
СЕМЕНОВ
Сергей Александрович
ISPS-Code
ФЕДЕРАЛЬНОЕ АГЕНТСТВО МОРСКОГО И РЕЧНОГО ТРАНСПОРТА
СЛУЖБА МОРСКОЙ БЕЗОПАСНОСТИ
Морская кибербезопасность.
Новое за 10 месяцев.

Действующие документы ИМО по кибербезопасности в морской отрасли (по состоянию на 02.07.2021)

Название документа (оригинал)	Дата принятия	Название документа в переводе
MSC Resolution: MSC.428(98) Maritime cyber risk management in safety management systems https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx	16.06.2017	**Резолюция КБМ: MSC.428(98) «Управление киберрисками в морской отрасли в рамках систем управления безопасностью»**
Circular MSC.1/Circ.1639 The guidelines on cyber security onboard ships (Version 4.0) https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx	14.06.2021	**Циркуляр КБМ: MSC.1/Circ.1639 Руководство по кибербезопасности на судах (Редакция 4.0)**
Circular MSC-FAL.1/Circ.3/Rev.1 Guidelines on maritime cyber risk Management www.imo.org https://docs.imo.org/	14.06.2021	**Циркуляр MSC-FAL.1/Circ.3/Rev.1 «Методические рекомендации по управлению киберрисками в морской сфере»**

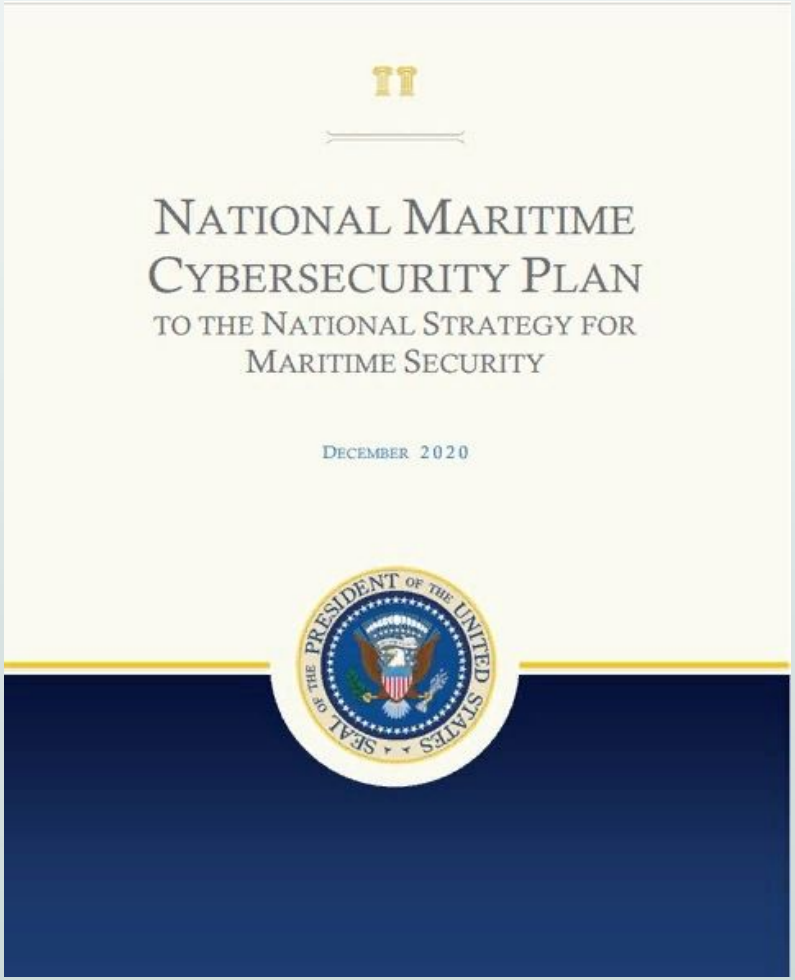
Документы, не выпущенные в виде циркуляров КБМ, однако рекомендованные ИМО в циркуляре MSC-FAL.1/Circ.3/Rev.1 (в помощь пользователям и на их усмотрение)

