МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет кораблебудування
Імені адмірала Макарова

**Ж. Ю. БУРУНІНА, А. М. ВОЙТАСИК,
О. П. КЛОЧКОВ, В.І. КОРИЦЬКИЙ,
П. В. МАЙДАНЮК, А. С. СІРІВЧУК**

ІНФОРМАЦІЙНО ЗАХИЩЕНА СИСТЕМА МОНІТОРИНГУ МОРСЬКОЇ АКВАТОРІЇ НА БАЗІ БЕЗЕКІПАЖНИХ ПІДВОДНИХ АПАРАТІВ

Під загальною редакцією д.т.н. Блінцова В.С.

Рекомендовано Методичною радою НУК

Миколаїв. НУК. 2018

УДК 629
ББК 39.47

Укладачі: Ж. Ю. БУРУНІНА, А. М. ВОЙТАСИК,
О. П. КЛОЧКОВ, В.І. КОРИЦЬКИЙ,
П. В. МАЙДАНЮК, А. С. СІРІВЧУК
Рецензент Г. В. Бабкін, канд. техн. наук

Ж. Ю. Буруніна
Інформаційно захищена система моніторингу морської акваторії на базі безекіпажних підводних апаратів: Методичні вказівки / Ж. Ю. Буруніна, А. М. Войтасик, О. П. Клочков, В.І. Корицький, П. В. Майданюк, А. С. Сірівчук// Під загальною редакцією д.т.н. Блінцова В.С.– Миколаїв: НУК, 2018.– 40 с.

Учбовий посібник описує основні види робіт які виконуються за допомогою підводних апаратів та методологію їх використання. Також описано методологію використання підводних апаратів в складі комплексу моніторингу підводної обстановки на захищеній акваторії.

Призначений для студентів денної і заочної форм навчання спеціальності 141 «Електроенергетика, електротехніка та електромеханіка», спеціалізація «Морська робототехніка»

УДК 629
ББК 39.47

ВСТУП

На даний час в Україні контроль стану підводних об’єктів та середовища в цілому контролюється дуже слабо. Для моніторингу стану підводної частини гідротехнічних споруд зазвичай використовуються водолази та прив’язні підводні апарати (ППА)[1].

Використання водолазів при проведені таких типів робіт є дуже затратним, неможливість використання при несприятливих погодних умовах та може призвести до погіршення стану людини в наслідок непередбачуваних обставин.

Використання ППА для значно спрощує проведення таких видів робіт оскільки не потребує спеціалізованого навчання персоналу та виключає присутність людини під водою. Основною проблемою таких засобів моніторингу є їх керування в ручному режимі, оскільки автоматизація даного процесу ускладнюється наявністю кабель-тросу яких може заплутатись за сторонні об’єкти, яких в портових акваторіях дуже багато.

1 ОСНОВНІ ПОЛОЖЕННЯ

Основні положення узагальненої методики підконтрольної експлуатації безекіпажних автономних та прив'язних підводних апаратів при виконанні морських робіт оборонного призначення.

Підконтрольна експлуатація має проводитись згідно Наказу Командування Військово-Морських Сил Збройних Сил України, у якому описано організацію приймання у підконтрольну експлуатацію БМАС для потреб Військово-Морських Сил Збройних Сил України, керуючись вимогами "Порядку постачання озброєння, військової і спеціальної техніки під час особливого періоду, введення надзвичайного стану та у період проведення антитерористичної операції", затвердженого постановою Кабінету Міністрів України від 25 лютого 2015 року № 345.

Мають бути визначені період проведення підконтрольної дослідної експлуатації та зазначена морська акваторія, температурний діапазон, видимість та умови хвилювання морської поверхні.

Також має буди призначена робоча група для проведення підконтрольної дослідної експлуатації безекіпажних автономних та прив'язних підводних апаратів.

Основні напрямки підконтрольної дослідної експлуатації:

– використання апарату в морських умовах:

а) приготування до роботи;

б) керування апаратом при виконанні режимів роботи за призначенням;

в) приведення апарату у вихідне положення;

– визначення спроможності апарата до виконання підводних робіт за призначенням:

а) щодо виконання пошуку затонулих предметів;

б) щодо виконання оглядів підводної частини об’єктів;

в) щодо інспектування підводних комунікацій, трубопроводів та кабелів;

г) щодо пошуку та ідентифікації вибухонебезпечних предметів;

– опрацювання пропозицій до загальних вимог до перспективного безекіпажного підводного апарату для потреб ВМС ЗС України.

2 ЗАСТОСУВАННЯ БЕЗЕКІПАЖНИХ АВТОНОМНИХ ТА ПРИВ'ЯЗНИХ ПІДВОДНИХ АПАРАТІВ ДЛЯ ПОБУДОВИ ІНФОРМАЦІЙНО ЗАХИЩЕНОЇ СИСТЕМИ МОНІТОРИНГУ МОРСЬКОЇ АКВАТОРІЇ

Україна є державою з розвиненою морською інфраструктурою, де проводиться активна господарська діяльність. Сучасні терористичні загрози вимагають створення єдиної системи моніторингу надводної, підводної та повітряної обстановки морських акваторій держави, яка має створюватись на основі безекіпажних морських систем [2]. Така система складається з дистанційно або програмно керованих підводних, надводних та повітряних апаратів-роботів, які у реальному часі надають до берегового центру відомості про обстановку у територіальних водах держави. Невід'ємною складовою утвореного нового об'єкту морської інфраструктури інформаційного характеру повинна бути система захисту інформації, яка циркулює між складовими системи моніторингу.

