Проблеми забезпечення інформаційної безпеки на водному транспорті в сучасних умовах

Автор: *О.В. Блінцов, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Інформаційна безпека є складовою морської безпеки морського та річкового транспорту будь-якої морської держави і являє собою постійно підтримуваний стан захищеності інформаційних ресурсів від загроз незаконного втручання.

Проблеми забезпечення інформаційної безпеки водного транспорту України у сучасних умовах обумовлені. як зовнішніми, так і внутрішніми загрозами морської безпеки України у цілому. Загрозами морської безпеки України вважаються протиправні дії на морському транспортному комплексі, що здатні призвести до збитків у сфері життєво важливих інтересів особи, суспільства і держави, а також процеси природного або техногенного характеру, викликані цими протиправними діями або намірами.

Основними чинниками для виникнення зовнішніх загроз у сфері морської безпеки України є:

– збільшення технологічного відриву провідних держав миру від України і їх протидія створенню конкурентоздатних українських технологій у морській транспортній сфері.

– економічна, демографічна і культурно-релігійна експансія суміжних держав на територію України;

– активізація діяльності транснаціональної організованої злочинності, а також зарубіжних терористичних організацій;

– діяльність іноземних політичних, економічних, релігійних, військових, розвідувальних і транспортних структур, направлених проти інтересів України в морській сфері;

– загострення міжнародної конкуренції щодо володіння новими морськими транспортними ринками, новими транспортними технологіями у морській сфері;

– прагнення низки країн до домінування на світовому морському транспортному просторі, витіснення України з традиційних морських транспортних ринків та перешкоджання їй виходу на нові.

Та обставина, що по території України пролягає найкоротший шлях між двома континентами - Європою і Азією, створює серйозні проблеми в роботі морського транспортного комплексу, що забезпечує цю сферу.

Можна прогнозувати, що зростання вантажопотоків через порти України буде супроводжуватися і зростанням спроб незаконного використання структурами транснаціональної організованої злочинності суден, морських і річкових портів, а також транспортних коридорів, що проходять по території України, в своїй корисних інтересах [1].

Основним спектром загроз інформаційній безпеці на морському та річковому транспорті сучасної держави є протиправні дії зловмисників, націлені на:

– організацію терористичних акцій (угон або захоплення морських та річкових суден, диверсії проти гідротехнічних споруд та ін.);

– несанкціоноване втручання у функціонування засобів зв'язку водного транспорту, що загрожує життю і здоров'ю пасажирів, несе прямий збиток водному транспортному комплексу, породжує у суспільстві негативні соціально-політичні, економічні, психологічні наслідки;

– кримінальні дії проти пасажирів;

– кримінальні дії проти вантажів.

У XXI столітті перед всезростаючим обсягом міжнародної торгівлі (морський транспорт продовжує обслуговувати близько 90% міжнародних комерційних перевезень) постала проблема протидії морському піратству та збройному пограбуванню суден, як одна зі складових боротьби з міжнародним тероризмом.

За останні роки зазнали піратських нападів судна понад 62 країн світу у прибережних морях 56 країн. Особливої гостроти ця проблема набула в районі Аденської затоки, східного узбережжя Сомалі і Червоного моря, що стало реально загрожувати сформованій системі світових торгових перевезень.

Протиправні дії мають місце і на р. Дунай, де українські судна піддаються збройному грабежу, особливо в районі від 240 до 350 км під час проведення переформування складу караванів для проходження рукавом Борча-Бала, а також в зоні відповідальності портів: Хірш, Фетешті, Галац, Чорна вода, а також рукава Борча в зоні Бордушани [2]. Ці злочини супроводжуються широким застосуванням сучасних технічних засобів телекомунікацій, у першу чергу, радіо- та стільникового зв'язку.

Таким чином, забезпечення інформаційної безпеки на водному транспорті є актуальним завданням як для морських, так і для річкових перевезень.

Головною метою зловмисників при їх атаках на інформаційні ресурси суден є їхні навігаційно-інформаційні системи та системи оперативного морського зв'язку. Для їх захисту використовують апробовані на практиці стандартні заходи: криптографічне кодування, політику паролів, електронний цифровий підпис тощо. Для захисту офіційних векторних карт

Міжнародною гідрографічною організацією (МГО, в англомовній літературі – International Hydrographic Organization, IHO) розроблено спеціальний стандарт S63 “IHO Data Protection Scheme”, яки визначає перелік заходів з метою [3]:

– попередження несанкціонованого копіювання електронних навігаційних карт;

– обмеження доступу тільки до тих карт колекції, на які користувачем отримано доступ;

– забезпечення гарантії того, що електронні навігаційні карти надійшли з уповноваженого джерела.

