Кристина В. Наташова[1], Сергей С. Соколов[2], Олег Н. Губернаторов[3],
Анатолий П. Ныркова[4], Антон В. Кириков[5]
[1-5]Государственный университет морского и речного флота имени адмирала С.О. Макарова, ул. Двинская, 5/7, Санкт-Петербург, 198035, Россия
[1]e-mail: natashov1397@mail.ru, https://orcid.org/0000-0003-4322-3223
[2]e-mail: sssokolov@mail.ru, https://orcid.org/0000-0002-4581-2518
[3]e-mail: ovel82@mail.ru, https://orcid.org/0000-0002-4581-2518
[4]e-mail: nyrkowap@gumrf.ru, https://orcid.org/0000-0002-9803-6284
[5]e-mail: tony-68@yandex.ru, https://orcid.org/0000-0002-2556-0915

К ВОПРОСУ О КАТЕГОРИРОВАНИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ МОРСКИХ ПОРТОВ

DOI: http://dx.doi.org/10.26583/bit.2020.1.03

Аннотация. Целью статьи является рассмотрение проблемных вопросов, возникающих при проведении категорирования объектов критической информационной инфраструктуры (КИИ). Морские порты имеют стратегическое значение для развития экономики Российской Федерации и транспортного обеспечения внешней торговли. Морские порты в соответствии с Федеральным законом №187-ФЗ от 26 июля 2017 года «О безопасности критической информационной инфраструктуры Российской Федерации» являются субъектами КИИ в сфере транспорта. Выполнение требований указанного закона, в частности решение вопросов по категорированию объектов КИИ в соответствии с Постановлением Правительства РФ от 8 февраля 2018 года № 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», требует тщательной проработки и оценки, по причине того, что субъекты КИИ все чаще сталкиваются с многогранностью процессов и необходимостью учета специфики той или иной сферы их деятельности. В данной статье рассмотрен субъект КИИ «Калининградский морской торговый порт» и проведено категорирование одной из информационных систем как авторские рекомендации по исполнению Постановления Правительства Российской Федерации №127 от 8 февраля 2018 года для информационных систем морских портов. В заключении авторы отмечают важность разработки отраслевых регламентов по категорированию и обеспечению защищенности КИИ, важность разработки типовых моделей нарушителей, которые бы учитывали отраслевые особенности, и необходимость привлечения к работе комиссии узконаправленных специалистов, как из состава организации, так и сторонних.

Ключевые слова: информационная безопасность, критическая информационная инфраструктура, категорирование, водный транспорт, морской порт.

Для цитирования: НАТАШОВА, Кристина В. et al. К ВОПРОСУ О КАТЕГОРИРОВАНИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ МОРСКИХ ПОРТОВ. Безопасность информационных технологий, [S.l.], v. 27, n. 2, p. 35-46, 2020. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1269>. Дата доступа: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.03.

Kristina V. Natashova[1], Sergey S. Sokolov[2], Oleg N. Gubernatorov[3],
Anatoliy P. Nyrkov[4], Anton V. Kirikov[5]
[1–5]Admiral Makarov State University of Maritime and Inland Shipping, Dvinskaya Str., 5/7, St. Petersburg, 198035, Russia
[1]e-mail: natashov1397@mail.ru, https://orcid.org/0000-0003-4322-3223
[2]e-mail: sssokolov@mail.ru, https://orcid.org/0000-0002-4581-2518
[3]e-mail: ovel82@mail.ru, https://orcid.org/0000-0002-4581-2518
[4]e-mail: nyrkowap@gumrf.ru, https://orcid.org/0000-0002-9803-6284
[5]e-mail: tony-68@yandex.ru, https://orcid.org/0000-0002-2556-0915

On the issue of categorization of objects of critical information infrastructure of seaports