На сьогодні загальні питання у сфері інформаційної безпеки опубліковано в [3-6]. Дослідженням з проблем правового забезпечення інформаційної безпеки присвячено роботи з теорії держави та права [7, 8]. Ці результати є основою для розробки систем, в яких передбачено захист інформації, проте питання

захисту інформації при моніторингу морських акваторій потребують проведення подальших досліджень.

Роботу [9] присвячено розробці та тестуванню автономних надводних та підводних апаратів для задач моніторингу морських акваторій. Результати застосування автономного підводного апарата типу «глайдер» для моніторингу акваторій в полярному регіоні викладено в [10]. Основну увагу в даних роботах приділено застосуванню спеціалізованих сенсорів, але питання захисту інформації в роботах не розглядаються.

Аналіз конструкцій ненаселених надводних апаратів, призначених для моніторингу морського середовища, виконано в [11]. Проте запропоновані конструкції не містять складової, призначеної для захисту інформації.

Роботу [12] присвячено розгляду можливостей ненаселених повітряних систем для виконання задач морського моніторингу. В [13] описано напрями застосування ненаселених повітряних систем для виконання морських операцій.

У цілому аналіз літературних даних показав, що на цей час теоретичні питання застосування безекіпажних морських систем для моніторингу морської обстановки, а також захисту інформації в таких системах розроблені недостатньо. Зокрема, представлені результати зосереджено або на моніторингу окремих складових навколишнього середовища, або на

особливостях застосування спеціалізованих сенсорів. Задача моніторингу морських акваторій з захистом інформації, яка генерується, обробляється, передається та використовується в них, в комплексній постановці не розглядається.

Розглянемо структуру та склад інформаційно захищеної системи моніторингу морської акваторії та основі застосування БМАС.

Втручання в процеси функціонування об’єктів морської інфраструктури (ОМІ) можуть призвести до збитків у сфері життєво важливих інтересах особи, суспільства і держави, а також негативно впливати на процеси природного або техногенного характеру. Реалізація загроз можлива через незаконне проникнення на захищену морську акваторію (ЗМА), розташовані на ній об’єкти, заволодіння інформацією, що циркулює на ОМІ та (або) відомостями про діяльність об’єкта.

Для здійснення моніторингу морської, повітряної та наземної обстановки на ЗМА та ОМІ пропонується використовувати комплекс апаратних засобів БМАС, представлений на рис. 1.

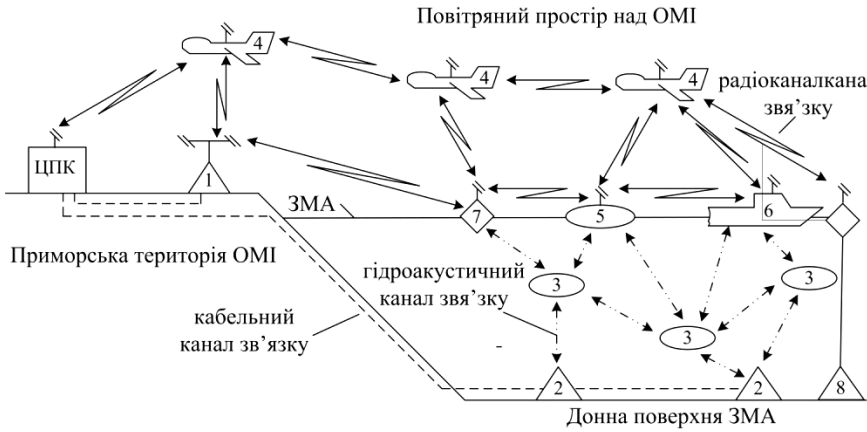

Рисунок 1 – Комплекс апаратних засобів для моніторингу надводної, підводної та повітряної обстановки на захищеній морській акваторії 1 – стаціонарні засоби моніторингу наземного базування; 2 – стаціонарні засоби моніторингу донного базування; 3 – безекіпажні підводні апарати; 4 – безпілотні літальні апарати; 5 – безекіпажні надводні апарати; 6 – плавзасоби, керовані екіпажами; 7 – дрейфуючі буї; 8 – стаціонарні засоби моніторингу донного базування з радіоканалом

Вказані технічні засоби є носіями пошукової та вимірювальної апаратури. Вони самостійно патрулюють акваторію та приморську територію об'єкта по заздалегідь закладеним маршрутам, у реальному часі проводять

радіотехнічний, радіолокаційний, гідроакустичний, магнітометричний та візуально-оптичний моніторинг підводної, надводної й повітряної обстановки. Результати моніторингу передаються по захищеним каналам до центрального поста керування (ЦПК) акваторією.

Запропонована система моніторингу ОМІ представляє собою розподілену мережу, до якої входять такі складові:

– підсистема контролю доступу (СКД) (електронні замки, турнікети – для забезпечення режиму доступу до приміщень та сухопутних територій; бонові загородження, електронно-оптичні, магнітометричні, сейсмічні, радіолокаційні, гідроакустичні прилади – для водних акваторій);

– підсистема охоронної сигналізації та відеоспостереження (камери відеоспостереження, відеореєстратори, датчики охоронної сигналізації – для контролю за перебуванням осіб в межах зони, що охороняється (внутрішній периметр об’єкта), та в межах зони, що контролюється (акваторія та прилегла територія);

– кабельна мережа (кабелі зв’язку та передачі даних, електроживлення, заземлення);

– мережа безпровідних каналів зв’язку (Wi-Fi, радіорелейні станції, обладнання прийому/передачі);

– засоби комутації та маршрутизації даних (комутатори, концентратори, маршрутизатори);

– автоматизовані робочі місця (АРМ) керування системою, з яких здійснюється управління, контроль, налагодження системи моніторингу;

– АРМ баз даних (сервери) для зберігання даних щодо роботи системи моніторингу;

– апаратні складові системи (безпілотні підводні, надводні, літальні апарати, стаціонарні апарати наземного та підводного базування).

