КІБЕРБЕЗПЕКА НА МОРСЬКОМУ ТРАНСПОРТІ ЯК ОДИН З ЕЛЕМЕНТІВ ПРОТИДІЇ ВОРОГОВІ В УМОВАХ ВІЙНИ

Кравцова Л.В., Камінська Н.Г.
Херсонська державна морська академія, Україна

Вступ. У сучасному світі об'єктами кібератак стають будь-які напрямки людської діяльності. Не є виключенням і морська галузь. Якщо провести аналіз інтенсивності кібератак та їх класифікацію, можна бачити наявну тенденцію збільшення їх кількості та різновидів. Так, навіть останні два роки підтверджують таки висновки. Причому, атакам піддаються як морські порти, так і самі судна, незалежно від того якого типу є це судно, чи те пасажирське, чи вантажне. Від цього страждають та несуть великі фінансові втрати навіть такі відомі компанії як, в першу чергу, Міжнародна морська організація [1], а також норвезька круїзна компанія Hurtigruten, британська поромна компанія Red Funnel, Італійське класифікаційне суспільство RINA, французька контейнерна судноплавна компанія CMA CGM, оператор поромної переправи Steamship Authority у Массачусетсі, флагманський контейнерний перевізник Південної Кореї HMM, японська судноплавна компанія Kawasaki Kisen Kaisha, та багато інших. Це однозначно говорить про те що треба завжди бути готовому до того що хтось забажає втрутитися до діяльності компанії, судна, особисто кожного зі співробітників цих структур.

Актуальність досліджень. Треба зазначити, що більшість експертів вважають, що першим та найважливішим кроком до забезпечення захисту структур від кібератак є обізнаність персоналу в цьому питанні. Приєднання до інтернету на борту є звичайною справою, фактично жодне морське судно не захищено від проникнення зовнішньої інформації, в тому числі і шкідливої, чи зовсім руйнівної. Тому вкрай важлива підготовленість екіпажу до розпізнавання кібератак, вміння запобігати їм, дотримуватись елементарних правил кібергігієни, та визнати, що такі заходи значно зменшать кількість кібератак та їх вплив на захищеність судна, вантажу та екіпажу.

Основна частина. З метою здійснення контролю над обізнаністю команди у питаннях підготовленості до кібератак, *Міжнародна палата судноплавства у співпраці з відомою організацією BIMCO та Witherbys* випустила друге видання «Робочого зошиту з кібербезпеки для використання на борту судна», що свідчить про велику увагу керівних органів до цього питання. Робочий зошит надає екіпажам суден практичні методи виявлення кіберзагроз та захисту бортових систем.

Яскравим підтвердженням великої уваги до проблем кібербезпеки на морському транспорті є Національний план морської кібербезпеки, що був затверджений 5 січня 2021 року Радою національної безпеки США. Інші морські держави також поквапилися прийняти конструктивні дії для підвищення кібербезпеки свого флоту.

Підкреслимо, що в першу чергу кібербезпека судна - це обізнаність екіпажу в цьому питанні. Варто звернути увагу на дослідження Марі Хауглі Ларсен [2], яка працює в Департаменті морських операцій та цивільного будівництва Норвезького університету науки і технологій та має великий досвід вивчення морської кібербезпеки. Її основний тезис – підготовленість екіпажу до можливих кібератак у будь-якому прояві. Не є секретом те, що більшість моряків, принаймі до останнього часу, безпечно відносяться до власних дій на судні стосовно використання цифрових технологій, та вважають кібербезпеку комп'ютерною проблемою, ніяким чином не пов'язаною з їх особистими діями. Ларсен на підставі глибокого аналізу статистичних даних підкреслює особливості психології моряка, який думає що його судно ніколи не стане об'єктом кібератаки.

Саме тому сьогодення змусило керівництво Херсонської державної морської академії переглянути програму підготовки моряків, визначити найбільш важливі питання, на які обов'язково треба звернути увагу. Отже, в перелік дисциплін програми підготовки майбутніх моряків включений курс «Кібербезпека суднових комп'ютерних систем і мереж», метою якого

є всебічний аналіз джерел кібернебезпеки, цілей кібератак, методів прогнозування та захисту від можливих проявів небезпеки, а також підвищення безпеки моряків, оточуючого середовища, судна та вантажу. Кібербезпека – це не тільки запобігання доступу зловмисників до систем та інформації, який може привести до втрати контролю або конфіденційності [3]. Це також забезпечення захисту суднових систем від будь-яких втручань, підтримка належної роботи всіх модулів судна та берегових служб.

Принциповий підхід до викладання дисципліни «Кібербезпека суднових комп'ютерних систем і мереж» заключається в тому, що програма базується на документах з кібербезпеки, що розроблені ІМО, які зобов'язують адміністрацію забезпечити належний розгляд кіберризиків в системах управління безпекою. Курс розроблений таким чином, щоб випускники академії могли на належному рівні представляти українську морську галузь на міжнародних морських просторах.

Висновки. В умовах повномасштабної війни, яка триває вже більше півроку, треба бути всебічно підготовленими до будь-яких диверсій, у тому числі інформаційних та у сфері комп'ютеризації. Спеціалісти морської галузі повинні володіти способами визначення джерел кібернебезпеки, методами розпізнавання кібератак, їх нейтралізації, та, мабуть у першу чергу, дотримуватися правил використання цифрових технологій на борту судна. Саме це є метою внесення в програму підготовки фахівців морського флоту Херсонської державної морської академії дисципліни «Кібербезпека суднових комп'ютерних систем і мереж».

ЛІТЕРАТУРА

1. Международная конвенция о подготовке и дипломировании моряков и несении вахты. (2011). Лондон.: ИМО. «Эшфорд Пресс».

2. Larsen, Marie Haugli; Erstad, Erlend. (2022) Maritime cyber security training and awareness. SFI- Move spring conference 2022 . NTNU; NTNU i Ålesund. 2022-06-14 - 2022-06-15.

3. Информационная безопасность судовождения : монография / Г. Б. Вильский ; Одес. нац. мор. акад. - Одесса ; Николаев : Швець В. Д., 2014. - 334 с.