https://www.sworldjournal.com/index.php/swj/article/view/swj15-01-031
DOI: 10.30888/2663-5712.2022-15-01-031

УДК 004.832.28

SAFETY PROBLEMS IN MARITIME TRANSPORT FROM THE POINT OF VIEW OF INFORMATION TECHNOLOGIES

ПРОБЛЕМИ БЕЗПЕКИ НА МОРСЬКОМУ ТРАНСПОРТІ З ТОЧКИ ЗОРУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Konovalov S.M. / Коновалов С.М.
ORCID: 0000-0002-2533-8660
Odessa National Maritime University, Odessa, Mechnikova 34, 65029
Одеський національний морський університет, Одеса, вул. Мечникова 34, 65029

Анотація. *У роботі розглядаються проблеми безпеки на морському транспорті з погляду інформаційних технологій. Для цього розглядалися приклади проблем, які можуть виникнути в результаті використання тих чи інших видів інформаційних технологій, найбільш поширених на морському транспорті. У процесі розгляду було виділено різні недоліки кожних з аналізованих видів інформаційних технологій, здатних тією чи іншою мірою призвести до різних негативних наслідків, здатних нашкодити як самому судну, так і товару на ньому, або екіпажу, у технічному чи економічному аспекті. У результаті, за даними проведеного аналізу, було позначено висновки, які узагальнюють подальші перспективи вирішення кожної з актуальних проблем кожної інформаційної технології.*

Ключові слова: *проблеми, безпека, морський транспорт, інформаційні технології, судно, товар, екіпаж.*

Вступ

Статистика повідомляє, що 90 % обсягу міжнародних перевезень на сьогоднішній день складає транспортування вантажів морським транспортом [1]. З цього видно, що морським перевезенням віддається дуже важлива роль сучасному світі. Будь-яка небезпека, яка може нашкодити судну, товару або екіпажу, може виявитися фатальною. Через те, що на сучасних судах використовується безліч сучасного високоточного обладнання, що працює за допомогою інформаційних технологій (ІТ), то й небезпеки, пов’язані з їхньою правильною роботою, є дуже важливими та поширеними. Це виходить з того, що будь-яка похибка у обчисленнях або дрібна аварія може призвести до фатальних наслідків.

Як різноманітні види ІТ, так різноманітні і небезпеки, пов'язані з їхньою роботою. Чим складніша та чи інша ІТ, тим більша ймовірність того, що вона може вийти з ладу.

Для запобігання подібних ситуацій краще знати заздалегідь, чого можна очікувати від різних видів ІТ, щоб бути заздалегідь озброєним, і готовим розуміти, що щось пішло не так.

Проблеми видів ІТ для морського транспорту

Однією з найпоширеніших проблем для ІТ у всіх галузях, у тому числі й для морського транспорту, є кібервразливість тих чи інших інформаційних систем. Так у 2017 році кібератаки показали вразливість у навігаційних та інших інформаційних системах на судах та портах. Наприклад: мало місце втручання у системи автоматичної ідентифікації та електронні карти, глушення глобальних систем позиціонування та маніпулювання системами управління

вантажами та судами, у тому числі, шляхом впровадження шкідливих програм, програм-вимагачів та вірусів [2].

Кібератаки все частіше є частиною та інструментом загального за задумом злочину, а не самодостатнім злочином. Зловмисники зараз зацікавлені не лише у крадіжці даних, а й активно намагаються зрозуміти, як взяти під контроль експлуатаційні мережі та системи суден. Еволюція морського піратства може призвести до того, що пірати зможуть захоплювати командні та контрольні системи судна [3].

На жаль, універсальним та надійним захистом від кібератак не існує. Основний захист, здатний запобігти подібним проблемам – встановлення антивірусного програмного забезпечення (ПЗ), а також навчання співробітників, що працюють з обчислювальними системами, цифрової грамотності [4].

Також поширеним застосуванням ІТ є технологія «Інтернет речей» (ІР). Так як ця технологія поєднує величезну кількість різних пристроїв, виникає підвищена небезпека застосування шкідливого ПЗ на децентралізованих точках входу. Завдяки дистанційним датчикам та моніторингу основного варіанту використання для ІР підвищується чутливість до контролю доступу та володіння даними. Інтеграція та тестування систем ІР з декількома платформами, і численними протоколами є проблемою. Швидкий розвиток програмних інтерфейсів додатків, найімовірніше, вимагатиме від розробників непередбачених витрат, що негативно вплине на можливості проектних команд щодо додавання нових функцій.

Величезна кількість гравців, що беруть участь у ІР, неминуче стикатимуться один з одним, прагнучи захистити свої системні переваги. Відсутність ясних варіантів застосування або прикладів, що ілюструють рівень прибутковості/збитковості, уповільнює розвиток ІР. Для масового застосування ІР знадобляться обґрунтовані, орієнтовані клієнта комунікації [5].