Невід'ємним компонентом захищеної системи моніторингу є інформаційно-телекомунікаційна мережа із впровадженою комплексною системою захисту інформації.

Запропонована схема інформаційно-телекомунікаційної мережі системи моніторингу ЗМА та ОМІ наведена на рис. 2.

На сземі можна виділити наступні функціональні модулі:

– модуль збору та обробки інформації – безпілотні підводні, надводні, літальні апарати, стаціонарні апарати наземного та підводного базування ("абоненти");

– модуль керування системою та зберігання даних – АРМ керування системою та баз даних, що розміщені на командному пункті;

– модуль комунікації – кабельна мережа, система безпровідних каналів зв’язку (радіоканал, гідроакустичний канал).

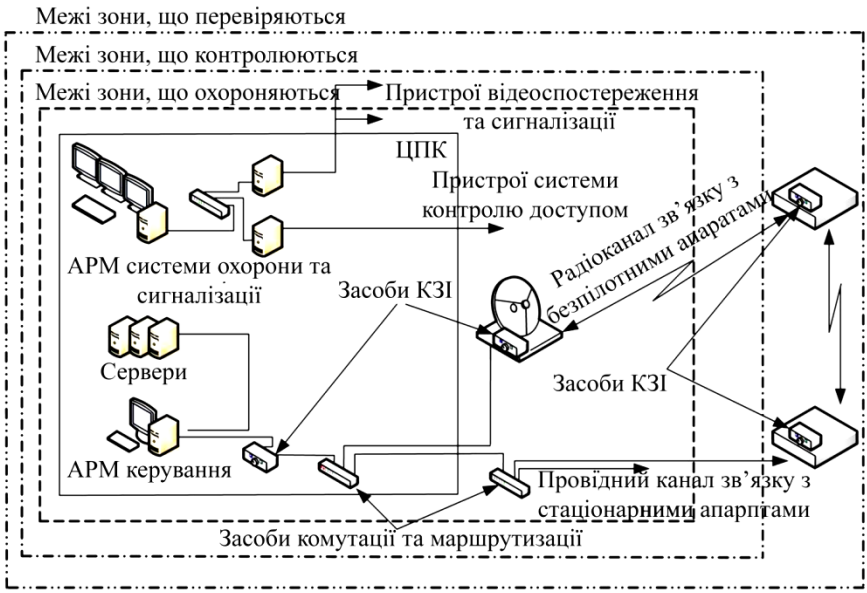

Рисунок 2 – Схема інформаційно-телекомунікаційної мережі системи моніторингу об’єкта морської інфраструктури

Телекомунікаційна мережа системи моніторингу ЗМА та ОМІ складається з взаємопов'язаних кабельних та безпровідних каналів зв’язку, тому в процесі передачі даних сигнали повідомлень підлягають різним перетворенням під час проходження у різних середовищах [2].

Розглянемо тепер питання забезпечення інформаційної безпеки акваторій за допомогою БМАС.

Базисом інформаційної безпеки в системі моніторингу ЗМА та ОМІ є сукупність методів і засобів, що забезпечують

цілісність, конфіденційність і доступність інформації, яка в ній циркулює.

Створення захищеної системи моніторингу (ЗСМ) морської обстановки з впровадженою комплексною системою захисту інформації дозволяє вирішувати наступні питання, а саме:

– захист інформації від витоку технічними каналами;

– захист інформації від несанкціонованих дій та несанкціонованого доступу;

– захист від спеціального впливу на інформацію.

Досягнення визначеної мети передбачає вирішення наступних завдань:

– визначення можливих загроз інформації, що циркулює на ЗМА та ОМІ;

– розробка системи захисту інформації, що циркулює на ЗМА та ОМІ.

Виконаємо аналіз агроз інформації, що циркулює в системі моніторингу.

В інформаційно-телекомунікаційній системи (ІТС) моніторингу морської обстановки циркулює наступна інформація, що підлягає захисту:

– дані та програмні коди у вигляді файлів різних форматів, що містять інформацію, що підлягає захисту (інформація про

результати моніторингу підводної, надводної та повітряної обстановки);

– відомості про стан системи сигналізації, відео-, гідроакустичного та магнітометричного спостереження та системи контролю доступу; алгоритми та режими роботи безпілотних апаратів;

– команди керування технічними засобами та управління системою та апаратними засобами моніторингу та контролю;

– технологічна інформація, яка використовується для забезпечення функціонування системи;

– файли комплексу засобів захисту інформації (криптоалгоритми, ключові дані, параметри налагодження системи).

Загрози для інформації, яка обробляється в ІТС, залежать від характеристик ІТС, складності системи, типу застосованих технічних засобів, фізичного середовища, персоналу та інших чинників, що можуть мати об'єктивну або суб'єктивну природу.

Основними видами загроз для безпеки інформації, які можуть виникнути в ІТС, є:

– зміна умов фізичного середовища (штормові та сейсмічні збурення, задимлення атмосфери над ЗМА, зміни прозорості води та її гідроакустичних характеристик або інші випадкові події);

– збої та відмови в роботі апаратних засобів системи моніторингу;

– помилки персоналу під час експлуатації системи моніторингу;

– навмисні дії потенційних порушників (виток інформації за рахунок: каналів побічних електромагнітних випромінювань і наведень, несанкціонованого доступу, використання закладних пристроїв, перехоплення інформації під час передачі каналами зв'язку, застосування руйнівних програмних засобів).

Виконаємо синтез моделі порушника захищеної акваторії.

