TEXNİKA ELMLƏRİ

TECHNICAL SCIENCES

DOI: https://doi.org/10.36719/2789-6919/57/167-173

Elnur Abbasov
Azərbaycan Dövlət Dəniz Akademiyası
texnika üzrə fəlsəfə doktoru
https://orcid.org/0009-0002-6687-6892
abbasovelnur1980@mail.ru
Fərman Nağıyev
Azərbaycan Dövlət Dəniz Akademiyası
magistrant
https://orcid.org/0009-0002-7627-828X
farman.nagiyev6613@gmail.com

Gəmilərin elektron idarəetmə və naviqasiya sistemlərində kibertəhlükəsizlik risklərinin təhlili

Xülasə

Müasir dəniz nəqliyyatında rəqəmsallaşma prosesinin sürətlənməsi gəmilərin elektron idarəetmə və naviqasiya sistemlərinin funksional imkanlarını əhəmiyyətli dərəcədə genişləndirmiş, eyni zamanda, bu sistemlərin kibertəhlükəsizlik baxımından həssaslığını artırmışdır. Təqdim olunan məqalədə gəmilərin naviqasiya, rabitə, mühərrik, radar və yük idarəetmə sistemlərində mövcud olan kibertəhlükəsizlik riskləri sistemli şəkildə təhlil edilmişdir.

Tədqiqatın əsas məqsədi dəniz nəqliyyatında istifadə olunan elektron idarəetmə və naviqasiya sistemlərinin – xüsusilə ECDIS, AIS, GPS, GMDSS, SCADA və avtomatik sükan idarəetmə sistemlərinin – kibertəhdidlərə qarşı zəif tərəflərini müəyyən etmək, bu riskləri strukturlaşdırılmış şəkildə təsnifləndirmək və onların azaldılması üçün effektiv müdafiə yanaşmaları təklif etməkdən ibarətdir.

Tədqiqat çərçivəsində keyfiyyət yönümlü metodologiyadan istifadə edilmiş, Beynəlxalq Dəniz Təşkilatı (IMO), BIMCO və digər beynəlxalq qurumların normativ sənədləri və tövsiyələri təhlil olunmuş, həmçinin, son illərdə dəniz nəqliyyatı sahəsində baş vermiş real kibertəhlükəsizlik insidentləri müqayisəli şəkildə araşdırılmışdır.

Aparılmış təhlillər göstərir ki, gəmilərin elektron idarəetmə sistemlərində kibertəhlükəsizlik risklərinin effektiv idarə olunması yalnız texniki tədbirlərlə məhdudlaşmır, eyni zamanda, təşkilati siyasətlərin formalaşdırılması, heyət hazırlığı və beynəlxalq standartlara uyğunluğun təmin edilməsi ilə kompleks şəkildə həyata keçirilməlidir. Məqalədə çoxqatlı müdafiə konsepsiyasına əsaslanan inteqrasiya olunmuş yanaşma çərçivəsində praktiki tövsiyələr irəli sürülmüşdür.

Açar sözlər: *kibertəhlükəsizlik, gəmi naviqasiyası, elektron idarəetmə sistemləri, ECDIS, AIS, SCADA, kiberrisklərin idarə olunması*

Elnur Abbasov
Azerbaijan State Marine Academy
PhD in Engineering
https://orcid.org/0009-0002-6687-6892
abbasovelnur1980@mail.ru
Farman Naghiyev
Azerbaijan State Marine Academy
Master's student
https://orcid.org/0009-0002-7627-828X
farman.nagiyev6613@gmail.com

Cybersecurity Risks in Electronic Control and Navigation Systems of Ships

Abstract

The acceleration of digitalization processes in modern maritime transport has significantly expanded the functional capabilities of electronic control and navigation systems on board ships, while simultaneously increasing their vulnerability to cybersecurity threats. This article presents a systematic analysis of cybersecurity risks associated with navigation, communication, engine, radar, and cargo management systems of vessels.

