# KAPITEL 1 / *CHAPTER 1* [1]

# SHIP'S INFORMATION SECURITY: TECHNOLOGIES, INTERNATIONAL REGULATIONS AND PRACTICAL ASPECTS

**DOI: 10.30890/2709-2313.2023-18-01-021**

## Вступ.

Інформаційна безпека на суднах - це один із найважливіших аспектів безпеки мореплавства. Сучасні технології дають змогу поліпшити захист суден від різних кіберзагроз, які можуть призвести до серйозних наслідків. Розроблення міжнародних нормативних документів на забезпечення інформаційної безпеки є необхідним заходом, який має допомогти в захисті суден і морських портів.

Сучасні судна залежать від комп'ютерних систем і технологій, які забезпечують безпеку плавання, контролюють рух суден, пожежу та інші небезпечні ситуації. Одночасно ці системи можуть бути піддаються кібератакам, що може викликати серйозні наслідки, такі як порушення безпеки плавання, загрози життю і здоров'ю екіпажу та пасажирів, забруднення довкілля та інші.

Однак, крім технологічних аспектів, слід враховувати роль людського фактора в системі інформаційної безпеки судна. Навчання екіпажів, а також контроль з боку портової влади і судновласників є не менш важливими питаннями. Серед перспективних технологій, які можуть бути використані для забезпечення інформаційної безпеки суден, можна виділити блокчейн, штучний інтелект, квантові технології, кіберфізичні системи та квантову криптографію.

Незважаючи на те, що забезпечення інформаційної безпеки на суднах є завданням кожного судновласника і портової влади, співпраця між різними країнами в цій галузі також необхідна. Загалом, забезпечення інформаційної безпеки на суднах - це складний і багатогранний процес, який потребує постійного вдосконалення та співпраці різних учасників мореплавства.

[1] ***Authors:*** *Melnyk Oleksiy Mykolayovych*

## 1.1. Огляд основних принципів забезпечення інформаційної безпеки судноплавства

У сучасному світі інформаційна безпека суден стає все більш важливою. Це пов'язано зі зростанням кількості кібератак на судна, що може призвести до серйозних наслідків. Для захисту суден від кіберзагроз необхідно використовувати сучасні технології, дотримуватися міжнародних нормативних документів і вживати практичних заходів. Питання забезпечення безпеки сучасного транспортного флоту пов'язане насамперед із захистом від несанкціонованого доступу та запобігання витоку інформації. Кожний судновласник, дбаючи про збереження конфіденційності даних, не тільки зменшує ризик та можливі збитки від їхнього витоку, але й підвищує рівень довіри в очах своїх клієнтів та партнерів. Якісні та кількісні зміни, що відбуваються на морських суднах останнім часом, значно підвищили безпеку їх експлуатації та умови безперервної роботи.

Сучасне судноплавство великою мірою залежить від інформаційного забезпечення, що є важливим елементом у процесах керування судном. Знайшло поширення застосування нових морських цифрових інформаційних систем на основі мережі передачі цифрових навігаційних даних для забезпечення безпеки мореплавання. Це дозволяє своєчасну обробку сукупності інформації для функціонування навігаційних систем судна. Також такі системи дозволяють виключити прийняття рішення щодо управління судна на основі неповної або недостовірної інформації та зумовлює вжиття спеціальних заходів для забезпечення її безпеки. Тому, завдання що постають, це розроблення засобів захисту інформаційних ресурсів судна, що є одними з першочергових та актуальних. С урахуванням наявності цих факторів та ситуації що склалася, з боку міжнародної морської організації було розроблено та прийнято ряд документів по забезпеченню кібербезпеки в морській галузі. Дана стаття представляє аналіз основних факторів, що справляють вплив на забезпечення інформаційної безпеки судна. Запропоновано концептуальну модель безпеки судна та основні чинники впливу на стан інформаційної безпеки судна.

Інформаційна безпека судноплавства - це сукупність заходів і дій,

спрямованих на захист інформації, яка використовується в морському і річковому транспорті. Вона охоплює захист від кібератак, збоїв у роботі обладнання, витоків конфіденційної інформації, а також протидію піратству та іншим незаконним діям у морі.

Деякі з основних принципів інформаційної безпеки судноплавства включають в себе:

- Захист систем і мереж суден і портів від несанкціонованого доступу, зокрема від зловмисних кібератак.
- Захист конфіденційної інформації, зокрема інформації про вантажі, пасажирів і маршрути.
- Навчання та підвищення обізнаності судновласників, команд і персоналу портів про можливі загрози інформаційній безпеці.
- Регулярне оновлення програмного забезпечення та обладнання на суднах і в портах.
- Встановлення фізичних і логічних заходів захисту, таких як шифрування, біометрична ідентифікація та контроль доступу.
- Розроблення планів дій у разі кібератаки, збою в роботі обладнання або інших надзвичайних ситуацій.
- Співпраця з організаціями, що займаються боротьбою з кіберзлочинністю і злочинами в морі.

Захист систем і мереж суден і портів від несанкціонованого доступу, зокрема від зловмисних кібератак, охоплює низку заходів і технологій для забезпечення безпеки інформації та захисту від загроз, таких як:

Файєрволи (firewalls) - це програмне забезпечення або апаратний пристрій, який контролює трафік, що проходить через мережу і блокує спроби несанкціонованого доступу до систем і мереж. Антивірусне ПЗ (antivirus software) - використовується для захисту від вірусів, троянів, шпигунських програм та інших шкідливих програм. VPN (Virtual Private Network) - це технологія, яка забезпечує безпечне з'єднання між віддаленими пристроями через інтернет, шляхом шифрування даних і захисту від несанкціонованого доступу. Шифрування (encryption) - це метод захисту інформації шляхом її перетворення у форму, яку можна прочитати лише з використанням

спеціального ключа. Багатофакторна автентифікація (multi-factor authentication) - це метод, що вимагає від користувача надання декількох форм ідентифікації, таких як пароль і біометричні дані, для отримання доступу до системи. Оновлення програмного забезпечення та патчів безпеки - це процес оновлення програмного забезпечення та патчів безпеки, який усуває вразливості та помилки в програмному забезпеченні та забезпечує його безпеку. Контроль доступу - це метод, який обмежує доступ до інформації та систем тільки уповноваженим користувачам.

Ці заходи допомагають захистити системи та мережі суден і портів від несанкціонованого доступу, зокрема від зловмисних кібератак, і забезпечити безпеку інформації. Однак, для ефективного захисту, необхідно регулярно оновлювати і вдосконалювати системи безпеки і навчати персонал правильним методам забезпечення безпеки інформації.