Название документа (оригинал)	Дата издания	Название документа в переводе
Recommendation on Cyber Resilience (No 166) Developed by IACS (the International Association of Classification Societies) http://www.iacs.org.uk/news/archive/2020 Heading "IACS launches single standalone recommendation on cyber resilience" (IACS is the IMO's principal technical advisor, and usual actively participates in MSC sessions.)	Апрель 2020	**Рекомендация по киберустойчивости (№ 166)** Разработано МАКО (Международная ассоциация классификационных обществ). Заголовок «МАКО представляет свою рекомендацию по киберустойчивости» (МАКО является главным техническим советником ИМО и обычно принимает активное участие в сессиях КБМ)
ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx https://www.iso.org/isoiec-27001-information-security.html	2018	**Стандарт ISO/IEC 27001** Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования.
Framework for Improving Critical Infrastructure Cybersecurity, developed by the US National Institute of Standards and Technology (NIST Framework) https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx https://www.nist.gov/cyberframework	Апрель 2018	**Рамочная программа усиления кибербезопасности критически важной инфраструктуры, разработанная Национальным институтом стандартов и технологий США** (Рамочная программа NIST)

В феврале 2021 года опубликовано «Руководство по кибербезопасности на судах»

* Международная палата судоходства (ICS)
* Международный союз морского страхования (IUMI)
* Балтийский и международный морской совет (BIMCO)
* Международный морской форум нефтяных компаний (OCIMF)
* Международная ассоциация независимых владельцев танкеров (INTERTANKO)
* Международная ассоциация владельцев сухогрузных судов (INTERCARGO)
* Международная ассоциация судовых менеджеров (InterManager)
* Всемирный совет судоходства (WSC)
* Ассоциация строителей суперяхт (Sybass)

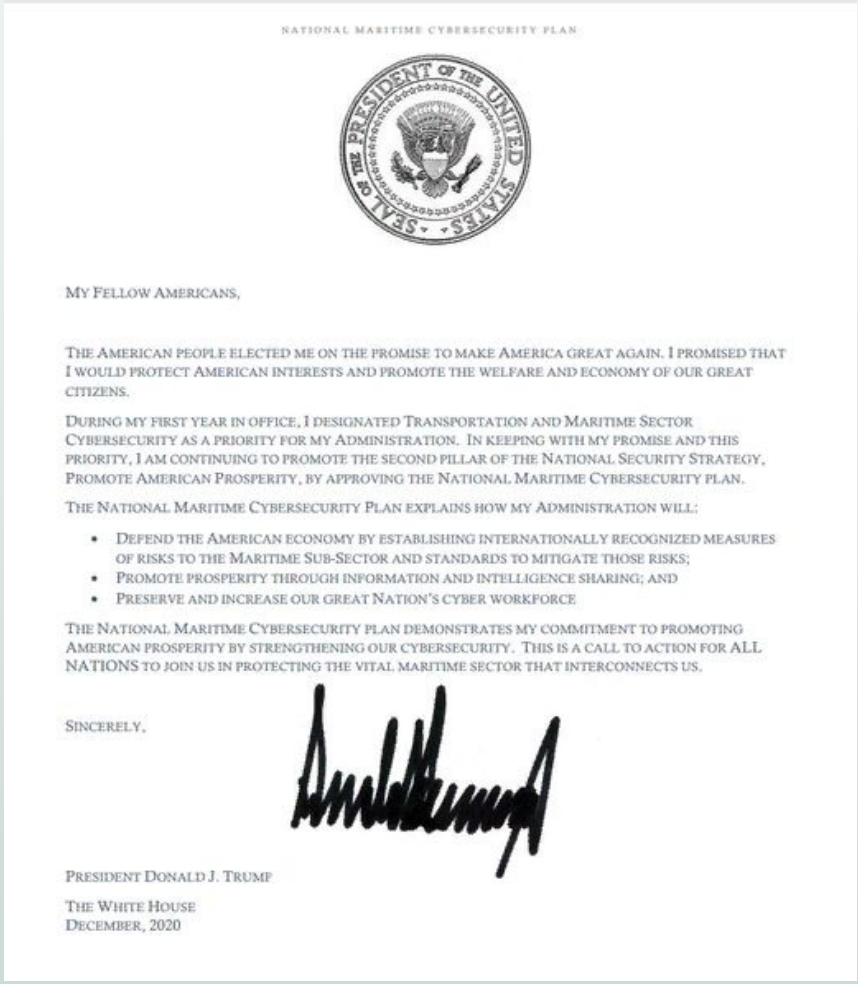
Совет национальной безопасности США 5 января выпустил обновление кибербезопасности для Национальной стратегии морской безопасности Правительства США.