The primary objective of the study is to identify vulnerabilities in electronic control and navigation systems used in maritime transport – particularly ECDIS, AIS, GPS, GMDSS, SCADA, and automatic steering systems – to classify these risks in a structured manner, and to propose effective approaches for their mitigation.

Within the framework of the research, a qualitative methodology was employed. Normative documents and guidelines issued by international organizations, including the International Maritime Organization (IMO) and BIMCO, were analyzed. In addition, recent real-world cybersecurity incidents in the maritime sector were comparatively examined.

The results indicate that effective management of cybersecurity risks in shipboard electronic control systems cannot be limited to technical measures alone, but requires an integrated approach involving organizational policies, crew training, and compliance with international standards. The article proposes practical recommendations based on an integrated, multi-layered (defense-in-depth) cybersecurity approach.

Keywords: *Cybersecurity, ship navigation, electronic control systems, ECDIS, AIS, SCADA, cyber risk management*

Giriş

Dəniz nəqliyyatı qlobal ticarətin əsas hissəsini təmin edən strateji əhəmiyyətli logistika sistemi kimi çıxış edir. Son onilliklərdə gəmiçilik sahəsində baş verən texnoloji transformasiya nəticəsində ənənəvi mexaniki idarəetmə üsulları elektron idarəetmə və naviqasiya sistemləri ilə əvəz olunmuş, bu isə naviqasiya dəqiqliyinin artmasına və əməliyyat səmərəliliyinin yüksəlməsinə səbəb olmuşdur (Tam və Jones, 2019).

Bununla yanaşı, rəqəmsallaşma prosesi yeni kibertəhlükəsizlik risklərini də formalaşdırmışdır. Müasir gəmilərdə ECDIS, AIS, GPS, GMDSS, SCADA və avtomatik sükan sistemləri vahid rəqəmsal mühitdə inteqrasiya olunaraq fəaliyyət göstərir. Bu sistemlərin şəbəkə əlaqələri və xarici məlumat mənbələrindən asılılığı onların funksionallığını artırmaqla yanaşı, kibertəhdidlər üçün geniş hücum səthi yaradır (Meland və b., 2021).

Ənənəvi olaraq gəmilər "təcrid olunmuş sistemlər" kimi qəbul edilsə də, peyk rabitəsi və internet texnologiyalarının geniş tətbiqi bu yanaşmanı dəyişmiş, gəmiləri qlobal informasiya məkanının bir hissəsinə çevirmişdir. Nəticədə onların kibertəhlükələrə məruz qalma ehtimalı əhəmiyyətli dərəcədə artmışdır (Bothur və b., 2017).

Dənizçilik sektorunda kiberrisklərin real təsiri 2017-ci ildə Maersk şirkətinə qarşı həyata keçirilmiş kiberhücum zamanı aydın şəkildə özünü göstərmişdir. Bu hadisə nəticəsində qlobal logistika zəncirində ciddi fasilələr yaranmış və böyük maliyyə itkiləri baş vermişdir (Greenberg, 2018).

Beynəlxalq səviyyədə bu risklərin tənzimlənməsi məqsədilə IMO tərəfindən qəbul edilmiş MSC.428(98) qətnaməsi kiberrisklərin təhlükəsizlik idarəetmə sistemlərinə inteqrasiyasını tələb edir (IMO, 2017). Bununla belə, praktikada bu tələblərin tətbiqi hələ də tam səviyyədə təmin olunmamışdır.

Bu baxımdan, gəmilərin elektron idarəetmə və naviqasiya sistemlərində kibertəhlükəsizlik risklərinin sistemli təhlili aktual elmi problem kimi çıxış edir. Məqalənin məqsədi bu sistemlərdə

mövcud kiberriskləri sistemləşdirmək, onların yaranma mexanizmlərini və təsirlərini təhlil etmək, həmçinin, risklərin azaldılması üçün kompleks müdafiə yanaşmaları təklif etməkdir.