DOI: http://dx.doi.org/10.26583/bit.2020.1.03

Abstract. The purpose of the article is to consider the problematic issues that arise during the categorization of CII objects. Seaports are of strategic importance for the development of the Russian Federation's economy and transport support for foreign trade. In accordance with Federal law No. 187-FZ of July 26, 2017 "on security of critical information infrastructure of the Russian Federation", seaports are subjects of CII in the field of transport. Compliance with the requirements of this law, in particular, addressing issues related to the categorization of CII objects in accordance with Russian Government Resolution No. 127 of February 8, 2018 "on approval of the rules for categorizing critical information infrastructure objects of the Russian Federation, as well as the list of indicators of the criteria for the significance of critical information infrastructure objects of the Russian Federation and their values", requires careful study and evaluation, because, that CI subjects are increasingly faced with the complexity of processes and the need to take into account the specifics of a particular area of their activities.

This article considers the subject of the Kaliningrad commercial sea port CII and categorizes one of the information systems as the author's recommendations for the implementation of the Decree of the Government of the Russian Federation No. 127 of February 8, 2018 for information systems of seaports. In conclusion, the authors note the importance of developing industry regulations for categorizing and ensuring the security of CII, the importance of developing standard models of violators that would take into account industry characteristics, and the need to attract narrowly focused specialists to the work of the Commission, both from the organization and from outside.

Keywords: information security, critical information infrastructure, categorization, water transport, seaport.

For citation: NATASHOVA, Kristina V. et al. On the issue of categorization of objects of critical information infrastructure of seaports. IT Security (Russia), [S.l.], v. 27, n. 2, p. 35-46, 2020. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1269>. Date accessed: 27 may 2020. doi:http://dx.doi.org/10.26583/bit.2020.2.03.

Введение

Сегодня морское портовое хозяйство почти невозможно представить без комплекса информационных систем и технологий, обеспечивающих его успешное функционирование. Процесс автоматизации информационных процессов водного транспорта продолжается, поэтому вопросы обеспечения информационной безопасности, как никогда актуальны [1].

Поскольку морской порт – это важный транспортный узел, обеспечивающий международные связи, необходимо организационно-правовое сопровождение решения вопросов по выполнению требований по обеспечению безопасности [2]. Одним из таких в части категорирования объектов КИИ, функционирующих в сфере транспорта является Приказ Министерства транспорта РФ от 14 декабря 2018 года № 449 «О создании Комиссии Министерства транспорта Российской Федерации по согласованию перечней объектов критической информационной инфраструктуры подведомственных Минтрансу России службы, агентств, предприятий, учреждений и организаций», изданный в рамках обеспечения реализации требований Федерального закона от 26 июля 2017 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Морские порты имеют важное значение в международной торговле и экономике России. Согласно Федеральному закону №187-ФЗ информационные системы и сети, автоматизированные системы управления морского порта могут быть отнесены к объектам КИИ. В ходе реализации требований Федерального закона №187-ФЗ обозначился ряд проблемных вопросов, которые будут рассмотрены в данной статье.

1. Морской порт как субъект критической информационной инфраструктуры

Субъектами критической информационной инфраструктуры являются «государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы (ИС), информационно-телекоммуникационные сети (ИТКС), автоматизированные системы управления (АСУ), функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей». При этом различают два вида субъектов КИИ: владельцы объектов КИИ и организации, обеспечивающие взаимодействие объектов КИИ.

Для проведения категорирования решением руководителя субъекта КИИ создается постоянно действующая комиссия по категорированию.

При определении принадлежности организации к понятию «Субъект КИИ» следует оценивать не принадлежность ИС, ИТКС и АСУ к перечисленным сферам, а виды деятельности организации.

Основные и вспомогательные виды деятельности организации отражены в учредительных документах организации (Устав) и лицензиях, сертификатах, и иных разрешительных документах на эти виды деятельности [3].

Согласно Общероссийскому классификатору видов экономической деятельности (ОКВЭД) к сфере транспорта могут относиться виды деятельности под классами 49, 50, 51, 52, 53. Морским портам характерны виды деятельность классов:

49. Деятельность сухопутного и трубопроводного транспорта;
50. Деятельность водного транспорта;
52. Складское хозяйство и вспомогательная транспортная деятельность.

