Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Я. Тодоров, *Connections QJ* 20, № 3-4 (2021): 63-83
https://doi.org/10.11610/Connections.rus.20.3-4.04

Рецензированная статья

Кибер(без)опасность на море: Растущая угроза странам ЕС

Явор Тодоров

Докторант Военно-морской академии Болгарии, http://www.naval-acad.bg/

Аннотация: Широкое применение передовых информационно-коммуникационных технологий на судах, в портах, в управлении движением и грузами повышает их эффективность, но одновременно создает уязвимости. Разного рода злоумышленники готовы воспользоваться доступом в киберпространстве для получения выгоды. В этой статье мы рассмотрим киберриски и угрозы в морской киберсфере и проанализируем действующие европейские, американские и международные нормы, стандарты и механизмы, направленные на укрепление кибербезопасности. Автор выделяет шесть направлений усилий в области обмена информацией, повышения осведомленности, сертификации и стойкости.

Ключевые слова: безопасность на море, вызовы кибербезопасности, нормы, гармонизация, правовая база, обмен информацией, информированность, обучение, стойкость.

Мир изменился. Я чувствую это в воде, вижу в земле, ощущаю в воздухе. Многое из того, что было – ушло.[1]

Вступление

За последние 10 лет морской сектор существенно вырос. Сейчас это обширная, тесно связанная сеть грузовых судов, нефтетанкеров, химовозов, контейнеровозов, пассажирских судов, страховых компаний, морских и береговых операторов, национальных и международных органов, военных флотов, служб навигации и управления на море, спутниковых систем, систем связи. Сегодня морская сфера прямо влияет на экономическую, политическую и демографическую динамику в мире.

[1] Джон Рональд Руэл Толкин, «Властелин колец: Братство кольца».

Катастрофы на море – не редкость. Ещё в 1912 г. затонул «Титаник», унеся 1 517 жизней. С ростом применения информационно-коммуникационных технологий (ИКТ) в морской сфере вероятность катастроф возрастает в геометрической прогрессии. Эти технологии обеспечивают основные услуги судоходства, такие как навигация, контроль двигателей, контроль доступа, развлечения, связь и управление экипажем. Но компьютеризация увеличивает такие риски, как остановка портов или судов, манипулирование основными услугами, а также массовые разрушения, беспорядки и гибель людей. Эти риски затрагивают всех – частные компании, правительства, отдельных граждан. Как отметила президент и главный исполнительный директор Палаты судоходства США Кэти Меткаф, морская отрасль остается уязвимой к кибератакам, которые могут спровоцировать катастрофические события, например, захват судна и таран моста Верразано-Нэрроуз.[2] Эта опасность подтверждается ростом кибератак в морской сфере на 400 % в 2020 г.[3]

Кибербезопасность на море регулируется многочисленными международными и национальными государственными и частными органами, включая Международную морскую организацию (ММО), Агентство кибербезопасности Европейского Союза (ENISA) и Балтийский и международный морской совет (BIMCO). К сожалению, эти организации не обладают достаточными техническими и кадровыми возможностями для внедрения, сертификации и мониторинга системы кибербезопасности судоходства. Нет у них и адекватной политики и процедур обеспечения соблюдения конкретных требований.

Нынешняя нормативная база не способна минимизировать риски и угрозы, прежде всего из-за разнобоя существующих стандартов кибербезопасности и процедур контроля морского сектора. Международный кодекс управления безопасностью ММО, Указания ММО по управлению морскими киберрисками, соответствующие директивы ЕС и национальные нормы слишком широки, и операторы не могут построить надёжную систему кибербезопасности судоходства.

Ещё одна проблема заключается в отсутствии стандарта протоколов кибербезопасности для судов разных стран. Это связано с количеством судов, работающих в разных условиях под флагами разных стран. Эти суда, как правило, следуют минимальным существующим стандартам, игнорируя требования национальных морских властей.[4]

---

[2] John Grady, "Experts: Maritime Industry Remains Vulnerable to Cyber Attacks," *USNI News*, September 28, 2020, https://news.usni.org/2020/09/28/experts-maritime-industry-remains-vulnerable-to-cyber-attacks.

[3] "Greater Cyber Security Needed for Coronavirus and Economic Crises," *Hellenic Shipping News*, May 6, 2020, https://www.hellenicshippingnews.com/greater-cyber-security-needed-for-coronavirus-and-economic-crises/.

[4] Jeff Spivey, "Security by Design," *United States Cybersecurity Magazine* (Fall 2017), https://www.uscybersecurity.net/csmag/security-by-design/.

Информационная система многих судов построена по принципу «конструктивной кибербезопасности». Согласно этой модели, кибербезопасность корабля планируется с самого начала проектирования и учитывается на каждом этапе строительства. Но этот «конструктивный» подход обеспечивает предупреждение и предотвращение, а не исправление и восстановление после инцидента.[5] Поскольку нынешние векторы атак многомерны, и для проникновения в системы используются самые современные инструменты, эта модель создает значительные риски и проблемы для судоходной отрасли.[6]

Многочисленные поставщики различного оборудования и услуг позволяют каждому подрядчику использовать свои средства защиты, что усложняет гармонизацию. Тот же принцип используется и в общедоступных системах, необходимые для идентификации и определения местонахождения терпящего бедствие судна.[7]

Вероятность срыва судоходства при помощи кибератак высока и чревата катастрофическим ущербом судам и критической инфраструктуре. Важно повышать информированность судовладельцев, экипажей и компетентных органов о морской кибербезопасности. Ниже приведены обоснованные рекомендации по совершенствованию международных правил, политики и принципов международной кибербезопасности на море для решения существующих проблем кибербезопасности.

Нынешнее положение дел на море

Значение портов для экономики Европейского Союза (ЕС) и всего мира возрастает. Это главные перекрёстки мировой торговли – на них приходится примерно три четверти торговли товарами ЕС с третьими странами и больше трети грузоперевозок внутри ЕС.[8]

С 1970 г. мировая морская торговля стабильно растёт как в объёме, так и по размеру судов. Конференция Организации Объединённых Наций по торговле и развитию (ЮНКТАД) ожидает роста объёмов морской торговли на 2,4 % в год до 2030 г. Примерно две трети мировой торговли товарами приходится на развивающиеся страны, что составляет 60 % мировых грузоперевозок. Больша́я часть этого роста пришлась на Восточную Азию, особенно

---

5 Reciprocity, “What is Security by Design?” *Reciprocity*, March 7, 2020, https://reciprocity.com/resources/what-is-security-by-design/.

