O bezpieczeństwie żeglugi, w tym bezpieczeństwie cybernetycznym, mówi Dariusz Rudziński, członek Zarządu PRS S.A.

Bezpieczeństwo cybernetyczne jako element bezpieczeństwa na morzu

Branża morska, jak żadna inna gałąź światowej gospodarki, może pochwalić się posiadaniem dedykowanej jej agendy Narodów Zjednoczonych, jaką jest Międzynarodowa Organizacja Morska (IMO), mająca siedzibę w Londynie. W ubiegłym roku obchodziliśmy 70-lecie powstania Organizacji.

IMO zajmuje się ustalaniem standardów bezpieczeństwa na morzu w skali globalnej. Jednymi z najlepiej znanych konwencji IMO, spośród kilkudziesięciu, są SOLAS, MARPOL, LL.

W skali regionalnej standardy bezpieczeństwa ustanawia Wspólnota Europejska, np. dyrektywa 2009/45/WE w sprawie bezpieczeństwa statków pasażerskich. Na szczeblu krajowym ustala je Administracja morska, w odniesieniu do zagadnień, które nie są uregulowane międzynarodowymi wymaganiami.

W światowy system zapewnienia bezpieczeństwa na morzu wpisują się również towarzystwa klasyfikacyjne, które opracowują standardy bezpieczeństwa dotyczące konstrukcji kadłubów i ich wyposażenia, urządzeń maszynowych, instalacji elektrycznych, itp. Towarzystwa klasyfikacyjne działają również z upoważnienia Administracji morskich, w których imieniu - poprzez system okresowych i doraźnych inspekcji i audytów - kontrolują na statkach wdrożenie wymagań międzynarodowych i krajowych.

W pierwszej połowie lat 90-tych XX w. IMO uchwaliło tekst Kodeksu ISM (ang. International Safety Management Code – Międzynarodowy kodeks zarządzania bezpieczną eksploatacją statków i zapobieganiem zanieczyszczaniu lub Międzynarodowy kodeks zarządzania bezpieczeństwem). Kodeks ISM, uchwalony przez IMO Rezolucją A741(18), zaczął obowiązywać z chwilą wejścia w życie 1 lipca 1998 rozdziału IX konwencji SOLAS, dotyczącego zarządzania bezpieczną eksploatacją statków.

Kodeks ISM jest pierwszym w historii żeglugi formalnym, obowiązkowym standardem zarządzania bezpieczeństwem. Jego stworzenie miało na celu m.in. całkowitą lub przynajmniej częściową eliminację błędów ludzkich, które są najczęstszą przyczyną katastrof morskich. Błędom tym zapobiega się poprzez opracowanie i wdrożenie w każdym przedsiębiorstwie żeglugowym i na statkach Systemu Zarządzania Bezpieczeństwem zgodnego z wymaganiami Kodeksu ISM. Za opracowanie, wdrożenie i utrzymanie systemu odpowiedzialny jest armator. ISM tradycyjnie dotyczył zarządzania bezpieczeństwem operacji fizycznie realizowanych.

Polski Rejestr Statków S.A.
al. gen. Józefa Hallera 126
80-416 Gdańsk, Polska
Tel. (+48) 58 75 11 301
Fax (+48) 58 34 60 392
E-mail: mailbox@prs.pl
https://www.prs.pl

Zarejestrowany w:
Sąd Rejonowy Gdańsk-Północ w Gdańsku
VII Wydział Gospodarczy KRS
KRS nr 0000019880
NIP: 584- 030-44-72
Kapitał zakładowy i wpłacony 8 000 000 PLN

Konta bankowe:
PLN: BIGBPLPW; PL61 1160 2202 0000 0000 6189 6958
EUR: BIGBPLPW; PL20 1160 2202 0000 0003 1549 9928
USD: BIGBPLPW; PL86 1160 2202 0000 0003 1550 0777
GBP: BIGBPLPW; PL63 1160 2202 0000 0003 1550 1385

Wraz z postępem technologicznym, który sprawił, że statki wyposażane są w coraz bardziej skomplikowane systemy informatyczne, bezpośrednio oddziałujące na wszystkie istotne funkcje, które statki jako obiekty techniczne realizują, zaistniała potrzeba systemowego podejścia do zagrożeń cybernetycznych. Mówiąc obrazowo, część operacji ze świata realnego przeniosła się do świata wirtualnego.