Tədqiqat

Məqalədə gəmilərin elektron idarəetmə və naviqasiya sistemlərinə olan kiber risklər aşağıdakı kimi təhlil olunmuşdur:

Elektron idarəetmə və naviqasiya sistemlərinin ümumi xarakteristikası. Müasir gəmilərdə elektron idarəetmə və naviqasiya sistemləri funksional təyinatına görə bir neçə əsas kateqoriyaya bölünür və əksər hallarda inteqrasiya olunmuş şəkildə fəaliyyət göstərərək vahid rəqəmsal idarəetmə mühiti formalaşdırır. Bu inteqrasiya əməliyyat səmərəliliyini artırmaqla yanaşı, sistemlərarası asılılığı gücləndirir və kibertəhlükəsizlik baxımından kompleks risklər yaradır.

Naviqasiya sistemlərinə GPS, ECDIS, radar və ARPA daxildir və gəminin mövqeyinin müəyyən edilməsi və qərarvermə prosesində əsas rol oynayır (Weintrit, 2009). Rabitə sistemləri (GMDSS, Inmarsat, VSAT, VHF/UHF, NAVTEX) isə gəminin digər obyektlərlə fasiləsiz əlaqəsini təmin edir. AIS və LRIT sistemləri gəmi hərəkətinin monitorinqi və identifikasiyası üçün istifadə olunur.

SCADA və digər idarəetmə sistemləri gəminin mühərrik və enerji proseslərini idarə edir, yük və ballast sistemləri isə gəminin dayanıqlığını təmin edən əsas texnoloji komponentlərdir. Avtomatik sükan sistemi (autopilot) isə naviqasiya məlumatlarına əsaslanaraq kursun avtomatik tənzimlənməsini həyata keçirir.

Bu sistemlərin ümumi xüsusiyyətləri onların proqram təminatına əsaslanması, şəbəkə bağlantısına malik olması və xarici məlumat mənbələrindən asılılığıdır ki, bu da onları kibertəhlükələr baxımından potensial hədəfə çevirir.

Kibertəhlükəsizlik risklərinin təsnifatı. Gəmilərin elektron idarəetmə və naviqasiya sistemlərində kibertəhlükəsizlik riskləri əsasən təhdid mənbələrinə və hücum vektorlarına görə təsnif olunur.

Şəkil 1. Gəminin elektron idarəetmə və naviqasiya sistemlərinin inteqrasiya olunmuş strukturu

Təhdid mənbələrinə görə risklər. Kibertəhdidlər mənşəyinə görə daxili və xarici olmaqla iki əsas qrupa bölünür. Xarici təhdidlər dövlət dəstəkli hücumlar, mütəşəkkil cinayət qrupları və kiberhücumçular tərəfindən həyata keçirilir və yüksək texniki imkanlara malik olduqları üçün daha təhlükəli hesab olunur. Məsələn, GPS siqnallarının manipulyasiyası bu tip müdaxilələrin mümkünlüyünü göstərir (Bhatti və Humphreys, 2017).

Daxili təhdidlər isə əsasən insan amili ilə bağlıdır və zəif parollar, zərərli faylların açılması və ya xarici daşıyıcıların istifadəsi kimi hallar nəticəsində yaranır. Tədqiqatlar göstərir ki, kibertəhlükəsizlik insidentlərinin əhəmiyyətli hissəsi məhz insan səhvləri ilə bağlıdır (BIMCO, 2020).

Əsas sistemlərdə kiberrisklər.

ECDIS. ECDIS sistemləri kommersiya tipli əməliyyat sistemləri üzərində işlədiyindən zərərli proqramlara qarşı həssasdır. Elektron xəritələrin USB vasitəsilə yenilənməsi və digər sistemlərlə inteqrasiya bu riskləri artırır. Tədqiqatlar göstərir ki, bəzi hallarda sistemə uzaqdan müdaxilə və məlumatların dəyişdirilməsi mümkündür (Svilicic və b., 2019).