2. Категорирование объектов критической информационной инфраструктуры морского порта

Первым шагом категорирования объектов КИИ является создание постоянно действующей комиссии по категорированию приказом руководителя морского порта, в которую должны входить:

а) Руководитель морского порта;

б) Руководитель критичных направлений деятельности, процессы которых автоматизируются одной из систем;

в) Руководитель подразделения информационных технологий;

г) В случае наличия – руководитель автоматизации;

д) Ответственный за промышленную безопасность;

е) В случае наличия – ответственный за контроль за опасными веществами и материалами;

ж) Руководитель подразделения защиты информации либо администратор информационной безопасности;

з) В случае наличия – руководитель подразделения по защите государственной тайны;

и) В случае наличия – руководитель отдела по гражданской обороне и чрезвычайным ситуациям;

к) Иные работники по решению Руководителя морского порта;

л) По согласованию с Федеральным органом или юридическим лицом, который определяет политику, нормативно-правовое регулирование в установленной сфере деятельности, могут быть включены представители данного юридического лица. Если субъект осуществляет деятельность водного транспорта, то по согласованию с Министерством транспорта РФ и (или) Федеральным агентством морского и речного транспорта, их представители могут быть включены в комиссию субъекта.

Следующие действия выполняет сформированная комиссия по категорированию. У комиссии нет ограничений по привлечению других работников.

Второй шаг категорирования – формирование перечня критических процессов. Критическими процессами морского порта являются управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности Субъекта КИИ в сфере транспорта.

Для определения критических процессов необходимо вновь обратиться к учредительным и разрешительным документам для выписки выполняемых организацией функций и видов деятельности [4]. Для каждой функции/вида деятельности формируется перечень процессов. После чего можно использовать перечень критериев значимости из Постановления Правительства РФ от 8 февраля 2018 года №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» для определения критичности процесса, т.е. повлечет ли нарушение процесса последствия, соответствующие этим критериям значимости.

Третьим шагом является определение объектов КИИ, обеспечивающих выполнение критических процессов, выделенных на предшествовавшем этапе. Для каждого критического процесса необходимо определить системы, осуществляющие обработку, управление, контроль или мониторинг этого процесса. Результатом данного шага является формирование перечня объектов КИИ, подлежащих категорированию, который согласовывается с Комиссией Министерства транспорта РФ [п. 15 Постановление Правительства РФ №127], после чего отправляется в ФСТЭК России согласно рекомендуемой форме [Информационное сообщение ФСТЭК России от 24.08.2018 №240/25/3752] в течение 10 дней со дня утверждения перечня [п. 15 Постановление Правительства РФ №127]. Согласно Постановлению Правительства РФ от 13 апреля 2019 года №452 «О внесении изменений в Постановление Правительства Российской Федерации от 8 февраля 2018 года №127» государственные органы и государственные учреждения были обязаны до 1 сентября 2019 года утвердить перечни объектов КИИ. Что касается российских юридических лиц данный срок несет рекомендательный характер. Со дня утверждения перечня объектов КИИ устанавливается максимальный срок не более 1 года со дня утверждения перечня для последующего категорирования этих объектов, т.е. не позднее 1 сентября 2020 года в случае соблюдения указанных выше сроков по представлению перечней объектов КИИ [п. 15 Постановление Правительства РФ №127].

На *четвертом шаге* осуществляется анализ уязвимостей и актуальных угроз безопасности. Для составления перечня уязвимостей исходными данными являются сведения о программном обеспечении, аппаратных платформах, операционных системах, используемых на рассматриваемых объектах.

Анализ угроз необходим для последующей оценки возможного ущерба при компьютерных инцидентах. Можно использовать уже существующие модели угроз безопасности информации, если они разрабатывались ранее для рассматриваемого объекта.

В отсутствии разработанных моделей угроз для получения исходных данных по угрозам безопасности информации рекомендуется использование банка данных угроз безопасности информации ФСТЭК России [4].

