Организация Объединенных Наций ECE/TRANS/SC.3/2021/3

Экономический и Социальный Совет

Distr.: General
28 October 2021
Russian
Original: English, French and Russian

Европейская экономическая комиссия

Комитет по внутреннему транспорту

Рабочая группа по внутреннему водному транспорту

Шестьдесят пятая сессия
Женева, 3–5 ноября 2021 года
Пункт 4 предварительной повестки дня
Рабочее совещание на тему «Кибербезопасность на внутреннем водном транспорте»

Рабочее совещание на тему «Кибербезопасность на внутреннем водном транспорте»

Записка секретариата[*, **]

Мандат

1. Настоящий документ представлен в соответствии с предлагаемым бюджетом по программам на 2021 год, часть V «Региональное сотрудничество в целях развития», раздел 20 «Экономическое развитие в Европе». Программа 17 «Экономическое развитие в Европе» (A/75/6 (разд. 20), п. 20.51).

2. На своей шестьдесят четвертой сессии Рабочая группа по внутреннему водному транспорту (SC.3) решила, что главной темой ее шестьдесят пятой сессии будет кибербезопасность на внутреннем водном транспорте (ECE/TRANS/SC.3/213, пункт 87).

3. В настоящем документе представлен краткий обзор нормативно-правовой базы в области кибербезопасности в морском и внутреннем судоходстве, деятельности Европейской экономической комиссии (ЕЭК) в этой области и предложения для обсуждения на рабочем совещании.

II. Обзор нормативно-правовой базы

4. Кибербезопасность является быстро растущим вызовом в отрасли внутреннего водного транспорта в связи с быстрым развитием цифровизации отрасли, что необходимо для успешного цифрового перехода во внутреннем судоходстве. Кроме того, существует острая необходимость в повышении осведомленности о кибербезопасности, разработке концепций кибербезопасности для обеспечения

[*] Настоящий документ был представлен после истечения установленного срока в связи с необходимостью включения в него самой последней информации.
[**] Настоящий документ выпускается без официального редактирования.

непрерывности обслуживания во внутреннем судоходстве и минимизации рисков, влияющих на надежность цифровой среды внутреннего судоходства. Стратегическая рекомендация № 8 Белой книги по развитию, достижениям и будущему устойчивого внутреннего водного транспорта подчеркивает необходимость развития сотрудничества между ключевыми заинтересованными сторонами на международном уровне и учета опыта и передовой практики других видов транспорта и предлагает конкретные действия для ЕЭК в этой области.

5. Учитывая растущее значение кибербезопасности и потребность в прагматическом и практическом подходе к борьбе с киберугрозами, в этой области на национальном и международном уровнях были приняты регламенты и стандарты, такие как:

- Директива (ЕС) 2016/1148 Европейского Парламента и Совета от 6 июля 2016 г. о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Европейского союза
- Стандарт ISO/IEC 27001 «Системы обеспечения информационной безопасности»
- Принципы кибербезопасности 2018 Национального института стандартов и технологий (NIST) Министерства торговли Соединенных Штатов Америки.

6. В морской отрасли основная нормативно-правовая база для кибербезопасности была заложена ИМО в следующих документах:

- Руководство по управлению киберрисками в морской отрасли (MSC-FAL.1/Circ.3), принятое в 2017 году. В руководстве представлены рекомендации высокого уровня по управлению киберрисками на море для защиты судоходства от текущих и возникающих киберугроз и уязвимостей
- Резолюция MSC.428(98) «Управление киберрисками в морской отрасли в рамках систем управления безопасностью», принятая Комитетом по безопасности на море в 2017 году. Резолюция настоятельно рекомендует администрациям обеспечить надлежащее рассмотрение киберрисков в системах управления безопасностью в соответствии с целями и требованиями Международного кодекса управления безопасностью не позднее первой ежегодной верификации документа о соответствии компании после 1 января 2021 года.

