Задължително управление на киберриска за корабите и компаниите

ЗАДЪЛЖИТЕЛНО УПРАВЛЕНИЕ НА КИБЕРРИСКА, НЕ ПО-КЪСНО ОТ ПЪРВИЯ ГОДИШЕН ПРЕГЛЕД ЗА ЗАВЕРКА НА ДОКУМЕНТА ЗА СЪОТВЕТСТВИЕ НА КОМПАНИЯТА СЛЕД 01.01.2021Г.

Съгласно Резолюция MSC.428(98) *Maritime Cyber Risk Management in Safety Management Systems*, компаниите трябва да внедрят управление на киберриска не по-късно от първия годишен преглед за заверка на Документа за съответствие с изискванията на Международния кодекс за управление на безопасната експлоатация на кораби и предотвратяване на замърсяването *(ISM Code)* след 01.01.2021г. След тази дата компаниите трябва ефективно да управляват киберриска изпълнявайки целите и функционалните изисквания на ISM кодекса.

MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management дава важни препоръки относно елементите и правилния подход при внедряване на управлението на киберриска в Системата за управление на безопасната експлоатация на кораби и предпазване от замърсяване (за по-кратко Система за Управление на Безопасността на Корабите (СУБК)).

С цел да предложат на компаниите начин, по който да имплементират ефективно управление на киберриска на борда на корабите, световно признатите морски организации ICS, BIMCO, InterManager, INTERCARGO, INTERTANKO, IUMI, OCIMF и WSC публикуваха съвместно Насоки за киберсигурност на борда на корабите *(Guidelines on Cyber Security Onboard Ships)*, съгласно които управлението на киберриска трябва:

- Да определи ролята и отговорностите на потребителите, ключовия персонал и ръководството на брега и на кораба
- Определи системите, активите, данните и функциите, нарушаването на които може да представлява риск за експлоатацията и безопасността на кораба
- Предвиди технически мерки и процедури за предотвратяване на киберинциденти и осигуряване на непрекъсната експлоатация
- Имплементира мерки за готовност за справяне с киберинциденти

Някои аспекти от управлението на киберриска могат да включват чувствителна за компанията или конфиденциална информация. Тази информация трябва да бъде защитена по подходящ начин и не следва да бъде включена в СУБК.

В съответствие с глава 8 от Международния кодекс за сигурност на корабите и пристанищните съоръжения, *(ISPS Code)*, трябва да се извърши оценка на сигурността на кораба, която изисква определяне и оценка на ключовите операции на борда и свързаните с тях потенциални заплахи. Съгласно част В, параграф 8.3.5 от *ISPS Code*, оценката трябва да включва радио и телекомуникационните системи, включително компютърните системи и мрежи. Това може да наложи в Корабния План за Сигурност (КПС) да бъдат добавени подходящи мерки за защита както на оборудването, така и на комуникационните връзки. Поради ускореното развитие и появата на нови цифрови системи, е препоръчително това да стане чрез препратки към СУБК, за да се осигури бързо актуализиране при необходимост.

Термини

IT системи – Information technology systems са системите предназначени основно за обработка на данни и информация, включително софтуер, хардуер и технологии за комуникация, например компютри, електронни ръководства, мрежи и приложения.

OT системи – Operational technology systems са системите използващи данни за да управляват или контролират физически процеси. Това е хардуерът и софтуерът, който директно управлява или контролира физически устройства или процеси, например управление на двигатели, ECDIS, системи за измерване и контрол, програмируеми логически контролери.

Критични системи – са тези OT, IT системи, софтуер и данни, чието неналичие или внезапно излизане от строя, може да доведе до опасна ситуация.

Изисквания и насоки

Изискване: MSC-FAL.1/Circ.3 – Определете задълженията и отговорностите

Изискване: ISM 2.1 Компанията трябва да създаде политика за безопасност и опазване на околната среда, която да посочва как могат да бъдат постигнати целите, дадени в чл. 1.2.

Насоки: Актуализирайте политиката по безопасност, като се адресира риска от киберзаплахи

Актуализираната политика по безопасност трябва да демонстрира:

- Ангажимент за управление на киберрисковете като част от цялостния подход за управление на безопасността (включително културата на безопасност) и опазването на околната среда;
- Разбиране, че управлението на киберриска засяга аспектите, както по отношение на сигурността, така и на безопасността, но акцентът е върху управлението на рисковете за безопасността породени от OT и IT мрежите;
- Разбиране, че без подходящи технически мерки и процедури за защита и контрол на риска, OT системите са уязвими по отношение на безопасната експлоатация на кораба и опазването на околната среда.