6 Rory Hopcraft and Keith M. Martin, “Effective Maritime Cybersecurity Regulation – the Case for a Cyber Code,” *Journal of the Indian Ocean Region* 14, no. 3 (2018): 354-366, http://doi.org/10.1080/19480881.2018.1519056.

7 Hopcraft and Martin, “Effective Maritime Cybersecurity Regulation.”

8 Boyan Mednikarov, Yuliyan Tsonev, and Andon Lazarov, “Analysis of Cybersecurity Issues in the Maritime Industry,” *Information & Security: An International Journal* 47, no. 1 (2020): 27-43, https://doi.org/10.11610/isij.4702.

Китай. Так же быстро растут объёмы на Транстихоокеанском торговом пути, связывающем Восточную Азию с Северной Америкой.[9]

Анализ кибербезопасности на море

Прогресс в мореплавании существенно зависит от технических инноваций судовых цифровых систем. Постоянно растёт важность информационных систем, поскольку они обеспечивают связь и принятие решений, повышают видимость, эффективность и надежность, укрепляют безопасность морских перевозок в различных условиях.

Год	Танкеры	Балкеровозы	Другие сухогрузы	Всего (все грузы)
1970	1 440	448	717	2 605
1980	1 871	608	1 225	3 704
1990	1 755	988	1 265	4 008
2000	2 163	1 186	2 635	5 984
2005	2 422	1 579	3 108	7 109
2006	2 698	1 676	3 328	7 702
2007	2 747	1 811	3 478	8 036
2008	2 742	1 911	3 578	8 231
2009	2 641	1 998	3 218	7 857
2010	2 752	2 232	3 423	8 408
2011	2 785	2 364	3 626	8 775
2012	2 840	2 564	3 791	9 195
2013	2 828	2 734	3 951	9 513
2014	2 825	2 964	4 054	9 842
2015	2 932	2 930	4 161	10 023
2016	3 058	3 009	4 228	10 295
2017	3 146	3 151	4 419	10 716
2018	3 201	3 215	4 603	11 019
2019	3 163	3 218	4 690	11 071
2020	2 918	3 181	4 549	10 648

Рис. 1: Международная морская торговля, 1970-2020 гг.[10]

В 2017 г. крупное событие изменило подход правительств и частного сектора к системам кибербезопасности судоходства и портов. В июне хакеры, работавшие на российскую военную службу безопасности, отправили программу-вымогатель *NotPetya* на объекты критической инфраструктуры. Воспользовавшись уязвимостями крупнейшего в мире судоходного конгломе-

[9] United Nations Conference on Trade and Development (UNCTAD), *Review of Maritime Transport 2021* (United Nations, 2021), https://unctad.org/webflyer/review-maritime-transport-2021.

[10] UNCTAD, *Review of Maritime Transport*.

рата Maersk, хакеры нарушили работу Глобальной системы морского транспорта.[11]

После этой атаки ММО выпустила Указания по управлению морскими киберрисками.[12] В Указаниях содержатся рекомендации касательно основных услуг судоходства, как то: мостовые системы, погрузочно-разгрузочные работы, системы управления, двигательные установки, системы питания, системы контроля доступа, пассажирское обслуживание, системы связи.[13] Для этих услуг используются следующие платформы:

- ECDIS (электронная система отображения графических данных и информации);
- AIS (система автоматической идентификации);
- Radar/ARPA (средства радиопеленгации, определения расстояния, радиолокационный автопрокладчик курса);
- Гирокомпас;
- Рулевое управление (компьютеризованная система автоматического управления курсом);
- VDR (морской маршрутный самописец);
- GMDSS (Глобальная система оповещения о бедствиях и обеспечения безопасности на море);
- ESD (системы аварийного отключения).

Технический анализ выявил следующие уязвимости некоторых из этих систем (Таблица 2).[14]

Кроме того, многие новые программы несовместимы с используемым оборудованием. Наиболее распространенной операционной системой на торговых судах является Windows XP, хотя срок её поддержки Microsoft истёк в 2014 г. В 2015 г. проведенное в США исследование показало, что 37 % серверов не обновлялись и считались потенциально уязвимыми для кибератак.[15] В 2020 г. были получены схожие цифры, поскольку главное судовое оборудование не менялось.

---

[11] Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[12] International Maritime Organization (IMO), “Maritime Cyber Risk,” www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

[13] IMO, “Maritime Cyber Risk.”

[14] Mednikarov, Tsonev, and Lazarov, “Analysis of Cybersecurity Issues in the Maritime Industry.”

[15] Ms. Smith, “Maritime Cybersecurity Firm: 37% of Microsoft Servers on Ships Vulnerable to Hacking,” *CSO*, May 4, 2015, https://www.csoonline.com/article/2917856/maritime-cybersecurity-firm-37-of-microsoft-servers-not-patched-vulnerable-to-hacking.html.

Таблица 2. Анализ угроз платформ судоходства [16]

Платформа	Применение	Уязвимость	Воздействие
ECDIS	Отображение навигационных карт	Отсутствие механизма идентификации	Изменение маршрута
AIS, GMDSS	Идентификация и оповещение о бедствии	Не имеет механизмов безопасности и проверки данных	Генерирование ложных команд AIS и изменение маршрута судна
Системы аварийного отключения (ESD)	Блокировка управления силовой установкой в чрезвычайной ситуации	Доступны с берега	Судовую машину можно остановить дистанционно

Источник: Mednikarov et al., 2020.