Захист від витоку конфіденційної інформації - це важливий аспект інформаційної безпеки судноплавства. Конфіденційна інформація може містити такі дані, як плани плавання, вантажі, маршрути, дані про пасажирів і моряків, фінансові дані та іншу чутливу інформацію. Для захисту від витоку конфіденційної інформації можуть бути застосовані наступні заходи (Табл.1):

**Таблиця 1 – Заходи захисту конфіденційної інформації**

| Вид | Призначення |
|---|---|
| Контроль доступу | Метод, який обмежує доступ до конфіденційної інформації тільки уповноваженим користувачам. Для контролю доступу можуть використовуватися багатофакторна автентифікація, різні рівні доступу та інші методи. |
| Шифрування | Метод захисту інформації шляхом її перетворення у форму, яку можна прочитати тільки з використанням спеціального ключа. Шифрування може застосовуватися для захисту конфіденційної інформації на всіх рівнях - від зберігання до передавання. |
| Навчання персоналу | Екіпаж суден і персонал портів мають бути навчені правильним методам поводження з конфіденційною інформацією, а також повідомлятися про загрози витоку інформації та про те, як їм запобігати. |

| Вид | Призначення |
|---|---|
| Аудит безпеки | Процес перевірки систем і мереж на наявність вразливостей і оцінки рівня безпеки. Аудит безпеки дає змогу виявити вразливості та проблеми, які можуть призвести до витоку конфіденційної інформації, і вжити заходів щодо їх усунення. |
| Захист від саботажу | Важливий аспект інформаційної безпеки судноплавства. Саботаж може бути здійснений як внутрішніми, так і зовнішніми загрозами, такими як шкідливі програми, фізичні атаки та інші методи. |

Для захисту від саботажу можуть бути застосовані такі заходи:

Контроль доступу - обмеження доступу до систем і мереж тільки уповноваженим користувачам. Навчання персоналу - співробітники суден і портів мають бути навчені правильним методам поводження з інформацією, а також повідомлятися про загрози саботажу і про те, як їм запобігати.

Навчання та підвищення обізнаності судновласників, команд і персоналу портів про можливі загрози інформаційній безпеці є важливим аспектом забезпечення безпеки судноплавства. У рамках такої програми можуть проводитися такі заходи як тренінги та семінари які можуть проводитися як у форматі онлайн-навчання, так і в класі. Вони можуть містити вивчення можливих загроз інформаційній безпеці, аналіз випадків інцидентів і методів захисту від загроз. Курси підвищення кваліфікації - навчання повинно включати в себе не тільки теоретичні знання, а й практичні навички. Курси підвищення кваліфікації можуть допомогти персоналу оволодіти навичками, необхідними для захисту інформації, і застосовувати їх на практиці. Система оповіщення - важливо мати систему, яка дає змогу швидко сповіщати персонал про можливі загрози інформаційній безпеці та надавати інструкції щодо дій у разі інциденту. Регулярні перевірки - проведення регулярних перевірок та аудитів може допомогти виявити вразливості та проблеми в системах і процедурах безпеки. Соціальна інженерія - в рамках програми навчання можна проводити симуляції атак з використанням методів соціальної інженерії, щоб персонал портів і суден могли навчитися розпізнавати і запобігати таким атакам. Організація прес-конференцій - прес-конференції можуть проводитися для привернення уваги до проблем інформаційної безпеки в судноплавстві та підвищення обізнаності серед

широкої аудиторії.

Регулярне оновлення програмного забезпечення та обладнання на суднах і в портах є ключовим аспектом забезпечення інформаційної безпеки в судноплавстві. Це включає в себе оновлення операційних систем і застосунків, оновлення обладнання, використання захищених протоколів тощо.

Регулярне оновлення операційних систем і застосунків допомагає усувати вразливості та виправляти помилки в коді програм. Оновлення антивірусного програмного забезпечення - оновлення антивірусного ПЗ дає змогу забезпечити надійніший захист від вірусів та інших шкідливих програм. Оновлення обладнання - регулярне оновлення обладнання (як апаратного, так і програмного) допомагає забезпечити сумісність і стабільність роботи всієї системи. Використання захищених протоколів і шифрування - використання захищених протоколів і шифрування даних під час передавання через мережу допомагає забезпечити безпеку даних і захистити їх від несанкціонованого доступу. Тестування безпеки - регулярне проведення тестів на безпеку допомагає виявити вразливості та проблеми в системах і процедурах безпеки. Моніторинг системи - постійний моніторинг системи допомагає оперативною мірою виявляти та реагувати на загрози безпеці, такі як кібератаки або несанкціонований доступ до систем. Резервне копіювання даних - регулярне створення резервних копій даних допомагає забезпечити збереження інформації в разі її втрати або пошкодження внаслідок інциденту. Усі ці заходи є необхідними для забезпечення безпеки судноплавства та захисту інформації від несанкціонованого доступу.

Встановлення фізичних і логічних заходів захисту є важливим аспектом забезпечення інформаційної безпеки в судноплавстві. Ці заходи можуть містити в собі такі:

- шифрування даних допомагає захистити інформацію від несанкціонованого доступу, шляхом перетворення інформації в незрозумілий для сторонніх вигляд.
- біометрична ідентифікація дає змогу визначити особу людини на основі її фізіологічних або поведінкових характеристик (наприклад, відбиток пальця, голос або обличчя).

- контроль доступу обмежує доступ до інформації та систем тільки авторизованим користувачам, що допомагає запобігти несанкціонованому доступу та знижує ризик злому.
- фізичний захист може включати в себе використання відеоспостереження, огорожі, замків та інших фізичних заходів для захисту обладнання та систем від несанкціонованого доступу.
- логічний захист охоплює використання паролів, багатофакторної автентифікації та інших заходів для захисту систем та інформації від несанкціонованого доступу.
- моніторинг і аудит дають змогу відстежувати активність користувачів і систем, виявляти несанкціонований доступ і проблеми безпеки в системах і процедурах.

Розробка планів дій на випадок кібератаки, збою в роботі обладнання або інших надзвичайних ситуацій є важливим аспектом забезпечення інформаційної безпеки в судноплавстві. Такі плани допомагають визначити заходи, яких необхідно вжити в разі виникнення певних ситуацій, а також вказують відповідальних за реалізацію цих заходів. План дій у разі кібератаки може містити визначення типу атаки, обсягу шкоди та масштабу атаки. Ізоляція системи - ізоляція компрометованої системи від інших систем, щоб запобігти поширенню атаки на інші частини мережі. Проведення аналізу вразливостей тобто виявлення вразливостей, які можуть бути використані зловмисниками. Далі усунення вразливостей та оновлення захисних заходів, відновлення системи після кібератаки. Аналіз причин - аналіз причин, які призвели до кібератаки, і вжиття заходів для запобігання подібних атак у майбутньому. План дій у разі збою в роботі обладнання може містити такі кроки:

- Визначення загрози - визначення причини збою в роботі обладнання.
- Визначення критичності збою - визначення критичності збою в роботі обладнання та оцінка можливих наслідків.
- Встановлення контролю - встановлення контролю над обладнанням і перемикання на резервне обладнання.
- Усунення збою - усунення збою в роботі обладнання.
- Відновлення - відновлення роботи обладнання та відновлення

нормального функціонування системи.

- Аналіз причин - аналіз причин, які призвели до збою в роботі обладнання, і вжиття заходів для запобігання подібних збоїв у майбутньому.
- Такі плани дій дають змогу оперативно реагувати на надзвичайні ситуації та зменшити ризики для безпеки судноплавства.

Дійсно, співпраця з іншими організаціями є важливим аспектом забезпечення інформаційної безпеки в судноплавстві. Це може включати співпрацю з правоохоронними органами, кіберфахівцями та іншими компаніями в індустрії. Наприклад, Міжнародна асоціація класифікаційних товариств (IACS) має угоди про співпрацю з багатьма організаціями, включно з Міжнародною морською організацією (IMO), Міжнародним союзом судновласників (ICS) і Міжнародною організацією зі стандартизації (ISO). Також важливо, щоб компанії в судноплавстві брали участь у спільноті обміну інформацією про загрози та інциденти інформаційної безпеки. Наприклад, Всесвітня асоціація з безпеки судноплавства (BIMCO) створила Групу з безпеки інформації в судноплавстві (ISWG), яка займається обміном інформацією та розробкою рекомендацій щодо забезпечення інформаційної безпеки в судноплавстві. Така співпраця дає змогу отримувати інформацію про нові загрози та методи їх запобігання, а також координувати дії в разі інциденту.

