ОЦІНКА РИЗИКІВ ТА ПЛАН РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

Зайцева Т.В.
Херсонська державна морська академія
(Україна)

Вступ. Питанням підвищення безпеки робітників морської галузі, навколишнього середовища, вантажів, суден, портів і, взагалі, безпечного функціонування всього бізнес-процесу транспортування товарів протягом останніх 10 років приділяється чимало уваги. Але, як свідчать приклади реальних кібератак, які були здійснені на морський сектор, це питання залишається актуальним. І це тільки приклади, які попали в ЗМІ або в статистику компаній. А знаючи, що багато судновласників, щоб не нести репутаційні збитки, замовчують інформацію про кіберінциденти, – можна уявити масштаби цих катастроф.

Відбуваються постійні оновлення в галузі інформаційних технологій, доступності даних, швидкості обробки та передачі даних з розширеними можливостями для оптимізації роботи, економії витрат, підвищення безпеки та стійкості бізнесу. Загальносвітовою тенденцією сьогодні є цифровізація економіки, природно, що це стосується й морського транспорту. На морському транспорті використовується та розвивається електронна навігація, використання мережевого трафіку, автоматизація процесів експлуатації судна. Тобто, бортові системи можуть отримувати оновлення під час плавання, а команди мають вихід в інтернет.

Актуальність досліджень. Тому такі питання, як розробка належного кіберзахисту, стратегії управління відповідно до правил та передової практики на борту судна з акцентом на робочі процеси, обладнання, навчання, реагування на інциденти та управління відновленням – є невід'ємною частиною системи управляння безпекою судна.

Кібербезпека – це не лише запобігання доступу хакерів до систем та інформації, що потенційно призводить до втрати конфіденційності та/або контролю. Це також стосується підтримки цілісності та доступності інформації та систем, забезпечення безперервності бізнесу та постійної корисності цифрових активів та систем. Судновласникам та операторам необхідно розуміти важливість кібербезпеки та підвищувати обізнаність про це співробітників, включаючи персонал на судні або в порту.

Постановка задачі. Якщо звернутися до нормативних документів, що регламентують дані процеси, то перш за все, слід згадати про Резолюцію MSC.428(98) – «Управління морськими кіберризиками у системах управління безпекою», яка була ухвалена Комітетом з безпеки на морі ІМО в червні 2017 року. Резолюція закликає адміністрації забезпечити належний облік кіберризиків у існуючих системах управління безпекою не пізніше за першу щорічну перевірку документа компанії про відповідність після 1 січня 2021 року. Міжнародна морська організація (ІМО) випустила вже четверту, оновлену, версію «Посібника з управління морськими кіберризиками».

На додаток до резолюції ІМО:

- Національний інститут стандартів і технологій США (NIST) прийняв документ Cybersecurity Framework Version 1.1 (квітень 2018 р.).
- Цифрова асоціація контейнерних перевезень (Digital Container Shipping Association) ухвалила «Посібник із впровадження DCSA для кібербезпеки на судах v1.0».
- Міжнародна асоціація класифікаційних товариств (МАКО) випустила «Рекомендацію з кіберстійкості» (№ 166) [1].
- Міжнародна палата судноплавства спільно з Балтійською та міжнародною морською радою (BIMCO) у 2019 році підготували «Cyber Security Workbook for On Board Ship Use» (Навчальний посібник з кібербезпеки для використання на борту судна).

З 1 січня 2021 р. морські адміністрації ряду країн розпочали перевірки суден, що входять до їх портів, на предмет виконання рекомендацій ІМО щодо кібербезпеки.

Звідси можна зробити висновок про те, що деякі судна в іноземних портах,

починаючи з 1 січня 2021 р., можуть мати ризики санкцій за невиконання рекомендацій ІМО з кібербезпеки. Невиконання рекомендацій щодо кібербезпеки може спричинити відмову судну в комерційному контракті з боку фрахтувальника. Тарифні ставки страхування морських вантажів, ймовірно, будуть відрізнятися для суден, які виконують і не виконують рекомендації щодо кібербезпеки, що може знизити конкурентну здатність таких судновласників.

З 2021 р. кіберінциденти на інтерфейсі судно/порт вже розглядаються через призму рекомендацій щодо кібербезпеки. У результаті: деякі порти можуть визнаватись небезпечними з погляду кібербезпеки та судам, які заходять у такі порти або побували в них, рекомендуватимуться підвищені заходи кібербезпеки. Відповідно, це вплине на економічну привабливість портів та вартість перевезень. Крім того, невиконання міжнародних норм може бути приводом для санкцій як щодо компанії-судновласника-члена ІМО, так і до відповідних портів [2].