NATIONAL MARITIME CYBERSECURITY PLAN

TO THE NATIONAL STRATEGY FOR MARITIME SECURITY

DECEMBER 2020



NATIONAL MARITIME CYBERSECURITY PLAN

MY FELLOW AMERICANS,

THE AMERICAN PEOPLE ELECTED ME ON THE PROMISE TO MAKE AMERICA GREAT AGAIN. I PROMISED THAT I WOULD PROTECT AMERICAN INTERESTS AND PROMOTE THE WELFARE AND ECONOMY OF OUR GREAT CITIZENS.

DURING MY FIRST YEAR IN OFFICE, I DESIGNATED TRANSPORTATION AND MARITIME SECTOR CYBERSECURITY AS A PRIORITY FOR MY ADMINISTRATION. IN KEEPING WITH MY PROMISE AND THIS PRIORITY, I AM CONTINUING TO PROMOTE THE SECOND PILLAR OF THE NATIONAL SECURITY STRATEGY, PROMOTE AMERICAN PROSPERITY, BY APPROVING THE NATIONAL MARITIME CYBERSECURITY PLAN.

THE NATIONAL MARITIME CYBERSECURITY PLAN EXPLAINS HOW MY ADMINISTRATION WILL:

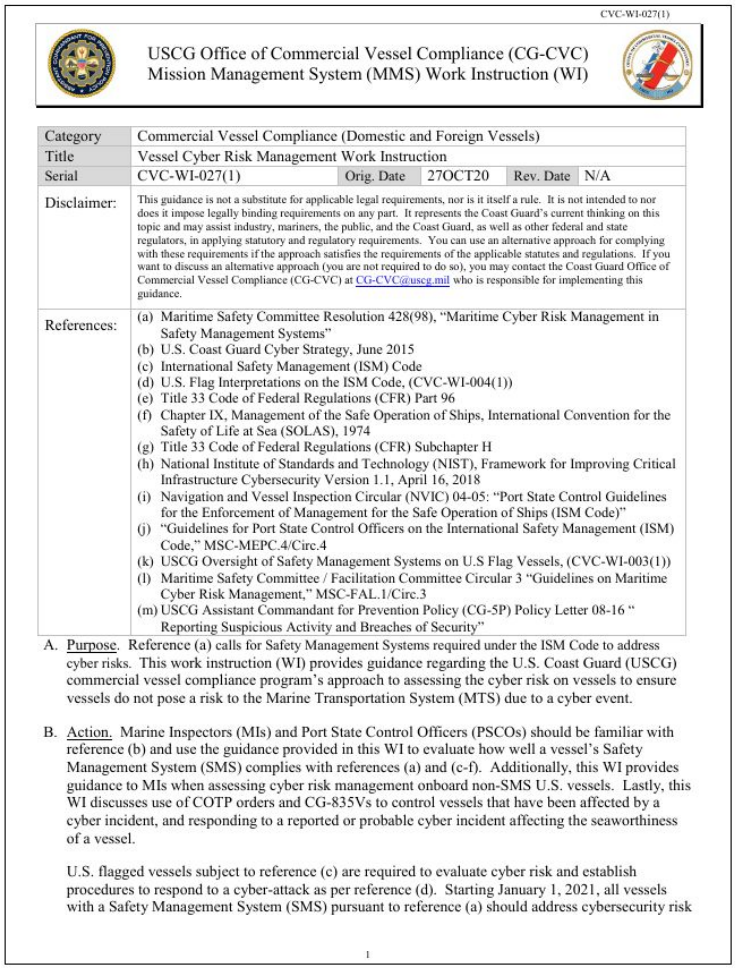
- DEFEND THE AMERICAN ECONOMY BY ESTABLISHING INTERNATIONALLY RECOGNIZED MEASURES OF RISKS TO THE MARITIME SUB-SECTOR AND STANDARDS TO MITIGATE THOSE RISKS;
- PROMOTE PROSPERITY THROUGH INFORMATION AND INTELLIGENCE SHARING; AND
- PRESERVE AND INCREASE OUR GREAT NATION'S CYBER WORKFORCE