Главные виды кибератак на суда с использованием существующих уязвимостей таковы:

- Фишинг – рассылка электронных сообщений на множество адресов с просьбой предоставить важную или конфиденциальную информацию. Такие атаки могут также спровоцировать пользователя обратиться к некоему ресурсу, открыв тем самым несанкционированный доступ к информационной инфраструктуре.
- Программы-вымогатели – действия, при которых вредоносный код шифрует хранящиеся в системе данные и требует выкуп за их расшифровку. Суда уязвимы к ним, поскольку у них отсутствуют планы проверки используемых файлов, а у большинства из них нет механизма проверки входящей и исходящей электронной почты.[17]
- Сканирование – процесс поиска уязвимостей в системе.
- Отказ в обслуживании – процесс, при котором трафик определенного количества удаленно управляемых компьютеров перегружает пропускную способность связи или прерывает доступ к определенному ресурсу или услуге.
- Атака на цепочку снабжения – процесс зловредного воздействия на системы судна через устройство, в которое внедрён хакерский код.
- Подмена GPS – процесс, при котором хакер вынуждает GPS-приёмник изменить отображение местоположения судна.

[16] Mednikarov, Tsonev, and Lazarov, “Analysis of Cybersecurity Issues in the Maritime Industry.”

[17] Mohamed Amine Ben Farah et al., “Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends,” *Information* 13, no. 1 (2022), 22, https://doi.org/10.3390/info13010022.

- Атака через посредника – процесс, при котором хакер может перехватывать обмен судна с берегом и воздействовать на него.

В Указаниях по кибербезопасности на борту [18] Балтийского и международного морского совета (BIMCO) описаны несколько типов источников киберугроз для судов. Первый из них – это активист. Его целью может быть, например, уничтожение или публикация конфиденциальных данных для привлечения внимания средств массовой информации или DoS (отказ в обслуживании) и кража интеллектуальной собственности.[19] Это может быть инсайдерская угроза, которая сорвёт обслуживание и испортит репутацию. Второй – преступники, стремящиеся получить финансовую выгоду посредством коммерческого и промышленного шпионажа. Их конечная цель – продажа и выкуп украденных данных, блокировка системы и организация мошеннических грузоперевозок. Третья группа, вероятно, самая опасная – это государственные субъекты, поддерживаемые государством, преследующим политические или военные цели, мешая работе судна или судоходной компании. Успешная кибератака может подорвать авторитет правительства или изменить политические цели и направленность действий государства.[20] Государственные субъекты, как правило, занимаются кражей конфиденциальных и секретных данных или воздействуют на важные услуги. Они имеют практически неограниченные ресурсы и могут идти к своей цели без ограничений во времени или получения финансовой прибыли. Среди примеров серьёзных нападений на государства – кибератака на избирательную систему в Эстонии в 2007 г.,[21] кибератаки во время русско-грузинской войны [22] и атаки DDoS на американские банки в 2013 г.[23]

Наиболее серьёзные примеры этих видов кибератак приведены в таблице ниже.

Правовая база кибербезопасности на море

Для оценки факторов, приведших к нынешнему состоянию системы безопасности на море, сначала нужно проанализировать основы кибербезопасности на море. В этом разделе описаны особые проблемы кибербез опасности на море, связанные с отсутствием последовательной и эффектив-

[18] Baltic and International Maritime Council, 2020.

[19] IMO, “Maritime Cyber Risk.”

[20] IMO, “Maritime Cyber Risk.”

[21] Patrick Howell O’Neill, “The Cyberattack That Changed the World,” *Daily Dot*, May 20, 2016, https://www.dailydot.com/debug/web-war-cyberattack-russia-estonia/.

[22] “The Russo-Georgian War 2008: The Role of the Cyber Attacks in the Conflict,” *AFCEA*, May 24, 2012, https://www.afcea.org/committees/cyber/documents/therussogeorgianwar2008.pdf.

[23] Nicole Perlroth and Quentin Hardy, “Banking Hacking was the Work of Iranians, Officials Say,” *The New York Times*, January 8, 2013, https://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

Таблица 2. Основные примеры морских кибератак

Тип атаки	Год	Описание
Вирус-вымогатель / фишинг	2021	Ведущая судоходная компания Южной Кореи HMM: кибератака ограничила доступ к электронной почте [24]
Вирус-вымогатель	2020	Порт вблизи Ормузского пролива: попытка кибератаки повредила некоторые системы порта [25]
Вредоносная программа	2020	Mediterranean Shipping Company (MSC): из-за проблем с безопасностью были закрыты сервера MSC для защиты данных компании, в результате упал вебсайт компании [26]
Вредоносная программа	2019	Атака на американское судно с хищением важных учётных данных. Береговая охрана и ФБР сообщили, что атака стала возможной из-за отсутствия мер безопасности на судне: весь экипаж пользовался одним и тем же логином и паролем для доступа к судовому компьютеру. Задачу хакера упростило и применение внешних устройств. Ещё одна серьёзная ошибка — отсутствие антивирусных программ [27]
Фишинг	2019	Хакеры получили несанкционированный доступ к британской компании «James Fisher and Sons»[28]
Вирус-вымогатель	2018	Китайские хакеры атаковали подрядчиков ВМС США [29]
Вирус-вымогатель Petya	2017	Зашифрованная вредоносная программа поразила все услуги судоходной компании Maersk. Атака *Not-Petya* повредила компьютерные сервера в Европе и Индии. Атака уничтожила операционную систему компьютеров, инфицировав основной загрузочный

[24] Naida Hakirevic Prevljak, "HMM Hit by Cyber Attack," *Offshore Energy*, June 15, 2021, https://www.offshore-energy.biz/hmm-hit-by-cyber-attack/.

[25] Tzvi Joffre, "Cyber Attack Targets Iranian Port near Strait of Hormuz," *The Jerusalem Post*, May 11, 2020, https://www.jpost.com/breaking-news/cyber-attack-targets-iranian-port-near-strait-of-hormuz-627616.

[26] Marcus Hand, "MSC Confirms Malware Attack Caused Website Outage," *Seatrade Maritime News*, April 17, 2020, https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage.

[27] Davey Winder, "U.S. Coast Guard Issues Alert after Ship Heading into Port of New York Hit by Cyberattack," *Forbes*, July 9, 2019, https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/.

[28] "Marine Firm James Fisher Reports Cyber Breach," *Reuters*, November 5, 2019, https://www.reuters.com/article/us-james-fisher-cybercrime-idUSKBN1XF1SQ.