Для ЗМА та розташованих на ній ОМІ існують джерела загроз, які можуть бути викликані внутрішніми або зовнішніми порушниками по відношенню до інформаційно захищеної системи моніторингу.

Внутрішні порушники – особи, що мають право постійного доступу в межі контрольованої зони акваторії (об'єкту), де розміщені складові системи моніторингу:

– технічний персонал, який обслуговує будови, приміщення та території (акваторії), в яких розташовані компоненти системи;

– персонал, який обслуговує технічні засоби системи (техніки, інженери);

– користувачі (оператори) системи моніторингу;

– співробітники служби захисту інформації в системі (адміністратори безпеки);

– керівники різних рівнів посадової ієрархії.

Зовнішні порушники – особи, що не мають права постійного доступу в межі контрольованої зони об’єкту, на якому розміщені складові системи моніторингу:

– особи, що знаходяться за межами контрольованої зони об’єкту;

– відвідувачі об'єкту;

– представники організацій, що взаємодіють з питань технічного забезпечення;

– співробітники закордонних служб або особи, які діють за їх завданнями.

Для кожної категорії порушників можна виділити п’ять різних специфікацій з визначенням рівня потенційної загрози (РЗ):

– за мотивами (безвідповідальність (РЗ-1); недостатня професійна кваліфікація (РЗ-2); самозатвердження (РЗ-3); корисливий інтерес (РЗ-4));

– рівнем кваліфікації (знає функціональні особливості системи, основні принципи збору, обробки, зберігання та передачі даних у системі, має навички щодо користування штатними засобами системи (РЗ-1); володіє високим рівнем

знань та практичними навичками роботи з технічними засобами системи та їх обслуговування (РЗ-2); володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації систем збору та передачі даних (РЗ-3); знає структуру, функції й механізми дії засобів захисту системи, їх недоліки (РЗ-4));

– можливістю використання засобів та методів подолання системи захисту (використовує лише агентурні методи одержання відомостей (РЗ-1); використовує пасивні засоби (технічні засоби приймання інформації без модифікації компонентів системи) (РЗ-2); використовує лише штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії інформації, які можуть бути приховано пронесено крізь охорону (РЗ-3); застосовує методи та засоби дистанційного упровадження програмних закладок та спеціальних програм збору (РЗ-4));

– часом дії (до впровадження системи моніторингу або її окремих компонентів (РЗ-1); під час бездіяльності складових системи (під час планових перерв у роботі, перерв для обслуговування та ремонту тощо) (РЗ-2); під час функціонування системи моніторингу (РЗ-3); як у процесі функціонування системи, так і під час обслуговування складових системи (РЗ-4));

– місцем дії (без доступу на території, до приміщень, споруд, об’єктів де розміщені складові системи (РЗ-1); на територіях, усередині приміщень, споруд, де розміщені складові системи, але без доступу до технічних засобів системи (РЗ-2); з робочих місць користувачів (операторів) системи з доступом до баз даних та (або) архівів даних (РЗ-3); з робочих місць користувачів (операторів) з доступом до керування засобами забезпечення безпеки системи (РЗ-4)).

Тут "РЗ" – визначений рівень загрози, відносного оцінки можливих збитків, які може заподіяти порушник за умови наявності відповідних характеристик. Рівень загрози характеризується наступними категоріями: 1 – незначні, 2 – значимі, але здебільшого припустимі, 3 – середні, 4 – дуже значні.

За допомогою позначень специфікацій та рівнів загроз можливо визначити профілі порушників (P) різних категорій щодо ефективності реалізації загроз відносно системи моніторингу на об’єкті морської інфраструктури, за формулою:

$$P_i = \frac{m + k + z + t + s}{5},$$

де i – категорія порушника; m – значення РЗ по специфікації "мотив"; k – значення РЗ по специфікації "рівень кваліфікації"; z – значення РЗ по специфікації "можливість використання засобів та методів подолання системи захисту"; t – значення РЗ по специфікації "час дії"; s – значення РЗ по специфікації "місце дії".

Оцінка здійснюється за умовною шкалою від 1 до 4:

– 1 – реалізація загрози неможлива;

– від 1 до 2 – вірогідність реалізації загрози мала, наслідки її можна не враховувати;

– від 2 до 3 – реалізація загрози можлива, необхідна оцінка її наслідків;

– від 3 до 4 – вірогідність реалізації загрози та можливі наслідки неприпустимо великі, необхідні додаткові заходи щодо блокування загрози.

Розглянемо питання методик захисту інформації, що циркулює в ІТС моніторингу ЗМА та ОМІ

Для захисту інформації від витоку каналами побічних електромагнітних випромінювань і наведень навколо складових ІТС ЗМА та ОМІ необхідно забезпечувати контрольовану зону (КЗ). Значення КЗ повинно бути отримано за результатами інструментальної перевірки електричних та магнітних полів розсіювання сигналів, які несуть інформацію (небезпечні

сигнали), що виникають навколо технічних засобів обробки інформації (ОТЗ). У разі неможливості забезпечення навколо ОТЗ та ліній комунікацій визначену контрольовану зону (проводи кабельної мережі, системи електроживлення, АРМ керування та баз даних, стаціонарні апарати та системи наземного базування, трансформаторні підстанції електроживлення, елементи заземлення), необхідно використовувати додаткові технічні заходи захисту:

– засоби активного захисту (генератори електромагнітного зашумлення генератори штучних завад ліній електроживлення тощо);

– виконання апаратних складових інформаційної системи в захищеному вигляді (екрановані кабелі та корпуса обладнання, екрановані приміщення, кожухи тощо).