AIS. AIS sistemində məlumatların şifrələnməməsi və autentifikasiyanın olmaması spoofing, jamming və məlumat manipulyasiyası kimi hücumlara şərait yaradır. Bu isə "xəyali hədəflərin" yaranmasına və toqquşma riskinin artmasına səbəb ola bilər (Balduzzi və b., 2014).

GPS. GPS sistemləri açıq siqnal strukturu səbəbindən spoofing hücumlarına həssasdır. Siqnal manipulyasiyası nəticəsində gəminin mövqeyi təhrif edilə bilər ki, bu da ciddi naviqasiya riskləri yaradır (Bhatti və Humphreys, 2017).

SCADA və mühərrik sistemləri. Bu sistemlərdə şifrələmənin zəifliyi, IT/OT inteqrasiyası və köhnəlmiş kontrollerlərin istifadəsi hücum səthini genişləndirir. Nəticədə idarəetmə siqnallarının dəyişdirilməsi və sistemlərin sıradan çıxarılması kimi kritik nəticələr mümkündür (Kavallieratos və b., 2020).

GMDSS və rabitə sistemləri. Bu sistemlərdə kibermüdaxilə saxta distress siqnallarının göndərilməsi, real siqnalların bloklanması və rabitənin pozulması ilə nəticələnə bilər ki, bu da birbaşa insan həyatına təhlükə yaradır.

Hücum vektorlarına görə risklər. Kibertəhlükələr şəbəkə, fiziki giriş, siqnal manipulyasiyası və proqram təminatı zəiflikləri vasitəsilə həyata keçirilir. Xüsusilə VSAT əsaslı şəbəkə hücumları, GPS/AIS spoofing və köhnəlmiş proqram təminatı bu baxımdan əsas risk mənbələri hesab olunur (Pavur və b., 2020).

Real kibertəhlükəsizlik insidentlərinin təhlili. Son illərdə baş vermiş kibertəhlükəsizlik insidentləri göstərir ki, dəniz nəqliyyatında kiberrisklər real və ciddi nəticələr doğuran təhlükələrdir.

Maersk – NotPetya hücumu (2017). Bu hücum nəticəsində şirkətin 49.000-dən çox kompüteri və 3.500 serveri sıradan çıxmış, 76 limanın 17-də əməliyyatlar dayandırılmış və bərpa prosesi təxminən 10 gün davam etmişdir. Ümumi zərər 250–300 milyon ABŞ dolları təşkil etmişdir (Greenberg, 2018). Bu hadisə kibertəhlükələrin qlobal logistika zəncirinə birbaşa təsirini nümayiş etdirir.

COSCO hücumu (2018). Hücum nəticəsində kommunikasiya sistemləri sıradan çıxmış, əlaqə kanalları məhdudlaşmış və əməliyyat koordinasiyası pozulmuşdur.

Qara dənizdə GPS spoofing hadisələri (2017–2018). Bu hadisələr zamanı gəmilərin faktiki mövqeyi ilə naviqasiya sistemlərində göstərilən koordinatlar arasında uyğunsuzluq yaranmış, bu isə səhv qərarvermə və qəza risklərinin artmasına səbəb olmuşdur (Tam və Jones, 2019).

Antverpen limanı insidenti (2011–2013). Kibermüdaxilə nəticəsində konteyner məlumatları manipulyasiya olunmuş və logistika sistemləri qeyri-qanuni məqsədlər üçün istifadə edilmişdir.

Aparılmış təhlil göstərir ki, kibertəhlükələr texniki, iqtisadi və əməliyyat səviyyələrində çoxşaxəli təsirə malikdir, sistemlərarası inteqrasiya isə risklərin miqyasını artırır. Xüsusilə naviqasiya sistemlərinə müdaxilə birbaşa qəza riskinə gətirib çıxara bilər.