[29] "China Hackers Steal Data from US Navy Contractor," *BBC*, 9 June 2018, https://www.bbc.com/news/world-us-canada-44421785.

		сектор. Пострадали 17 контейнерных терминалов, убытки превысили 200 млн. долларов [30]
Подмена GPS	2017	Об атаке сообщила морская администрация США. GPS судна в порту Новороссийск (Россия) показывала неверное местоположение [31]
Атака на систему навигации	2017	Столкновение корабля ВМС США Fitzgerald с контейнеровозом, приведшее к смерти семи моряков (у побережья Японии) [32]
Подмена GPS	2013	Группе учёных Техасского университета удалось подменить сигнал GPS приёмника яхты [33]

ной нормативной базы для минимизации рисков и угроз и повышения киберустойчивости. Тут же представлен общий обзор международно-правовой базы, а также нормы и правила ЕС и США.

Общий обзор основ международной кибербезопасности на море

Меры безопасности на море, например, Международный кодекс по охране судов и портовых сооружений (ОСПС),[34] обычно принимались в ответ на крупные глобальные потрясения или катастрофы. В ответ на угрозы судам и портам в 2004 г. в соответствии с главой XI-2 Международной конвенции по охране человеческой жизни на море (Конвенция SOLAS) был принят Кодекс ОСПС, в котором признаётся важность портов для мировой безопасности и изложен набор обязательных инструментов и рекомендаций для судов и портовых сооружений.[35] Кодекс исходит из того, что обеспечение безопасности судов и портов является видом управления рисками. Хотя Кодекс и имеет отношение к кибербезопасности (например, меры контроля доступа и требования аутентификации), он прежде всего нацелен на обеспечение физической безопасности портовых сооружений.

Ещё одной важной международной нормой, тоже разработанной в рамках ММО, является Конвенция об облегчении международного морского

[30] Greenberg, “The Untold Story of NotPetya.”

[31] David Hambling, “Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon,” *NewScientist*, August 10, 2017, https://www.newscientist.com/ article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/.

[32] Sam LaGrone, “7 Sailors Missing, CO Injured after Destroyer USS Fitzgerald Collided with Philippine Merchant Ship,” *USNI News*, June 16, 2017, https://news.usni.org/2017/06/16/destroyer-uss-fitzgerald-collides-japanese-merchant-ship.

[33] Brian Dodson, “University of Texas Team Takes Control of a Yacht by Spoofing Its GPS,” *New Atlas*, August 11, 2013, https://newatlas.com/gps-spoofing-yacht-control/28644.

[34] International Maritime Organization (IMO), “SOLAS XI-2 and the ISPS Code,” https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx.

[35] IMO, “SOLAS XI-2 and the ISPS Code.”

судоходства (FAL).[36] Эта конвенция, действующая с 1967 г., направлена на повышение эффективности морских перевозок. Она стандартизует формы обмена информацией в морских портах, особенно при связи портов с судами.[37] Для повышения действенности FAL в 2019 г. её обновили, добавив требование к государственным органам внедрить системы, обеспечивающие электронный обмен информацией между судами и портами.[38] Важным нововведением конвенции стало поощрение концепции «единого окна», при которой все заинтересованные стороны обмениваются данными через единую точку доступа. Её недостаток заключается в том, что если злоумышленник получит доступ к любой из точек входа, он получит доступ ко всей сети.

В 2017 г. ММО приняла резолюцию MSC.428(98) об управлении морскими киберрисками в системах управления безопасностью (СУБ).[39] В резолюции сказано, что утвержденная СУБ должна учитывать управление киберрисками в соответствии с целями и функциональными требованиями Международного кодекса управления безопасностью (ISM Code).[40] Она также призвала национальные органы обеспечить надлежащий учёт киберрисков в системах управления безопасностью в Документе о соответствии компании до 1 января 2021 г. Если они не устранены, судно считается небезопасным и рассматривается как морская угроза для мира.

Главным документом ММО, прямо касающимся кибербезопасности на море, является документ ММО под названием «Руководство по управлению морскими киберрисками» (MSC-FAL.1/ Circ.3), принятый на 41-й сессии Комитета FAL.[41] По сути, документ признаёт, что морская сфера нуждается в лучшем информировании о кибербезопасности и реализации конкретных рекомендаций для повышения киберустойчивости.[42] Руководство признаёт, что все участники морской отрасли индивидуальны. Поэтому каждый должен реализовать наиболее подходящие ему требования, введённые руководством страны регистрации. Руководство[43] также призывает соблю-

[36] International Maritime Organization (IMO), “FAL Convention,” 1967, www.imo.org/en/OurWork/Facilitation/Pages/FALConvention-Default.aspx.

[37] IMO, “FAL Convention,” 1967.

[38] International Maritime Organization (IMO), “FAL Convention,” 2017, www.imo.org/en/OurWork/Facilitation/Pages/FALConvention-Default.aspx.

[39] IMO, “Maritime Cyber Risk Management in Safety Management Systems,” Resolution MSC.428(98), adopted on June 16, 2017, https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.428(98).pdf.

[40] IMO, *ISM Code: International Safety Management Code with Guidelines for Its Implementation* (London, UK: IMO Publishing, 2018).

[41] IMO, “Maritime Cyber Risk.”

[42] Akash Rana, “Commercial Maritime and Cyber Risk Management,” *Safety & Defense* 5, no. 1 (2019):46-48, https://doi.org/10.37105/sd.42.

[43] IMO, “Maritime Cyber Risk.”

дать международные стандарты безопасности, в частности, ISO/IEC 27001,[44] где изложены требования к системе информационной безопасности. В Руководстве принят к сведению передовой опыт отрасли и упомянуты пять элементов: идентификация, защита, обнаружение, реагирование и восстановление. Новым в этом правиле стала возможность признания судна непригодным, если рекомендации не будут выполнены.[45] Хотя Руководство ММО по управлению морскими киберрисками содержит рекомендации по защите судов от существующих киберрисков и угроз, там нет конкретных указаний об обеспечении безопасности каналов связи между портом и судном. Ещё одна серьёзная проблема заключается в том, что контроль реализации возложен на страну регистрации и национальные морские власти.[46]

Для повышения совместимости ММО совместно с Международной электротехнической комиссией (МЭК) ввела новый стандарт оборудования и систем морской навигации и радиосвязи IEC 63.154 «Кибербезопасность – Общие требования, методы испытаний и требуемые результаты испытаний».[47] Этот стандарт устанавливает требования, методы тестирования и стандарты для судового оборудования, обеспечивающие базовый уровень защиты от киберинцидентов.