Однією з потенційних проблем, пов’язаних із цифровими інноваціями в морській галузі, є недостатня стандартизація електронного обміну даними та необхідність загального формату даних для обміну інформацією. Електронний обмін даними включає електронний переклад комерційних або адміністративних операцій з одного комп’ютера на інший, із застосуванням узгодженого стандарту для структурування даних операцій або повідомлень. Цей недолік, поряд із загальною неясністю щодо потенційних застосувань блокчейн, відноситься до факторів, здатних пояснити тривалу залежність суднової галузі від паперової документації при перевезеннях вантажу в контейнерах.

Експлуатація автономних надводних суден, здатних без екіпажу здійснювати перевезення різних вантажів, поки що залишається лише проектом. Такі судна зможуть забезпечити високу безпеку та економію коштів через видалення людського фактора з певних операцій, проте в найближчому майбутньому людське втручання, як і раніше, буде необхідним у більшості суднових операцій, а перевезення вантажів і пасажирів на повністю автоматизованих судах залишається у віддаленій перспективі [2].

Важливою проблемою є і супутниковий зв'язок, який активно застосовується на судах. Проблеми ця полягає в довгому часі між подачею сигналу та його отриманням, протоколах передачі інформації, програмному забезпеченні, сховищах та базах даних з віддаленим доступом. Це збільшує ризики несанкціонованого втручання у компоненти зв'язку. Крім цього, загрозу становить і електронне апаратне забезпечення, через яке можуть контролювати та прослуховувати інформацію [5].

Часто для забезпечення безпеки судноплавства також використовуються мобільні системи управління рухом суден (МСУРС). Ці системи дозволяють спростити та прискорити процедуру прийняття рішення, і при цьому знизити участь людини у процедурі вироблення керуючого рішення. Однак неможливість обслуговування одним оператором одночасного великого числа суден, а також «прив'язка» до стаціонарних берегових служб та споруд, які не дають використовувати в МСУРС традиційний підхід в якості аналога [6].

Для контролю роботи різних складних технічних систем на суднах все частіше використовуються різні гібридні експертні системи (ГЕС). Однак і вони не позбавлені недоліків, внаслідок яких безпека судна може бути під загрозою. Це недоліки, які притаманні, як загалом експертним системам:

- знання не завжди легкодоступні;
- важко видобувні знання з експертів;
- часті випадки існування декількох правильних оцінок;
- обмеження часом;
- користувачі мають обмеження в знанні предмета;
- добре працюють тільки у вузькій галузі знань;
- багато експертів не мають незалежний засіб для перевірки достовірності результатів;
- словник часто обмежений і його важко зрозуміти;
- дорога допомога від інженерів;
- вразливість в розпізнаванні кордонів своїх можливостей, і демонстрація ненадійного функціонування поблизу меж їх застосування;
- великі трудовитрати, які необхідні для поповнення БЗ;
- можливість виникнення протиріч через невідповідність правил змістовним зв'язкам між статичними відомостями про предметну область.

Так і недоліки, притаманні конкретно ГЕС [7]:

- труднощі та неприродність реалізації певних умов господарства автоматики та телемеханіки;
- труднощі в умовах невизначеності, нестачі знань.

Однак, незважаючи на це, ГЕС з кожним роком дедалі більше вдосконалюються, а отже, є ймовірність, що у майбутньому вплив цих недоліків зведеться до мінімуму.

Висновки

У результаті було розглянуто різні типи проблем ІТ для морського транспорту, залежно від класифікацій самих ІТ. Було проаналізовано, наскільки

та чи інша проблема впливає на роботу судноплавства в цілому та самих систем IT, зокрема. Більшість цих проблем, на сьогоднішній день, не має остаточних рішень, а менша частина, прогнозовано, повинна зникнути з часом, у міру розвитку тих чи інших видів IT.

Література:

1. Семёнов С.А. Кибербезопасность морского и речного транспорта / С.А. Семёнов. // Транспорт Российской Федерации. – 2018. – № 1 (74). – С. 43–46.

2. IT-технологии в морской индустрии [Электронный ресурс] // «Обзор морского транспорта – 2018 год» (Конференция ООН по торговле и развитию, ЮНКТАД). – 2018. – Режим доступа к ресурсу: https://interlegal.com.ua/ru/publikacii/it_tehnologii_v_morskoj_industrii/ (дата обращения: 28.03.2022).

3. Семёнов С. Морская кибербезопасность – ситуация, проблемы и риски [Электронный ресурс] / С. Семёнов. – 2020. – Режим доступа к ресурсу: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/ (дата обращения: 28.03.2022).

