УДК 629.123 Технічні науки

РІЗНОВИДИ КІБЕРАТАК НА СУДНІ В КОНТЕКСТІ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

Слатвінська В.М.
аспірантка кафедри
господарського права і процесу
Національного університету
«Одеська юридична академія»
м. Одеса, Україна

Судна являють собою технічно складні системи, що характеризуються значними розмірами. Таким чином, вони потребують декількох членів екіпажу на борту, що виконують найважливіші функції з охорони пасажирів, судна і вантажів [1, с. 4]. Натомість наразі судноплавна галузь вступає в нову еру, коли проектуються, будуються і експлуатуються автономні судна. Однак їх впровадження відбувається за рахунок збільшення числа небезпечних сценаріїв через потенційні кібератаки.

Значно загострюється ризик зовнішнього втручання і зриву роботи ключових систем судноплавства. Зростаюча технічна складність судів ними послуг, що надаються через Інтернет, роблять суднові системи все більш уразливими перед кібератаками, які можуть перешкодити управлінню судном в цілому або роботі суднових систем, навігаційного обладнання, від'єднати всі зовнішні комунікації судна або роздобути конфіденційні дані [2, с. 154].

Морські судна стають жертвами кібератак набагато частіше. Судновий екіпаж стикається з тими ж проблемами з кібербезпеки, що і представники інших професійних галузей. Як результат, морська спільнота усвідомлюючи усі ризики, повинна реагувати, а отже і розробляти різні, дієві, способи запобігання кібератак [3, с. 182].

Нова концепція автономності досягається ціною додаткової складності, обумовленої кількістю систем, які повинні бути

встановлені на борту і на березі, інтенсивністю програмного забезпечення всієї системи, залученими взаємодіями між системами, компонентами і людьми і збільшеною зв'язністю. Все вищесказане призводить до підвищеної уразливості системи до кібератак, що може привести до недоступності або небезпечної поведінки критичних суднових систем [4, с. 1].

Відомими прикладами кібератаки на судно є: зміна даних про судно, включаючи його місцерозташування, курс, інформацію про вантаж, швидкість і ім'я; створення «кораблів-примар»; відправка помилкової погодної інформації конкретним судам, щоб змусити їх змінити курс для обходу неіснуючого шторму; активація помилкових попереджень про зіткнення, що також може стати причиною автоматичного коректування курсу судна; можливість зробити існуюче судно «невидимим»; створення неіснуючих пошуково-рятувальних вертольотів; фальсифікація сигналів EPIRB, що активують тривогу; можливість проведення DoS-атаки на всю систему шляхом ініціювання збільшення частоти передачі AIS-повідомлень.

Кібератаки можуть проводитися в чотири етапи:

Розвідка / розвідка: отримання інформації про мету, яка може бути використана для підготовки до кібератаки. Вивчення та аналіз наявної інформації для виявлення потенційних вразливостей.

Доставка: зловмисник може спробувати отримати доступ до систем і даних цілі. Уразливість може бути використана. Методами отримання доступу можуть бути, наприклад, електронний лист, що містить шкідливий файл / посилання або заражений знімний носій в рамках оновлення програмне забезпечення.

Порушення: використання уразливості для отримання несанкціонованого доступу. Ступінь порушення залежить від того, наскільки істотна вразливість і Який метод обраний для здійснення атаки.

Афект: зловмисник здійснює дії всередині системи для досягнення своєї мети. Наприклад, це може бути розширення доступу, вивчення систем або маніпулювання інформація [5, с. 4].

Натомість відповідно до "Керівництва по управлінню кіберризиками в морській галузі" визначено функціональні елементи, що сприяють ефективному управлінню кіберризиками [6]:

- ідентифікація: визначення завдань і обов'язків персоналу по управліню кіберризиками і виявлення систем, ресурсів, даних і функціональних можливостей, які в разі збоїв можуть представляти загрозу для експлуатації судна;

- захист: реалізація процедур і заходів контролю ризиків; планування дій на випадок надзвичайної ситуації з метою запобігання кіберпригод і забезпечення безперебійної експлуатації судна;

- виявлення: розробка та вжиття заходів, необхідних для своєчасного виявлення кіберпригод;

- реагування: розробка та виконання заходів і планів щодо забезпечення відновлення систем, необхідних для експлуатації судна, або функцій, порушених в результаті кіберпригоди;

- відновлення: ідентифікація заходів з резервного дублювання і відновлення необхідних для експлуатації судна кіберсистем, постраждалих в результаті кіберпригоди.

Отже, управління кібербезпекою в судноплавстві відбувається шляхом ідентифікації кібератак на судна та запобіжним мірам.

Література:

1. Caprolu, Maurantonio & Pietro, Roberto & Raponi, Simone & Sciancalepore, Savio & Tedeschi, Pietro. (2020). Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. IEEE Communications Magazine. 58. 90-96. 10.1109/MCOM.001. 1900632.

2. Мазур Т.Н. Кибербезопасность судов. Сучасні підходи до високоефективного використання засобів транспорту: Матеріали X Міжнародної науково-практичної конференції. / За загальною редакцією Турлак Л.П. / – Запоріжжя: АА Тандем, 2019. С. 154-157.

3. Онищук М.М., Толстих М.О. Кібербезпека на судні: основні поняття та способи запобігання інформаційних небезпек.

Матеріали IX Всеукраїнської студентської наукової конференції [Сучасні проблеми морського транспорту та безпека мореплавства] в 2-х т.., (м. Херсон, 21 листопада 2019 року). – Херсон : Видавництво ХДМА, 2019. – Том. 1. –С. 182-184.

4. Bolbot, Victor & Theotokatos, Gerasimos & Boulougouris, Evangelos & Vassalos, Dracos. (2019). Safety related cyber-attacks identification and assessment for autonomous inland ships. 15 p. URL: https://www.autoship-project.eu/wp-content/uploads/2020/04/BTBV_ISSAV2019_Paper_13September2019-1.pdf (дата звернення: 23.02.21).

5. BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO (2016) The guidelines on cyber security onboard ships. Bagsvaerd: BIMCO. Tilgjengelig fra: https://10a4adff-267b-483c8bea-93a8e5be67fb.filesusr.com/ugd/0c0cb0_114e06b3750d4a5d918508e3aee308dc.pdf (дата звернення: 23.02.2021).

6. Maritime Cyber-Risks, CyberKeel, URL: https://www.cyberkeel.com/ services (дата звернення: 23.02.21).

УДК 356.5.64 Історичні науки

СУЧАСНИЙ СТАН ПІДГОТОВКИ ОФІЦЕРІВ ЗАПАСУ МЕДИЧНОЇ СЛУЖБИ МЕДИЧНИХ СИЛ ЗБРОЙНИХ СИЛ УКРАЇНИ

Слободяник Г.І.
професор, доктор психологічних наук,
спеціаліст вищої категорії, майор м/с резерву ЗСУ
Інститут медичних та фармацевтичних наук
Міжрегіональної академії управління персоналом
м. Київ, Україна

Важливою складовою Збройних Сил України була і залишається військово-медична служба, яка здійснює безперервне піклування про збереження та зміцнення здоров'я військово-службовців, приймає активну участь у підтриманні боєздатності особового складу, вносить свою частку у забезпечення високої