Kwestie zarządzania ryzykiem związanym z zagrożeniami cybernetycznymi zostały podjęte przez Międzynarodową Organizację Morską IMO. Dwa stałe komitety tej organizacji, tj. Komitet Bezpieczeństwa na Morzu (MSC) i Komitet Ułatwień w Obrocie Morskim (FAL), w lipcu 2017 wydały wytyczne dotyczące Maritime Cyber Risk Management (MSC-FAL. 1/Circ.3). Ich znaczenie zostało podkreślone w Rezolucji MSC.428(98), która zachęca Administracje morskie do podjęcia działań w ramach Kodeksu ISM zmierzających do zapewnienia, że zagrożenia cybernetyczne zostały uwzględnione w systemach zarządzania firm armatorskich i zweryfikowane w czasie pierwszego audytu przypadającego po dniu 1 stycznia 2021.

Wytyczne IMO wskazują na systemy statkowe, które mają krytyczne znaczenia dla bezpieczeństwa lub ochrony i mogą być podatne na zagrożenia cybernetyczne. Są to:

- systemy mostka nawigacyjnego,
- systemy przeładunkowe,
- systemy napędowe i maszynowe oraz sterowania nimi,
- systemy kontroli dostępu,
- systemy obsługi pasażerów,
- systemy komunikacyjne.

Oczywiście powyższa lista nie jest kompletna i może się rozszerzać wraz z pojawianiem się i aplikacją nowych technologii.

Wytyczne zachęcają do tego, aby efektywne zarządzanie zagrożeniami cybernetycznymi rozpoczynać od poziomu najwyższego kierownictwa firm armatorskich. Zarządzający powinni zachować świadomość istnienia zagrożeń cybernetycznych na wszystkich poziomach kierowania w ich firmach. Ocena powinna mieć całościowy charakter, a zarządzanie zagrożeniami być nacechowane elastycznością i nieustanną analizą informacji zwrotnych.

Wytyczne wskazują również kilka elementów funkcjonalnych, które wspierają proces efektywnego zarządzania zagrożeniami cybernetycznymi:

Polski Rejestr Statków S.A.
al. gen. Józefa Hallera 126
80-416 Gdańsk, Polska
Tel. (+48) 58 75 11 301
Fax (+48) 58 34 60 392
E-mail: mailbox@prs.pl
https://www.prs.pl

Zarejestrowany w:
Sąd Rejonowy Gdańsk-Północ w Gdańsku
VII Wydział Gospodarczy KRS
KRS nr 0000019880
NIP: 584- 030-44-72
Kapitał zakładowy i wpłacony 8 000 000 PLN

Konta bankowe:
PLN: BIGBPLPW; PL61 1160 2202 0000 0000 6189 6958
EUR: BIGBPLPW; PL20 1160 2202 0000 0003 1549 9928
USD: BIGBPLPW; PL86 1160 2202 0000 0003 1550 0777
GBP: BIGBPLPW; PL63 1160 2202 0000 0003 1550 1385

- Identyfikacja: należy określić personel i przypisać zakresy odpowiedzialności w związku z zagrożeniami cybernetycznymi, a także zidentyfikować systemy, aktywa, dane, które w przypadku zakłóceń będą zagrożeniem dla bezpiecznej eksploatacji statku.
- Ochrona: należy wdrożyć proces kontroli i pomiaru zagrożeń oraz przygotować plan awaryjny w celu ochrony przed nimi.
- Wykrywanie: należy opracować działania niezbędne do wczesnego wykrycia incydentów cybernetycznych.
- Odpowiedź: należy opracować działania i plany w celu zapewnienia odporności lub przywrócenia funkcjonowania systemów niezbędnych do prowadzenia operacji żeglugowych, które zostały nadwyrężone w wyniku incydentu cybernetycznego.
- Odzyskanie: należy zidentyfikować środki do tworzenia kopii zapasowych i przywracania systemów dotkniętych incydentem cybernetycznym.