Аналіз показує, що за останні роки до переліку вже добре відомих технологій злочинного втручання у засоби зв’язку (несанкціонований доступ до інформації, блокування доступу тощо) додались ще три нових види загроз для інформаційних ресурсів, що використовуються на водного транспорті:

– несанкціонований доступ до каналів супутникового обміну між судном та офісом його керування з метою отримання оперативної інформації про техніний стан та завдання судна чи іншого рухомого об’єкту;

– викривлення навігаційних GPS-даних, які отримуються судном чи іншим рухомим об’єктом, з метою направлення його руху по хибній траєкторії;

– несанкціонований доступ до супутникового каналу оперативного керування судном чи іншим рухомим об’єктом з метою його викрадення або знищення.

Щодо першої загрози, то схожі задачі вже успішно розв’язувались іракськими повстанцями по відношенню до безпілотних літальних апаратів (БПЛА) США. Так, у 2009 році з’ясувалося, що вони за допомогою супутникової антени-тарілки і купленого в Інтернеті російського програмного забезпечення «SkyGrabber» перехоплювали розвідувальні відеопотоки з американських БПЛА і, тим самим, успішно планували власні військові контроперації. Це стало можливо завдяки тому, що на БПЛА RQ/MQ-1 Predator і MQ-9 Reaper використовувалися нешифровані канали зв’язку.

Програма «SkyGrabber» була розроблена як засіб «супутникового рибальства», щоб перехоплювати музику, фотографії, відео й інший контент, який несанкціоновані користувачі «закачують» з Інтернету [4]. Пакет «SkyGrabber» приймає й обробляє трафік, переданий з супутника, вилучає з нього файли й зберігає їх на жорсткий диск користувача відповідно до налагоджених фільтрів. На сьогодні програма працює тільки з незашифрованими даними, які передаються через VPN-з'єднання (Virtual Private Network – віртуальна приватна закрита мережа [5]), але цього виявилось достатньо для доступу до відеопотоків БПЛА США.

Щодо другої загрози, то її дієвість на практиці також перевірено. Зокрема, дослідники інженерної школи Кокрелла (Cockrell School of Engineering) при Університеті Техасу (США) під керівництвом доцента Тодда Хамфрі (Todd Humphrey) вже створили пристрій вартістю близько тисячі доларів, який дає змогу перехоплювати управління безпілотними рухомими об'єктами. Пристрій одержав назву "GPS-спуфер" (GPS spoofer); він дає змогу втручатися в роботу систем GPS-навігації безпілотних рухомих об'єктів, перенаправляти їх на нові траєкторії руху або провокувати їх втрату. Принцип роботи "GPS-спуфера" полягає в тому, що пристрій посилає безпілотнику GPS-сигнал більш потужний, ніж той, який апарат отримує з супутників. Таким чином, стає можливою передача до безпілотного рухомого об'єкта фальшивих поточних координат його руху, що призводить до автоматичного переводу цього об'єкта на бажану для зловмисників траєкторію.

За допомогою комплекту апаратури у складі ноутбуку, невеликої антени і "GPS-спуфера", зібраного за 3000 доларів, дослідники під керівництвом Тодда Хамфрі змогли перехопити керування яхтою класу люкс «White Rose of Drachs» довжиною 65 метрів і вартістю $80 млн, яка перебувала в Середземному морі. Вони отримали керування морським судом, посилаючи підроблені GPS-сигнали для навігаційної системи яхти. Екіпаж яхти приймав ці сигнали за справжні й використовував для навігації, що призвело до відхилення яхти від її первинного курсу [6].

Щодо третьої загрози, то її реальність було продемонстровано у грудні 2011 року, коли в Ірані був захоплений унікальний за своїми характеристиками американський розвідувальний безпілотник RQ-170 Sentinel. За деякими джерелами, це сталось завдяки застосуванню російського наземного комплексу виконавчої радіотехнічної розвідки 1Л222 "Автобаза" [7]. Безпілотник було приземлено на території Ірану без будь-яких пошкоджень, що дало змогу детально вивчити його авіоніку, енергетику, інформатику, автоматику і керування. Це відкриває нові можливості для несанкціонованого оперативного втручання у процес керування тисячами автономних телекерованих морських рухомих об'єктів – ненаселених підводних апаратів (Autonomous Underwater Vehicles, AUV), надводних безпілотних морських рухомих об'єктів (Unmanned Surface Vessels, USV), безпілотних літальних апаратів морського базування (Unmanned Carrier-Launched Airborne Surveillance and Strike, UCLASS) та ін., які сьогодні активно застосовуються провідними морськими країнами світу, а також плануються до будівництва і застосування в Україні [8].