Нищо в политиката не трябва да създава впечатление, че управлението на киберриска е с по-голям приоритет от всеки друг установен от компанията риск.

Изискване: ISM 3.2 Компанията трябва да определи и документира отговорностите, правомощията и взаимоотношенията между персонала, който управлява, изпълнява и проверява работата, свързана и оказваща влияние върху безопасността и предотвратяването на замърсяване.

Насоки: Актуализирайте отговорностите и правомощията, като определите подходящи такива за управление на киберриска.

Като цяло IT персоналът трябва да разбира потенциалните уязвимости в компютърно базираните системи и да знае подходящите технически мерки и процедури за защита, за да се гарантира наличието и целостта на системите и данните. Корабните оператори и техническият персонал трябва да разбират въздействието на нарушената работата на критичните системи на борда на корабите върху безопасността и околната среда и са отговорни за прилагането на СУБК.

Определянето на отговорностите и правомощията трябва да включва:

- Определяне на правомощия и отговорности, които насърчават сътрудничеството между IT персонала и корабните оператори и техническият персонал на компанията;
- Добавяне на съответствие с политиките и процедурите за управление на киберриска към съществуващите правомощия и отговорности на капитана;

Изискване: ISM 6.5 Компанията трябва да разработи и поддържа процедури за определяне на всякакъв вид обучение, което може да се наложи във връзка със системата за управление на безопасната експлоатация на кораби и предотвратяване на замърсяване, и да осигурява такова обучение на целия персонал за който се налага.

Насоки: Определете необходимостта от обучение

Трябва да се използват съществуващите вече процедури за обучение за да се оцени необходимостта:

- Всички служители на компанията да преминат основно обучение по киберсигурност за да се осигури спазване на политиките и процедурите на компанията по управление на киберриска;
- Служителите на компанията, които имат задължения по управление на киберриска да преминат необходимото обучение, съответстващо на техните отговорности и правомощия.

Изискване: MSC-FAL.1/Circ.3 – Определете системите, активите, данните и функциите, повредата на които представлява риск за кораба

Изискване: ISM 10.3 Компанията трябва да определи оборудването и техническите системи, внезапното прекъсване на работата на които може да доведе до опасни ситуации. В системата за управление на безопасната експлоатация на кораби и предотвратяване на замърсяване трябва да се предвидят специални мерки за поддържане надеждността на това оборудване и системи. Тези мерки трябва да включват редовна проверка на резервните *(stand-by)* механизми и оборудване или технически системи, които не са в непрекъсната експлоатация.

Насоки: Определете оборудването и техническите системи (OT и IT), чието внезапно излизане от строя, може да доведе до опасна ситуация (критичните системи)

Оборудването и техническите системи (включително OT и IT), чието внезапно излизане от строя, може да доведе до опасна ситуация (критични системи или оборудване) следва вече да са определени в СУБК. Въпреки това за да се имплементира управлението на киберриска в СУБК, трябва да бъдат разгледани и данните в контекста на внезапна оперативна повреда. Загубата или повредата на данни използвани от критичните системи може да има същия негативен ефект върху безопасността или околната среда, както излизането на системата от строя по всяка друга причина. Препоръчително е списъкът на критичните системи / оборудване да бъде допълнен с данните, които тези системи използват и техния източник.

Изискване: MSC-FAL.1/Circ.3 – Внедрете мерки и процеси за управление на киберриска

Изискване: ISM 1.2.2 Целите на компанията по управление на безопасността трябва да включват оценка на всички установени рискове за нейните кораби, персонал и околната среда и предприемане на подходящи предпазни мерки.

Насоки: Оценете всички установени рискове за кораба, екипажа и околната среда и въведете подходящи предпазни мерки

Техническите и процедурните мерки, които трябва да бъдат предприети включват:

- Инвентаризация на хардуера – създайте и поддържайте регистър на хардуера на всички критични системи на борда, включително оторизираните и неоторизираните устройства от мрежата на компанията. СУБК трябва да включва процедури за поддържането и актуализирането на този регистър през целия жизнен цикъл на кораба;
- Инвентаризация на софтуера – създайте и поддържайте регистър на всичкия оторизиран и неоторизиран софтуер инсталиран на поддържания от компанията хардуер, включително версия и режим на обновяване. СУБК трябва да бъде допълнена с процедури за:
    - Актуализиране на регистъра при промяна на хардуера;
    - Актуализиране на регистъра при промяна или обновяване на софтуера;
    - Пълномощия за обновяване или инсталиране на нов софтуер;
    - Предотвратяване на инсталирането на неоторизиран софтуер и неговото изтриване в случай че бъде открит такъв;
    - Поддръжка на софтуера.
- Схема на мрежовите връзки и потоците от данни – опишете мрежовите връзки и потоците от данни между критичните системи и другото оборудване / технически системи на борда и на брега, включително тези от трети страни. Установените по време на този процес уязвимости трябва да бъдат записани и сигурно пазени от компанията. СУБК трябва да бъде допълнена с процедури за:
    - Поддържане на карта на мрежовите връзки и потоците от данни за да се регистрират промени в хардуера, софтуера и/или свързаността;
    - Действия при откриване на уязвимости предизвикани от създаването на нови мрежови връзки и потоци от данни при инсталиране на нов хардуер;
    - Преглед на необходимостта от свързаност между критичните системи и другите OT и IT системи. Този преглед трябва да се базира на принципа, че системите

трябва да бъдат свързани само когато това е необходимо за безопасната и ефективна експлоатация на кораба или осигуряване на плановата му поддръжка;
    - Контрол върху използването на преносими устройства, точки за достъп и създаването на специфични или неконтролирани потоци от данни. Това може да се постигне чрез ограничаване на използването на преносими устройства и деактивиране на USB и други портове на критичните системи.
- Конфигуриране на защитни настройки за всичкия хардуер поддържан от компанията. Това трябва да включва документиране и поддържане на общоприетите стандарти за защитни настройки за целия оторизиран хардуер и софтуер. СУБК трябва да включва политики за определяне и използване на административни права от екипажа, брегови служители и трети страни. Въпреки това конфигурацията на защитните настройки не трябва да бъде част от СУБК. Тази информация трябва да се съхранява на отделно и сигурно място;
- Проверка на достъпа – записите за достъпа до системите трябва да бъдат периодично преглеждани. Правата за достъп трябва да бъдат активирани на всички критични системи, които имат такава възможност. СУБК трябва да бъде допълнена с процедури за:
    - Политики и процедури за поддръжка на записите за достъпа и периодичната им проверка от оторизирано лице като част от рутинната поддръжка;
    - Процедури за събиране и съхранение на записите за достъп, ако е подходящо.
- Обучение и тренировки,
- Физическа сигурност – трябва да се предприемат мерки за ограничаване на физическия достъп до критичните системи и мрежовата инфраструктура на борда. Физическата сигурност на кораба се осигурява чрез съответствие с Корабния План по Сигурността (КПС), изискван от Международния кодекс за сигурност на корабите и пристанищните съоръжения, *(ISPS Code)*.

Изискване: MSC-FAL.1/Circ.3 – Създайте аварийни планове

Изискване: ISM 7 Компанията трябва да разработи процедури, планове и инструкции, включително чек-листи, когато е подходящо, за основните корабни операции, свързани с безопасността на персонала, кораба и опазване на околната среда. Отделните задачи трябва да се определят и възлагат на квалифициран персонал.

Насоки: Актуализирайте процедурите, плановете и инструкциите за ключовите операции на борда, които разчитат на ОТ системи, ако се налага.

Ключовите операции на борда би следвало вече да са адресирани в СУБК. Ефектът от загуба на ОТ система или загуба на целостта на данните използвани от системата е същият както при излизане на самата ОТ система от строя. Независимо от това следва да се обмислят инструкции за действията при съмнение за нарушена работа на критичните системи.

Изискване: ISM 8.1 Компанията трябва да определи възможните аварийни ситуации на борда на кораба и да разработи процедури за справяне с тях.

Насоки: Актуализирайте аварийните планове с процедури за действия при киберинцидент.

Аварийните планове при повреди на критичните системи свързани с безопасната експлоатация на кораба и опазване на околната среда, би следвало вече да са адресирани в СУБК. Като цяло тези планове би трябвало да останат незасегнати от внедряването на управлението на киберриска в СУБК, тъй като ефектът от общокорабните аварии не зависи от коренната причина.

Въпреки това следва да се прецени необходимостта от аварийни процедури в случай на повреда на ОТ системите или данните използвани от тях.