THE NATIONAL MARITIME CYBERSECURITY PLAN DEMONSTRATES MY COMMITMENT TO PROMOTING AMERICAN PROSPERITY BY STRENGTHENING OUR CYBERSECURITY. THIS IS A CALL TO ACTION FOR ALL NATIONS TO JOIN US IN PROTECTING THE VITAL MARITIME SECTOR THAT INTERCONNECTS US.

SINCERELY,

PRESIDENT DONALD J. TRUMP

THE WHITE HOUSE
DECEMBER, 2020



CVC-WI-027(1)

USCG Office of Commercial Vessel Compliance (CG-CVC)
Mission Management System (MMS) Work Instruction (WI)

Category	Commercial Vessel Compliance (Domestic and Foreign Vessels)				
Title	Vessel Cyber Risk Management Work Instruction				
Serial	CVC-WI-027(1)	Orig. Date	27OCT20	Rev. Date	N/A

Disclaimer: This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is not intended to nor does it impose legally binding requirements on any part. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements. You can use an alternative approach for complying with these requirements if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach (you are not required to do so), you may contact the Coast Guard Office of Commercial Vessel Compliance (CG-CVC) at CG-CVC@uscg.mil who is responsible for implementing this guidance.

References:
(a) Maritime Safety Committee Resolution 428(98), "Maritime Cyber Risk Management in Safety Management Systems"
(b) U.S. Coast Guard Cyber Strategy, June 2015
(c) International Safety Management (ISM) Code
(d) U.S. Flag Interpretations on the ISM Code, (CVC-WI-004(1))
(e) Title 33 Code of Federal Regulations (CFR) Part 96
(f) Chapter IX, Management of the Safe Operation of Ships, International Convention for the Safety of Life at Sea (SOLAS), 1974
(g) Title 33 Code of Federal Regulations (CFR) Subchapter H
(h) National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018
(i) Navigation and Vessel Inspection Circular (NVIC) 04-05: "Port State Control Guidelines for the Enforcement of Management for the Safe Operation of Ships (ISM Code)"
(j) "Guidelines for Port State Control Officers on the International Safety Management (ISM) Code," MSC-MEPC.4/Circ.4
(k) USCG Oversight of Safety Management Systems on U.S Flag Vessels, (CVC-WI-003(1))
(l) Maritime Safety Committee / Facilitation Committee Circular 3 "Guidelines on Maritime Cyber Risk Management," MSC-FAL.1/Circ.3
(m) USCG Assistant Commandant for Prevention Policy (CG-5P) Policy Letter 08-16 " Reporting Suspicious Activity and Breaches of Security"

A. Purpose. Reference (a) calls for Safety Management Systems required under the ISM Code to address cyber risks. This work instruction (WI) provides guidance regarding the U.S. Coast Guard (USCG) commercial vessel compliance program's approach to assessing the cyber risk on vessels to ensure vessels do not pose a risk to the Marine Transportation System (MTS) due to a cyber event.

B. Action. Marine Inspectors (MIs) and Port State Control Officers (PSCOs) should be familiar with reference (b) and use the guidance provided in this WI to evaluate how well a vessel's Safety Management System (SMS) complies with references (a) and (c-f). Additionally, this WI provides guidance to MIs when assessing cyber risk management onboard non-SMS U.S. vessels. Lastly, this WI discusses use of COTP orders and CG-835Vs to control vessels that have been affected by a cyber incident, and responding to a reported or probable cyber incident affecting the seaworthiness of a vessel.