Данный этап включает в себя оценку возможного ущерба при возникновении компьютерного инцидента на объекте КИИ. Необходимо ориентироваться на последствия, которые соответствуют показателям значимости из Правил категорирования. В соответствии с оцененным ущербом присваивается категория значимости по данному показателю.

Пятый шаг – это присвоение категории значимости, которая является наивысшей из определенных на предшествовавшем шаге. Этот шаг оформляется актом категорирования, в котором перечислены сведения о самом объекте КИИ, присвоенной категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Акт подписывается комиссией и в течение 10 дней со дня его утверждения в ФСТЭК России представляются Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий по утвержденной форме в соответствии с Приказом ФСТЭК России № 236 от 22 декабря 2017 года.

3. Практический пример категорирования

В качестве примера субъекта КИИ рассмотрим Калининградский морской торговый порт (ОАО «КМТП»).

Основным видом деятельности ОАО «КМТП» по коду ОКВЭД является транспортная обработка грузов (код 52.24), что в соответствии с пунктом 8 статьи 2 Федерального закона № 187-ФЗ означает, что морской порт функционирует в сфере транспорта. Кроме данного способа определения принадлежности к субъектам КИИ можно обратиться к разрешительным и учредительным документам организации. Так в Уставе Калининградского морского порта в разделе 3 пункте 4 перечислены основные виды деятельности. Также стоит ответить на вопрос, есть ли у организации системы, автоматизирующие эти виды деятельности. Так, транспортно-экспедиторское обслуживание и складские операции автоматизированы системами управления грузовым и контейнерным терминалами [5]. Таким образом, можно принять решение о признании ОАО «КМТП» субъектом КИИ.

Первый шаг. Создается комиссия по категорированию.

Второй шаг. Для формирования перечня процессов Калининградского морского торгового порта выпишем основные виды деятельности:

а) Погрузо-разгрузочные работы (стивидорная деятельность);

б) Шипчандлерское обслуживание (снабжение) судов, прибывающих в порт;

в) Транспортно-экспедиторское обслуживание и складские операции;

г) Перевозки грузов, багажа, почты, на судах порта, а также другими видами транспорта;

д) Агентское обслуживание судов;

е) Перевозочная и транспортно-экспедиционная деятельность;

ж) Осуществление швартования морских судов в морских портах;

з) Учреждение склада временного хранения[1]. [6]

[1] Устав Акционерного Общества «Морской торговый порт»
URL: http://www.kscport.ru/index.php/ru/aktsioneram/ustav-oao-kmtp/

Далее для каждого осуществляемого вида деятельности сформируем перечень процессов, реализуемых в рамках этого вида деятельности для получения полного перечня процессов Калининградского морского торгового порта.

Для каждого процесса из перечня определим критичность его нарушения (табл. 1).

Таблица 1. Выделение критических процессов

№ п/п	Наименование	Негативные последствия				
		Социальная значимость	**Политическая значимость**	**Экономическая значимость**	**Экологическая значимость**	**Значимость для обеспечения обороны страны, безопасности государства и правопорядка**
1.	Бухгалтерский и налоговый учет	-	-	-	-	-
2.	Кадровый учет и расчет заработной платы	-	-	-	-	-
3.	Оперативный учет с планированием поставок, отгрузок и внутрипортовых операций	+	-	+	-	-
4.	Планирование и учет погрузочно-разгрузочных работ	+	-	+	-	-
5.	Подготовка и оформление документации на размещение и отгрузку груза	+	-	+	-	-
6.	Получение информации по переработанным грузам и контейнерам	-	-	-	-	-
7.	Получение отчетов	-	-	-	-	-
8.	Погрузка и выгрузка судов	+	-	+	-	-

№ п/п	Наименование	Негативные последствия				
		Социальная значимость	**Политическая значимость**	**Экономическая значимость**	**Экологическая значимость**	**Значимость для обеспечения обороны страны, безопасности государства и правопорядка**
9.	Тарификация и биллинг услуг	+	-	+	-	-
10.	Учет и адресное хранение грузов	-	-	-	-	-
11.	Учет и адресное хранение контейнеров	-	-	-	-	-
12.	Электронный обмен с клиентами	-	-	-	-	-

Таким образом, критическими процессами порта являются:

- Оперативный учет с планированием поставок, отгрузок и внутрипортовых операций;
- Планирование и учет погрузочно-разгрузочных работ;
- Подготовка и оформление документации на размещение и отгрузку груза;
- Погрузка и выгрузка судов;
- Тарификация и биллинг услуг.