## 1.2. Міжнародні стандарти та рекомендації забезпечення інформаційної безпеки

Забезпечення інформаційної безпеки судноплавства є важливим завданням для забезпечення безпеки судноплавства в цілому. Для цього потрібно вживати відповідні заходи, які включають:

1. Захист інформації, що стосується суден і портів, від несанкціонованого доступу, викрадення, втрати та пошкодження. Для цього необхідно використовувати різні технічні засоби захисту інформації, такі як шифрування, брандмауери, системи виявлення вторгнень тощо.
2. Захист інформації про перевезення небезпечних вантажів, таких як нафта

та інші хімічні речовини, від несанкціонованого доступу.

3. Забезпечення захисту інформації, яка збирається з суден, від несанкціонованого доступу та зміни.
4. Захист від кібератак, які можуть призвести до порушення роботи електронних систем управління судном та портовими системами.
5. Захист від шкідливих програм та вірусів, які можуть негативно вплинути на роботу електронних систем управління судном та портовими системами.
6. Регулярне оновлення програмного забезпечення та систем безпеки для забезпечення захисту від нових загроз та вразливостей.
7. Організація навчання та підвищення кваліфікації персоналу з питань інформаційної безпеки.
8. Розробка та виконання планів дій в разі порушення інформаційної безпеки.

Забезпечення інформаційної безпеки судноплавства є складним і відповідальним завданням, яке потребує відповідального ставлення до захисту інформації.

Крім того, для забезпечення інформаційної безпеки судноплавства використовують різні стандарти та рекомендації, наприклад:

•Міжнародний кодекс з безпеки суден і портових споруд (ICM кодекс) - включає вимоги щодо забезпечення інформаційної безпеки на суднах і в портах.

•Стандарти ISO 27001 та ISO 27002 - визначають вимоги щодо управління інформаційною безпекою в організаціях.

•Рекомендації Міжнародної морської організації (ММО) - включають рекомендації щодо забезпечення інформаційної безпеки в морській індустрії.

•Рекомендації Міжнародної телекомунікаційної спілки (МТС) - включають рекомендації щодо захисту інформації в морській індустрії.

•Крім того, морські компанії та порти можуть найняти спеціалізовані компанії та консультантів, щоб оцінити рівень інформаційної безпеки та розробити плани дій у разі інцидентів.

Загалом, інформаційна безпека судноплавства є важливим аспектом безпеки в морській індустрії, який вимагає постійного моніторингу та вдосконалення.

Дійсно, Міжнародний кодекс з безпеки суден і портових споруд (ISM

кодекс) містить вимоги щодо забезпечення інформаційної безпеки на суднах і в портах. ISM кодекс був розроблений Міжнародною морською організацією (IMO) з метою забезпечення безпеки судноплавства та запобігання забрудненню морського середовища.

Кодекс ISM містить загальні принципи і вимоги щодо безпеки судноплавства та безпеки портових споруд, а також конкретні вимоги щодо забезпечення інформаційної безпеки. Він розглядає питання забезпечення безпеки інформації на борту суден, у тому числі забезпечення захисту від кібератак та забезпечення конфіденційності інформації про грузи, пасажирів і маршрути.

Окрім того, кодекс ISM вимагає від компаній з судноплавства розробки політики і процедур забезпечення інформаційної безпеки, а також проведення навчань і тренувань з цього питання для персоналу. Він також передбачає регулярний аналіз і оцінку ризиків інформаційної безпеки на суднах і в портах та розробку планів дій в разі кібератак та інших інцидентів.

Так, стандарти ISO 27001 та ISO 27002 включають вимоги до управління інформаційною безпекою в організаціях, включаючи організації, які займаються судноплавством та портовою діяльністю. ISO 27001 визначає вимоги до системи управління інформаційною безпекою, в той час як ISO 27002 надає рекомендації щодо застосування цієї системи управління. Ці стандарти допомагають організаціям забезпечувати адекватний рівень захисту інформації та даних, включаючи захист від кібератак, забезпечення конфіденційності, цілісності та доступності даних, а також забезпечення безпеки мереж та інших інформаційних систем.

Для організацій, які займаються судноплавством та портовою діяльністю, важливо враховувати вимоги стандартів ISO 27001 та ISO 27002 при розробці та впровадженні своїх політик та процедур щодо інформаційної безпеки. Окрім цього, для забезпечення інформаційної безпеки в судноплавстві та портовій діяльності використовуються такі міжнародні стандарти та рекомендації:

- Міжнародний кодекс з безпеки суден і портових споруд (ISM кодекс), який включає вимоги щодо забезпечення інформаційної безпеки на суднах і в портах.

- Рекомендації Міжнародної морської організації (ММО) щодо захисту інформації в системах електронного навігаційного обладнання на суднах.
- Стандарти та рекомендації Міжнародної телекомунікаційної співдружності (ІТУ) щодо захисту телекомунікацій в морських та річкових судноплавних системах.
- Рекомендації Міжнародної асоціації портів (ІАП) щодо захисту інформації та даних в портах.

Використання цих стандартів та рекомендацій допомагає забезпечити високий рівень захисту інформації та даних в судноплавстві та портовій діяльності.

Так, Міжнародна морська організація (ММО) також розробляє рекомендації щодо забезпечення інформаційної безпеки в морській індустрії. До цих рекомендацій належать:

1. Risk Management Guidelines (рекомендації з управління ризиками) - документ, який надає вказівки щодо ідентифікації, оцінки та управління ризиками в морській індустрії, включаючи ризики в галузі інформаційної безпеки.
2. Guidelines on Cyber Security Onboard Ships (рекомендації щодо кібербезпеки на суднах) - документ, який містить рекомендації з питань кібербезпеки на суднах, включаючи захист від кібератак та рекомендації щодо розробки та впровадження політик і процедур з кібербезпеки.
3. Guidelines on Maritime Cyber Risk Management (рекомендації щодо управління кіберризиками в морській індустрії) - документ, який надає рекомендації щодо управління кіберризиками в морській індустрії, включаючи визначення ризиків, розробку стратегії управління кіберризиками та розробку процедур реагування на інциденти з кібербезпеки.
4. Guidelines on the Application of SOLAS Chapter XI-2 and the ISPS Code (рекомендації щодо застосування Конвенції SOLAS та Кодексу ISPS) - документ, який містить рекомендації щодо застосування вимог Конвенції SOLAS та Кодексу ISPS, включаючи заходи забезпечення інформаційної безпеки на суднах і портах.

Міжнародна телекомунікаційна спілка (МТС) також створює рекомендації щодо захисту інформації в морській індустрії. Наприклад, МТС розробляє стандарти та рекомендації щодо захисту суднових систем зв'язку та навігації від перешкод та втручання. Вони також займаються питаннями захисту морських кабельних систем від кібератак та інших загроз. Рекомендації МТС є важливими джерелами інформації для розробки національних та міжнародних стандартів щодо захисту інформації в морській індустрії.

Додатковою важливою організацією, яка займається захистом інформації в морській галузі, є Міжнародна асоціація класифікаційних товариств (IACS). IACS розробляє і рекомендує стандарти та вимоги щодо безпеки та надійності морських суден і забезпечує їх дотримання через проведення іспитів та атестацій.

Крім того, національні органи влади країн також приділяють значну увагу питанням інформаційної безпеки в морській галузі. Наприклад, у США федеральне відомство з питань безпеки транспорту (Transportation Security Administration, TSA) має відповідальність за забезпечення безпеки в морському транспорті, включаючи захист інформації на суднах та портах. У Європейському Союзі питання інформаційної безпеки в морській галузі регулюються директивою щодо безпеки морського транспорту (Maritime Transport Security Directive, MTSD).