U.S. flagged vessels subject to reference (c) are required to evaluate cyber risk and establish procedures to respond to a cyber-attack as per reference (d). Starting January 1, 2021, all vessels with a Safety Management System (SMS) pursuant to reference (a) should address cybersecurity risk

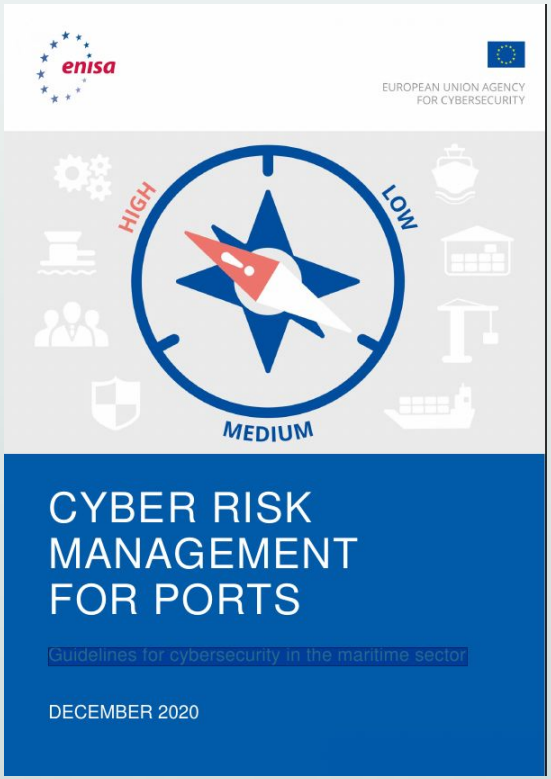
1

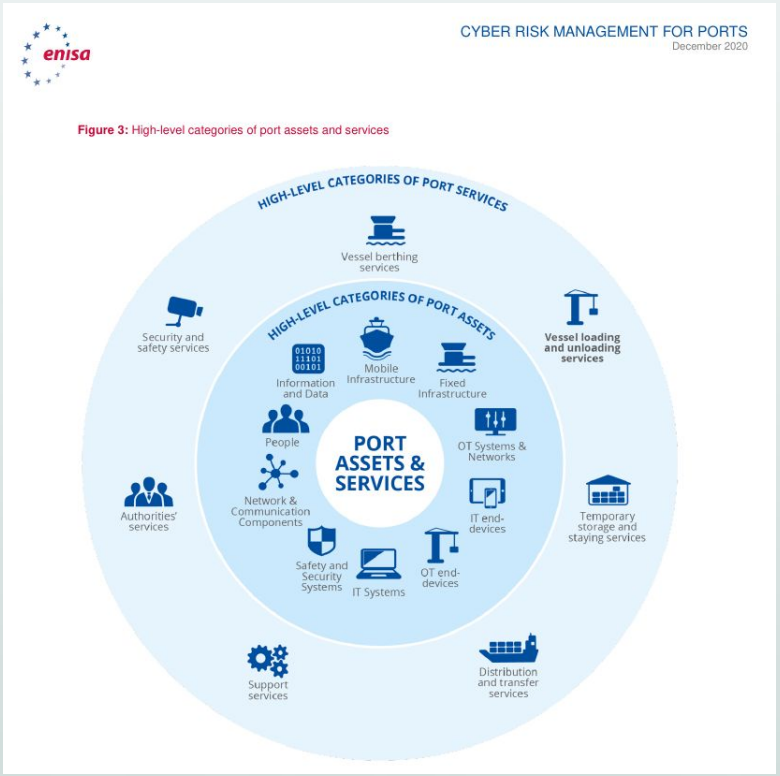
Согласно инструкции, если **управление киберрисками не было включено в систему управления безопасности судна** до первой ежегодной проверки документа компании о соответствии после 1 января 2021 года, то судно может быть **задержано** с требованием внешнего аудита в течение 3 месяцев.