Третий шаг. Для определения объектов КИИ необходимо провести инвентаризацию информационных, программных и технических ресурсов [7] и отобрать те, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов:

1. Информационные системы:
   1.1. Береговые информационные системы;
   1.2. Бортовые информационные системы;
   1.3. Электрокартографические системы;
   1.4. Портовые технологические системы.
2. Информационно-телекоммуникационные сети;
3. Автоматизированные системы управления[2].

Для обеспечения критических процессов необходимую информацию обрабатывает: автоматизированная система управления грузовым терминалом ОАО «Калининградский морской торговый порт» (АСУ ГТ КМТП). На основе этих данных формируется перечень объектов КИИ [8].

Четвертый шаг. Рассмотрим возможные действия нарушителей и угрозы безопасности информации в отношении АСУ ГТ КМТП [5] (Табл. 2).

[2] Отчёты// ОАО «КМТП» URL: http://www.scport.ru/index.php/ru/aktsioneram/otchety

Таблица 2. Возможные действия нарушителей и угрозы безопасности информации

1.	Категория нарушителя, краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	1. Внешний нарушитель со средним потенциалом, обладающий следующими возможностями: − Информация о системе из общедоступных источников; − Общедоступная информация об уязвимостях отдельных компонент ИС. Данный тип нарушителя может использовать следующие каналы реализации угроз: − Общедоступные каналы передачи данных, имеющие подключение к ИС; − Реализация атак посредством направленных воздействий на работников организации (социальная инженерия). 2. Внутренний нарушитель со средним потенциалом, обладающий следующими возможностями: − Осведомленность о мерах защиты информации, применяемых в ИС; − Осведомленность о структурно-функциональных характеристиках и особенностях функционирования ИС Данный тип нарушителя может использовать следующие каналы реализации угроз: − Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический); − Использование штатных средств доступа к ИС.
2.	Основные угрозы безопасности информации или обоснование их неактуальности	− Угроза внедрения вредоносного ПО; − Угроза несанкционированного доступа с использованием компрометированных/подобранных данных идентификации и аутентификации пользователей и администраторов; − Угроза реализации направленных атак на пользователей (фишинг и иные методы социальной инженерии); [9] − Угроза доступа к информации в обход или с использованием ошибок в настройке средств разграничения доступа; − Угроза несанкционированного удаления данных, обрабатываемых в системе; − Угроза нарушения работоспособности системного ПО; − Угроза нарушения работоспособности прикладного ПО; − Угроза проведения атак типа «отказ в обслуживании» на каналы связи; [10] − Угроза проведения атак типа «отказ в обслуживании» на компоненты системы; − Угроза использования недекларированных возможностей/закладок прикладного ПО; − Угроза использования недекларированных возможностей/закладок системного ПО; − Угроза несанкционированного доступа к конфигурации системы/раскрытия данных технологического процесса; − Угроза создания нештатных режимов работы; − Угроза блокирования передаваемых управляющих команд; − Угроза несанкционированного удаления конфигурационных файлов.

Пятый шаг. На основании показателей критериев значимости осуществим категорирование объекта КИИ (табл. 3).