Загалом, захист інформації в морській галузі є складним завданням, що вимагає уваги і зусиль від багатьох сторін. На даний момент існує значна кількість стандартів, рекомендацій та протоколів, які допомагають забезпечити безпеку та надійність інформації на суднах та в портах. Однак, зважаючи на швидкий технологічний прогрес та поширення кіберзагроз, важливо постійно вдосконалювати та адаптувати заходи захисту до нових умов.

Спеціалізовані компанії та консультанти з інформаційної безпеки можуть надати професійну допомогу морським компаніям та портам у питаннях інформаційної безпеки. Це може включати проведення аудитів безпеки, оцінку ризиків, розробку та впровадження політик та процедур інформаційної безпеки, а також навчання персоналу та розробку планів дій у разі інцидентів. Важливо зазначити, що такі консультанти повинні мати відповідні кваліфікації та досвід

роботи в галузі інформаційної безпеки, щоб забезпечити високий рівень якості послуг.

Також, морські компанії та порти можуть підписати угоди з провайдерами послуг з інформаційної безпеки, які надають послуги з моніторингу, детекції та реагування на кібератаки, а також забезпечують резервне копіювання даних та відновлення систем після інцидентів.

Для забезпечення безпеки в морській індустрії також важливо забезпечити взаємодію між судном та портом, щоб уникнути можливих порушень інформаційної безпеки під час обміну даними між ними. Для цього можуть бути використані стандарти електронного обміну даними, такі як EDIFACT або XML, які забезпечують стандартизований формат даних і протоколи зв'язку.

Усі працівники морських компаній та портів повинні бути свідомі можливих ризиків, пов'язаних з інформаційною безпекою, та вміти виявляти та реагувати на потенційні загрози. Для цього можуть проводитися тренінги та семінари з інформаційної безпеки для персоналу та команд суден.

Отже розглянуті заходи становлять важливість для забезпечення інформаційної безпеки в морській індустрії, а також декілька підходи до забезпечення безпеки інформації на суднах та портах. Серед цих підходів були захист систем та мереж від несанкціонованого доступу, захист конфіденційної інформації, повідомлення про можливі загрози та підвищення свідомості персоналу, регулярне оновлення програмного забезпечення та обладнання, встановлення фізичних та логічних заходів захисту, розробка планів дій в разі кібератак або інших надзвичайних ситуацій та співпраця з організаціями, що борються з кіберзлочинністю та злочинами в морі. Також міжнародні стандарти та рекомендації, які допоможуть компаніям та портам забезпечувати безпеку інформації в морській індустрії. І, нарешті, наголошено на тому, що морські компанії та порти можуть найняти спеціалізовані компанії та консультантів, для оцінки рівню інформаційної безпеки та розроблення плану дій у разі інцидентів.

## 1.3. Практичні аспекти забезпечення інформаційної безпеки судна

Метою загроз до інформаційної безпеки на судні є здійснення незаконних дій, таких як витік конфіденційної інформації, втручання у систему управління судном, шахрайство, вимагання викупу за доступ до важливих даних тощо. Крім того, можуть існувати загрози, пов'язані з ризиками кібератак на системи керування та навігації суден, що можуть призвести до серйозних наслідків, таких як аварії та загибель людей. Таким чином, метою заходів із захисту інформаційної безпеки на судні є забезпечення безпеки людей та забезпечення стабільності функціонування судна та його систем управління в умовах зростаючих загроз від кіберзлочинців.

Під засобами забезпечення інформаційної безпеки судна прийнято розуміти сукупність заходів спрямованих на забезпечення цілісності, доступності і, якщо необхідно, конфіденційності інформації та ресурсів, що використовуються для її обробки.

Сучасні суднові інформаційні системи представляють наступну інформацію:

- Дані про власне судно (поточне місце, кінематичні параметри, минулий шлях, запланований маршрут та ряд інших елементів);

- Радіолокаційне зображення та кінематичні параметри цілей с засобів автоматичної радіолокаційної прокладки;

- Дані з автоматичної ідентифікаційної системи про інші судна;

- Відомості про навігаційні огорожі, про оптичні та радіотехнічні навігаційні засоби, настанови для плавання;

- Інформацію берегових систем управління рухом;

- Гідрометеорологічні відомості про поточний стан погоди, дані про льодову обстановку, прогноз, тощо;

Варто зазначити що недоліком сучасних систем управління морськими транспортними суднами є висока частка участі людини у процедурі прийняття рішення та велика залежність процесу управління від психофізичного стану фахівців. Ключовим моментом при розгляді питань, що стосуються забезпечення безпеки інформаційних систем є виняткова важливість та необхідність

використання системного підходу до вирішення даної проблеми. Це пояснюється тією обставиною, що безпека системи в цілому обумовлюється безпекою її найслабшої ланки. З цього приводу, набуває принципової важливості розгляд проблеми в комплексі, інакше вжиті заходи не принесуть очікуваного ефекту або виявляться надмірними та невиправдано дорогими.

Іншим важливим моментом під час вирішення питань безпеки інформаційних систем судна є принцип дотримання балансу. Слід чітко розуміти, що забезпечення абсолютної безпеки практично неможливе. Захистити від усього різноманіття загроз неможливо з цілої низки причин, серед яких досить назвати лише деякі:

- абсолютний захист зробить інформаційну систему практично недоступною та непридатною для використання;
- не всі можливі шляхи подолання системи забезпечення безпеки можуть бути відомі і, отже, не всім загрозам може протистояти застосована система забезпечення безпеки;
- безпека комп'ютерних систем судна залежить від "людського фактору".

Таким чином ще раз за необхідне підкреслити, що будь-які заходи не можуть гарантувати абсолютну безпеку. З цієї причини слід досягати такого співвідношення складності системи забезпечення безпеки та реальних умов функціонування інформаційних систем, яке не призводило до перевищення вартості розробки, впровадження, експлуатації та обслуговування системи забезпечення безпеки над величиною можливої шкоди у разі її порушення. Концептуальна модель безпеки судна представлена на рис. 1;

Об'єктами загроз на судні можуть бути як апаратні засоби, так і програмне забезпечення. Серед апаратних засобів можна виділити комп'ютери та інші пристрої, що містять важливу інформацію (наприклад, GPS-навігатори, радіосистеми, ехолоти), а також комунікаційні засоби (наприклад, супутникові телефони). Програмне забезпечення може бути вразливим до атак, які можуть знищити або зламати його. До цих атак відносяться віруси, черви, троянські програми, шпигунське програмне забезпечення тощо.