Общий обзор нормативной базы кибербезопасности на море Европейского Союза

На стратегическом уровне главные усилия ЕС сосредоточены на Стратегии безопасности ЕС в 2020-2025 гг.[48] Стратегия утверждает, что кибератаки и киберпреступность продолжают расти, и её основная цель – вовлечь всё общество в решение проблем безопасности. Сюда входят отраслевые инициативы по устранению конкретных рисков, угрожающих критической инфраструктуре, включая транспорт и судоходство.

Общие усилия по обеспечению безопасности морских перевозок ЕС основаны на Директиве (ЕС) 2016/1148, также известной как Директива NIS (сетевая и информационная безопасность).[49] Её разработали, чтобы повы-

---

[44] International Organization for Standardization (ISO), "ISO/IEX 27001: Information Security Management," 2013, www.iso.org/isoiec-27001-information-security.html.

[45] IMO, "Maritime Cyber Risk."

[46] Nineta Polemi, *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains* (Amsterdam: Elsevier, 2017).

[47] International Electrotechnical Commission (IEC), "IEC 63154:2021 – Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results," по состоянию на 13 мая 2021, https://webstore.iec.ch/publication/61003.

[48] European Commission, "About the European Security Union," https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en.

[49] "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network

сить безопасность сетей, услуг и информационных систем.[50] Цель Директивы NIS – усилить потенциал кибербезопасности ЕС, снизить угрозы сетям и информационным системам, используемым при предоставлении основных услуг в критических секторах, и обеспечить сохранение таких услуг после инцидентов в сфере кибербезопасности.[51] Директива подчеркивает, что растущая взаимозависимость различных основных услуг может нарушить деятельность организаций и секторов и оказать каскадное негативное воздействие на предоставление услуг на рынках. Поэтому операторы основных услуг стран-участниц должны делать всё возможное для снижения рисков нападения и сообщать властям о покушениях на их кибербезопасность.[52]

Директива NIS требует от каждой страны ЕС определить операторов основных услуг, работающих на их территории для достижения своих целей. Важным фактором недейственности Директивы NIS стали широкие критерии определения этих операторов основных услуг (ООС). Требования таковы:

- Предприятие предоставляет услугу, нужную для поддержания критически важной общественной и экономической деятельности;
- Предоставление этой услуги зависит от сети и информационных систем;
- Инцидент может иметь существенные негативные последствия для этой услуги.[53]

Применение этих критериев зависит от оценки риска национальным органом для конкретной базовой услуги. Другими словами, хотя транспорт назван критической услугой в ЕС, некоторые страны-участницы могут решить, что какая-то их морская инфраструктура не соответствует этим критериям. Поэтому не все порты и суда в ЕС отнесены к критической инфраструктуре.

Ещё одной особенностью морской сферы ЕС является разнообразие национальных морских компетентных органов. Различные организации, перечисленные в таблице ниже, имеют разные цели, нормативную базу, партнеров и бюджеты, что усугубляет несогласованность в данной сфере.

В ответ на растущие угрозы, связанные с компьютеризацией и ростом кибератак, Комиссия ЕС предложила заменить Директиву NIS, ужесточить

and information systems across the Union," Document 32016L1148, *EUR-Lex*, July 19, 2016, https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

50 "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016."

51 "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016."

52 ENISA, https://www.enisa.europa.eu.

53 "NIS Directive – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016."

требования безопасности и ввести более строгие меры надзора и правоприменительные требования, включая общие санкции Евросоюза.[54] После добавления новых секторов в список основных услуг NIS 2 обеспечит безопасность цепочек поставки и унифицирует требования отчётности.

Таблица 2. Компетентные национальные органы стран ЕС [55]

Страна	Компетентный орган
Бельгия	Федеральный министр по вопросам мобильности (Федеральная служба мобильности)
Болгария	Министерство транспорта
Венгрия	Национальный генеральный директорат защиты от бедствий
Германия	Федеральное управление информационной безопасности (BSI)
Греция	Национальный орган кибербезопасности (Генеральный секретариат цифровой политики – Министерство цифровой политики, телекоммуникаций и средств массовой информации)
Дания	Датское управление транспорта, строительства и жилищного хозяйства
Ирландия	Национальный центр кибербезопасности (NCSC)
Испания	Государственный секретарь по вопросам безопасности (Министерство внутренних дел) – через Национальный центр защиты инфраструктуры и кибербезопасности (CNPIC)
Латвия	Министерство транспорта
Литва	Министерство национальной обороны
Люксембург	Люксембургский институт регулирования
Мальта	Отдел защиты критической инфраструктуры Мальты (CIP)
Нидерланды	Министерство инфраструктуры и водопользования
Польша	Министерство морской экономики и внутренней навигации
Португалия	Национальный центр кибербезопасности Португалии
Румыния	Группа реагирования на компьютерные чрезвычайные ситуации (CERT-RO)
Словакия	Министерство транспорта и строительства Словацкой Республики
Словения	Управление информационной безопасности

[54] European Parliament, "The NIS2 Directive: A High Common Level of Cybersecurity in the EU," EU Legislation in Progress, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

[55] ENISA, "National Competent Authorities for the Water transport subsector," www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/nis-visualtool.

Финляндия	Управление транспорта и связи Финляндии (Traficom)
Франция	Национальное агентство кибербезопасности (ANSSI)
Хорватия	Министерство моря, транспорта и инфраструктуры
Чехия	Национальное агентство кибернетической и информационной безопасности (NCISA)
Швеция	Шведское транспортное агентство
Эстония	Управление информационных систем (RIA)

NIS 2 преследует следующие главные цели:

- Повышение уровня киберстойкости служб стран ЕС путём введения правил, которые обязаны соблюдать все государственные и частные органы, ответственные за эти услуги;
- Уменьшение несоответствий в обеспечении безопасности на внутреннем рынке в важных секторах услуг путём дальнейшей гармонизации требований безопасности и отчётности об инцидентах, а также национального надзора и правоприменения;
- Улучшение коллективного понимания ситуации и коллективных способностей подготовки и реагирования, принимая меры по укреплению доверия между компетентными органами. Расширение обмена информацией и установление правил и процедур на случай крупномасштабного инцидента или кризиса;[56]
- Совершенствование списков операторов основных услуг стран-участниц на основе стандартного набора критериев.