7. Документы ИМО получили дальнейшее развитие и поддержку в ряде руководящих принципов и рекомендаций, таких как:

- Кибербезопасность портов – Передовой опыт кибербезопасности в морской отрасли (ноябрь 2019 года) и Руководство по управлению киберрисками для портов (декабрь 2020 года) Агентства Европейского союза по кибербезопасности (ENISA)
- Руководство по кибербезопасности на борту судов, версия 4 (декабрь 2020 года), опубликованное БИМКО, Американской палатой судоходства, Ассоциацией цифрового контейнерного судоходства, Международной ассоциацией судовладельцев сухогрузных судов (INTERCARGO), InterManager, Международной ассоциацией независимых владельцев танкеров (INTERTANKO), Международной палатой судоходства (ICS), Международным союзом морского страхования (IUMI), Международным морским форумом нефтяных компаний (ОКИМФ), Ассоциацией строителей суперъяхт и Всемирным советом судоходства
- Рекомендации по кибербезопасности для портов и портовых сооружений Международной ассоциации портов и гаваней (МАСПОГ) (сентябрь 2021 года)
- Рекомендация по киберустойчивости (№ 166) Международной ассоциации классификационных обществ (МАКО) (июль 2020 года).

8. В области внутреннего судоходства Всемирная ассоциация инфраструктуры водного транспорта (ПМАКС) выпустила в 2019 году Информационный документ о кибербезопасности во внутреннем судоходстве.

III. Деятельность Европейской экономической комиссии в области кибербезопасности

9. Всемирный форум для согласования правил в отношении транспортных средств (WP.29) принял в июне 2020 года правила ООН о единообразных предписаниях, касающихся официального утверждения транспортных средств в отношении кибербезопасности и системы обеспечения кибербезопасности, которые вступили в силу в январе 2021 года.. Данные правила обеспечивают основу для авто внедрения в автомобильной отрасли необходимых процессов для:

- Выявления и управления рисками кибербезопасности при проектировании транспортных средств.
- Проверки наличия управления рисками, включая тестирование
- Обеспечения актуальности оценок рисков.
- Отслеживания кибератак и эффективного ответа на них
- Поддержки анализа удавшихся атак или них попыток
- Оценки того факта, продолжают ли оставаться эффективными меры кибербезопасности в свете новых угроз и уязвимостей.

10. Рабочая группа по политике в области стандартизации и сотрудничества по вопросам нормативного регулирования (WP.6) в 2017 году одобрила предложение о новой секторальной инициативе по кибербезопасности. Данная секторальная инициатива направлена на содействие сближению национальных технических регламентов в этой области с целью выработки общих рамок на основе подхода, основанного на оценке рисков, и прочего передового международного опыта.

IV. Цель рабочего совещания и вопросы для обсуждения

11. В соответствии со Стратегической рекомендацией № 8 Белой книги по развитию, достижениям и будущему устойчивого внутреннего водного транспорта целью настоящего рабочего совещания является повышение осведомленности о кибербезопасности, достигнутом прогрессе, текущей работе и перспективах в этой области, обмен опытом и освещение передовой практики, достигнутой на других видах транспорта, который может быть полезен для внутреннего водного транспорта.

12. Предлагаемые темы для обсуждения на рабочем совещании:

a) передовая практика и опыт морской отрасли;

b) перспективы для внутреннего водного транспорта;

c) кибербезопасность в автоматизированном и автономном судоходстве;

d) оценка рисков кибербезопасности и меры по смягчению их последствий во внутреннем судоходстве;

e) меры, которые могут быть приняты на международном и национальном уровнях, а также развитие сотрудничества.

13. SC.3, возможно, пожелает обсудить реализацию действий в области кибербезопасности, предложенных в Стратегической рекомендации № 8 Белой книги по развитию, достижениям и будущему устойчивого внутреннего водного транспорта.