Для захисту від несанкціонованого доступу (НСД) до складових системи повинні виконуватись організаційні та режимні заходи на ЗМА та ОМІ. Для захисту системи від упровадження спеціальних програмно-апаратних засобів, що дозволяють здійснити НСД, та впровадження в систему програмних або апаратних механізмів, які порушують структуру й функції системи, реалізується політика безпеки для інформації в ІТС – комплекс засобів захисту.

Для захисту інформації від витоку через канали зв'язку пропонується забезпечити контрольовану зону навколо комунікацій з метою унеможливлення несанкціонованого доступу до них та виконання заходів щодо захисту інформації від витоку технічними каналами:

– для провідних каналів зв’язку: використання протизавадних фільтрів, мінімізація або виключення спільного пробігу кабелів мережі передачі даних з лініями, які мають вихід за межі КЗ, застосування в системі комунікації екранованих кабелів;

– для радіоканалів зв’язку: зниження потужності радіоелектронних засобів (РЕЗ), введення територіальних, просторових, часових обмежень на роботу РЕЗ, застосування режимів короткочасного випромінювання, створенням завад, створення хибних сигналів;

– для гідроакустичних каналів зв’язку: використання природних та промислових гідроакустичних завад, забезпечення необхідного рівня маскуючої гідроакустичної завади, введення територіальних, просторових, часових обмежень на роботу засобів гідроакустичного випромінювання.

Окрім використання організаційних та технічних заходів захисту під час передачі інформації каналами зв’язку необхідно впроваджувати систему криптографічного захисту інформації.

Необхідне встановлення в апаратних складових ІТС (АРМ керування системою та баз даних, безпілотні підводні, надводні, літальні апарати, стаціонарні апарати наземного та підводного базування, засоби моніторингу та контролю) засобів криптографічного перетворення інформації (засобів наскрізного шифрування трафіку) відповідного рівня обмеження доступу.

Розглянемо питання контролю ефективності захисту інформації.

Визначення ефективності захисту інформації, яка циркулює на ЗМА та ОМІ базується на якісному дослідженні метрик, що характеризують стан захисту інформації у різних середовищах її обігу. Це дозволить визначати потенційні загрози витоку інформації, здійснювати оцінку ефективності захисту інформації за допомогою розрахунку інтегрального індексу стану інформаційної захищеності інформації ЗМА та ОМІ.

Рівень стану захисту інформації ЗМА та ОМІ визначається шляхом оцінки його основних процесів (етапів) залежно від показників їх метрик, щодо визначення методів та заходів протидії визначеним загрозам. Також це допоможе при визначені достатності технічного та організаційного забезпечення, стану та контролю за виконанням необхідних заходів тощо.

Формування переліків метрик захищеності інформації здійснюється на основі відбору показників, які найбільш повно

характеризують стан захисту інформації ЗМА та ОМІ, з урахуванням досвіду оцінювання стану технічного та криптографічного захисту інформації.

Нормування метрик захищеності інформації здійснюється за допомогою лінійної функції таким чином, щоб характеристичні значення індикаторів потрапляли в зіставні за величиною інтервали. Перехід від абсолютних до нормованих значень індикаторів дозволяє вимірювати індикатори за шкалою від 0 до 1 або у відсотках, де 0 відповідає 0 %, а 1 відповідає 100 %.

Таким чином, отримане нормоване значення індикатора характеризує своєю величиною ступінь наближення до найвищого значення 1.

Під ваговим коефіцієнтом метрики мається на увазі коефіцієнт, визначений за методом експертних оцінок, який характеризує розмір внеску конкретного показника захищеності в інтегральний індекс стану захищеності інформації.

Розрахунок інтегральних індексів стану інформаційної захищеності здійснюється окремо для кожного середовища функціонування складових ІТС об’єкту морської інфраструктури на всіх етапах життєвого циклу. Після розрахунків інтегральних індексів здійснюється розрахунок рівня захищеності інформації в цілому на ЗМА та ОМІ.

Розрахунок інтегрального індексу стану інформаційної захищеності ЗМА та ОМІ здійснюється на основі даних, отриманих під час виконання робіт із розробки та впровадження заходів із захисту інформації.

Після впровадження системи захисту інформації здійснюється розрахунок інтегрального індексу стану інформаційної захищеності у кожному середовищі перебування складових інформаційно-телекомунікаційної системи ЗМА та ОМІ за наступною формулою:

$$Y_m = \sum_i n_{im} k_{im},$$

де Y_m – інтегральний індекс стану захищеності m-го середовища функціонування; n_{im} – нормоване значення i-го індикатора захищеності m-го середовища функціонування; k_{im} – визначений за методом експертних оцінок ваговий коефіцієнт, який характеризує розмір внеску i-го індикатора захищеності в інтегральний індекс стану захищеності m-го середовища функціонування;

Узагальнюючий інтегральний індекс стану захищеності ІТС ЗМА та ОМІ розраховується за наступною формулою:

$$Y = \sum_{m} \frac{Y_m}{m},$$

де m – кількість середовищ функціонування.

Визначення рівня стану захисту інформації здійснюється шляхом порівняння числових значень, отриманих за допомогою розрахунку узагальнюючого інтегрального індексу стану захищеності інформації, та характеристичних значень, які діагностують рівень стану захищеності.

