проведен обзор готовых решений задачи обнаружения БВС гражданского применения.

Таблица 1

Готовые решения для обнаружения БВС гражданского применения

Table 1

Ready-made solutions for detecting unmanned aerial vehicles for civilian use

Производитель	Система	Радиус обнаружения, км	Обнаружение оператора	Тип детекции
АО НПП Алмаз	Атака - DBS	1,5	-	Радиочастотная
ООО ТАиП	Стриж-3	3,0	+	Радиочастотная
	Скворец	1,5	-	Радиочастотная
	Снегирь	1,5	+	Радиочастотная
НИИ Вектор	ЭГИДА	20,0	+	Полуактивная радиолокация
	Защита	20,0	+	
ООО АнтиДрон	АнтиДрон	1,5	+	Радиочастотная
АО НПЦ Элвис	РЛС Енот	2,5	+	Радиолокация
Лаборатория Касперского	Kaspersky Antidrone	4,0	+	Полный комплекс

Из табл. 1 видно, что существующие системы обнаружения используют методы, основанные на анализе радиоволн.

Для решения поставленной задачи необходимо разработать модель нарушителя обеспечения транспортной безопасности морского порта, где в качестве нарушителя будет рассмотрены БВС малой взлетной массы, с целью разработки новых и внесения изменения в существующие методы и средства обеспечения безопасности морского порта как объекта транспортной безопасности [9, 10].

При разработке существующих методов и средств автоматизированного обнаружения нарушителя безопасности на объекте транспортной инфраструктуры частично учтены особенности эксплуатации объектов, например, в отличие от морского порта, железнодорожная станция не имеет струю организованность потоков пассажиров, менее предсказуема интенсивность потока, чем в морском порту, таким образом требуется полное покрытие территории, например, системой видеоверификации, с минимальной фокусировкой на отдельных зонах. В тоже время, в морском порту, в виду наличия более жёсткого конструкционного разделения, можно сконцентрироваться на определённых зонах.

Также, следует отметить, что характер шумов, потенциально влияющих на работу приборов в железнодорожном транспорте более предсказуем, чем на морском (на морском транспорте большее разнообразие технических средств, обеспечивающих функционирование порта и эксплуатацию судна), что также важно учитывать при настройке системы защиты, однако, это не всегда представляется возможным, что также даёт почву дальнейшим исследованиям.

Заключение

В наше время габариты БВС становятся все меньше, при этом некоторые модели уже применяют маскировку под окружающую среду, что значительно снижает эффективность обнаружения БВС системами, которые основаны на традиционных методах (оптическом, радиолокационном, радиочастотном).

В результате проведенного исследования авторы работы ставят задачу по разработке системы, основанной на акустическом методе обнаружения с последующей видеоверификацией. В дальнейшем данная система может быть использована в качестве дополнительного модуля для систем обнаружения БВС, которые основаны на других методах обнаружения. Комплексная система позволит минимизировать риск возникновения ошибок первого и второго рода, что позволит использовать её в качестве технического средства обеспечения транспортной безопасности (в том числе для морских портов).

Для решения поставленной задачи необходимо разработать модель нарушителя обеспечения транспортной безопасности, где в качестве нарушителя будет рассмотрены БВС малой взлетной массы.

СПИСОК ИСТОЧНИКОВ

1. Sokolov S., Glebov N., Natashova K., Gubernatorov O. Categorization of objects of critical information infrastructure of water transport // E3S Web of Conferences. 2019. Vol. 110. DOI: 10.1051/e3sconf/201911002003 EDN: SSMWSP

2. Соколов С.С., Ныркov А.П, Глебов Н.Б. Кибербезопасность на водном транспорте // Сборник тезисов докладов. Национальная научно-практическая конференция профессорско-преподавательского состава ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова». 2018. edn: wuigfg.

