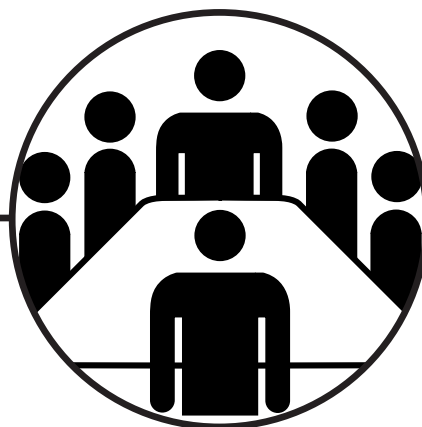


УПРАВЛІННЯ ПРОЕКТАМИ



DOI 10.15589/jnn20160109

УДК 004.056.5

Б69

CONCEPTION OF SYSTEM INFORMATION PROTECTION THAT CIRCULATES ON OBJECTS OF MARINE INFRASTRUCTURE

КОНЦЕПЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ НА ОБ'ЄКТАХ МОРСЬКОЇ ІНФРАСТРУКТУРИ

Volodymyr S. Blintsov

volodymyr.blintsov@nuos.edu.ua

ORCID: 0000-0002-3912-2174

Pavel V. Maidaniuk

pashamaydanuk@gmail.com

ORCID: 0000-0000-1289-019X

В. С. Блінцов

д-р техн. наук, проф.¹

П. В. Майданюк

здобувач²

¹*Admiral Makarov National University of Shipbuilding, Mykolaiv*

²*State service of special communication and information protection of Ukraine, Mykolaiv*

¹*Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

²*Управління Державної служби спеціального зв'язку та захисту інформації України
в Миколаївській області, м. Миколаїв*

Abstract. The paper contains the results of research aimed at developing information security systems for telecommunication networks of data transmission. The basic threats to the information have been determined, as well as requirements to the system protection, methods of providing confidentiality, integrity and availability of information circulating in telecommunication networks of data transmission on the marine infrastructure object. Realization of the functions of information protection is described by an association in the single system of the system safety, cryptographic and technical information protection, use of organizational, engineering and technological methods of information protection.

Keywords: information; information protection; information safety; data transmission network; information telecommunication system; technical information protection; cryptographic information protection.

Анотація. Робота містить результати досліджень, спрямованих на розвиток систем захисту інформації в телекомунікаційних мережах передачі даних. Визначено основні загрози інформації й вимоги до методів захисту інформації в телекомунікаційній мережі передачі об'єкта даних морської інфраструктури.

Ключові слова: інформація; захист інформації; інформаційна безпека; мережа передачі даних; інформаційно-телекомунікаційна система; технічний захист інформації; криптографічний захист інформації.

Аннотация. Работа содержит результаты исследований, направленных на развитие систем защиты информации в телекоммуникационных сетях передачи данных. Определены основные угрозы информации и требования к методам защиты информации в телекоммуникационные сети передачи данных объекта морской инфраструктуры.

Ключевые слова: информация; защита информации; информационная безопасность; сеть передачи данных; информационно-телекоммуникационная система; техническая защита информации; криптографическая защита информации.