Защита и киберстойкость основаны на систематизации масштабных киберинцидентов общеевропейскими группами сотрудничества в рамках NIS,[57] где определены все возможные злонамеренные действия в привязке к соответствующим правилами реагирования на политические кризисы в ЕС. Другие нормы снижения рисков и угроз европейской морской отрасли включают Европейскую программу защиты критической инфраструктуры (EPCIP) [58] и Директиву по определению и обозначению европейской критической инфраструктуры.[59] Недавний проект Директивы по обеспечению

[56] ENISA, https://www.enisa.europa.eu.

[57] Группа сотрудничества NIS включает представителей стран-участниц ЕС, ENISA и Европейской Комиссии. Создана согласно Статье 11 Директивы NIS.

[58] European Programme for Critical Infrastructure Protection.

[59] "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)," Document 32008L0114, *EUR-Lex* December 23, 2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114.

устойчивости важных объектов предлагает более целенаправленный подход к защите критической инфраструктуры.[60]

Конкретные меры регулирования морской кибербезопасности основаны на Стратегии безопасности на море ЕС (EUMSS).[61] Эта стратегия определяет риски и угрозы морской безопасности – «терроризм и другие преднамеренные незаконные действия на море и в портах против судов, грузов, экипажей и пассажиров, портов и портовых сооружений, а также критической морской и энергетической инфраструктуры, включая кибератаки».[62] EUMSS была принята в 2014 г. и пересмотрена в 2018 г., как общий и всеобъемлющий инструмент выявления, предотвращения и реагирования на любые проблемы, затрагивающие безопасность европейцев, деятельность и активы в морской экосистеме. Пересмотр EUMSS, утверждённый Советом по общим вопросам 26 июня 2018 г., нацелен на более чёткий процесс отчётности для улучшения понимания и лучшего выполнения стратегии.

Для реализации нормативной базы в ЕС создали специализированные органы, такие, как Агентство кибербезопасности Европейского Союза (ENISA),[63] Европейский центр киберпреступности (EC3) [64] в составе Europol и Группа реагирования на компьютерные чрезвычайные ситуации (CERT-EU).[65] Генеральный директорат по мобильности и транспорту (DG MOVE) и Европейское агентство по безопасности на море (EMSA) осуществляют общий надзор на выполнение требований национальными органами. ЕС также выступил с инициативами по повышению кибербезопасности в ряде важных секторов. В частности, Центры обмена и анализа информации (ISAC) [66] должны завоевать доверие в деле обмена информацией и передовым опытом в области физических и кибернетических угроз и их снижения, но пока что ЕС отстает в создании ISAC для морской сферы.

Важную для стран ЕС программу представили странам-участницам в

---

[60] "Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities," Document 52020PC0829, *EUR-Lex*, December 16, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN.

[61] Council of the European Union, "Maritime Security Strategy," June 26, 2018, https://ec.europa.eu/oceans-and-fisheries/ocean/blue-economy/other-sectors/maritime-security-strategy_en.

[62] Council of the European Union, "Maritime Security Strategy."

[63] ENISA, https://www.enisa.europa.eu.

[64] "European Cybercrime Centre – EC3: Combating Crime in a Digital Age," *Europol*, updated March 1, 2022, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[65] "CERT-EU – The Computer Emergency Response Team for the EU institutions, bodies and agencies," https://cert.europa.eu/.

[66] "Information Sharing and Analysis Centers (ISACs)," https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing.

марте 2021 г.: это «Цифровой компас 2030»,[67] цель которого – внедрить конкретные процедуры продвижения цифровой трансформации ЕС, усиления его цифрового суверенитета и политики, а также устранить уязвимости и угрозы. Эта программа должна содействовать компьютеризации и обменам на море путём реализации самых современных мер кибербезопасности. «Цифровой компас 2030» опирается на четыре ключевые идеи:

- Цифровые возможности населения;
- Повышение связанности и производительности цифровой инфраструктуры;
- Цифровая трансформация бизнеса;
- Цифровизация общественных услуг.[68]

В целом «Цифровой компас 2030» является наглядной демонстрацией амбиций ЕС по реализации расширенной политики и стратегии кибербезопасности и созданию других инструментов для продвижения цифровизации, улучшения экономических и социальных показателей ЕС.

Важной задачей стран-участниц является соблюдение правил ЕС. В настоящее время большинство стран-участниц не обладают техническими возможностями для мониторинга критической морской информационной инфраструктуры и не внедрили специальные правила защиты своих основных услуг. Недостатком является и отсутствие эффективных платформ для обмена передовым опытом и укрепления сотрудничества между странами-участницами и их зарубежными коллегами, например, государственно-частного партнерства.[69]

Ещё одним серьёзным препятствием для достижения реальной киберстойкости в ЕС является наложение штрафов на организации, не соблюдающие требований. Из-за отсутствия воли у стран-участниц штрафы в большинстве случаев не применяются.[70]

Общий обзор базы кибербезопасности на море в США

База кибербезопасности на море в США принципиально не отличается от подхода ЕС. Кибербезопасность на море регулирует американский Национальный план кибербезопасности на море. Его принципы:

- Свобода мореплавания;
- Поддержка и защита торговли для обеспечения бесперебойных поставок;

---

67 "2030 Digital Compass: The European Way for the Digital Decade," *EU4Digital*, March 9, 2021, https://eufordigital.eu/library/2030-digital-compass-the-european-way-for-the-digital-decade/.

68 "2030 Digital Compass."

69 Cecilia Gondard and Enrique Guerrero Salom, "The Problem with Public-Private Partnerships and the Role of the EU," *Eurodad*, December 4, 2018, https://www.eurodad.org/PPPs-EU.