Şəkil 2. Gəmi sistemlərinə qarşı kibertəhdidlərin və hücum vektorlarının modeli

Beynəlxalq tənzimləmə çərçivəsi. Dənizçilik sektorunda kibertəhlükəsizliyin tənzimlənməsi beynəlxalq standartlara əsaslanır. IMO-nun MSC.428(98) qətnaməsi kiberrisklərin ISM Code çərçivəsində təhlükəsizlik idarəetmə sistemlərinə inteqrasiyasını tələb edir (IMO, 2017). MSC-FAL.1/Circ.3 sənədi isə risklərin idarə olunmasını Identify–Protect–Detect–Respond–Recover mərhələləri üzrə müəyyən edir və NIST yanaşması ilə uyğunluq təşkil edir. BIMCO təlimatları praktik tövsiyələr təqdim edir, IACS (UR E26/E27) tələbləri isə gəmi sistemlərinin kiberdavamlılığını təmin etməyə yönəlmişdir.

Kiberrisklərin azaldılması strategiyaları. Gəmi sistemlərində kibertəhlükəsizliyin təmin olunması texniki, təşkilati və insan amilini birləşdirən çoxqatlı yanaşma tələb edir.

Texniki tədbirlər şəbəkə seqmentasiyası, şifrələmə və autentifikasiya, proqram təminatının müntəzəm yenilənməsi, IDS/IPS sistemlərinin tətbiqi və ehtiyat nüsxələmə mexanizmlərini əhatə

edir. Xüsusilə IT və OT şəbəkələrinin ayrılması və köhnəlmiş sistemlərin yenilənməsi risklərin azaldılmasında mühüm rol oynayır.

Təşkilati tədbirlər kiberrisklərin idarə olunması planının hazırlanmasını və onun təhlükəsizlik idarəetmə sistemlərinə inteqrasiyasını nəzərdə tutur. Bu plan risklərin müəyyənləşdirilməsi, qiymətləndirilməsi, cavablandırılması və bərpası mərhələlərini əhatə etməlidir.

İnsan amili baxımından isə heyətin müntəzəm təlimi, kibergigiyena qaydalarına riayət olunması və təhlükəsizlik mədəniyyətinin formalaşdırılması əsas şərtlərdən biridir.

Təchizat zənciri təhlükəsizliyi və insidentlərə cavab. Gəmi sistemləri üçün proqram təminatı və avadanlıq təmin edən təchizatçıların kibertəhlükəsizlik standartlarına uyğunluğu əvvəlcədən yoxlanılmalı, üçüncü tərəf xidmət təminatçılarının sistemlərə çıxışı ciddi nəzarət altında saxlanılmalıdır. Uzaqdan giriş yalnız zəruri hallarda və təhlükəsiz kanallar vasitəsilə təmin edilməlidir.

Kibertəhlükəsizlik insidentlərinə cavab prosedurları əvvəlcədən müəyyən edilməli və aşkarlama, təcridetmə, aradan qaldırma, bərpa və hesabatlandırma mərhələlərini əhatə etməlidir. Bu prosedurların effektivliyi müntəzəm təlimlər və ssenari əsaslı simulyasiyalar vasitəsilə yoxlanılmalıdır.

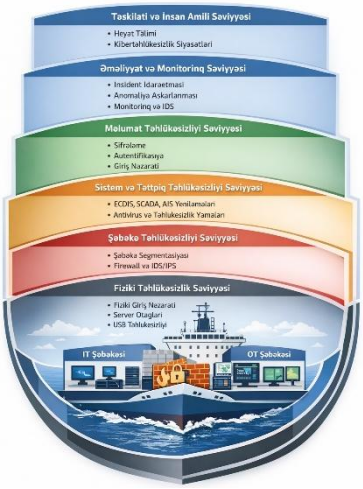
İnsan amili ilə bağlı tədbirlər. Gəmi heyətinin kibertəhlükəsizlik üzrə müntəzəm təlimi kiberrisklərin azaldılmasında mühüm rol oynayır. Bu təlimlər təhlükəsiz parol siyasəti, fişinq hücumlarının tanınması və şübhəli fəaliyyətlərin bildirilməsi kimi əsas davranış qaydalarını əhatə etməlidir (Tam və Jones, 2019).