REFERENCES

- [1] Averchikov V. I. *Audit informatsionnoy bezopastnosti* [Audit of information safety]: ucheb. Posobie, V.I. Averchenkov. — Bryansk: BGTU PUBL., 2005. 269 p.
- [2] Antopolskiy A. B. *Informatsionnye resursy Rossii* [Informative resources of Russia]: nauchno-metodicheskoe posobie, A. B. Antopolskiy. Moskva, Libereya Publ., 2004. 423 p.
- [3] Blintsov V. S., Kyryzyuk O. M., Krasnykh O. V., Yakym'yak S. V. *Bezekipazhna viys'kovo-mors'ka tekhnika — stan ta osnashchennya VMS ZS Ukrayiny* [Unmanned naval machinery: the current state and equipment of the Naval Forces of the Armed Forces of Ukraine] / «*Nauka i oborona*» [«Science and defence»]. 2012, no. 4, pp. 61–64.
- [4] Dergausov M. M. *Ukraina — derzhava morskaya* [Ukraine as the marine state]. Donetsk, Donechchina Publ., 2000. 269 p.
- [5] Domarev V. V. *Bezopasnost informatsionnykh tekhnologiy. Sistemnyy podkhod*. [Information technology safety. Systematic approach.]. Kyiv.: TID, DS Publ, 2004. 992 p.
- [6] DSTU 3396.2-97. *Zakhist informatsii. Tekhnichnyi zakhist informatsii. Terminy ta viznachennya*. [Information protection. Technical information protection. Terms and definitions]. Available at: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38934&cat_id=38836.
- [7] Kormych V. A *Informatsiyna bezpeka Ukrayiny: orhanizatsiyno-pravovi osnovy* [Information safety of Ukraine: organizational and legislative foundations]: Navch. Posibnyk, Kyiv, Kondor Publ., 2004. 384 p.
- [8] Lipkan V. A. *Informatsiyna bezpeka yak skladova natsional'noyi bezpeky Ukrayiny* [Information safety as a part of national safety of Ukraine], *Informatsiyni tekhnolohiyi v ekonomitsi, menedzhmenti i biznesi : Problemy nauky, praktyky i osvity* [Information technologies in economy, management and business]: Zb. nauk. prats' VIII Mizhnar. nauk.-prakt. konf. Ch. 2. Kyiv, Vyd-vo Yevrop. un-tu, 2003, pp. 443–453.
- [9] Lytvynenko O. V. *Informatsiyna bezpeka Yevropy* [Information safety of Europe]: Kosp. Lektsiy, Kyiv, KNU im. T. Shevchenka, 1999. 61 p.
- [10] Makarenko V. *Pravove rehulyuvannya zakhystu konfidentsiynoyi informatsiyi, shcho ye vlasnistyu derzhavy: stanovlennya, rozvytok, problemni pytannya* [Legal regulation of confidential information held by the State: formation, development issues], *Pravo Ukrayiny*, 2006, no. 1, pp. 132–135.
- [11] Makohon Yu. V., Lysyy A. F., Harkusha H. H., Hruzan A. V. *Ukrayna — derzhava morskaya* [Ukraine as a marine state] monohrafiya, pod red. Makohona Yu.V. Donetsk, DonNU Publ, 2010. 393 p.
- [12] *Mizhnarodne pravo* [International law]: Navch. posibnyk / Za red. M. V. Buromens'koho. Kyiv, Yurinkom Inter Publ., 2005. 336 p.
- [13] ND TZI 1.1-003-99 *Terminolohiya v haluzi zakhystu informatsiyi v komp'yuternykh systemakh vid nesanktsionovanoho dostupu* [Terminology in the sphere of information protection from unauthorized access in computer systems].
- [14] Pocheptsov G. G. *Kommunikativnye tekhnologii dvadtsatogo veka*. [Communicative technologies of the twentieth century]. Moscow, Refl-buk Publ; Kyiv, Vakler Publ, 2000. 352 p.
- [15] Rabynovych P. M. *Osnovy zahal'noyi teoriiy prava i derzhavy* [Foundations of general law and state theory] : [posib. dlya stud. spets-ti «Pravoznavstvo»], P. M. Rabynovych. Kyiv, 1994. 236 p.
- [16] Rach V.A. *Pryntsypy formuvannya kontseptsiy*. [Principles of forming concepts], Kyiv, *Visnyk Derzhavnoyi sluzhby Ukrayiny*, 2000, no.3, pp. 93–95.
- [17] *Stratehiya rozvytku mors'kykh portiv Ukrayiny na period do 2038 roku. Zatverdzheno rozporyadzhenniam Kabinetu Ministriv Ukrayiny vid 11 lypnia 2013 r. N 548-r*. [Strategy of development of marine ports of Ukraine for the period up to 2038. Ratified by the order of Cabinet of Ministers of Ukraine dated July, 11 in 2013 N 548-p.]. Kyiv, Ukraine Cabinet of Ministers, 2013. 7 p.
- [18] *Teoriya derzhavy ta prava* [State and law theory]: [navch. posib.] / A. M. Kolodiy, V. V. Kopeychikov, S. L. Lysenkov ta in.; Za zah. red. S. L. Lysenkova, V. V. Kopeychikova. Kyiv, Yurinkom Inter Publ, 2003. 368 p.
- [19] Web site of LTD “IIT”. Available at: www.iit.com.ua.
- [20] Web site of LTD “Tryte”. Available at: www.trite.ua.
- [21] *Zahal'ni polozhennya shchodo zakhystu informatsiyi v komp'yuternykh systemakh vid nesanktsionovanoho dostupu* [General provisions for information protection from unauthorized access in computer systems ND TZI 1.1-002-99]. Available at: <http://www.dsszzi.gov.ua/dstszi/doccatalog/document?id=117620>.

- [22] *Nakaz Administratsiyi Derzhavnoyi sluzhby spetsial'noho zv'yazku ta zakhystu informatsiyi Ukrainy # 100 «Pro zatverdzhennya polozhennya pro derzhavnu ekspertyzu v sferi kryptohrafichnoho zakhystu informatsiyi»* [Order of Administration of the State service of special communication and information protection of Ukraine № 100 “On approval of the state expertise in the field of cryptographic protection”]. Available at: <http://zakon4.rada.gov.ua/laws/show/z0651-08>.
- [23] *Poryadok provedennya robot zi stvorenniya kompleksnoyi systemy zakhystu informatsiyi v informatsiyno-telekomunikatsiyniy systemi* [Operational procedure for creating a complex system of information protection in telecommunication systems] ND TZI 3.7-003-05. Available at: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835.