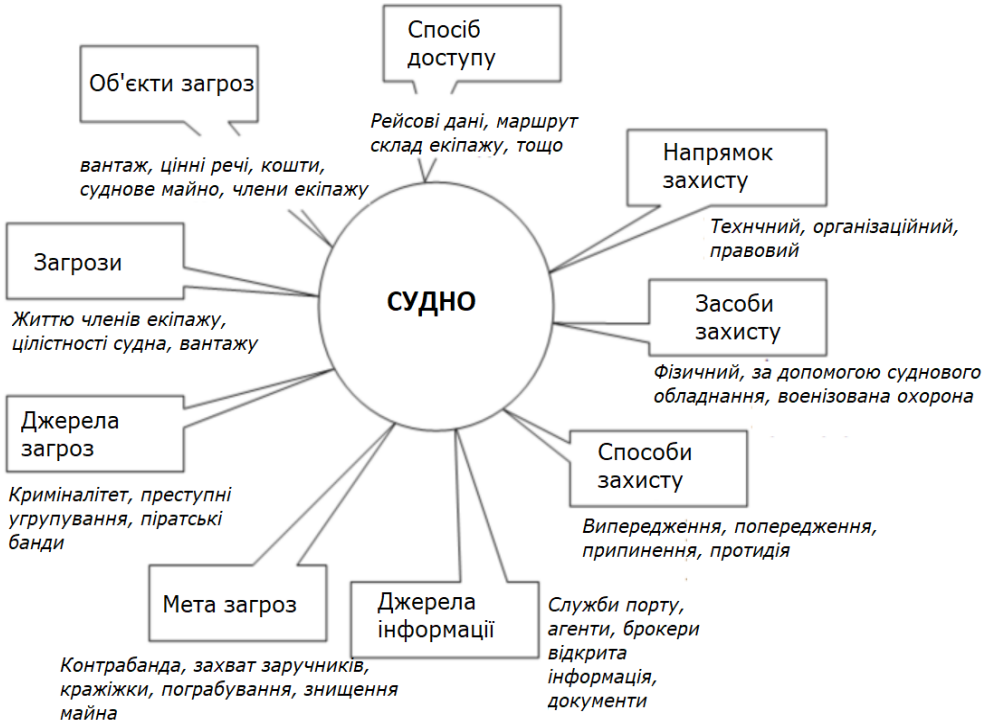


**Рис. 1 - Концептуальна модель безпеки судна**

Також об'єктом загрози може стати людський фактор, коли члени екіпажу судна надають доступ до важливої інформації стороннім особам, не забезпечуючи достатнього контролю за доступом іншими працівниками. У зв'язку з цим, необхідно ретельно вивчати всі можливі об'єкти загроз та приймати всі необхідні заходи з їх забезпеченням.

Способи доступу до даних на судні можуть залежати від того, які системи збереження даних використовуються на судні. Найпоширенішими способами доступу до даних на судні є:

1. Доступ через комп'ютери та інші пристрої на борту судна: це можуть бути персональні комп'ютери, планшети, смартфони, які використовуються для керування системами судна, моніторингу стану судна та навігації.

2. Доступ до систем управління судном (Shipboard Control Systems): це можуть бути системи автоматичного керування судном, системи контролю за енергозабезпеченням, системи контролю за рухом судна, системи автоматичного розпізнавання голосу, системи відеоспостереження тощо.

3. Доступ до систем зв'язку на судні: це можуть бути системи супутникового зв'язку, радіозв'язку, мережі Wi-Fi на борту судна.

4. Доступ до систем збереження та обробки даних на судні: це можуть бути системи управління грузом, системи пасажирського обслуговування, системи навігації, системи енергозабезпечення, системи безпеки та протипожежного захисту.

Ці способи доступу до даних на судні можуть бути використані зловмисниками для здійснення кібератак на судно. Тому важливо забезпечити захист всіх систем, які зберігають та обробляють конфіденційну інформацію на борту судна.

Напрямки захисту включають:

1. Фізичний захист: контроль доступу до приміщень, обмеження доступу до обладнання та інфраструктури, встановлення систем відеоспостереження та сигналізації.

2. Логічний захист: шифрування даних, контроль доступу до мережі, встановлення програмного забезпечення для виявлення та запобігання кібератак.

3. Організаційний захист: розробка політики інформаційної безпеки, проведення навчання та підвищення обізнанності персоналу, регулярні аудити безпеки та оновлення систем захисту.

4. Захист даних: визначення класифікації даних, контроль доступу до них, резервне копіювання та забезпечення безпеки під час зберігання та передачі.

5. Планування та реагування на інциденти: розробка планів дій у разі кібератак та інших надзвичайних ситуацій, регулярні тренування та тестування планів, виявлення та відновлення роботи систем після інцидентів.

Існує безліч засобів захисту судна від кібератак і злочинної діяльності. Основні засоби захисту включають:

- Фізична безпека: це забезпечення безпеки фізичного доступу до комп'ютерних систем та мереж на судні. Це може включати встановлення фізичних засобів захисту, таких як система контролю доступу, відеоспостереження та інші пристрої.
- Шифрування: шифрування даних - це процес перетворення звичайного тексту в криптографічно захищений текст за допомогою спеціальних алгоритмів. Шифрування захищає дані від несанкціонованого доступу та злому.
- Віддалений доступ: забезпечення безпечного віддаленого доступу до

комп'ютерних систем та мереж на судні. Це дозволяє диспетчерам та іншим відповідальним особам з допомогою безпечних засобів доступу керувати системами та мережами на судні з-поза судна.

- Антивірусне програмне забезпечення: програмне забезпечення, яке призначене для виявлення та блокування вірусів, черв'яків та інших шкідливих програм. Воно допомагає запобігти атакам на системи та мережі на судні.
- Брандмауер: програмне забезпечення або апаратне забезпечення, яке захищає комп'ютерні системи та мережі від несанкціонованого доступу, вірусів та інших загроз з мережі Інтернет.
- Контроль доступу: це система, яка дозволяє обмежувати фізичний та логічний доступ до комп'ютерних систем та мереж на судні.
- Система виявлення вторгнень: програмне забезпечення або апаратне забезпечення, яке призначене для виявлення спроб несанкціонованого доступу.

Втім існують два основних варіанти щодо забезпечення безпеки суднової інформації: самостійний та із залученням фахівців-консультантів. Перший підхід виявив свою неспроможність у сучасних умовах через неможливість передбачити всі можливі ймовірні загрози та розмір можливої шкоди від їх прояву, що визначає жорсткі вимоги до питання захисту інформації та другий експертний що передбачає більш професійний підхід.

Приступаючи до вирішення завдання забезпечення інформаційної безпеки, необхідна побудова її моделі і чітке визначення проблем. При цьому формальну модель на першому етапі бажано розглядати на концептуальному рівні, не зупиняючись на конкретних особливостях інформаційних систем. Далі після розгляду принципів стратегії розробки системи забезпечення безпеки рекомендується перейти до реального змісту концептуальних положень і здебільшого такий підхід є виправданим.

Найважливішим чинником при побудові формальної моделі безпеки є поняття "середовища безпеки" Необхідність введення даного терміну визначається тим, що безпека інформаційної системи судна не може забезпечуватися за будь-яких умов. Таким чином, поняття "середовище безпеки" служить для обмеження (визначення) областей безпеки суднових системи.

У багатьох дослідженнях проблеми безпеки інформаційних систем у складі

середовища безпеки виділяють кілька самостійних компонентів, кожен з яких утворює певну область безпеки, що відповідає тому чи іншому аспекту забезпечення безпеки. Іншими словами, дані області дозволяють декомпозувати проблему забезпечення безпеки суднових систем та вирішувати її частинами.

На жаль, проблеми інформаційної безпеки найчастіше відносять до другорядних, або взагалі змішують їх із загальними проблемами безпеки та автоматизації. При цьому передбачається, що у разі виникнення проблем, пов'язаних з порушенням конфіденційності, цілісності інформації, вдасться вжити своєчасних і адекватних заходів, однак як свідчить практика, такий підхід не є виправданим з приводу того що:

1) Раптовість атаки може призвести до таких наслідків, що реакція на неї вже не матиме сенсу.
2) При описаному вище підході керівництво перебуває у стані очікування будь-яких порушень інформаційної системі як наслідки інформаційної атаки. Якщо говорити про витік інформації, то, зазвичай, подібні факти виявляються з великим запізненням. До моменту прояву і згодом можна буде лише констатувати про відсутність своєчасно вжитих заходів захисту.
3) Вживання заходів захисту в терміновому порядку може призвести до неадекватної оцінки ситуації з боку екіпажу судна, що, безсумнівно, позначиться на якості його роботи. Крім того, якість будь-якого рішення в умовах дефіциту часу знижується, і швидше за все створити оптимальну систему захисту даних не вдасться.