Діапазон значень, які діагностують рівень стану захисту інформації, може поділятися на такі інтервали:

$[Y_0, Y_{\text{нездв}})$; $[Y_{\text{нездв}}, Y_{\text{небезп}})$; $[Y_{\text{небезп}}, Y_{\text{крит}})$; $[Y_{\text{крит}}, Y_{\text{здв}})$; $[Y_{\text{здв}}, Y_{\text{опт}}]$,

де Y_0 – значення інтегрального індексу, що характеризує абсолютно небезпечний рівень стану захищеності інформації – 0 % або 0; $Y_{\text{нездв}}$ – значення, що характеризує незадовільний рівень стану захищеності інформації на рівні 20 % або 0,2 від оптимального значення; $Y_{\text{небезп}}$ – значення, що характеризує небезпечний рівень стану захищеності інформації на рівні 40 % або 0,4 від оптимального значення; $Y_{\text{крит}}$ – значення, що характеризує критичний (мінімальний) рівень стану захищеності інформації на рівні 60 % або 0,6 від оптимального значення; $Y_{\text{здв}}$ – значення, що характеризує задовільний рівень стану

захищеності інформації на рівні 80 % або 0,8 від оптимального значення; $Y_{опт}$ – значення, що характеризує оптимальний рівень стану захищеності інформації (100 % або 1).

Таким чином, впровадження захищених систем моніторингу морської, повітряної та наземної обстановки на морських та приморських об'єктах дозволить попередити можливі незаконні (небажані) дії будь-якого характеру. Це досягається за рахунок об'єднання комплексу апаратних засобів моніторингу навколишнього середовища в єдину інформаційно-телекомунікаційну систему з центральним постом керування.

Особливістю розробленої системи моніторингу ЗМА є захист інформації, які в ній циркулює. Це суттєво ускладнює будь-яке стороннє втручання в функціонування складових системи та підвищує надійність систем моніторингу від відмов та від нав'язування хибної інформації. Захищені інформаційно-телекомунікаційні мережі систем моніторингу є перспективними для передачі інформації з обмеженим доступом між кореспондентами в межах об'єкта або в межах ЗМА. Крім того, універсальність систем моніторингу дозволяє без суттєвих структурних змін будувати системи моніторингу об'єктів незалежно від географічних особливостей ЗМА та типу ОМІ. Це утворює перспективу їх широкого застосування.

Перевагою запропонованої захищеної системи моніторингу є можливість її застосування на промислових, транспортних, науково-дослідних морських та приморських об'єктах та інших

ОМІ. Їх використання можливе підрозділами прикордонної служби та збройних сил України у складі систем контролю державного кордону, охорони військових об’єктів тощо. А запропоновані узагальнюючий індекс стану захищеності та методика його розрахунку дають змогу кількісно оцінити рівень захищеності інформації в системі моніторингу.

В ролі недоліку захищеної системи моніторингу ЗМА слід зазначити високу вартість її апаратної частини, конкретно – безекіпажних підводних та літальних апаратів. Цей недолік може бути усунутий шляхом організації їх серійного виробництва при широкому впровадженні. Крім того, кількісна оцінка рівня захищеності здійснюється на основі вагових коефіцієнтів індикаторів, які обираються на основі експертних оцінювань. Для цих даних також бажаною була б розробка процедури їх отримання у формальний спосіб.

Розвиток результатів, представлених в даному дослідженні, вбачається в поетапній розробці (від ескізного проекту до серійного виробництва) захищеної системи моніторингу для ЗМА або ОМІ з певними параметрами. Але на кожному етапі, можливо, виникатиме потреба проводити аналіз загроз та уточнювати модель порушника. Коригування технічного завдання між етапами пропонується здійснювати на основі кількісної оцінки рівня захищеності інформації в системі моніторингу.

3 РЕЗУЛЬТАТИ ЗАСТОСУВАННЯ МЕТОДИКИ ПІД ЧАС ЕКСПЛУАТАЦІЇ ДОСЛІДНОГО ЗРАЗКА ППА «МР-1»

Відповідно до Наказу Командування Військово-Морських Сил Збройних Сил України від 22 грудня 2016 року № 314/АГЧ “Про організацію приймання у підконтрольну експлуатацію дослідного зразка безекіпажного підводного апарата для потреб Військово-Морських Сил Збройних Сил України типу “МР-1”, від 28 квітня 2017 року № 140/АГЧ “Про організацію та проведення підконтрольної дослідної експлуатації дослідного зразка безекіпажного підводного апарата типу “МР-1”, у військовій частині А3053 протягом 2017 року була проведена підконтрольна дослідна експлуатація дослідного зразка безекіпажного підводного апарата типу “МР-1”. В основу експлуатації було покладено основні положення узагальненої методики підконтрольної експлуатації безекіпажних автономних та прив’язних підводних апаратів при виконанні морських робіт оборонного призначення, яка викладена вище.

Розглянемо основні результати такої експлуатації.

Приготування до роботи:

переваги: всепогодність застосування апарату; можливість застосування апарату вдень та вночі; апарат відносно мобільний,

можливе пересування і розгортання особовим складом у кількості 2-3 осіб.

пропозиції: розглянути можливість удосконалення системи живлення та керування, в комплектації апарату повинен бути передбачений ЗІП з необхідним устаткуванням для розгортання апарату.

Керування апаратом при виконанні режимів роботи за призначенням:

переваги: зручний набортний пристрій керування апаратом; відносно проста система керування на базі стандартного ігрового джойстику, яка не потребує спеціального довготривалого навчання особового складу; для контролю параметрів апарата застосовується персональний комп'ютер (ноутбук) з встановленим графічним середовищем "Simulink" з системи математичного моделювання "Mathlab", що дозволяє оперативно змінювати параметри системи, проводити експериментальні розрахунки та дослідження; глибина занурення апарату задовольняє потреби користувача відповідно до визначених умов використання.

пропозиції: внести зміни в проект в частині, що стосується засобів об'єктивного контролю апарату та його підводного позиціювання; затвердити в керівній та експлуатаційній документації штат для обслуговування апарату.