Kibertəhlükəsizlik mədəniyyətinin formalaşdırılması bütün heyətin kollektiv məsuliyyəti kimi qəbul edilməli, gündəlik əməliyyatlarda kibergigiyena qaydalarına riayət olunmalıdır.

Gələcək perspektivlər və yeni risklər. Dənizçilik sənayesində rəqəmsallaşmanın dərinləşməsi yeni texnologiyaların tətbiqi ilə yanaşı, daha mürəkkəb kiberrisklərin formalaşmasına səbəb olur.

Avtonom gəmilərin inkişafı insan müdaxiləsinin azalması ilə kibermüdaxilələrin nəticələrini daha kritik edir və kiberdavamlılığın layihələndirmə mərhələsindən təmin olunmasını zəruri edir. Süni intellekt texnologiyaları isə həm anomaliyaların aşkarlanması baxımından effektiv vasitə olmaqla yanaşı, daha mürəkkəb kiberhücumların yaradılmasına da imkan verir.

IoT qurğularının geniş tətbiqi əməliyyat səmərəliliyini artırsa da, əlavə hücum nöqtələri formalaşdıraraq təhlükəsizlik risklərini genişləndirir. Blokçeyn texnologiyası isə məlumatların bütövlüyünün qorunması və təchizat zəncirinin izlənməsi baxımından perspektivli hesab olunur, lakin praktik tətbiqi hələ məhduddur.



Şəkil 3. Gəmi sistemlərində çoxqatlı kibertəhlükəsizlik müdafiə modeli

Azərbaycanın dəniz sektorunda kibertəhlükəsizlik məsələləri. Azərbaycan Xəzər dənizində mühüm nəqliyyat-logistika mövqeyinə malik olmaqla, xüsusilə Bakı Beynəlxalq Dəniz Ticarət Limanı vasitəsilə Orta Dəhliz çərçivəsində strateji tranzit rolunu yerinə yetirir. Dəniz daşımalarının

intensivləşməsi və infrastrukturun rəqəmsallaşması kibertəhlükəsizlik məsələlərinin milli səviyyədə aktuallaşmasına səbəb olur.

Xəzər dənizində gəmi hərəkətinin artması və idarəetmə sistemlərinin şəbəkələşməsi kiberrisklərin sistemli idarə olunmasını zəruri edir. Xüsusilə ASCO donanmasında istifadə olunan elektron naviqasiya və idarəetmə sistemlərinin qorunması nəqliyyat təhlükəsizliyi və milli maraqlar baxımından mühüm əhəmiyyət kəsb edir. Bu baxımdan milli kibertəhlükəsizlik strategiyasının formalaşdırılması, kadr hazırlığının gücləndirilməsi və normativ bazanın təkmilləşdirilməsi prioritet istiqamətlərdir.

Nəticə

Aparılmış təhlillər göstərir ki, gəmilərin elektron idarəetmə və naviqasiya sistemləri (ECDIS, AIS, GPS, SCADA, GMDSS və s.) kibermüdaxilələrə qarşı yüksək həssaslığa malikdir və bu həssaslıq həm texnoloji arxitektura, həm də istismar xüsusiyyətləri ilə bağlıdır.

Müəyyən edilmişdir ki, real kibertəhlükəsizlik insidentləri bu risklərin praktik xarakter daşıdığını təsdiqləyir və onların təsiri yalnız texniki səviyyə ilə məhdudlaşmayaraq logistika zəncirinə, iqtisadi sabitliyə və naviqasiya təhlükəsizliyinə birbaşa təsir göstərir.

Təhlil nəticəsində müəyyən olunmuşdur ki, kiberrisklərin effektiv idarə olunması yalnız texniki tədbirlərlə mümkün deyil və çoxqatlı yanaşma tələb edir. Bu yanaşma texniki həlləri, təşkilati idarəetmə mexanizmlərini və insan amilini birləşdirən kompleks model kimi çıxış edir.

