БАЗОВА ПІДГОТОВКА МАЙБУТНІХ МОРЯКІВ З ПИТАНЬ КІБЕРБЕЗПЕКИ НА МОРСЬКИХ СУДНАХ

Кравцова Людмила Володимирівна
канд. техн. наук, доцент, доцент кафедри інноваційних технологій та технічних засобів судноводіння
Херсонська державна морська академія, Україна

Зайцева Тетяна Василівна
канд. пед. наук, доцент,доцент кафедри інноваційних технологій та технічних засобів судноводіння
Херсонська державна морська академія, Україна

Безбах Олег Михайлович
канд. техн. наук, доцент, доцент кафедри інноваційних технологій та технічних засобів судноводіння
Херсонська державна морська академія, Україна

Сьогодні питання кібербезпеки на морському транспорті - це не просто популярна тема, якій в останній час приділяється багато уваги. Це проблема, яка торкнулася всіх, чия професійна діяльність пов'язана з морем, чи то моряк, який працює безпосередньо на морському судні, чи то офіцер що обслуговує морські порти. Великі масиви даних про кожне судно, його технічне обладнання, можливість детальної діагностики з берегу в той час коли судно знаходиться далеко в морі з метою максимального забезпечення безпеки для пасажирів, членів екіпажу, збереження вантажу, покращення умов праці та відпочинку є об'єктом інтересу різного роду злочинців, і в першу чергу мова йде про кіберзлочинців. Це можуть бути як конкуренти, які контролюють ринок морських перевезень, так і вимагачі або піратські корпорації. Можна тільки здогадуватися, які спеціалісти задіяні у цих процесах. Але ясно, що це спеціалісти високого рівню. Шкода від їх діяльності оцінюється в мільярди доларів, приводить до втрати довіри потенційних клієнтів, а іноді і до розвалу судноплавної компанії. Тому як береговим службам, так і судновласникам треба мати можливості протистояти всім проявам кібератак, вміти їх вчасно виявляти та приймати вірне управлінське рішення щодо ліквідації як самої кіберзагрози, так і її наслідків, що потребує достатніх знань у цієї сфері.

Як справедливо зауважив Кевін Джонс, професор, керівник міждисциплінарної дослідницької групи Maritime Cyber Threats, університет Плімута (Великобританія), специфіка саме морської галузі глобально відрізняє її від будь якої іншої. Насправді, в практиці морських перевезень абсолютно нормально почати черговий рейс, скажемо, у берегів Америки, пройти через порти Франції, Нідерландів, Данії, а потім спрямувати судно на Шанхай. У кожному порту міняються пасажири, вантажі, періодично екіпаж судна. Тобто, це дуже динамічний процес, і вимоги до судноплавних компаній повинні враховувати всі нюанси та специфіку будь-яких країн, аби забезпечити захист цих компаній, їх флоту, портів, що їх обслуговують, на навіть довкілля від кібератак, здатних нанести непоправну шкоду. Чесно кажучи, статистика кібератак в морської галузі невтішна, але і методи боротьби з ними також вдосконалюються. Причому, за думкою Кевіна Джонса, треба чітко усвідомлювати, що кібернебезпека – це лише з одного боку технічна проблема, тобто захист цифрової

інфраструктури відомими в ІТ – сфері методами. З іншого боку вибудовується ціла низка проблем, пов’язаних з абсолютно різними факторами. Морські судна розрізняються за розміром, віком, призначенням, насиченістю обладнанням. Тому, при формуванні стратегії захисту, в першу чергу треба розуміти, хто та навіщо може здійснювати кібератаку на конкретне судно.

Звісно, суто технічним рішенням цих питань займаються відповідно підготовлені досвідчені фахівці, як берегові, так і ті що займають офіцерські посади на судні [1]. Але самий непередбачений ризик у сфері кібербезпеки пов'язаний саме з людським фактором. Усвідомлене ставлення до ризиків, пов’язаних з порушенням елементарних правил поведінки на судні, здатно значно знизити ймовірність деяких видів кібератак. Навіть підключення власного ноутбука, смартфону до бездротових мереж судна, відкриття спаму та інші аналогічні дії можуть нанести велику шкоду не тільки тому члену екіпажу, який це скоїв, а і судну та компанії в цілому.

За даними експертів з кібербезпеки в морському секторі найбільш уразливими до кібератак є системи наземного і космічного обладнання; системи глобального позиціонування, електронно-картографічні і навігаційно-інформаційні системи; системи реєстрації даних рейсу; системи вантажних операцій; системи управління двигунами, машинами і живленням; системи контролю доступу; публічні інтернет-мережі судна; адміністративні системи та мережі; системи зв'язку та портова інфраструктура.