Приведення апарату у вихідне положення:

переваги: зручність та швидкість під час опріснення, доступ до всіх вузлів та агрегатів апарату;

пропозиції: у зв'язку з використанням в конструкції алюмінієво-магнієвих сплавів після використання апарату обов'язковим має бути обмив прісною водою, що не завжди можливе в морських умовах; скоротити перевірку міцних корпусів та вузлів уведення кабель-тросу на герметичність.

Визначення спроможності апарата щодо виконання пошуку затонулих предметів:

переваги: у випадку знаходження предмету в секторі відеокамери він гарантовано буде визначений та ідентифікований оператором;

пропозиції: розширити сектор пошуку; розташувати підводні світильники ак, щоб мінімізувати вплив колоїдної суспензії (має місце "залив світлом"); створити канал керування відеокамерою у горизонтальній площині.

Визначення спроможності апарата щодо виконання оглядів підводної частини об'єктів:

переваги: можливість виконання водолазних оглядів об'єктів без присутності водолаза на глибинах до 60 метрів протягом необмеженого часу;

недоліки: до візуального контакту з предметом обстеження оператор не має інформації о місцезнаходженні апарату; поступальний рух апарата уздовж цілі (корабля) на заданій дальності обстеження із стабілізацією кутового положення неможливий, у зв’язку з особливостями системи керування (відсутні система стабілізації руху та утримання по напрямку відносно орієнтирів);.

пропозиції: розглянути можливість удосконалення системи керування.

Визначення спроможності апарата щодо інспектування підводних комунікацій, трубопроводів та кабелів:

переваги: можливість контролювати розташування та стан трубопроводів, кабелів або комунікацій на ґрунті;

недоліки: незручність при керуванні апаратом по заданому напрямку (необхідність постійної коректури руху); стабілізація (“зависання”) в потрібній точці з метою більш доскональної відео-фото зйомки, у випадку великої кількості витравленого кабелю та присутності течії, неможлива внаслідок зовнішнього коливання від кабелю;

пропозиції: розглянути можливість удосконалення системи керування.

Визначення спроможності апарата щодо ідентифікації вибухонебезпечних предметів:

переваги: можливість проведення пошуку та ідентифікації вибухонебезпечних предметів у випадку відносної прозорості води;

недоліки: відсутність відеокамери з якісним зображенням та відеокамери з високою чутливістю (доцільно використовувати 2 відеокамери); відсутність системи компенсації власного магнітного поля (або антимагнітних кожухів на електродвигунах); відсутність системи керування освітленням (для більш якісного визначення іноді буває потрібно направити промінь світла в потрібне місце);

пропозиції: розглянути можливість щодо внесення конструктивних змін.

Опрацювання пропозиції до загальних вимог до перспективного безекіпажного підводного апарату для потреб ВМС ЗС України.

1. Ідентифікація донної цілі з відомими географічними координатами повинна складатися з наступних етапів:

виведення апарату по поверхні води в район цілі за даними супутникової навігаційної системи;

заглиблення апарату і вихід до цілі за даними від маяків гідроакустичної навігаційної системи;

додатковий пошук цілі в ході оглядово-пошукової зйомки дна за допомогою гідролокатора бокового огляду (далі – ГБО);

наведення по ГБО до візуального контакту з ціллю;

детальне обстеження донної цілі за допомогою ГБО, відеокамер і фото системи.

При виконанні даних етапів обов’язково вести графічну реєстрацію маршруту пошуку на моніторі з можливістю подальшого аналізу району пошуку, що обстежувався.

2. Збільшення продуктивності інспектування гідротехнічних споруд і бездокового огляду підводної частини корпусів кораблів (суден, катерів) вимагає виконання наступних операцій:

поступовий рух апарату уздовж корпусу корабля на заданій дальності обстеження із стабілізацією кутового положення по сигналах від ехолокаційної системи (далі – ЕЛС), доплеровського лага (далі – ДЛ) і навігаційних датчиків;

визначення координат апарату відносно корпусу корабля, що обстежується, на підставі даних від ДЛ на поворотній платформі і ЕЛС;

відео-фото зйомку поверхні корпусу корабля з регулюванням кута нахилу платформи відео-фотокамерами в подовжньо-вертикальній площині;

визначення координат переміщень відносно об'єкту за даними цифрової фото системи;

передачу в реальному часі інформації, що поступає від відеокамер і ГБО, а також координат відносно корпусу обстежуваного корабля.

3. Напрямки подальшого розвитку досліджень по створенню ППА в інтересах ВМС ЗС України. Дослідна експлуатація ППА проекту «МР-1» показала, що доцільно дообладнати апарат наступним чином:

системою ехолокації дна;

системою визначення координат (відносно маяків гідроакустичної системи);

допплерівським лагом;

системою керування світлом та відео-фотокамерами;

можливістю трансляції усіх даних оператору в реальному часу;

системою стабілізації руху;

системою регулювання плавучості апарата оператором дистанційно, в залежності від задач;

системою автоматичного аварійного спливання у разі пошкодження (обриву) кабелю з подачею аварійних сигналів (проблисковим світлом та в радіодіапазоні);

провести удосконалення тракту передачі зображення з метою передачі відеосигналу високої якості.

4. Результати проведення підконтрольної дослідної експлуатації дослідного зразка ППА типу “МР-1”.

За результатами проведення підконтрольної дослідної експлуатації визначено, що ППА типу “МР-1” в існуючій комплектації придатний для вирішення задач щодо пошуку затонулих предметів, виконання оглядів підводної частини об’єктів, інспектування підводних комунікацій, трубопроводів та кабелів, а також для пошуку та ідентифікації вибухонебезпечних предметів.