Вразливими, з погляду кібербезпеки об'єктами судна, є бортові системи, що керуються та контролюються відповідним програмним забезпеченням, інформаційними системами, мережевим обміном даних. Міжнародна морська організація до вразливих суднових систем відносить майже всі бортові системи (рис.1).

Рисунок 1 – Бортові системи, які вразливі до кібератак

Морська галузь має низку характеристик, які впливають на її вразливість до кіберінцидентів:

1. участь багатьох зацікавлених сторін в експлуатації судна, що призводить до відсутності відповідальності за інфраструктуру систем інформаційних та операційних технологій та суднові мережі;
2. використання застарілих систем інформаційних та операційних технологій;
3. використання систем операційних технологій, на яких не можна оновити чи запустити антивірусні програми;
4. судна, які взаємодіють онлайн із береговими сторонами та іншими ланками глобального ланцюжка поставок;
5. постачання обладнання, за яким здійснюється віддалений моніторинг та доступ, наприклад: виробниками або службою підтримки;
6. обмін важливою для бізнесу, конфіденційною інформацією та комерційною конфіденційною інформацією з берегом, з постачальниками послуг, включаючи морські

термінали та стивідори, з громадянською владою;

7. наявність та використання критично важливих систем з комп'ютерним керуванням, які можуть не мати новітнього програмного забезпечення або належним чином не забезпечують безпеку судна;

8. культура управління кіберризиками, яка ще має потенціал для поліпшення, наприклад, за рахунок додаткового навчання, вправ і уточнення ролей та обов'язків при реагуванні на кіберінцидент;

9. часто система автоматизації складається з кількох підсистем від багатьох постачальників, які приділяють мінімальну увагу до кіберпроблем та питанням апаратно-програмному інтерфейсу.

Особливим напрямком розв’язування питання кібербезпеки морської галузі – є зменшення ролі особистості в забезпеченні безпеки системи в цілому. Недоліком сучасних систем управління морськими транспортними суднами є висока частка участі людини у процедурі прийняття рішень. Тому важливо використовувати системний підхід до вирішення цієї проблеми. Від забезпечення персональної безпечної роботи та поведінки кожного члена екіпажу – до виявлення існуючих вразливостей всіх бортових систем та зменшення, по можливості, рівня вразливостей. Слід розуміти, що забезпечення сто відсоткової безпеки судна або функціонування портових систем неможливе.

Варто зосередитись на захисті того, що нам важливо, від супротивників, яким ми справді цікаві, які готові витрачати час і ресурси на отримання нашої цінної інформації. Окрім онлайн-загроз – того, що з інформацією або повідомленнями може трапитися, в мережі, варто врахувати й загрози офлайн, тобто людський фактор. Врахування контексту загроз, специфіки робочої системи допоможе правильно оцінити власні ризики. По-перше, людська увага має межі – фізично не вийде витрачати весь ресурс на захист цифрових активів. По-друге, судновласники не завжди зацікавленні витрачати чималі ресурси на системи захисту. По-третє, у зловмисників так само є обмеження ресурсів. Тому варто зосередитись на захисті того, що важливо.

З іншого боку, захистити від усього різноманіття загроз неможливо, тому що, наприклад, абсолютний захист зробить інформаційну систему практично недоступною для використання, а методи та технології атак весь час змінюються та вдосконалюються, тому не всі шляхи подолання загроз можуть бути відомі і не всім загрозам система захисту може протистояти. Кіберризики залежить від компанії, судна, операції та торгівлі. При оцінці ризику компанії повинні враховувати будь-які конкретні аспекти своєї діяльності, які можуть підвищити вразливість їх перед кіберінцидентами.

Слід досягати оптимального, на сьогодні, співвідношення системи забезпечення безпеки та реальних умов функціонування бортових систем, щоб не перевищувати вартості впровадження та обслуговування системи кіберзахисту в порівнянні з розмірами шкоди в разі кіберінциденту. В управління кіберризиками має залучатися вище керівництво компаній на постійній основі та постійне консультування з зовнішніми експертами в галузі кібербезпеки. Деякі аспекти управління кіберризиками можуть містити комерційну таємницю або конфіденційну інформацію. Наприклад, оцінка кіберризиків та пов'язане з нею обладнання та програмне забезпечення, інвентаризація та мережеві карти. Тому компаніям слід подумати про захист цієї інформації належним чином та по можливості не включати конфіденційну інформацію до своїх SMS-повідомлень.