Сучасний підхід до захисту інформації від несанкціонованого доступу полягає у комплексному застосуванні організаційних та технічних заходів. Заходи для забезпечення безпеки конфіденційної інформації проводяться, як правило, у трьох основних напрямках: захист від витоку технічних каналів, захист від несанкціонованого доступу до комп'ютерної інформації, обмеження вільного доступу сторонніх осіб до приміщень, де встановлено суднове критичне обладнання. Комплекс заходів, що необхідні для забезпечення безпеки інформації, визначається виходячи з необхідного рівня захищеності конкретного об'єкта і з допустимого рівня ризику, тому на попередньому етапі при розробці

плану захисту має проводитися визначення ймовірних загроз і розмірів можливих збитків від їх прояву. Крім того, необхідно враховувати гарантію безконфліктності функціонування встановлених засобів захисту для забезпечення надійності загальної системи захисту. Зрештою, неможливо побудувати систему інформаційної безпеки без урахування вимог нормативних документів, яких чимало, тому необхідне як глибоке знання змісту документів, так і певний досвід практичної діяльності з їх використання. Щодо базових принципів забезпечення інформаційного захисту необхідно відділити наступні:

- Цілісність даних – захист від збоїв що призводять до втрати інформації, захист від неавторизованого створювання і знищення даних;
- Конфіденційність інформації та доступ до неї авторизованих користувачів.

Також можна виділити кілька основних етапів створення системи захисту, однак насамперед доцільно з'ясувати та визначити загрози інформаційній безпеці та можливі збитки які вони можуть завдати після прояву, тобто аналіз ризиків. Основні проблеми під час проведення такого аналізу виникають у зв'язку зі складністю визначення кількісного значення ймовірності прояву тих чи інших загроз та розміру можливих збитків від їхнього впливу. Тому захищеність інформації на судні описується якісними показниками, набір яких визначається спеціальними методиками.

З аналізу ризиків розробляється план захисту, що містить повний опис всіх рекомендованих заходів для захисту інформації.

- інструкція для керівництва компанії;
- модель потенційних загроз;
- економічне обґрунтування запропонованих рекомендацій;
- календарні план впровадження систем захисту;
- перелік відомостей, що становлять комерційну таємницю;
- перелік організаційних заходів та документів;
- рекомендації щодо виконання вимог керівних документів.

Склад технічних засобів визначається на основі чітких критеріїв, що виділяються у вигляді рекомендацій щодо вибору засобів захисту. Наступним етапом після виявлення можливих загроз та визначення заходів щодо їх

нейтралізації є створення спеціального підрозділу у компанії або відповідальної особи, яка відповідає за виконання плану захисту суден. Та визначення завдань, чисельності, складу технічних засобів, характеру та режиму взаємодії його з іншими службами.

Регулювання взаємовідносин членів екіпажу щодо правил і режиму використання спеціальних технічних засобів при вирішенні завдань інформаційної безпеки є ще одним видом завдань для професійної організації системи захисту інформації на судні тому регламентуючі документи, що стосуються організації систем захисту, повинні розглядати всі можливі ситуації, пов'язані з експлуатацією суднових інформаційних систем.

## 1.4. Перспективи та технології майбутнього у захисті інформації судна

Існує безліч перспективних технологій, які можуть використовуватися для забезпечення інформаційної безпеки на судні. Деякі з них уже використовуються в деяких галузях і можуть стати більш широко поширеними в майбутньому. Деякі з цих технологій включають:

- Блокчейн - технологія розподіленого зберігання даних, яка може забезпечити захист від кібератак шляхом створення надійного ланцюжка блоків, які не можна змінити без консенсусу всіх учасників мережі.
- Штучний інтелект - може використовуватися для виявлення загроз і аналізу великих обсягів даних, що дає змогу ефективніше захищати інформацію на судні.
- Квантові технології - квантові комп'ютери можуть вирішувати складні завдання шифрування, які не можуть бути розгадані класичними комп'ютерами. Це може бути корисно для захисту інформації на судні.
- Кіберфізичні системи - це інтеграція фізичних систем з мережевими технологіями, що дає змогу забезпечити більший ступінь захисту за допомогою різних сенсорів і пристроїв, які можуть реагувати на загрози.
- Квантова криптографія - це методи шифрування, засновані на принципах квантової механіки, які забезпечують вищий рівень безпеки, ніж класичні методи

шифрування.

Загалом, ці технології все ще перебувають на початковій стадії розвитку, і майбутнє їхнього використання на судні залежатиме від багатьох чинників, включно з їхньою ефективністю, доступністю та вартістю. Однак, з розвитком технологій, можна очікувати, що з'являтимуться дедалі новіші та більш просунуті засоби і методи захисту інформації на судні.

Блокчейн - це технологія розподіленого зберігання даних, яка може використовуватися для забезпечення безпеки інформації на судні. Блокчейн заснований на децентралізації та криптографії, що забезпечує високий рівень захисту даних від несанкціонованого доступу (Рис.2).


**Рис.2 - Транспортні перевезення з використанням технології блокчейн**

З використанням блокчейн-технології на судні можна реалізувати систему, де кожен член екіпажу має доступ тільки до певних даних, а всі зміни та операції з даними фіксуються в блокчейн-сховищі, що дає змогу контролювати історію змін і відстежувати будь-які несанкціоновані дії. Наприклад, система блокчейн може використовуватися для управління контейнерами на судні, де кожен контейнер має унікальний код, що фіксується в блокчейн-сховищі. Таким чином, можна забезпечити більш безпечний та ефективний контроль за переміщенням контейнерів на судні. Однак, використання блокчейн-технології на судні вимагає високого ступеня автоматизації та комп'ютеризації процесів, що може вимагати додаткових витрат на обладнання та програмне забезпечення.

Так, штучний інтелект може використовуватися для виявлення загроз на

судні і в порту, а також для автоматичного реагування на ці загрози. Наприклад, застосування систем машинного навчання для аналізу поведінки користувачів і виявлення аномальних дій, що можуть свідчити про кібератаку. Такі системи можуть автоматично відключати доступ користувача до системи або запускати інші захисні механізми. Крім того, штучний інтелект може використовуватися для розробки інтелектуальних систем моніторингу, які будуть автоматично виявляти загрози на судні і в порту і реагувати на них. Наприклад, система відеоспостереження зі штучним інтелектом може автоматично виявляти підозрілі об'єкти або дії, такі як незаконне проникнення на борт судна або порушення правил безпеки в порту.

Також можна використовувати штучний інтелект для аналізу великих обсягів даних, які збираються на судні, для виявлення потенційних загроз і вдосконалення систем захисту в режимі реального часу.

Квантові технології можуть мати потенціал для інформаційної безпеки суден у майбутньому. Наприклад, квантове шифрування може забезпечити більш високий рівень захисту даних на судні, оскільки воно базується на квантових властивостях матеріалів, які є надзвичайно складними для взлому. Крім того, квантові комп'ютери можуть бути використані для розв'язання складних задач, пов'язаних з інформаційною безпекою, таких як аналіз великих обсягів даних і прогнозування можливих кібератак. Однак, застосування квантових технологій для захисту інформації на суднах потребує подальших досліджень і розробок, а також значних інвестицій.