70 Этот вопрос решён в NIS2.

- Содействие перемещению нужных товаров и людей через границы при отсеивании опасных людей и материалов.[71]

План охватывает ресурсы, участников и инициативы, снижая текущие угрозы, уязвимости и т.д.[72]

Другими документами США, касающимися кибермер в морской сфере, является Циркуляр по навигации и инспекции судов № 01-20 «Руководство по устранению киберрисков в Законе о безопасности морского транспорта» (MTSA) [73] и Рабочая инструкция по соблюдению требований для коммерческих судов CVC-WI-018(1).[74] Эти документы устанавливают сроки включения мероприятий по киберзащите судов и прибрежных сооружений в оценки и планы безопасности.

Разработка конкретной политики и самостоятельная оценка надёжности инфраструктуры кибербезопасности является одной из важных задач американских морских властей – Береговой охраны США, что связано с недостаточным обменом и отчётностью, а также с отсутствием возможностей и процедур оценки уязвимости.

Серьёзной задачей для межнациональных и региональных механизмов кибербезопасности на море является минимизация угроз для портов и грузов от судов, использующих «удобные флаги». Их регистры не предъявляют особых национальных требований к судоходным компаниям, использующих их флаг.[75] По данным ЮНКТАД, почти 73 % судов зарегистрированы не в той стране, где судовладелец.[76] Проблема состоит в том, что несмотря на ратификацию нескольких международных морских и трудовых конвенций, у стран «удобных флагов» часто нет ресурсов и воли для реального обеспечения соблюдения международных норм безопасности на море и кибербезопасности. Поэтому они создают критическую уязвимость для всей морской транспортной системы.

Таким образом, основные проблемы эффективности действующей нормативной базы связаны со следующими основными факторами:

---

[71] "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security" (The White House, December 2020), https://www.hsdl.org/?view&did=848704.

[72] "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security."

[73] U.S. Coast Guard, "Navigation and Vessel Inspection Circular (NVIC) No. 01-20 – Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities," February 26, 2020, https://www.dco.uscg.mil/Our-Organization/NVIC/Year/2020/.

[74] USCG Office of Commercial Vessel Compliance (CG-CVC), "Commercial Vessel Compliance Work Instruction – CVC-WI-018(1)2020," September 1, 2020, www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/CVC-WI-018(1).pdf.

[75] "Flags of Convenience," *NGO Shipbreaking Platform*, https://shipbreakingplatform.org/issues-of-interest/focs.

[76] "Review of Maritime Transport," *UNCTAD*, https://unctad.org/topic/transport-and-trade-logistics/review-of-maritime-transport.

- Несогласованность и отсутствие стандартизации существующих нормативных баз;
- Недостаток воли для обеспечения применения эффективных инструментов кибербезопасности и санкций за их невыполнение;
- Недостаточная киберграмотность.

Примеры

К счастью, несмотря на все сложности и проблемы, примеры показывают, что киберстойкость и киберзнания вполне можно обеспечить. Норвежское морское ведомство предупредило судовладельцев и судоходные компании, что хакеры используют социальные сети, в частности LinkedIn, Facebook Messenger и WhatsApp, для внедрения вредоносных программ, и дало судам конкретные рекомендации, сумев снизить потенциальную эффективность кибератак.[77]

Страховая компания Shipowners Claims Bureau, Inc. разработала новый метод обучения персонала на борту и в портовых терминалах при помощи иллюстрированной брошюры под названием «Cyber Awareness». Рисунки и юмор помогают объяснить, что морякам нужно знать о мерах противодействия кибератакам, будь то вирус-вымогатель или фишинг.[78]

Некоторые страны-члены ЕС включили инициативы в области киберзнаний в свои Национальные стратегии кибербезопасности. В Хорватии эти инициативы охватывают электронную связь, критическую информационную инфраструктуру и киберпреступность.[79] В Национальной стратегии кибербезопасности Чехии этому вопросу посвящена отдельная глава под названием «Устойчивое общество 4.0».[80] Национальная стратегия кибербезопасности Эстонии включает конкретные меры по обучению граждан, предотвращению инцидентов кибербезопасности и информированию людей о возможных угрозах.[81] Главная цель Стратегии кибербезопасности Польши – повысить устойчивость к киберугрозам, что включает специальные программы информирования о кибербезопасности.[82]

---

77 Norwegian Maritime Authority, https://www.sdir.no/en/.

78 Shipowners Claims Bureau, Inc., “Shipboard Safety Cartoon,” https://www.americanclub.com/files/files/Shipboard_Safety.pdf.

79 “The National Cybersecurity Strategy of the Republic of Croatia,” Zagreb, October 7, 2015 (Official Gazette No.108/2015), https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf.

80 “Czech Republic Cybersecurity,” *International Trade Administration*, по состоянию на 13 мая 2021, www.trade.gov/market-intelligence/czech-republic-cybersecurity.

81 Ministry of Economic Affairs and Communications, *Cybersecurity Strategy, Republic of Estonia 2019-2022*, https://www.mkm.ee/media/703/download.

82 Waldemar Kitler, “The Cybersecurity Strategy of the Republic of Poland,” in *Cybersecurity in Poland*, ed. Katarzyna Chałubińska-Jentkiewicz, Filip Radoniewicz, and Tadeusz Zieliński (Cham: Springer, 2022), https://doi.org/10.1007/978-3-030-78551-2_9.

Инструмент по управлению киберрисками для портов ENISA – ещё один пример благотворного эффекта морского сотрудничества. Этот инструмент позволяет операторам портов проводить оценку киберрисков в четыре этапа, следуя общим принципам управления рисками. Кроме того, операторы определяют меры безопасности, исходя из своих приоритетов, и оценивают своё умение в реализации этих мер.[83]

Для обмена морской информацией в США действуют Центры обмена и анализа информации для обмена данными о киберугрозах. В морском секторе США имеются ещё три Центра обмена и анализа информации (MPS-ISAO, Морской ISAC, и ISAC системы морского транспорта).[84]

Реагирование

С компьютеризацией и внедрением ИКТ в торговом судоходстве суда столкнулись с рисками и угрозами кибербезопасности. В отрасли торгового морского судоходства в настоящее время действует множество участников и регулирующих органов, использующих разные нормы. Из-за недостатка киберзнаний и современных технических возможностей для мониторинга информационной инфраструктуры судов, а также из-за того, что существующие нормы слишком широки и необязательны, морское судоходство уязвимо для кибератак, способных нанести серьёзный ущерб.