Изискване: MSC-FAL.1/Circ.3 – Определете и внедрете действия за своевременно откриване на киберинцидент

Изискване: ISM 9.1 Системата за управление на безопасната експлоатация на кораби и предотвратяване на замърсяване трябва да включва процедури, чрез които несъответствията, инцидентите и опасните ситуации се докладват на компанията, разследват се и се анализират с цел усъвършенстване на безопасността и предотвратяване на замърсяването.

Насоки: Актуализирайте процедурите за докладване на инциденти, несъответствия и опасни ситуации да включват докладване на събития свързани с киберсигурността.

Примери за инциденти по киберсигурността са:

- Неоторизиран достъп до мрежовата инфраструктура;
- Неоторизирано или несъответстващо използване на администраторски права;
- Подозрителна мрежова активност;
- Неоторизиран достъп до критични системи;
- Неоторизирано използване на преносими устройства;
- Неоторизирано свързване на персонални устройства;
- Несъответствие с процедури за софтуерна поддръжка;
- Невъзможност за актуализиране на защитите от зловреден софтуер;
- Загуба или нарушена работа на критични системи;
- Загуба или повреда на данни използвани от критичните системи.

Изискване: MSC-FAL.1/Circ.3 – Определете и внедрете планове и действия за осигуряване на устойчива работа и възстановяване на системи и/или услуги необходими за експлоатацията на кораба при инцидент по киберсигурността

Изискване: ISM 3.3 Компанията е отговорна за осигуряването на подходящи средства и подкрепа от брега, за да може назначеното лице или лица да изпълняват своите функции.

Насоки: Осигурете адекватни ресурси и съдействие на назначеното лице на брега за справяне със ситуации на загуба или повреда на критични системи.

Необходимите ресурси и съдействие би трябвало вече да са осигурени от съществуващата СУБК. Въпреки това, имплементирането на управлението на киберриска в СУБК изисква адекватни IT ресурси, включително персонал. Те може да са част от компанията или да бъдат предоставени от трети страни. Следното трябва да се има предвид:

- Техническият персонал трябва да познава ОТ и IT системите на борда на корабите;
- Трябва да се осигури аварийна група за справяне с аварийни ситуации;
- Да се осигури алтернативен начин за комуникация между кораба и брега който да може да функционира независимо от всички други корабни системи;

- Вътрешните одити трябва да удостоверят съответствие с изискванията.

Изискване: ISM 9.2 Компанията трябва да разработи процедури за имплементиране на коригиращи действия, включително мерки за недопускане на повторяемост.

Насоки: Актуализирайте процедурите за имплементиране на коригиращи и превантивни действия така, че да включват инцидентите по киберсигурността.

Съществуващата СУБК би трябвало вече да включва процедури за докладване на несъответствия и назначаване на коригиращи и превантивни действия. Въпреки това тези процедури трябва да осигурят участието на персонала отговорен за управлението на киберриска при анализа на несъответствията и назначаването на коригиращи и превантивни действия.

Изискване: ISM 10.3 Компанията трябва да определи оборудването и техническите системи, внезапното прекъсване на работата на които може да доведе до опасни ситуации. В системата за управление на безопасната експлоатация на кораби и предотвратяване на замърсяване трябва да се предвидят специални мерки за поддържане надеждността на това оборудване и системи. Тези мерки трябва да включват редовна проверка на резервните *(stand-by)* механизми и оборудване или технически системи, които не са в непрекъсната експлоатация.

Насоки: Актуализирайте мерките насочени към осигуряване на надеждността на ОТ системите

Съществуващата СУБК би трябвало вече да включва процедури за поддръжка и осигуряване на надеждността на оборудването на борда. СУБК която инкорпорира управлението на киберриска трябва да съдържа процедури за:

- Софтуерна поддръжка, като част от рутинната поддръжка. Тези процедури трябва да осигурят, че актуализациите на софтуера, включително кръпките по сигурността се прилагат и тестват своевременно от отговорните служители;
- Разрешаване на отдалечен достъп за поддръжка на критичните системи, ако е необходимо и подходящо. Това трябва да включва оторизиране на достъпа като цяло (включително проверка дали доставчиците на услуги са предприели подходящи защитни мерки) и за всяка отделна отдалечена сесия;
- Предотвратяване на използването на неконтролирани или инфектирани носители от доставчиците на услуги за актуализиране на софтуера;
- Периодична проверка на информацията подавана от критичните системи към операторите и потвърждение на акуратността на тази информация когато системите са в определено известно състояние;
- Контролирано използване на администраторски права за осигуряване че софтуерната поддръжка се извършва от компетентния за това персонал.