Зупинимося більш детально на аналізі кіберстійкості суднової інформаційної системи (ІТ-системи).

Ідентифікація ризику – це процес визначення елементів ризику, складання їх переліку та опису кожного з елементів. Після визначення ризику, необхідно стежити за ним в журналі ризиків або реєстрі.

Оцінка ступеня небезпеки та ймовірності виникнення факторів ризику – забезпечує аналіз вхідних даних процесу загальної оцінки ризику, допомагає в прийнятті рішень щодо необхідності обробки ризику, а також допомагає вибрати відповідні стратегії та методи. Тут оцінюється ймовірність виникнення ризику та масштаб впливу на інформаційні або операційні технології. Аналіз може бути якісним (використовуючи шкали, наприклад: «відсутній», «низький», «середній», «високий», «критичний») або кількісним (використовуючи числові терміни, наприклад: фінансовий вплив, процентна ймовірність, іміджевий критерій).

Аналіз наслідків – визначення характеру і типу впливу, який може статися при виникненні конкретної події, ситуації або обставини.

Визначення рівня захисту критично важливих систем – визначення пріоритетів захисту і методів, що застосовуються для зниження конкретного ризику.

Порівняння заходів безпеки з цілями та пріоритетними діями – застосування методів обробки ризику, що забезпечують досягнення прийнятного рівня ризику; перевірка відповідності методів управління ризиком запланованим цілям і докази їх ефективності.

Чек-листи інформаційних та операційних систем – можуть бути використані для ідентифікації небезпек і ризику або оцінки ефективності засобів управління на всіх стадіях життєвого циклу суднових систем, а також як частина інших методів оцінки ризику. Однак вони найбільш корисні для перевірки повноти розгляду досліджуваної проблеми при ідентифікації нових проблем.

План реагування – базується «на комплексній ідентифікації ризиків з визначенням основних етапів дій в надзвичайних ситуаціях і кризах, дозволяє організувати кризове управління на основі деталізації факторів ризику і визначенні

його типів» [3].

Аналіз кіберстійкості – виявлення прогалин у взаємодії систем і документуванні; моніторинг виконання планів реагування та аналіз наслідків.

Саме тому Херсонська морська академія, яка успішно співпрацює з відомими компаніями, приділяє велику увагу базовій підготовці майбутніх моряків з питань кібербезпеки на морських суднах. 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. Розроблені навчальні програми також охоплюють найважливіші питання, що стосуються впливу наслідків прояви безвідповідальності з боку членів екіпажу, та допомагають закріпити алгоритм професійної поведінки моряка на судні.

Під час бойових дій херсонські курсанти, навіть знаходячись на плавальної практиці у рейсі, продовжують навчання дистанційно, розуміючи, що тільки якісна освіта надає можливість бути конкурентоспроможним на міжнародному ринку праці у сфері морських перевезень. Та треба обов’язково сказати, що саме викладачі, фахівці з величезним досвідом, забезпечили свої курси необхідними навчальними матеріалами, розташованими на платформі дистанційного навчання MOODLE. Використання платформи ZOOM проведення відеоконференцій дозволяє максимально підлаштовуватися під графік вахт курсантів що перебувають на практиці, під розбіжність часу у різних країнах, навіть під графіки відключення енергії на території України. Дуже важливим є те що, знаходячись на плавальної практиці, наші курсанти користуються тими рекомендаціями з кібербезпеки, які вони отримують під час вивчення матеріалів з дисципліни «Кібербезпека суднових комп'ютерних систем і мереж». Наразі ми ретельно фіксуємо всі випадки кібератак, з якими стикнулися на практиці наші курсанти, систематизуємо їх та досліджуємо ті фактори, які можливо привели до кіберзагрози. Це допомагає вдосконалювати план підготовки, корегувати фактичні матеріали та робити курс максимально наближеним до вимог Міжнародної морської організації (ІМО) [2].

Список використаних джерел:

1. Резолюція MSC.428(98) «Управління морськими кіберризиками в системах управління безпекою» http://rise.odessa.ua/texts/MSC428_98.php3.
2. Международная конвенция о подготовке и дипломировании моряков и несении вахты. (2011). Лондон.: ИМО. «Эшфорд Пресс».
3. Guidelines on Cyber Security Onboard Ships, https://www.ics-shipping.org/publication/guidelines-on-cyber-security-onboard-ships-3rd-edition/.