Также, когда объективные доказательства указывают на **наличие серьезного сбоя в реализации системы управления безопасностью судна** в отношении управления киберрисками, который непосредственно привел к инциденту кибербезопасности, влияющему на работу судна (например, снижению безопасности судна или повышению риска для окружающей среды), то судно также может быть **задержано** с требованием внешнего аудита в течение 3 месяцев.

17 декабря 2020 года агентство Европейского Союза по кибербезопасности (ENISA) выпустило руководство

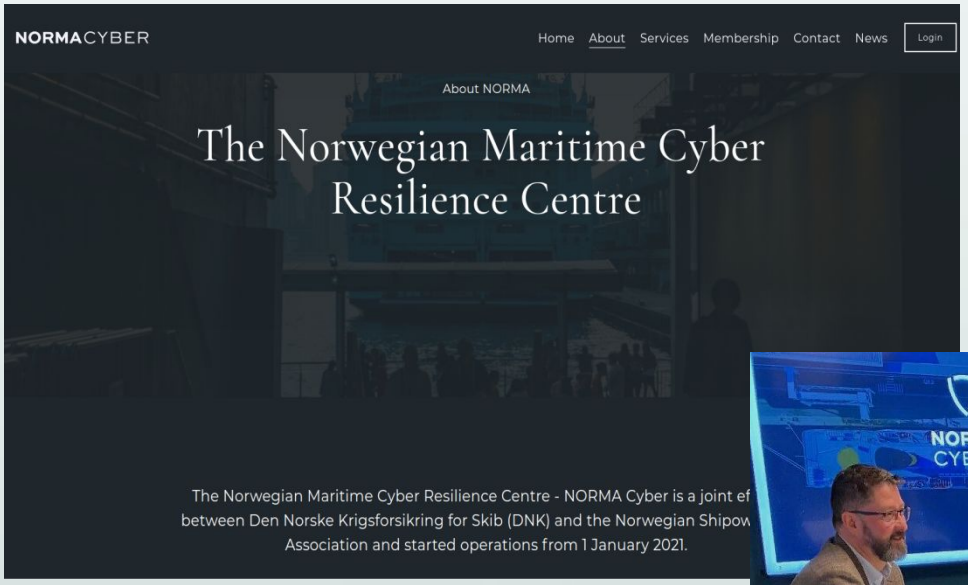
«Управление киберрисками для портов»





https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

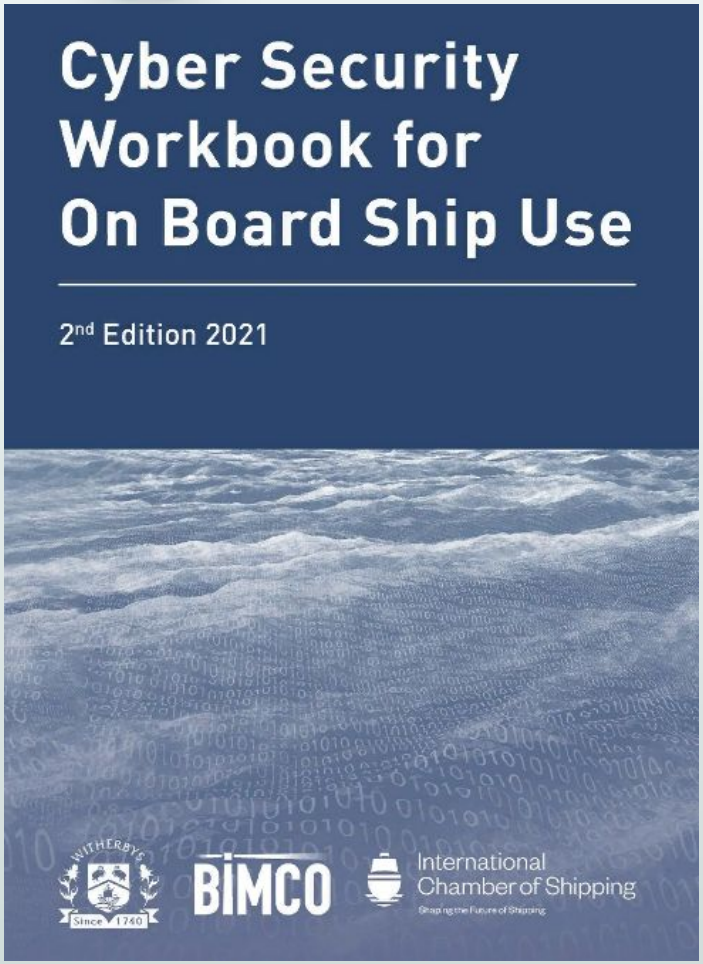
1 января 2021 года в Норвегии открыт «Норвежский морской центр киберустойчивости» (NORMA Cyber).