4. Альнамер З. Интернет вещей (IoT): проблемы и будущие направления [Электронный ресурс] / З. Альнамер // Логистика. – 2018. – Режим доступа к ресурсу: http://www.logistika-prim.ru/articles/internet-veshchey-iot-problemy-i-budushchie-napravleniya (дата обращения: 28.03.2022).

5. Мамаков А.А. Проблемы безопасности информационной радиосвязи на море [Электронный ресурс] / А.А. Мамаков, Л.М. Перерва // Владивостокский государственный университет экономики и сервиса, Владивосток – Режим доступа к ресурсу: https://studfile.net/preview/8167047/ (дата обращения: 28.03.2022).

6. Борисова Л.Ф. Факторы безопасности мореплавания в мобильной системе управления судоходством / Л.Ф. Борисова, А.А. Соловьев. // Вестник МГТУ. – 2013. – том 16. – № 3. – С. 601-604.

7. Коновалов С.Н. Информатизация противоаварийного управления сложными техническими системами / С.Н. Коновалов, В.В. Вычужанин. // Информатика и математические методы в моделировании, Одесса: ОНПУ. – 2017. – том 7. – № 4. – С. 265-275.

References:

1. Semonov S.A. Kiberbezopasnost' morskogo i rechnogo transporta [Cybersecurity of maritime and river transport]. Transport Rossiyskoy Federatsii. – 2018. – № 1 (74). – pp. 43–46.

2. IT-tekhnologii v morskoy industrii [IT-technologies in the maritime industry]. «Obzor morskogo transporta – 2018 god» (Konferentsiya OON po torgovle i razvitiyu, YUNKTAD), 2018, available at: https://interlegal.com.ua/ru/publikacii (accessed 28 March 2022).

3. Semonov S. Morskaya kiberbezopasnost' – situatsiya, problemy i riski [Maritime cybersecurity – situation, challenges and risks], available at: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/morskaya-kiberbezopasnost-situatsiya-problemy-i-riski/ (accessed 28 March 2022).

4. Al'namer Z. Internet veshchey (IoT): problemy i budushchiye napravleniya [Internet of Things (IoT): challenges and future directions], Logistika, 2018, available at: http://www.logistika-prim.ru/articles/internet-veshchey-iot-problemy-i-budushchie-napravleniya (accessed 28 March

2022).

5. Mamakov A.A., Pererva A.A. Problemy bezopasnosti informatsionnoy radiosvyazi na more [Safety issues of information radio communications at sea]. Vladivostokskiy gosudarstvennyy universitet ekonomiki i servisa, Vladivostok, available at: https://studfile.net/preview/8167047/ (accessed 28 March 2022).

6. Borisova L.F., Solov'yev A.A. Faktory bezopasnosti moreplavaniya v mobil'noy sisteme upravleniya sudokhodstvom [Safety factors of navigation in a mobile navigation management system]. Vestnik MGTU, 2013, vol. 16, no. 3, pp. 601-604.

7. Konovalov S.N., Vychuzhanin V.V. Informatizatsiya protivoavariynogo upravleniya slozhnymi tekhnicheskimi sistemami [Informatization of emergency control of complex technical systems]. Informatika i matematicheskiye metody v modelirovanii. Odessa: ONPU, 2017, vol. 7, no. 4, pp. 265-275.

Abstract. *Most of the international transport today is sea transport. In today's world, maritime transport plays a very important role. Any hazard capable of causing harm to the ship, goods or crew could be fatal. Modern ships use a lot of modern high-precision equipment that works with the help of information technology. The dangers associated with their proper operation are very important and common. As the types of information technologies are diverse, so are the dangers associated with their work. To prevent similar situations, it is better to know in advance what you can expect from different types of information technology. One of the most common problems for information technology in all industries, including maritime transport, is the cyber vulnerability of certain information systems. Cyberattacks are increasingly a part and tool of a universal crime by design, rather than a crime in itself. Unfortunately, there is no universal and reliable protection against cyberattacks. Since this Internet of Things technology combines a huge number of different devices, there is an increased risk of malware being used on decentralized entry points. The operation of autonomous surface vessels capable of transporting various cargoes without a crew is still only a project. An important problem is also satellite communications, which are actively used on ships. To control the operation of various complex technical systems on ships, various hybrid expert systems are increasingly being used, which are not without drawbacks; in the future, the impact of these shortcomings will be minimized. It was analyzed how this or that problem affects the work of shipping in general and the information technology systems themselves, in particular. Most of these problems, today, do not have final solutions, and a smaller part, predictably, should disappear over time.*

Key words: *problems, security, maritime transport, information technology, cybersecurity, hybrid expert systems, ship, goods, crew.*

Стаття відправлена: 26.09.2022 р.