Изискване: MSC-FAL.1/Circ.3 – Определете мерки за създаване на резервни копия и възстановяване работата на електронните системи засегнати от киберинцидента

Изискване: ISM 10.4 Прегледите, посочени в 10.2, както и мерките, посочени в 10.3, трябва да се включат в установената на кораба практика за текущо техническо поддържане.

Насоки: Добавете създаването и поддържането на резервни копия към установената практика за техническо поддържане на кораба.

Съществуващата СУБК би трябвало вече да съдържа процедури за поддръжка и тестване на резервното оборудване. Въпреки това, те може да не включват поддържане и съхранение офлайн на резервни копия на данните необходими за безопасната експлоатация на кораба и опазване на околната среда.

СУБК която инкорпорира управлението на киберриска трябва да съдържа процедури за:

- Проверка на създаването и съхранението на резервни копия за критичните системи;
- Проверка на алтернативните режими на работа на критичните системи;
- Създаване или получаване на резервни копия, включително чисти имиджи за ОТ системите за възстановяване след киберинцидент;
- Поддържане на резервни копия на данните необходими за безопасната работа на критичните системи;
- Съхранение на резервните копия и чистите имиджи офлайн, ако това е подходящо;
- Периодично тестване на резервните копия и процедурите свързани с тях.

Управлението на киберриска следва да включва:

1. Определяне на заплахите

1.1. Определете външните заплахи за кораба.
1.2. Определете вътрешните заплахи за кораба от неправилно използване или липса на осведоменост.

2. Определяне на уязвимостите

2.1. Изгответе инвентарен опис на системите с директни и индиректни комуникационни връзки.
2.2. Определете последствията от киберзаплахите за тези системи.
2.3. Определете възможностите и ограниченията на съществуващите защитни мерки.
2.4. Като примери за уязвимости могат да бъдат посочени:
- Стари и неподдържани операционни системи;
- Неактуализирана или липсваща защита от зловреден софтуер, антивирусна защита;
- Неподходящо конфигурирани настройки за сигурност, включително неефективно мрежово управление и използване на администраторски акаунти и пароли по подразбиране;
- Незащитени и несегментирани мрежи;
- Критично оборудване или системи постоянно свързани с брега;
- Недостатъчен контрол на достъпа от трети страни включително доставчици на услуги.

3. Оценка на риска

3.1. Определете вероятността уязвимостите да бъдат послужат за реализиране на външни заплахи.
3.2. Определете вероятността уязвимостите да се превърнат в реални заплахи поради неправилна употреба (вътрешни заплахи).
3.3. Определете последствията за безопасността и сигурността от използването на единични или комбинация от уязвимости.

3.4. Съществуващата СУБК би трябвало вече да включва процедури за оценка на риска, които могат да бъдат използвани.

4. Определяне на мерки за защита и откриване

4.1. Чрез защитни мерки намалете вероятността уязвимостите да бъдат използвани.
4.2. Намалете потенциалните вреди от използването на уязвимостите.

5. Разработване на аварийни планове

5.1. Изгответе приоритетен авариен план за справяне с всеки установен потенциален киберриск.
5.2. Като цяло, аварийните планове за справяне с киберинцидентите, включително загуба на критични системи и необходимостта от използване на алтернативни режими на работа, трябва да бъдат реферирани от съответните оперативни и аварийни процедури в СУБК.
5.3. Аварийните планове и свързаната с тях информация трябва да бъдат налични на борда на кораба на хартиен носител, тъй като някои киберинциденти могат да доведат до изтриване на информация и прекъсване на комуникационните връзки.

6. Справяне с инцидента по киберсигурността и възстановяване на засегнатите системи

6.1. Извършете действията за справяне с инцидента по киберсигурността предвидени в аварийния план.
6.2. Плановете за възстановяване на системите трябва да бъдат налични на борда на кораба и в бреговия офис на хартиен носител. Те трябва да бъдат разбрани от персонала отговорен за киберсигурността.
6.3. Оценете ефективността на аварийния план и извършете преоценка на заплахите и уязвимостите.

23.04.2020г.

Инж. Филип Карагьозов

Използвана литература:

[1] Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems
[2] MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management
[3] Guidelines on Cyber Security Onboard Ships 3rd Edition, *supported by ICS, BIMCO, InterManager, INTERCARGO, INTERTANKO, IUMI, OCIMF and WSC*
[4] DSCA Implementation Guide for Cyber Security on Vessels