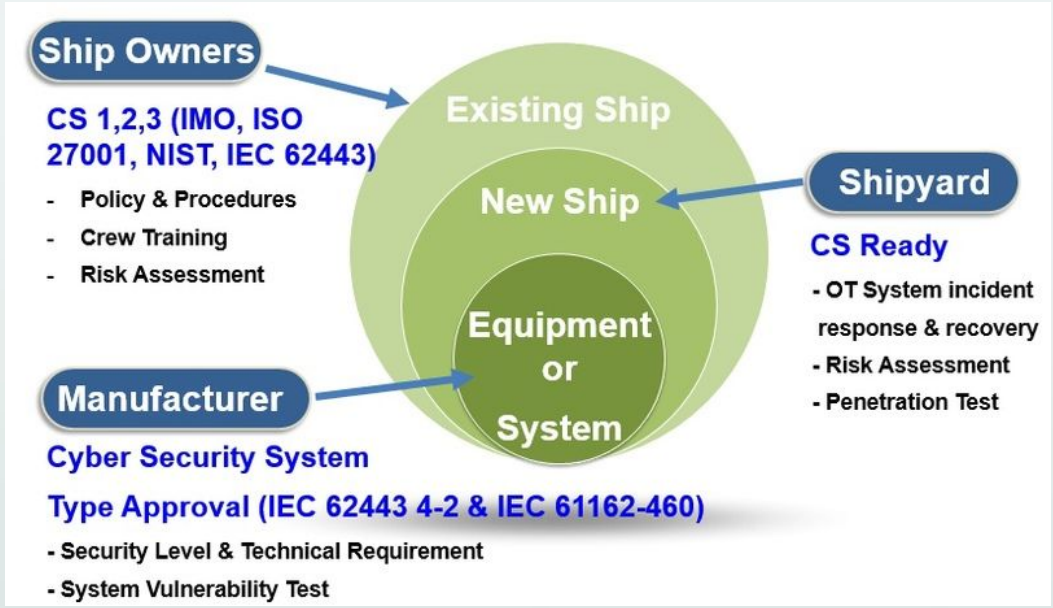
Стоимость членства:
- 1 000 долларов США за судно в год
- максимум 10 000 долларов США за флот в год

https://www.normacyber.no/en/home

Услуги:
- Предупреждения
- Индикатор компрометации данных
- Уведомления об уязвимостях
- Отчеты разведки
- Рекомендации по смягчению последствий
- Рекомендации по реагированию на кризисные ситуации и т.д.



https://www.ics-shipping.org/publication/cyber-security-workbook-second-edition/



KR Maritime Cyber Security сертификация проводится в отношении компании или судна с системой менеджмента киберезопасности (SCMS). Соответствие требованиям кибербезопасности для компании / существующего судна разделено на 3 уровня (CS1, CS2 и CS3) в соответствии со зрелостью кибербезопасности и состоит из 35 зон обследования и 144 пунктов обследования.

- **CS1, CS2 , CS3**: требования CSMS к существующему судну (Судоходная компания)
- **CS-Ready** : требования к созданию комплексной системы информационной безопасности нового судна (Судостроитель)
- **CS Type Approval** : требования к функциональности информационной безопасности системы Оборудование (Производители оборудования)

25 May 2021

IUMI

IUMI Policy Agenda

3. Cyber risks

Brief description

The growing use and reliance on information technology, of data networks, transmissions and connectivity in the daily work within the marine and energy sectors increase their exposure to cyber related risks. Ransomware attacks may result in economic loss or costs of rebuilding lost data. Stand-alone ransomware insurance products are now available both within the marine and non-marine insurance markets to protect against this risk. Consequential damages to hull, cargo and third-party liabilities from a cyber-attack on board a vessel or mobile offshore unit poses a different and more costly risk. The limited data on the frequency, severity of loss or probability of physical damage, is a challenge to underwriters.