Powyższe aspekty należy rozpatrywać równocześnie i w sposób ciągły, tak aby na stałe wpasowały się w ramy systemu zarządzania ryzykiem cybernetycznym.

Warto również wskazać, że oprócz IMO wytyczne w sprawie bezpieczeństwa cybernetycznego na statkach przygotowały inne organizacje i stowarzyszenia z branży morskiej, np. BIMCO, Międzynarodowa Izba Żeglugowa (ICS), stowarzyszenia armatorskie: CLIA, INTERCARGO i INTERTANKO, morski przemysł wydobywczy (OCIMF), a także ubezpieczyciele (IUMI). Tak szerokie podejście do problemu bezpieczeństwa cybernetycznego świadczy o tym, że branża rozumie zagrożenia, jakie niesie ze sobą postęp technologiczny.

Towarzystwa klasyfikacyjne w coraz większym stopniu koncentrują się na niezawodności i wydajności operacyjnej systemów komputerowych istotnych dla bezpieczeństwa statku. W tym celu klasyfikatorzy rozwijają wymagania swoich przepisów dotyczących układów automatyki. Dominuje pogląd, że obecnie systemy cybernetyczne są tak samo ważne dla bezpieczeństwa statku, jak jego integralny kadłub czy sprawne urządzenia maszynowe. Uznając wagę kwestii bezpieczeństwa cybernetycznego, towarzystwa klasyfikacyjne zrzeszone w Międzynarodowym Stowarzyszeniu Towarzystw Klasyfikacyjnych IACS, w tym Polski Rejestr Statków, przygotowały 12 zaleceń, które są krokiem w kierunku wypracowania wspólnych praktycznych rozwiązań na rzecz operacyjnego bezpieczeństwa statków i uzyskania zgodności z wymaganiami Kodeksu ISM. Kolejne działania IACS będą podejmowane ze świadomością potrzeby stworzenia pewnego rygoru przepisowego

a zarazem z przekonaniem, że nieuzasadnione wymagania mogą doprowadzić zainteresowane strony do takiej alokacji środków, która nie będzie optymalna dla uzyskania koniecznego poziomu bezpieczeństwa. Mając powyższe na uwadze, IACS będzie szeroko konsultował swoje prace z branżą morską przed wdrażaniem wymagań w zakresie bezpieczeństwa cybernetycznego. Doprowadzi to do uzyskania wyników w postaci:

- zapewnienia środków wspierających uzyskanie odporności na incydenty cybernetyczne,
- stworzenia rozwiązań prewencyjnych, które wzmocnią ochronę statków przed celowymi lub incydentalnymi zagrożeniami cybernetycznymi,
- określenia kryteriów do projektowania i weryfikacji, które branża morska wykorzysta jako podstawę do przeciwdziałania zagrożeniom cybernetycznym.

Polski Rejestr Statków S.A.
al. gen. Józefa Hallera 126
80-416 Gdańsk, Polska
Tel. (+48) 58 75 11 301
Fax (+48) 58 34 60 392
E-mail: mailbox@prs.pl
https://www.prs.pl

Zarejestrowany w:
Sąd Rejonowy Gdańsk-Północ w Gdańsku
VII Wydział Gospodarczy KRS
KRS nr 0000019880
NIP: 584- 030-44-72
Kapitał zakładowy i wpłacony 8 000 000 PLN

Konta bankowe:
PLN: BIGBPLPW; PL61 1160 2202 0000 0000 6189 6958
EUR: BIGBPLPW; PL20 1160 2202 0000 0003 1549 9928
USD: BIGBPLPW; PL86 1160 2202 0000 0003 1550 0777
GBP: BIGBPLPW; PL63 1160 2202 0000 0003 1550 1385