ISBN 978-5-901722-96-1

УДК 342.9:004.9:656.6

КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В СФЕРЕ ВОДНОГО ТРАНСПОРТА

Белоусова Екатерина Павловна[1], студент
e-mail: belousova.katerinaa@mail.ru
Валяев Александр Владимирович[1], к.т.н., доцент кафедры систем информационной безопасности, управления и телекоммуникаций
e-mail: wav-dk@mail.ru

[1] Волжский государственный университет водного транспорта, Нижний Новгород, Россия

Аннотация. В статье рассматривается роль информационных технологий в обеспечении функционирования объектов водного транспорта. Внедрение автоматизированных систем управления, средств связи и навигации приводит к уязвимости объектов водного транспорта перед компьютерными атаками, несанкционированным доступом и иными угрозами. Корректное категорирование объектов критической информационной инфраструктуры (КИИ) позволяет выявить наиболее значимые объекты, оценить ущерб от угроз посредством комплекса организационных, технических и правовых мер защиты.

Ключевые слова: водный транспорт, информационные технологии, информационная безопасность, критическая информационная инфраструктура, транспортная безопасность.

CATEGORIZATION OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES IN THE FIELD OF WATER TRANSPORT

Ekaterina P. Belousova[1], Student
e-mail: belousova.katerinaa@mail.ru
Alexander V. Valyaev[1], Candidate of Technical Sciences, Associate Professor of the Department of Information Security Systems, Management and Telecommunications
e-mail: wav-dk@mail.ru

[1] Volga State University of Water Transport, Nizhny Novgorod, Russia

Abstract. The article considers the role of information technologies in ensuring the functioning of water transport facilities. The introduction of automated control systems, communication and navigation facilities leads to vulnerability of water transport facilities to computer attacks, unauthorized access and other threats. The correct categorization of critical information infrastructure (CI) facilities makes it possible to identify the most significant facilities and assess damage from threats through a set of organizational, technical and legal protection measures.

Keywords: water transport, information technology, information security, critical information infrastructure, transport security.

Информационные технологии в обеспечении функционирования объектов водного транспорта выступают одним из ключевых критериев безопасности, поскольку позволяют своевременно выявлять, анализировать и минимизировать риски, связанные с эксплуатацией судов и портовой инфраструктуры. Их применение обеспечивает автоматизацию процессов мониторинга навигационной обстановки, контроля технического состояния оборудования и обмена данными между участниками транспортного процесса. В условиях возрастающей уязвимости объектов воднотранспортной инфраструктуры, информационные технологии выступают не только в качестве инструмента улучшения их деятельности, но и как средство правовой и организационной защиты. Нарушение их функционирования приводит к сбоям в управлении перевозками, снижению уровня транспортной безопасности и возникновению аварийных ситуаций. Таким образом, развитие информационных технологий на водном транспорте должно сопровождаться комплексными мерами по обеспечению киберустойчивости и правого регулирования используемых решений в цифровом пространстве.

Нормативно-правовое регулирование в данной отрасли характеризуется не только наличием общих организационно-правовых предписаний, но и самостоятельным отраслевым закреплением правовых механизмов. Кодекс торгового мореплавания РФ [1] и Кодекс внутреннего водного транспорта РФ [2] закрепляют общие правовые основы организации и осуществления морского и внутреннего водного транспорта, включая вопросы безопасности судоходства, эксплуатации инфраструктуры, навигации, связи и управления перевозочным процессом. Вместе с тем правовое регулирование отношений, связанных с критической информационной инфраструктурой, конкретизируется в специальных нормативных актах:

1. Федеральный закон от 26.07.2017 № 187-ФЗ – устанавливает правовые и организационные основы обеспечения безопасности КИИ [3];
2. Постановлении Правительства РФ от 08.02.2018 № 127 – определяет правила категорирования объектов КИИ и критерии их значимости [4].

В совокупности указанные акты формируют специальный режим правовой защиты цифровых и технологических систем, функционирующих в транспортной сфере, и обеспечивают переход от общих отраслевых предписаний к детализированному регулированию безопасности объектов КИИ.

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» определяет критическую информационную инфраструктуру как совокупность информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, функционирование которых имеет существенное значение для обеспечения устойчивости и безопасности значимых объектов. В сфере водного транспорта к таким объектам относятся:

1. Системы управления движением судов;
2. Информационные комплексы, обеспечивающие портовую деятельность и обработку грузов;
3. Средства навигации;
4. Средства связи и обмена данными;
5. Системы управления инфраструктурой портов, шлюзов, причалов и терминалов;
6. Решения, используемые для бронирования, оформления перевозок, учета грузов и пассажиров, а также для обеспечения безопасности перевозочного процесса и оперативного реагирования на инциденты.

Перечень типовых объектов критической информационной инфраструктуры, функционирующих в сфере морского и речного транспорта, включает установлен Постановление Правительства РФ от 08.02.2018 № 127 следующие объекты:

1. Информационные системы, предназначенные для контроля деятельности морского пассажирского транспорта.

