Захист інформаційного обміну судноплавства

УДК 004; 621.391 Геннадій Вільський
Міжнародний технологічний університет «Миколаївська політехника» , *g_vilsky@mksat.net*

Реалії морської практики говорять і показують доцільність підвищення навігаційної і комерційної безпеки суден, яка залежить від захищеності інформаційного забезпечення судноплавства. Потребують серйозного захисту відомості і повідомлення від появи недостовірних даних, викривлення інформації в результаті цілеспрямованого або випадкового втручання.

Метою роботи є уточнення суднового контенту, якому необхідне посилення захисту і вироблення пропозицій з розширення заходів кібербезпеки в інформаційному обміні судноплавства.

Дослідження інцидентів з морськими суднами говорить про важливість захищеності: логістичної інформації керуючих компаній і судновласника; підтверджуючої оперативної навігаційної інформації, у вигляді друкованої публікації; вихідної з судна інформації щодо забезпечення і приватних переговорів. Особливо небезпечно цілеспрямоване втручання у взаємодію між постами служб регулювання руху суден при реплікації інформації Баз Даних про судна, їх маршрутах, вантажах, графіках руху, яке можливо при відкритості інформації або недостатньої захищеності передачі даних. Випадкове втручання в навігаційні або логістичні повідомлення відбувається, як результат помилкових дій при підготовці відомостей і повідомлень, або технічних збоях, зникненні частини інформації через тимчасову відсутність зв'язку, або інших причин.

Виходячи з дослідження, в інформаційних навігаційно-комерційних системах судноплавства оператори обміну даними повинні реєструватися. Судовим операторам-користувачам (включаючи приватні переговори) додатково повинно пропонувати генерацію ключових пар і присвоєння паролів, а в судновому блоці банку даних, розміщувати відкриті криптографічні ключі. Зазначену вище обмінну інформацію слід зашифровувати і розшифровувати сеансовими ключами, які потрібно міняти при кожному сеансі. Інформацію засвідчують електронним цифровим підписом, за допомогою створених особистих криптографічних ключів та записують в блок банку даних судна, ведуть електронне протоколювання та вхідний і вихідний контроль суперечливості інформації. При виявленні розбіжності даних сеанси припиняються.

Наукові і загальні результати дослідницької роботи містять визначення особливого навігаційно-комерційного контенту і процедурні заходи кібербезпеки інформаційного обміну судноплавства. Запропонований інструментарій, що включає наступні елементи, процеси і дії, як криптографічні ключі, сеансові паролі, шифрування і криптографування суднового контенту, дозволяє забезпечити захищеність достовірності та цілісності інформаційного банку даних руху суден. Реалізація вказаних дій гарантує підвищення рівня інформаційної безпеки судноплавства.