Рекомендується, щоб судноплавна компанія спочатку провела оцінку потенційних загроз, з якими реально можна зіткнутися. Після цього має бути проведена оцінка систем та бортових процедур, щоб скласти карту їхньої стійкості для боротьби з поточним рівнем загрози. Цьому можуть сприяти внутрішні експерти або сторонні експерти, знайомі з морською галуззю та її ключовими процесами. Результатом має стати стратегія, яка зосереджена на ключових ризиках.

Управління кіберризиками має:

- визначити ролі та обов'язки користувачів, ключового персоналу та керівництва як на березі, так і на борту судна;
- ідентифікувати системи, активи, дані та можливості, які у разі порушення можуть становити небезпеку для судових операцій та безпеки;
- своєчасно впроваджувати технічні та процедурні заходи для захисту від кіберінцидентів, виявлення інцидентів та забезпечення безперервності роботи;
- скласти план дій у разі непередбачених обставин, який регулярно виконується;
- на постійній основі проводити моніторинг дієвості плана реагування на кіберінциденти, а в разі необхідності, поновлювати заходи безпеки.

Для нормальної роботи організації нагально необхідним стає процес управління інцидентами інформаційної безпеки, який включає в себе аналіз рівнів безпеки, оцінювання ефективності заходів із забезпечення безпеки, впровадження коригувальних, попереджувальних або інших заходів, наприклад, план-реагування, якщо подія вже сталося. По всім випадкам складається Звіт про інцидент та порядок реагування та наслідки.

Якщо було зафіксовано порушення кібербезпеки, то співробітники мають вжити наступних заходів:

1) ідентифікувати інцидент і переконатися, що він насправді відбувався;

2) локалізувати область IT-інфраструктури, задіяної в інциденті;

3) обмежити доступ до об’єктів, задіяних в інциденті;

4) повідомити підрозділ та керівництво про факт виникнення інциденту;

5) залучити компетентних фахівців для консультування;

6) створити групу з розслідування інциденту, скласти план робіт зі збору доказів і відновлення систем, а також забезпечити ведення протоколу подій;

7) після збереження та оформлення доказів відновити роботоздатність системи.

Завдяки плану реагування команда буде знати, що саме потрібно робити. При цьому у кожного буде задокументована роль і власна відповідальність і не потрібно давати додаткові інструкції, щоб не було втрати часу або перерв в спілкуванні.

Висновки. Значний вплив на розвиток міжнародного регулювання морської кібербезпеки належить Міжнародній морській організації, яка ухвалює відповідні резолюції, та рекомендаційні акти. План реагування на інциденти кібербезпеки - це письмовий документ, в якому чітко вказані кроки, які повинні виконуватись при виявленні порушення безпеки. Він схвалюється керівництвом компанії, і є алгоритмом дій.

Сучасний підхід до захисту інформації від несанкціонованого доступу полягає в комплексному застосуванні організаційних і технічних заходів. Існує потреба у підвищенні рівня обізнаності та розуміння, пов’язаного з реальними кіберризиками. Найефективнішим способом досягти цього є просування культури кібербезпеки.

ЛІТЕРАТУРА

1. Gary C. Kessler, Steven D. Shepard. Maritime Cybersecurity: A Guide for Leaders and Managers (2020).
2. DiRenzo, J., Goward, D.A., Roberts, F.S. The Little-known Challenge of Maritime Cybersecurity (2015). In Proceedings of the 6th International Conference on Information, Intelligence, Systems and Applications (IISA). 1–5.
3. Alcaide, J.I., Llave, R.G. Critical Infrastructures Cybersecurity and the Maritime Sector (2020). Transp. Res. Procedia. 45. 547–554.
4. Kavallieratos, G., Katsikas, S., Gkioulos, V. Cyberattacks Against the Autonomous Ship (2028). In Computer Security: Springer: Berlin/Heidelberg, Germany. 20–36.
5. Трофименко А.О., Майданевич С.Б., Войченко Т.О., Дорофєєва З.Я. Деякі проблемні питання впровадження стандартів кібербезпеки на морському транспорті (2023). Водний транспорт. 1 (37). 179–188.