Можливо використання апарату для контролю дій особового складу під час виконання водолазних робіт, для проведення навчально-тренувальної підготовки операторів без екіпажної підводної техніки.

Також апарат може використовуватись, як навчальний тренажер для підготовки особового складу по керуванню апарату.

На можливості використання апарата суттєво впливає особливості живлення апарату, що значно обмежує його придатність до виконання оглядів в морських умовах.

В подальшому дані, які отримані у ході проведення підконтрольної дослідної експлуатації ППА типу “МР-1”, доцільно врахувати під час виконання оперативного завдання щодо розробки проекту оперативно-тактичних вимог до універсального безекіпажного підводного апарату – шукача мін в інтересах вирішення питань протимінного та протипідводно-диверсійного забезпечення ВМС ЗС України (“Краб-М”).

ПЕРЕЛІК ПОСИЛАНЬ

1. Блінцов О. В. Телекеровані підводні апарати на службі морегосподарської діяльності Миколаївщини [Текст] / О.В. Блінцов, М.Г. Грицаєнко // Підводна техніка і технологія: Матеріали всеукраїнської науково-технічної конференції з міжнародною участю: В 2 ч .– Миколаїв: НУК, 2014 .– Ч.1 – 100с.

2. Blintsov, O. Development of informationally-protected system of marine water area monitoring [Text] / O. Blintsov, P. Maidaniuk // Eastern-European Journal of Enterprise Technologies. – 2017. – Vol. 6, Issue 9 (90). – P. 10–16. doi: 10.15587/1729-4061.2017.118851

3. Ліпкан В. А. Інформаційна безпека як складова національної безпеки України / В. А. Ліпкан // Інформаційні технології в економіці, менеджменті і бізнесі : Проблеми науки, практики і освіти : Зб. наук. праць VIII Міжнар. наук.-практ. конф. — Ч. 2. — К. : Вид-во Європ. ун-ту, 2003. — С. 443— 453.

4. Почепцов Г. Г. Коммуникативные технологии двадцатого века. - М.: Рефл-бук; К.: Ваклер, 2000. - 352 с.

5. Кормич В. А Інформаційна безпека України: організаційно-правові основи: Навч. посібник. - К.: Кондор, 2004. - 384 с.

6. Дергаусов М.М. Украина – держава морская / М.М. Дергаусов. – Д.: Изд-во "Донеччина", 2000. – 269 с.

7. Рабинович П. М. Основи загальної теорії права і держави: [посіб. для студ. спец-ті "Правознавство"] / П. М. Рабинович. — К., 1994. — 236 с.

8. Теорія держави та права: [навч. посіб.] / А. М. Колодій, В. В. Копейчиков, С. Л. Лисенков та ін.; За заг. ред. С. Л. Лисенкова, В. В. Копейчикова. — К. : Юрінком Інтер, 2003. — 368 с.

9. Anderson, B. Autonomous Surface Vehicles for Arctic Data Collection [Text] / B. Anderson, A. Kleiner // Society of Petroleum Engineers: OTC Arctic Technology Conference, 10-12 February, Houston, Texas. – 2014. doi: 10.4043/24556-MS.

10. Field, M. Barents Sea monitoring with a SEA EXPLORER glider [Text] / M. Field, L. Beguery, L. Oziel, J. C. Gascard// IEEE: OCEANS 2015 – Genova, 18-21 May, Genoa, Italy. – 2015. doi: 10.1109/OCEANS-Genova.2015.7271540.

11. Heo, J. Analysis of Design Directions for Unmanned Surface Vehicles (USVs) [Text] / J. Heo, J. Kim, Y. Kwon // Scientific Research Publishing : Journal of Computer and Communications. – 2017. – Issue 5. – P. 92–100. doi: 10.4236/jcc.2017.57010.

12. Klimkowska, A. Possibilities of UAS for maritime monitoring [Text] / A. Klimkowska, I. Lee, K. Choi // The

International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLI-B1, XXIII ISPRS Congress, 12–19 July, Prague, Czech Republic. – 2016. – Issue 5. – P. 885–891. doi: 10.5194/isprsarchives-XLI-B1-885-2016

13. de Sousa, J. B. Unmanned Aircraft Systems for Maritime Operations [Text] / J. B. de Sousa, P. McGuillivary, J. Vicente, M. N. Bento, J. A. P. Morgado, M. M. Matos, R. A. G. Bencatel, P. M. de Oliveira // Springer Science+Business Media Dordrecht: Handbook of Unmanned Aerial Vehicles. – 2015. – Volume 3. – P. 2787–2811. doi: 10.1007/978-90-481-9707-1_75

ЗМІСТ

Навчальне видання

Ж. Ю. БУРУНІНА, А. М. ВОЙТАСИК,
О. П. КЛОЧКОВ, В.І. КОРИЦЬКИЙ,
П. В. МАЙДАНЮК, А. С. СІРІВЧУК

ІНФОРМАЦІЙНО ЗАХИЩЕНА СИСТЕМА МОНІТОРИНГУ МОРСЬКОЇ АКВАТОРІЇ НА БАЗІ БЕЗЕКІПАЖНИХ ПІДВОДНИХ АПАРАТІВ

Під редакцією д.т.н. проф. В.С. Блінцова
Комп’ютерне верстання А. С. Сірівчук

Формат 60х84/16. Ум. друк. арк. 6,6. Тираж 100 прим. Зам. № 127.
Видавець і виготівник Національний університет кораблебудування
імені адмірала Макарова
просп. Героїв України, 9, м. Миколаїв, 54025, E-mail : publishing@nuos.edu.ua
Свідоцтво суб'єкта видавничої справи ДК № 2506 від 25.05.2006 р.