Кіберфізичні системи - це системи, які поєднують фізичні та кібернетичні елементи в єдину систему, де кожен компонент взаємодіє з іншими компонентами та середовищем навколо них. У контексті інформаційної безпеки судна, кіберфізичні системи можуть бути використані для автоматизованого контролю та управління різними аспектами безпеки, включаючи виявлення вторгнень, контроль доступу до систем та даних, інформаційну аналітику та прийняття рішень в режимі реального часу.

Кіберфізичні системи використовують різноманітні технології, включаючи мережі датчиків та інтернет речей (IoT), системи автоматичного управління (SCADA), технології машинного навчання та штучного інтелекту, а також засоби

збору та обробки даних.

У контексті судноплавства, кіберфізичні системи можуть бути використані для покращення безпеки та ефективності суден, зменшення ризику аварій та забезпечення надійності комунікації та обміну даними між суднами та портами. Окрім цього, кіберфізичні системи можуть бути використані для моніторингу динаміки стану судна, що дозволяє зменшити ризик аварій та оптимізувати роботу обладнання, забезпечуючи максимальну безпеку та ефективність роботи судна.

Квантова криптографія - це технологія, що використовує властивості квантових систем для захисту передачі даних від несанкціонованого доступу та зламу. Вона використовує квантові стани для забезпечення безпеки передачі даних, відрізняючись від класичних криптографічних методів, що базуються на обчислювальних складнощах. За допомогою квантових систем можна створювати криптографічні ключі, які не можуть бути зламані класичними методами, тому що будь-яка спроба зламати ключ буде змінювати квантовий стан системи, що буде помічено.

У майбутньому квантова криптографія може бути використана для забезпечення захисту передачі даних на суднах, що дозволить зменшити загрозу кібератак та забезпечити більш високий рівень інформаційної безпеки. Однак, на даний момент, квантова криптографія ще не є повністю комерційно доступною технологією, і її застосування обмежене відносною складністю квантових систем і низькою масштабованістю реалізації.

## 1.5. Роль портової влади та судновласників у забезпеченні інформаційної безпеки судна

Крім технічних заходів, люди також є важливою складовою системи інформаційної безпеки на судні. Людський фактор може створювати істотні ризики для безпеки інформації, тому необхідно забезпечити належний рівень освіти та підготовки екіпажу. До ризиків, пов'язаних з людським фактором, можна віднести такі:

1. Несанкціонований доступ до інформації адже людина може несанкціоновано отримати доступ до інформації, що створює загрозу для безпеки інформації. Це може бути зумовлено злочинними намірами або просто відсутністю достатнього рівня усвідомлення з боку працівника.
2. Соціальна інженерія де злочинці можуть використовувати соціальну інженерію для отримання доступу до інформації, використовуючи при цьому невпевненість, довіру або недостатню освіту працівників.
3. Неправильна обробка інформації або недбале ставлення до інформації, її неправильна обробка або передача можуть створювати загрози для безпеки інформації на судні.
4. Недостатня свідомість, відсутність належної освіти або свідомості щодо інформаційної безпеки можуть призвести до недостатнього рівня захисту інформації на судні.

Для зменшення ризиків, пов'язаних з люлським фактором, необхідно проводити належну освіту та навчання екіпажу щодо інформаційної безпеки. Крім того, важливо забезпечити дотримання внутрішніх правил та процедур, а також контролювати доступ до інформації.

Людський фактор є одним із ключових аспектів інформаційної безпеки судна. Незалежно від того, які технології та процедури використовуються на судні для захисту інформації, людський фактор може виявитися слабкою ланкою, яка може призвести до порушення безпеки даних на судні. Приклади людських помилок, які можуть призвести до вразливості інформаційної безпеки на судні, включають в себе неправильне встановлення паролів або їх ненадійність, залишення пристроїв із доступом до конфіденційної інформації без належного захисту. Також відкриття шкідливих вкладень в електронній пошті або перехід за посиланнями, які можуть призвести до інфікування комп'ютера вірусом. Неправильне налаштування безпеки мережевих пристроїв на судні, неправильне використання та обробка конфіденційної інформації.

Щоб мінімізувати ризики, пов'язані з людським фактором, необхідно проводити навчання і тренінги для екіпажу, щоб підвищити їхню обізнаність про безпеку інформації на судні. Також слід встановлювати належні процедури і політики щодо захисту інформації, щоб скоротити можливість людських

помилок.

Тому судновласники та керівники морських компаній повинні надавати своїм працівникам достатню кількість навчань та тренінгів щодо захисту інформації та кібербезпеки. Важливо також регулярно проводити тестування працівників на їхню компетентність у питаннях кібербезпекию. Необхідно мати чітко встановлені правила доступу до інформації на судні, включаючи контроль доступу до фізичного обладнання та програмного забезпечення. Важливо вживати заходів для запобігання соціальному інжинірингу, зокрема забороняти спілкування з незнайомими особами, особливо щодо обміну конфіденційною інформацією. Необхідно також встановлювати процедури реагування на інциденти зі зберігання та обробки інформації на судні. При виборі постачальників обладнання та програмного забезпечення необхідно приділяти увагу їхній репутації та досвіду в галузі кібербезпеки.

На суднах слід встановлювати системи моніторингу трафіку, що дозволять виявляти незвичайні підключення до мережі, а також системи виявлення вторгнень та інші засоби для раннього виявлення та запобігання інцидентів. Необхідно також забезпечити резервне копіювання важливих даних, а також розробити плани дій в разі кібератак та інших інцидентів з інформацією.

Крім розробки політик і стандартів, важливо навчати персонал судна про заходи безпеки інформації та використання інструментів захисту. Персонал повинен бути вмілим у розпізнаванні загроз і практичному застосуванні процедур захисту, таких як встановлення паролів, зашифрування даних, контроль доступу тощо. Постійне оновлення системи безпеки тому що інформаційні загрози постійно змінюються, тому системи захисту повинні постійно оновлюватись і покращуватись, щоб відповідати новим викликам. Системи повинні бути перевірені і оцінені регулярно для виявлення слабких місць і покращення заходів безпеки.

Співпраця з партнерами і постачальниками послуг з приводу того що у сучасному світі більшість компаній працює з різними партнерами і постачальниками послуг, тому важливо, щоб всі з них дотримувалися високих стандартів безпеки інформації. Угоди з постачальниками повинні містити вимоги щодо захисту інформації та механізми їх забезпечення. Навіть з усіма

заходами безпеки інформації, інциденти все ж можуть траплятись. Важливо мати процедури виявлення інцидентів, оцінки їх серйозності, вжиття заходів для зупинки та усунення інцидентів, а також повідомлення про них відповідним органам. Загалом, захист інформації на судні - це комплексний процес, який потребує поєднання технічних, організаційних і людських заходів.

Забезпечення інформаційної безпеки є важливим завданням для багатьох країн, оскільки це необхідно для захисту державних інтересів і забезпечення економічної безпеки. Різні країни вживають різних заходів для забезпечення інформаційної безпеки, зокрема розробляють законодавчі акти, створюють національні центри кібербезпеки, проводять навчання і тренінги, а також здійснюють міжнародне співробітництво в галузі кібербезпеки.

Деякі країни розробляють свої національні стратегії та програми із забезпечення інформаційної безпеки, наприклад, США мають національну стратегію кібербезпеки та програму із забезпечення кібербезпеки критичної інфраструктури. У Європейському союзі було розроблено Загальну стратегію кібербезпеки ЄС і Національні стратегії кібербезпеки.