Таблица 3. Категорирование объекта КИИ

1.	Категория значимости объекта	III категория
2.	Полученные значения по каждому из рассчитываемых показателей критериев значимости или информация о неприменимости показателя к объекту	Далее номер – это порядковый номер Показателя. **1.** ***Показатель к объекту КИИ не применим*****;** **2.** ***Показатель к объекту КИИ не применим*****;** **3.** ***а) в пределах одной внутригородской территории города федерального значения. Данное значение дает основу для присвоения III категории объекту по данному показателю. б) показатель к объекту КИИ не применим;*** **4-7.** ***Показатель к объекту КИИ не применим*****;** **8.** ***0,06% от годового объема доходов, усредненного за прошедший 5-летний период. Данного значения недостаточно для присвоения категории по данному показателю;*** **9.** ***0,00000006% прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период. Данного значения недостаточно для присвоения категории по данному показателю;*** **10.** ***Показатель к объекту КИИ не применим*****;** **11.** ***а) в пределах одной внутригородской территории города федерального значения. Данное значение дает основу для присвоения III категории объекту по данному показателю. б) до 300 чел. Значения недостаточно для присвоения категории по данному показателю;*** **12-14.** ***Показатель к объекту КИИ не применим*** **[11]**
3.	Обоснование полученных значений по каждому из показателей критериев значимости или обоснование неприменимости показателя к объекту	1. ***Объект КИИ не управляет процессами, связанными с причинением ущерба жизни и здоровью людей.*** 2. ***Нарушение функционирования объекта КИИ не оказывает влияние на нарушение функционирования объектов обеспечения жизнедеятельности населения, так как объект КИИ не участвует в каких-либо процессах обеспечения жизнедеятельности населения.*** 3. ***а) В пределах одной внутригородской территории города федерального значения; б) Нарушение функционирования объекта КИИ не оказывает влияние на недоступность предоставление транспортных услуг пассажирам.*** 4. ***Объект КИИ не обеспечивает функционирование сетей электросвязи.*** 5. ***Объект КИИ единолично не обеспечивает доступ к государственной услуге.*** 6. ***Объект КИИ не обеспечивает функционирование государственных органов*** 7. ***Объект КИИ не обеспечивает соблюдение условий международного договора, заключенного Российской Федерацией с иностранным государством либо с международной организацией.*** 8. ***0,06% от годового объема доходов, усредненного за прошедший 5-летний период. Данного значения недостаточно для присвоения категории по данному показателю;*** 9. ***0,00000006% прогнозируемого годового дохода федерального бюджета, усредненного за планируемый 3-летний период.***

		Данного значения недостаточно для присвоения категории по данному показателю; 10. ***Объект КИИ не обеспечивает поведение банковских операций.*** 11. ***а) В пределах одной внутригородской территории города федерального значения; б) вредным воздействиям в случае нарушения функционирования могут подвержены до 300 человек. Данного значения недостаточно для присвоения категории.*** *12.* ***Нарушение функционирования объекта не может привести к прекращению или нарушению функционирования пункта управления (ситуационного центра), так как объект не участвует в управлении или мониторинге процессов пунктов управления (ситуационных центров).*** *13.* ***Нарушение функционирования объекта не может привести к снижению показателей государственного оборонного заказа, так как объект не з в процессах реализации, управления или контроля данных процессов.*** *14.* ***Нарушение функционирования объекта не может привести к прекращению или нарушению функционирования информационной системе в области обеспечения обороны страны, безопасности государства и правопорядка, так как объект не задействован в процессах реализации, управления и контроля данных процессов.***

Для расчета показателей экономической значимости объектов КИИ (8 и 9 показатель) необходимо участие специалистов финансово-экономического отдела, поскольку у комиссии по категорированию могут возникнуть трудности в связи с недостатком сведений и профессиональной специфики вопроса.

Заключение

В данной статье были рассмотрены проблемные вопросы, возникающие при проведении категорирования объектов КИИ. Новое законодательство определило новые меры и средства обеспечения защищенности наиболее важных объектов. Однако, при категорировании, субъекты все чаще сталкиваются с многогранностью процессов и необходимостью учета специфики транспортной отрасли. Субъекты КИИ в ходе категорирования сталкиваются с необходимостью привлечения специалистов, не входящих в комиссию по категорированию как внутри Организации (как расчет 8 и 9 экономического показателя), так и сторонних (услуги аутсорсинга по обеспечению защиты значимых объектов КИИ: как категорирование, так и проектирование систем защиты). Категорирование КИИ – это лишь первый этап. Далее следует проектирование подсистемы безопасности значимого объекта и разработка рабочей документации на значимый объект.