2. Автоматизированные системы, предназначенные для управления деятельностью по навигационному обеспечению судоходства на морском и внутреннем водном транспорте.

3. Система управления инженерными системами вокзального комплекса.

4. Автоматизированные системы, обеспечивающие управление ледокольными судами [5].

Таким образом, правовой режим КИИ охватывает ключевые цифровые и технологические элементы транспортной системы, от надежности которых напрямую зависит бесперебойность и безопасность функционирования водного транспорта.

Одной из основных проблем при обеспечении безопасности объектов КИИ на водном транспорте является использование зарубежного программного обеспечения, поскольку навигационные комплексы, системы диспетчерского управления, портовые информационные платформы и средства мониторинга нередко зависят от иностранных программ или их компонентов. Так как хозяйствующий субъект КИИ не всегда обладает полномочиями контроля за механизмом обновлений, то затрудняется оценка уязвимостей и последствий инцидента. Если поставщик прекращает техническую поддержку или вводит ограничения на обновления, то сбой в такой системе способен остановить перевалку грузов, нарушить логистику и создать основания для отнесения объекта к значимой категории. Аналогично, если навигационно-информационная система на судне или в диспетчерском центре функционирует на зарубежной платформе, риск нарушения безопасного судоходства существенно возрастает. Таким образом, устойчивость объекта обеспечивается продуктом, поставки и поддержка которого могут быть прекращены по внешним причинам, что осложняет выполнение требований по импортозамещению, предотвращению аварий и локализации мер защиты.

Неоднозначность в определении отнесения систем и процессов на водном транспорте к объектам, требующим повышенное внимание к обеспечению безопасности, является одним и ключевых вопросов. Не всегда очевидно, относится ли конкретная информационная система к объекту КИИ, либо является частью технологического процесса, в том числе актуален вопрос соотношения с объектами транспортной безопасности с целью разграничения вспомогательных и основных функций. Не каждая система автоматически является объектом КИИ, но может иметь его признаки. Так, система электронного документооборота порта может восприниматься как элемент администрирующего сервиса, однако если через неё проходит оформление разрешений на заход судов, выпуск грузов и координация операций с опасными грузами, её отказ способен прервать деятельность всего объекта. В такой ситуации требуется идентификация системы – проверка оснований для ее включения в перечень объектов КИИ.

Перегруженность законодательной базы не позволяет обеспечить единый подход для правоприменения мер по обеспечению безопасности объектов КИИ на водном транспорте, поскольку хозяйствующим субъектам и контрольно-надзорным органам необходимо одновременно ориентироваться на нормы о КИИ, транспортной безопасности, информационной безопасности, техническом регулировании, отраслевые правила водного транспорта и многочисленные подзаконные акты. Например, порт обязан выполнять требования по транспортной безопасности и безопасности КИИ, поэтому одна система контроля доступа подпадает под несколько режимов. Так как отсутствует единый подход к тому, какие меры должны применяться в первую очередь, какова очередь оформления

документов, возникает пересечение и дублирование проверок, что создаёт риск формального исполнения и разнообразного толкования норм.

Кроме того, процедура выявления и категорирования объектов КИИ нередко воспринимается как чрезмерно сложная, формализованная и ресурсоёмкая, поскольку необходимо провести анализ процессов, определить перечень объектов, создать комиссию, собрать сведения, оценить возможные последствия инцидента и документально обосновать принятое решение. Для крупных транспортных организаций требуются значительные кадровые, технические и временные затраты, где ошибки в документации или в оценке критериев могут повлечь дополнительные проверки со стороны надзорных органов. В связи с этим, организации зачастую стремятся формально исполнить требования, не вникая в сущность процессов, что снижает качество категорирования и повышает риск необоснованного отнесения объекта к высокой категории, либо, наоборот, его недооценки.

В целях улучшения системы обеспечения безопасности объектов КИИ на водном транспорте целесообразно предложить следующие решения:

1. Планомерный переход с иностранных программных решений на российские разработки. Предлагается целесообразным проведение по итогам предварительного анализа и классификации ИТ-объектов с формированием реестра критически значимых компонентов. В этих целях следует провести инвентаризацию используемого программного обеспечения, оценить его значение для критических процессов и классифицировать системы по уровню значимости и устойчивости к прекращению зарубежных обновлений. Перевод портовой системы учёта грузов на отечественную платформу позволит исключить зависимость от иностранных поставщиков, снизить риск отказа в условиях внешних ограничений и обеспечить непрерывность логистических операций.