The risks can be either malignant or due to innocent breach caused by a lack of awareness or insufficient understanding about systems and how they interact with each other. Both need to be dealt with, starting with top-level commitment and the proper implementation of risk assessment procedures.

Techopedia[1] defines cyber-attacks as deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber-attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cyber-crimes, such as information and identity theft. Cyber-attack is also known as a computer network attack (CNA).

A successful cyber-attack can have several implications relevant to insurance: Loss of life, personal injury, pollution, loss of property, business interruption, loss of production, loss of data and loss of reputation. From a cargo perspective, there are in particular concerns related to the potential risks and implications of cyber-attacks directed at unmanned truck convoys and mega hubs.

In December 2016, the USCG published a cyber-security policy letter regarding the criteria and process for the reporting of suspicious activity and breach of security, and added cybersecurity to the list of security items covered by the 2002 Maritime Transportation Security Act (MTSA). This could also mean penalties of up to USD 25,000 per cyber preparedness violation.

[1] http://www.techopedia.com/definition/24748/cyberattack

1

https://iumi.com/document/view/3Cyber_risks__60ace8bd2358b.pdf

https://astaara.co.uk/wp-content/uploads/2020/09/Astaara-IMO-Cyber-Security-Regime.pdf

Документы, пока не выпущенные ИМО в виде циркуляров, однако рекомендованные ведущими судоходными компаниями мира

Название документа (оригинал)	Дата издания	Название документа в переводе
Code of Practice: Cyber security for ships The UK's IET Standards, submitted to the IMO https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice	13.09.2017 Сайт минтранса Великобритании	**Свод правил кибербезопасности для судов** Стандарты Инженерно-технологического института Великобритании, предложенные ИМО
Good practice guide: Cyber security for ports and port systems Developed by the UK's IET and submitted to the IMO https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice	27.01.2020 Сайт Минтранса Великобритании и сайты ведущих компаний мира	**Руководство по эффективной практике: Кибербезопасность портов и портовых систем** Разработано Инженерно-технологическим институтом Великобритании и предоставлено ИМО

Статьи докладчика по теме:

С.А.Семёнов. **Кибербезопасность морского и речного транспорта**//Транспорт Российской Федерации. – 2018. – 1 (74). – С. 43-46. (http://www.msecurity.ru/documents/view812/)

Семёнов С.А. **Морская кибербезопасность в России**//Транспорт Российской Федерации. – 2019. – 3 (82). – С. 11-14. (http://www.msecurity.ru/documents/view856/)

Семёнов С.А. **Морская кибербезопасность: новые угрозы и зарубежный опыт**//Транспорт Российской Федерации. – 2020. – 5 (90). – С. 9-12. (https://msecurity.ru/documents/view892/)

Сергей Семенов. **Морская кибербезопасность — ситуация, проблемы и риски**//Российский совет по международным делам : [сайт]. URL (https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/ , https://msecurity.ru/documents/view886/)

Сергей Семенов. **Нормативное регулирование морской кибербезопасности в США**//Российский совет по международным делам : [сайт]. URL (https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/normativnoe-regulirovanie-morskoy-kiberbezopasnosti-v-ssha/)

ISPS-Code

ФЕДЕРАЛЬНОЕ АГЕНТСТВО МОРСКОГО И РЕЧНОГО ТРАНСПОРТА

СЛУЖБА МОРСКОЙ БЕЗОПАСНОСТИ

Спасибо за внимание!

Доклады и презентации будут размещены на сайте http://www.msecurity.ruhttp://www.msecurity.ru в группах в Телеграмм https://t.me/transsecurity и в Вконтакте

m.cyber.security

trans.security