В соответствии с законодательством, ответственность за результаты категорирования объектов КИИ несет непосредственно субъект КИИ. Это определяет важность разработки отраслевых регламентов по категорированию и обеспечению защищенности КИИ, важность разработки типовых моделей нарушителей, которые бы учитывали, например, такие отраслевые особенности как трансграничное взаимодействие с иностранными контрагентами. Обеспечение информационной безопасности – это процесс и его нельзя завершать, им необходимо централизованно управлять на всех уровнях, начиная с создания федеральных центров отраслевых компетенций в области информационной защищенности ключевых активов. Это ставит новые задачи и определяет перспективы развития направления обеспечения безопасности КИИ, в том числе на водном транспорте.

СПИСОК ЛИТЕРАТУРЫ:

1. Sokolov, S., Glebov, N., Natashova, K., Gubernatorov, O. Categorization of objects of critical information infrastructure of water transport // E3S Web of Conferences Volume 110, 9 August 2019. DOI: 10.1051/e3sconf/201911002003.
2. Соколов С.С., Ныркoв 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.
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://science-education.ru/ru/article/view?id=18583 (дата обращения: 23.10.2020).
4. Ныркoв 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)». Санкт-Петербург, 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.
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. Vol. 150. P. 609–615 (2019).
11. Наташова К.В., Об основных темах для обсуждения и итогах 11-й межссесионной 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.

REFERENCES:

[1] Sokolov, S., Glebov, N., Natashova, K., Gubernatorov, O. Categorization of objects of critical information infrastructure of water transport. E3S Web of Conferences Volume 110, 9 August 2019. DOI: 10.1051/e3sconf/201911002003.
[2] S.S. Sokolov, A.P. Nyrkov, N.B. Glebov. Cybersecurity on water transport. CONFERENCE ABSTRACTS. National scientific and practical conference of teaching staff Admiral Makarov State University of Maritime and Inland Shipping. 2018.
[3] Data Bank of threats to information security of FSTEC of Russia. URL: https://bdu.fstec.ru (accessed: 16.10.2019) (in Russian).
[4] S.S. Sokolov. Methods and models for ensuring information security of transport infrastructure objects classified as critically important for the national security of the Russian Federation. Modern problems of science and education. 2015. No. 1 (part 1).
[5] A.P. Nyrkov, R.I. Kislov, A.V. Belov. On the issue of categorization of objects of critical information infrastructure of water transport. Proceedings of the XVI St. Petersburg International Conference “Regional Informatics (RI-2018).
[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] Li I.V., Natashova K.V. Problems of ensuring information security of automated systems for water transport. Regional Informatics and Information Security. Proceedings. Vol. 5. SPOISU. SPb., 2018. – 549 p.

[8] Li I.V., Natashova K.V. Legal regulation of information security in marine transport. Proceedings of the XVI St. Petersburg International Conference “Regional Informatics (RI-2018). SPOISU. SPb., 2018. – 631 p.

[9] Natashova K.V., Li I.V. Current status of its and it on water transport. Materials of the IX interuniversity scientific and practical conference of postgraduates, students and cadets “Current trends and prospects for the development of water transport in Russia” May 23, 2018. – 928 p.

[10] Glebov N., Zhilenkov A., Chernyi S., Sokolov S., "Process of the Positioning Complex Modeling Objects with Elements of Intellectual Analysis", Procedia Computer Science, vol. 150. P. 609–615 (2019).

[11] Natashova K.V., On the main topics for discussion and the results of the 11th inter-session meeting of the ASEAN regional forum on Maritime security. Materials of the XI interuniversity scientific and practical conference of postgraduates, students and cadets “Current trends and prospects for the development of water transport in Russia” May 22, 2019.

Поступила в редакцию – 18 января 2020 г. Окончательный вариант – 25 мая 2020 г.
Received – January 18, 2020. The final version – May 25, 2020.