3. Соколов С.С. Методы и модели обеспечения информационной безопасности объектов транспортной инфраструктуры, отнесенных к критически важным для национальной безопасности РФ объектам // Современные проблемы науки и образования. 2015. № 1-1. URL: http://scienceeducation.ru/ru/article / view?id=18583 (дата обращения: 23.10.2020).

4. Ныркov А.П., Кислов Р.И., Белов А.В. К вопросу о категорировании объектов критической информационной инфраструктуры водного транспорта. // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». СанктПетербург, 24-26 октября 2018 г.: Материалы конференции. \ СПОИСУ. – СПб, 2018. – 631 с. ISBN 978–5–907050–44–0.

5. Банк данных угроз безопасности информации // ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» URL: https://bdu.fstec.ru (дата обращения: 16.10.2019).

6. Sokolov S.S., Glebov N.B., Antonova E.N., Nyrkov A.P. The Safety Assessment of Critical Infrastructure Control System // Proceedings of the 2018 International Conference «Quality Management, Transport and Information Security, Information Technologies», IT and QM and IS 2018. DOI: 10.1109/ITMQIS. 2018.8524948.

7. Ли И.В., Наташова К.В., Проблемы обеспечения информационной безопасности автоматизированных систем на водном транспорте //Сборник трудов «Региональная информатика и информационная безопасность», Выпуск 5 / СПОИСУ. СПб., 2018. 549 с.

REFERENCES

1. Sokolov S., Glebov N., Natashova K., Gubernatorov O. Categorization of objects of critical information infrastructure of water transport // E3S Web of Conferences. 2019. Vol. 110. DOI: 10.1051/e3sconf/201911002003 EDN: SSMWSP

2. Sokolov S.S., Nyrkov A.P., Glebov N.B. Cybersecurity in water transport // Collection of abstracts. National scientific-practical conference of professors-teaching staff of FGBOU VO "Admiral S.O. Makarov HSMRF". 2018. edn: wuigfg.

3. Sokolov S.S. Methods and models of information security of transport infrastructure objects, referred to the critical for the national security of the Russian Federation // Modern problems of science and education. 2015. no. 1-1. URL: http://scienceeducation.ru/ ru/article/ view?id=18583 (date of reference: 23.10.2020).

4. Nyrkov A.P., Kislov R.I., Belov A.V. On the categorization of critical information infrastructure objects of water transport. // Regional Informatics (RI-2018). XVI Saint-Petersburg international conference "Regional Informatics (RI-2018)". St. Petersburg, October 24-26, 2018: Conference materials. SPOISU. SPb. 2018. 631 c. ISBN 978-5-907050-44-0.

5. Data bank of threats to information security // FSTEC of Russia, FAU GNII PTZI FSTEC of Russia URL: https://bdu.fstec.ru (date of access: 16.10.2019).

6. Sokolov S.S., Glebov N.B., Antonova E.N., Nyrkov A.P. The Safety Assessment of Critical Infrastructure Control System // Proceedings of the 2018 International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2018. DOI: 10.1109/ITMQIS. 2018.8524948.

7. Lee I.V., Natashova K.V., Problems of information security of automated systems on water transport. // Collection of works "Regional informatics and information security", Issue 5 / SPOISU. SPb. 2018. 549 c.

8. Ли И.В., Наташова К.В., Нормативно-правовое регулирование информационной безопасности на водном транспорте // Региональная информатика (РИ-2018). XVI Санкт-Петербургская международная конференция «Региональная информатика (РИ-2018)». Санкт-Петербург, 24-26 октября 2018 г.: Материалы конференции. \ СПОИСУ. СПб. 2018. 631 с. ISBN 978–5–907050–44–0.

9. Наташова К.В., Ли И.В., Современное состояние ИТС и ИТ на водном транспорте // Материалы IX межвузовской научно-практической конференции аспирантов, студентов и курсантов «Современные тенденции и перспективы развития водного транспорта России» 23 мая 2018 года. СПб.: Изд-во ГУМРФ им. адм. С.О. Макарова. 2018. 928 с.