Таким чином, на цей час у світі активізувались розробки програмно-технічних засобів, які спроможні не тільки перехоплювати потоки аудіо- та відеоданих з борту морських та авіаційних

рухомих об'єктів, а й активно впливати на процес їх експлуатації. Це створює нову загрозу безпеці на водному транспорті у цілому і робить актуальною прикладну науково-технічну задачу створення апаратно-програмних засобів протидії загрозам інформаційній безпеці у цьому секторі діяльності підприємств і організацій України.

На тлі нових загроз інформаційній безпеці на водному транспорті доцільним є формування та узгодження з зацікавленими вітчизняними організаціями технічного завдання на науково-дослідну роботу «Удосконалення методів забезпечення інформаційної безпеки на водному транспорті та об'єктах морської інфраструктури», метою якої є розробка теоретичних основ та інженерних методів захисту інформаційних ресурсів, які циркулюють на водному транспорті та об'єктах морської інфраструктури.

Крім того, доцільним вбачається удосконалення підготовки фахівців за напрямком «Інформаційна безпека» шляхом уведення до навчальних планів їх професійної підготовки факультативної навчальної дисципліни «Інформаційна безпека на водному транспорті та об'єктах морської інфраструктури».

ВИСНОВКИ.

1. Традиційно головною метою зловмисників при їх атаках на інформаційні ресурси морських рухомих об'єктів є їхні навігаційно-інформаційні системи та системи оперативного морського зв'язку.

2. В останній час виникли нові загрози для інформаційних ресурсів, що використовуються на водного транспорті, які суттєво знижують інформаційну безпеку морських і річкових рухомих об'єктів та потребують розробки відповідних науково-технічних рішень:

– несанкціонований доступ до каналів супутникового відеообміну між судном та офісом його керування;

– викривлення навігаційних GPS-даних, які отримуються судном чи іншим рухомим об'єктом;

– несанкціонований доступ до супутниковоих каналів оперативного керування морськими чи річковими рухомими об'єктами.

3. З метою удосконалення науково-технічного і навчально-методичного забезпечення галузі знань «Інформаційна безпека» в інтересах українського воднотранспортного комплексу доцільним вбачається формування та узгодження з зацікавленими вітчизняними організаціями технічного завдання на науково-дослідну роботу «Удосконалення методів забезпечення інформаційної безпеки на водному транспорті та об'єктах морської інфраструктури» та введення до навчальних планів підготовки фахівців у зазначеній галузі знань факультативної

навчальної дисципліни «Інформаційна безпека на водному транспорті та об'єктах морської інфраструктури».

Список літератури:

1. Пономарьов І. Транзит наркотиків через територію України – загроза національній безпеці. / «Чорноморська безпека», 2010. – 3(17).

2. На Дунае появились пираты, которые грабят суда пароходств // [Электронный ресурс]: http://dumskaya.net/news/na-dunae-poyavilis-piraty-oni-grabyat-suda-nashe-016906/

3. IHO Data Protection Scheme. IHO Publication S-63. Published by the International Hydrographic Bureau MONACO, 2012. – 108 p.

4. Оборудование и программное обеспечение SkyGrabber // Електронний ресурс: http://as.radugainternet.ru/skygrabber.php

5. A Framework for IP Based Virtual Private Networks [Электронный ресурс] / B. Gleeson, A. Lin, J. Heinanen. – http://www.ietf.org/rfc/rfc2764.txt

6. Уязвимость в GPS позволяет угонять корабли и самолеты // Електронний ресурс: http://www.securitylab.ru/news/442680.php

7. «Кандагарского зверя» приземлила наша «Автобаза»? // Електронний ресурс: http://svpressa.ru/war21/article/50815/

8. Блінцов В.С., Киризюк О.М., Красних О.В., Яким'як С.В. Безекіпажна військово-морська техніка – стан та оснащення ВМС ЗС України / «Наука і оборона», 2012. – №4. – С. 61-64.