Первая и самая важная программа должна быть сосредоточена на улучшении обмена информацией об угрозах на море. Этого можно достичь при использовании Центров обмена и анализа информации (ISAC) и содействии государственно-частному партнерству. Вторая программа должна повышать киберзнания во всей морской сфере. Этого можно достичь, организуя занятия, семинары и конференции для всех участников морской сферы. Кроме того, обучение и сертификация на протяжении года могут быть предусмотрены и организованы государственными органами, которые регулируют и стандартизируют этот процесс. Обе инициативы являются важными элементами Директивы ЕС NIS 2.[85]

Третья программа должна заняться стандартизацией существующей правовой базы. Этого можно достичь, приняв Глобальный кодекс кибербезопасности на море, который будет легче отслеживать и соблюдать. Кроме того, Глобальный кодекс обобщит существующий передовой опыт в области стандартов кибербезопасности. Поскольку эти стандарты уже получили международное признание, их соблюдение должно встречать меньшее со-

---

[83] “Cyber Risk Management for Ports,” *ENISA*, https://www.enisa.europa.eu/cyber-risk-management-for-ports#/.

[84] Jaikumar Vijayan, “What is an ISAC or ISAO? How These Cyber Threat Information Sharing Organizations Improve Security,” *CSO*, July 26, 2021, www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html.

[85] European Parliament, “The NIS2 Directive.”

противление судовладельцев и национальных властей. Кодекс кибербезопасности на море должен включать как обязательные, так и добровольные положения. Обязательная часть должна быть нацелена на обеспечение судами основных услуг. В добровольном разделе должны быть описаны методы реализации дополнительных мер безопасности. Отдельная подпрограмма должна охватывать аккредитацию и сертификацию «удобных флагов» путём введения дополнительных обязательных требований к их информационной инфраструктуре. Кроме того, Морской кибер-кодекс должен содержать конкретные указания и процедуры для установления и наказания виновных в кибератаках.

Четвертая программа должна обеспечить возможность заблаговременного обнаружения разрушительных киберсобытий. Заблаговременное обнаружение может осуществляться по-разному, включая мониторинг сетей и потоков данных. На оперативном уровне эта программа также должна предусматривать гарантированные средства для совместного использования сторонами и эффективные средства, гарантирующие непрерывность работы судна. Киберстойкость должна включать четкие планы альтернативных каналов связи, альтернативных баз данных, полностью независимых от обычных систем, и альтернативных инструментов и систем на борту судов, гарантирующих бесперебойную работу основных служб судна в случае взлома систем. Эта программа может быть реализована через специальные программы и фонды ЕС и США.

Пятая программа должна восполнить недостаток навыков обнаружения кибератак. Обучение должно гарантировать способность каждого обнаружить аномальное поведение системы и сообщить о нем в установленном порядке. Кроме того, экипаж должен быть обучен строгим правилам кибергигиены, включая сложные методы аутентификации, ограниченный доступ к ресурсам и проверку съёмных устройств памяти.

Наконец, последняя программа должна быть посвящена восстановлению после киберинцидентов. Она может включать специальные упражнения и обучение восстановлению основных служб судна, восстановлению данных, реагированию и расследованию цифровых инцидентов. Важный аспект этой программы составляет компенсация пострадавшим, путём страхования ответственности или государственных выплат. Адекватная компенсация снижает социальные риски и ущерб и способствует восстановлению экономики, социальной стабильности и доверию к институтам.

Заключение

В заключение отметим, что морская киберсфера — это «Титаник», плывущий к айсбергу. Без должного предвидения и способности руководителей морского сообщества устранить возникающие уязвимости, катастрофическое воздействие кибератак на море на глобальную морскую транспортную систему будет лишь вопросом времени. Хотя исследования показали, что

различные организации признают угрозы системе кибербезопасности судоходства в своих нормах и стратегиях, анализ свидетельствует, что это мало повлияло на глобальную кибербезопасность. В этой связи международное морское сообщество при поддержке региональных и национальных морских властей должно реализовать комплексную программу информирования о кибербезопасности и гармонизации существующей нормативной базы для противодействия этой угрозе. Успех такой программы зависит от того, насколько активно все субъекты морского сообщества будут снижать свою кибер-уязвимость и противодействовать рискам и угрозам. Только так можно обойти айсберг.

Примечание

Представленные здесь взгляды принадлежат исключительно автору и не выражают официальную позицию Консорциума военных академий и институтов изучения проблем безопасности программы «Партнёрство ради мира», организаций-участниц или издателей Консорциума.

Благодарность

Connections: The Quarterly Journal, Vol. 20, 2021, вышел при поддержке правительства США.

Об авторе

Явор Тодоров – стипендиат Центра Маршалла, старший эксперт Государственного агентства национальной безопасности /ДАНС/ Болгарии, возглавляет подразделение Департамента кибербезопасности. Г-н Тодоров имеет 20-летний опыт работы в болгарских службах безопасности и в последние восемь лет занимал различные должности, в том числе в сфере борьбы с терроризмом, контрразведки и кибербезопасности. Г-н Тодоров – бывший военно-морской офицер, принимал участие в ряде многонациональных учений, направленных на укрепление безопасности в Черноморском регионе. Член Горизонтальной рабочей группы по киберпроблемам при Совете ЕС, автор проекта Национального закона о кибербезопасности и подзаконных актов. В настоящее время его команда проводит оценку уязвимости критической национальной информационной инфраструктуры. Тесно сотрудничает с правоохранительными органами и службами Болгарии. Владеет английским, итальянским и русским языками. Имеет степень магистра в области телекоммуникаций и управления портами Болгарской военно-морской академии и магистра стратегических исследований Университета национальной обороны в Вашингтоне. В настоящее время заканчивает диссертацию на тему «Кибербезопасность на море».