10. Glebov N., Zhilenkov A., Chernyi S., Sokolov S., «Process of the Positioning Complex Modeling Objects with Elements of Intellectual Analysis». Procedia Computer Science. 2019. Vol. 150. P. 609-615.

11. Наташова К.В. Об основных темах для обсуждения и итогах 11-й межсессионной встречи регионального форума АСЕАН по безопасности на море // Современные тенденции и перспективы развития водного транспорта России: материалы X межвузовской научно-практической конференции аспирантов, студентов и курсантов. 22 мая 2019 года. СПб.: Изд-во ГУМРФ им. адм. С.О. Макарова. 2019. 777 с.

8. Lee I.V., Natashova K.V., Normative-legal regulation of information security on water transport.// Regional Informatics (RI-2018). XVI Saint-Petersburg international conference "Regional informatics (RI-2018)". St. Petersburg, October 24-26, 2018: Conference materials. SPOISU. SPb. 2018. 631 c. ISBN 978-5-907050-44-0.

9. Natashova K.V., Lee I.V., Modern state of ITS and IT on water transport.//Materials of IX interuniversity scientific and practical conference of graduate students, students and cadets "Modern trends and prospects of development of water transport of Russia" 23 May 2018. St. Petersburg: Publishing house of S.O. Makarov State University of Maritime Transport. 2018. 928 c.

10. Glebov N., Zhilenkov A., Chernyi S., Sokolov S., "Process of the Positioning Complex Modeling Objects with Elements of Intellectual Analysis", Procedia Computer Science. 2019. Vol. 150. P. 609-615.

11. Natashova K.V., On the main topics for discussion and the results of the 11th intersessional meeting of the ASEAN regional forum on maritime safety.// Modern trends and prospects for the development of water transport in Russia: materials of X interuniversity scientific and practical conference of graduate students, students and cadets. St. Petersburg: Publishing house of S. O. Makarov GUMRF, 2019. 777 c.

Информация об авторах:

Соколов Сергей Сергеевич
заведующий кафедрой комплексного обеспечения информационной безопасности государственного университета морского и речного флота имени адмирала С.О. Макарова, ORCID 0000-0002-4581-2518, Scopus Autor ID: 56606754000

Губернаторов Олег Николаевич
аспирант кафедры комплексного обеспечения информационной безопасности государственного университета морского и речного флота имени адмирала С.О. Макарова, ORCID 0000-0002-7337-632X, Scopus Autor ID: 57210562929

Кныш Татьяна Петровна
доцент кафедры прикладной математики государственного университета морского и речного флота имени адмирала С.О. Макарова, ORCID 0000-0003-3745-4375, Scopus Autor ID: 6506293872

Information about the authors:

Sokolov Sergey Sergeevich
head of Department of Complex Information Security Admiral Makarov State University of Maritime and Inland Shipping, Scopus Autor ID: 56606754000

Gubbernatorov Oleg Nikolaevich
graduate student in the Department of Complex Information Security Admiral Makarov State University of Maritime and Inland Shipping, Scopus Autor ID: 57210562929

Knysh Tatiana Petrovna
associate Professor of Department Applied Mathematic Admiral Makarov State University of Maritime and Inland Shipping, Scopus Autor ID: 6506293872

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации.

Contribution of the authors: the authors contributed equally to this article.

Авторы заявляют об отсутствии конфликта интересов.
The authors declare no conflicts of interests.

Статья поступила в редакцию 09.09.2022; одобрена после рецензирования 28.10.2022; принята к публикации 01.11.2022.

The article was submitted 09.09.2022; approved after reviewing 28.10.2022; accepted for publication 01.11.2022.

Рецензент – Рытов М.Ю., кандидат технических наук, доцент, Брянский государственный технический университет.

Reviewer – Rytov M.Yu., Candidate of Technical Sciences, Associate Professor, Bryansk State Technical University.