2. Унификация подходов и внедрение цифровых инструментов. Необходимо разработать единую методику оценки и применения электронных форм документов с конкретизированным перечнем сведений для контроля, что позволит сократить сроки категорирования и минимизировать ошибки, связанные с человеческим фактором. Применение единой электронной формы оценки обеспечит формирование согласованного перечня объектов КИИ без дублирования проверочных мероприятий. Представляется целесообразным внести изменения в ФЗ № 187 посредством формирования общей нормы для цифрового и унифицированного категорирования, однако конкретный порядок, форму и перечень сведений оставить в виде подзаконного акта. Авторами статьи предлагается ст. 7 ФЗ № 187 после положения о порядке категорирования объектов критической информационной инфраструктуры дополнить новой частью следующего содержания:

«Категорирование объектов критической информационной инфраструктуры может осуществляться с применением электронных форм документов и автоматизированной обработки сведений. Единые методические подходы, состав сведений, порядок их представления, проверки и актуализации устанавливаются уполномоченным федеральным органом исполнительной власти. При осуществлении категорирования не допускается дублирование сведений и проверок, ранее проведенных в отношении таких объектов, если иное не предусмотрено федеральным законом».

Введение данной нормы будет способствовать структурированию электронного формата категорирования объектов критической информационной инфраструктуры и закреплению возможности автоматизированной обработки сведений в рамках соответствующей процедуры. Исключение дублирования сведений и повторных проверок позволит повысить эффективность правоприменения и ускорит процесс согласованности действий федерального и подзаконного уровней нормативного регулирования.

3. Разработка единого реестра для проверки объектов КИИ, включающего разделы о критериях отнесения, требования по транспортной безопасности, правила эксплуатации ИТ-инфраструктуры и порядок межведомственного взаимодействия. Представляется обоснованным дополнение Федерального закона № 187-ФЗ самостоятельной нормой, закрепляющей правовые основы единого информационного обеспечения категорирования объектов критической информационной инфраструктуры. Например, внести изменения следующим образом:

«Статья 7.1. Единое информационное обеспечение категорирования объектов критической информационной инфраструктуры».

1. В целях обеспечения категорирования объектов критической информационной инфраструктуры, повышения согласованности правоприменения и исключения дублирования контрольных процедур допускается ведение единого электронного реестра сведений об объектах критической информационной инфраструктуры.

2. Единый электронный реестр формируется на основе сведений, представляемых субъектами критической информационной инфраструктуры, а также данных, получаемых в порядке межведомственного информационного взаимодействия.

3. Использование сведений, содержащихся в едином электронном реестре, осуществляется для целей категорирования объектов критической информационной инфраструктуры, а также разграничения требований, применяемых к таким объектам, и требований, установленных иными федеральными законами в смежных сферах регулирования.

4. Порядок формирования, ведения, актуализации и использования единого электронного реестра, состав включаемых в него сведений, а также порядок межведомственного информационного взаимодействия устанавливаются Правительством Российской Федерации.»

Введение такой статьи позволит закрепить электронный реестр как инструмент межведомственной координации, обеспечить унификацию сведений, используемых при принятии решений о категорировании, а также исключить повторное и избыточное истребование идентичных данных в рамках контрольно-надзорных мероприятий. Закрепление единого электронного реестра на уровне федерального закона позволит создать нормативную основу для межведомственного обмена данными, обеспечить сопоставимость и актуальность сведений, а также повысить эффективность принятия решений в сфере категорирования. Тем самым будет достигнут не только организационный, но и правовой эффект, выражающийся в оптимизации контрольных механизмов, снижении административных издержек и повышении согласованности правоприменительной практики.

Таким образом, вопросы обеспечения безопасности критической информационной инфраструктуры исследуются либо в общем виде, либо применительно к отдельным отраслям, тогда как специфика категорирования объектов КИИ в сфере водного транспорта раскрыта поверхностно. В связи с отсутствием необходимых мер требуется комплексный подход, сочетающий правовые, организационные и технологические меры с учётом особенностей водного транспорта.

Список литературы:

1. «Кодекс внутреннего водного транспорта Российской Федерации» от 07.03.2001 N 24-ФЗ (ред. от 31.07.2025). – URL: www.pravo.gov.ru (дата обращения: 16.03.2026).

2. «Кодекс торгового мореплавания Российской Федерации» от 30.04.1999 N 81-ФЗ (ред. от 31.07.2025). – URL: www.pravo.gov.ru (дата обращения: 16.03.2026).

3. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ (ред. от 07.04.2025). – URL: www.pravo.gov.ru (дата обращения: 17.03.2026).

4. Постановление Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (ред. от 07.11.2025). – URL: www.pravo.gov.ru (дата обращения: 17.03.2026).

5. Баранов Л. А., Иванова Н. Д., Михалевич И. Ф. Цифровой испытательный стенд анализа безопасности объектов критической информационной инфраструктуры интеллектуальных систем водного транспорта // Журнал: Надежность. 2025. Т. 25, № 3. С. 50-59. ISSN: 1729-2646 eLIBRARY.RU. – URL: https://elibrary.ru/item.asp?id=82833256 (дата обращения: 20.03.2026).

6. Раткин Л.С. Особенности обеспечения безопасности критической информационной инфраструктуры // Журнал: Алгоритм безопасности. 2018. № 5. С. 56-59. eLIBRARY.RU. – URL: https://elibrary.ru/item.asp?id=37172372 (дата обращения: 20.03.2026).