Beynəlxalq təcrübə göstərir ki, mövcud normativ çərçivə (IMO və digər təşkilatların tələbləri) kibertəhlükəsizliyin idarə olunması üçün əsas baza yaratsa da, texnoloji inkişafın sürəti yeni risklərin tam əhatə olunmasını çətinləşdirir.

Azərbaycan kontekstində isə dəniz nəqliyyatının inkişafı və tranzit rolunun artması milli dəniz infrastrukturunun kiberdavamlılığının gücləndirilməsini zəruri edir. Bu istiqamətdə strateji yanaşmanın formalaşdırılması və beynəlxalq əməkdaşlığın genişləndirilməsi mühüm əhəmiyyət kəsb edir.

Beləliklə, kibertəhlükəsizlik dəniz nəqliyyatının təhlükəsiz və dayanıqlı inkişafını müəyyən edən əsas amillərdən biri kimi çıxış edir və onun təmin olunması kompleks, risk əsaslı idarəetmə yanaşmasını tələb edir.

Gələcək tədqiqat istiqamətləri. Gələcək tədqiqatlar üçün avtonom gəmilərdə kibertəhlükəsizlik arxitekturalarının işlənməsi, süni intellekt əsaslı anomaliya aşkarlama sistemlərinin tətbiqi və regional kibertəhlükəsizlik əməkdaşlığı modellərinin araşdırılması perspektivli hesab olunur.

Ədəbiyyat

1. Balduzzi, M., Wilhoit, K. və Pasta, A. (2014). A security evaluation of AIS automated identification system. *Proceedings of the 30th Annual Computer Security Applications Conference*, 19–29. https://doi.org/10.1145/2664243.2664257
2. Bhatti, J. və Humphreys, T. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. *NAVIGATION: Journal of the Institute of Navigation*, *64*(1), 51–66. https://doi.org/10.1002/navi.183
3. BIMCO. (2020). *The guidelines on cyber security onboard ships* (Version 4). BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, IUMI, World Shipping Council.
4. Bothur, D., Zheng, G. və Valli, C. (2017). A critical analysis of security vulnerabilities and countermeasures in a smart ship system. *Australian Information Security Management Conference*, 81–89. https://doi.org/10.4225/75/5a84f7b1b3540
5. Greenberg, A. (2018). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.
6. IMO. (2017). *Maritime cyber risk management in safety management systems – Resolution MSC.428(98)*. International Maritime Organization.

7. Kavallieratos, G., Katsikas, S. və Gkioulos, V. (2020). Cybersecurity and Safety Co-Engineering of Cyberphysical Systems – a Comprehensive Survey. *Future Internet*, *12*(4), 65. https://doi.org/10.3390/fi12040065
8. Meland, P., Bernsmed, K., Wille, E., Rødseth, Ø. və Nesheim, D. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(2), 263–272. https://doi.org/10.12716/1001.15.02.04
9. Pavur, J., Moser, D., Strohmeier, M., Lenders, V. və Martinovic, I. (2020). A tale of sea and sky: On the security of maritime VSAT communications. *2020 IEEE Symposium on Security and Privacy*, 1384–1400. https://doi.org/10.1109/SP40000.2020.00056
10. Svilicic, B., Kamahara, J., Rooks, M. və Yano, Y. (2019). Maritime cyber risk management: An experimental ship assessment. *The Journal of Navigation*, *72*(5), 1108–1120. https://doi.org/10.1017/S0373463318001157
11. Tam, K. və Jones, K. (2019). Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *4*(2), 147–164. https://doi.org/10.1080/23738871.2019.1596644
12. Weintrit, A. (2009). *The Electronic Chart Display and Information System (ECDIS): An operational handbook*. CRC Press.
13. Zăgan, R., Raicu, G., Hanzu-Pazara, R. və Enache, S. (2020). Realities in maritime domain regarding cyber security concept. *Advanced Engineering Forum*, *34*, 101–110. https://doi.org/10.4028/www.scientific.net/AEF.34.101

Daxil oldu: 02.01.2026
Qəbul edildi: 13.04.2026