Також проводиться міжнародне співробітництво в галузі кібербезпеки, зокрема шляхом підписання міжнародних договорів і угод. Наприклад, Рада Європи ухвалила Конвенцію про кіберзлочинність, а США і Китай підписали Угоду про взаємне нерозголошення кібератак. Також проводяться спільні навчання і тренінги міжнародних команд з кібербезпеки.

Деякі країни також розробляють свої національні закони і регулятивні акти, спрямовані на забезпечення інформаційної безпеки. Наприклад у США діє Закон про інформаційну безпеку, а в ЄС запроваджено загальний регламент про захист персональних даних. Таким чином, забезпечення інформаційної безпеки є важливим питанням для багатьох країн і розглядається як національний пріоритет. Країни вживають різних заходів для забезпечення безпеки своїх інформаційних систем і національної кіберінфраструктури, а також співпрацюють на досягнення високого рівню безпеки.

У сфері забезпечення інформаційної безпеки суден і портів існують міжнародні організації та стандарти, які ставлять завдання забезпечити безпеку на міжнародному рівні. Однією з таких організацій є Міжнародна морська

організація (ММО), яка розробила Міжнародний кодекс із забезпечення безпеки суден і портів (ISPS Code). Цей кодекс визначає вимоги до систем забезпечення безпеки на борту суден і в портах, а також встановлює процедури, які мають бути виконані для захисту судна, вантажів і пасажирів.

Крім того, існують різні міжнародні стандарти щодо забезпечення інформаційної безпеки, такі як стандарти ISO 27001 та ISO 27002. Ці стандарти визначають вимоги до систем управління інформаційною безпекою в організаціях і надають рекомендації щодо захисту інформації.

Різні країни також розробляють свої національні нормативні акти і стандарти щодо забезпечення інформаційної безпеки суден і портів, які часто засновані на міжнародних стандартах і вимогах. Однак, деякі країни можуть мати свої власні особливості та специфічні вимоги, які відрізняються від міжнародних стандартів і норм. Загалом, забезпечення інформаційної безпеки в морській індустрії вимагає глобального підходу, врахування міжнародних стандартів і нормативних актів, а також співробітництва та координації між країнами та міжнародними організаціями.

Портова влада відіграє важливу роль у забезпеченні інформаційної безпеки судна. По-перше, вона може встановити правила і стандарти для захисту інформації на судні, яких мають дотримуватися всі судна, що заходять у порт. По-друге, портова влада може перевіряти судна на відповідність цим стандартам і вимогам, а також забезпечувати навчання і вдосконалення кваліфікації персоналу, відповідального за інформаційну безпеку на судні.

Крім того, портова влада може співпрацювати з іншими державними та міжнародними організаціями, такими як Міжнародна морська організація (IMO), для розроблення стандартів і рекомендацій у сфері інформаційної безпеки на суднах і портах. Також портова влада може співпрацювати з приватними компаніями та консультантами, щоб поліпшити захист інформації на суднах і в портах.

Загалом, забезпечення інформаційної безпеки судна вимагає зусиль з боку всіх учасників морської індустрії, включно з портовою владою, судновласниками, перевізниками, консультантами та іншими. Воно охоплює різні аспекти, як-от захист інформації, забезпечення фізичної безпеки судна та

екіпажу, навчання персоналу тощо.

Судновласники відіграють ключову роль у забезпеченні інформаційної безпеки судна. Вони несуть відповідальність за підтримання безпеки інформаційних систем і даних на борту судна, а також за захист цих систем від зовнішніх загроз.

Для забезпечення інформаційної безпеки судна судновласникам необхідно регулярно оновлювати програмне забезпечення та апаратне забезпечення на борту судна, зокрема системи захисту від вірусів і зловмисників. Вони також повинні переконатися в тому, що ці системи працюють належним чином і не мають вразливостей.

Судновласники також повинні навчати членів екіпажу судна правилам безпеки і регулярно проводити тренування для поліпшення рівня обізнаності екіпажу в галузі інформаційної безпеки. Крім того, судновласники повинні співпрацювати з портовою владою та іншими зацікавленими сторонами в забезпеченні безпеки суднових операцій та інформаційної безпеки. Вони також можуть наймати фахівців і консультантів для забезпечення високого рівня інформаційної безпеки на своїх суднах.

Додаткові аспекти, які можуть бути пов'язані з інформаційною безпекою судна це співпраця з іншими судновласниками і портовою владою: судновласники можуть співпрацювати з іншими компаніями і портовою владою, щоб обмінюватися інформацією про потенційні загрози і оцінювати рівень ризику. Це може допомогти поліпшити безпеку не тільки на окремому судні, а й у морській індустрії загалом.

Навчання екіпажу адже екіпаж судна повинен мати необхідні знання і навички щодо забезпечення інформаційної безпеки, щоб правильно поводитися з обладнанням і програмним забезпеченням на борту судна. Навчання має проводитися регулярно, щоб екіпаж міг ефективно реагувати на можливі загрози. Впровадження стандартів з боку судновласників які можуть впроваджувати стандарти і рекомендації в галузі інформаційної безпеки, такі як ISO/IEC 27001, щоб забезпечити дотримання належних процедур і захистити інформацію на борту судна. Використання спеціалізованого програмного забезпечення, судновласники можуть використовувати спеціалізоване програмне забезпечення

для захисту даних і управління доступом на борту судна. Наприклад, можуть бути використані системи управління доступом, шифрування даних і виявлення вторгнень.

Взаємодія з постачальниками послуг де судновласники можуть співпрацювати з постачальниками послуг, такими як постачальники хмарних рішень і провайдери інтернет-з'єднань, щоб забезпечити безпеку своїх систем і даних. Також може бути важливо перевіряти безпеку постачальників послуг, щоб уникнути ризиків, пов'язаних з їхніми діями. Регулярна оцінка рівня ризику з боку судновласників, які повинні проводити регулярну оцінку рівня ризику, пов'язаного з інформаційною безпекою на борту судна. Це дасть їм змогу реагувати на нові загрози і покращувати свої системи безпеки.

**Висновки**.

Для забезпечення інформаційної безпеки на судні необхідно вживати комплекс заходів, що охоплює технічні та організаційні засоби захисту, а також навчання і забезпечення культури безпеки серед персоналу. Технології майбутнього, такі як блокчейн, штучний інтелект, квантові технології та кіберфізичні системи, можуть допомогти в підвищенні рівня захисту на суднах. Важливу роль у забезпеченні інформаційної безпеки судна відіграють міжнародні нормативні документи, як-от ISPS-код і рекомендації ММО та МТС. Однак, існує необхідність у поліпшенні міжнародного співробітництва в галузі інформаційної безпеки судна і забезпечення узгоджених стандартів і правил. Важливу роль у цьому процесі відіграють портова влада і судновласники, які повинні брати активну участь у забезпеченні безпеки на своїх суднах і співпрацювати з міжнародними організаціями та іншими країнами. Для побудови ефективної системи захисту та інформаційної безпеки судна необхідно проведення ретельного аналізу законодавчої бази та сучасних існуючих засобів захисту інформації в інших галузях. Правильний вибір методів та засобів захисту інформації дозволить організувати оптимальну та гнучку систему та забезпечить необхідний рівень її надійності та захищеності. За необхідне є реалізація єдиних

підходів щодо інтеграції систем зв'язку, навігації, гідрометеорологічного забезпечення з метою створення єдиного інформаційного простору на основі сучасних цифрових технологій. Також подальший розвиток сучасних інформаційних .технологій та їх впровадження на сучасних суднах у елементах суднового навігаційного обладнання повинно бути узгоджено та скоординовано з береговими інформаційними системами та мати єдині стандарти для їх ефективного сумісного використання.