ПОСТАНОВКА ПРОБЛЕМИ

Україна є державою з розвинутою морською інфраструктурою, де проводиться активна господарська діяльність. Вона має більше 20 морських портів і портпунктів на Азово-Чорноморському басейні, через її територіальні води пролягають морські транспортні шляхи. У винятковій морській економічній зоні України ведеться видобуток морепродуктів, вуглеводнів тощо [4, 11]. Згідно з вимогами Міжнародного морського права безпека такої діяльності має бути гарантована державою [12].

Крім того, сучасні загрози територіальній цілісності України вимагають створення єдиної системи моніторингу надводної, підводної й повітряної обстановки у територіальному морі України, яка має організовуватися на основі безекіпажних морських систем [3]. Така система складається з дистанційно або програмно керованих підводних, надводних і повітряних апаратів-роботів, які в реальному часі надають до берегового центру відомості про морську обстановку в територіальних водах держави й утворює новий об'єкт морської інфраструктури інформаційного характеру.

Інформаційна безпека є невід'ємним напрямом функціонування морської інфраструктури, який повинен розвиватись не тільки через нарощування технологічних можливостей здійснення інформаційного обміну, але й через глибоке усвідомлення усіма суб'єктами інформаційних відносин необхідності здійснення всіх заходів щодо гарантування інформаційної безпеки.

Одним з найважливіших напрямів діяльності у сфері захисту інформації є захист інформації технічними й криптографічними методами.

Базисом інформаційної безпеки на об'єктах морської інфраструктури (ОМІ) є сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації, яка в ній циркулює. На цей час морегосподарська діяльність в Україні не супроводжується гарантованими технічними й організаційними засобами, які б задовольняли цим вимогам, що й зумовлює актуальність даного дослідження.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Над загальними й конкретними питаннями у сфері інформаційної безпеки працюють В. Ліпкан, Г. По-

чепцов, В. Кормич [7, 8, 14]. Дослідженням з проблем правового забезпечення інформаційної безпеки присвячені роботи з теорії держави і права П. Рабиновича, А. Колодій, В. Копейчикова, С. Лисенков [15, 18]. Серед вітчизняних дослідників з питань організації діяльності у сфері криптографічного і технічного захисту інформації доцільно виділити В. Домарева та В. Хорошко [5].

Серед зарубіжних дослідників з питань державно-правового гарантування інформаційної безпеки варто відзначити роботи А. Антопольського, В. Аверченкова, Е. Макаренка, О. Литвиненко [9, 10, 2, 1].

Проте на цей час теоретичні питання захисту інформації, яка генерується, обробляється, передається й використовується на ОМІ, у науково-технічній літературі не висвітлено.

МЕТА ДОСЛІДЖЕННЯ — розробка концепції створення системи захисту інформації, що циркулює на ОМІ, яка забезпечує запобігання або максимальне ускладнення порушень конфіденційності, цілісності й доступності інформації, що оброблюється в інформаційній системі й прикладних програмних засобах (ППЗ), що функціонують у її складі.

ВИКЛАДЕННЯ ОСНОВНИХ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

Як методологічну основу розробки концепції захисту інформації, що циркулює на ОМІ, у роботі прийнято підхід, запропонований в [16], що передбачає виконання вимог за такими принципами:

— принцип «узгодженості цілей», який вимагає, щоб основна мета концепції була сумісна з цілями інших концепцій, що визначають функціонування різних елементів системи, а також із глобальними цілями і завданнями системи; виходячи з завдань загальнодержавного значення, які покладені на морську галузь України, система захисту інформації (СЗІ) на ОМІ має розроблятися як складова інформаційного забезпечення функціонування морської галузі держави поряд з іншими її системами — зв'язку і керування, оперативного і стратегічного планування, гарантування безпеки мореплавання, життя й здоров'я людей і господарської діяльності тощо [17];

— принцип «повної системи», згідно з яким рівень деталізації, що фіксується в концепції положень, повинен відповідати рівню деталізації елемента систе-

ми, для якої вона розробляється; виходячи з цього в роботі пропонуються технічні й організаційні рішення, які мають постановочний характер, а теоретичне обґрунтування їхньої практичної реалізації є предметом подальших досліджень;

– принцип «єдності основи», який передбачає використання термінів і понять, що мають однозначне й однакове трактування як на рівні елемента системи, так і на рівні системи загалом; у зв'язку з цим у роботі застосовуються виключно терміни і визначення, які регламентуються державними стандартами України й керівними документами Державної служби спеціального зв'язку й захисту інформації України [6, 13];

– принцип «неповної детермінованості і стохастичності», який припускає відсутність у концепції однозначних точних значень показників і параметрів елементів системи або системи в цілому; у зв'язку з цим у роботі викладаються загальні принципи побудови СЗІ; визначення конкретних технічних характеристик її апаратних і програмних засобів має бути результатом подальших прикладних наукових досліджень;

– «принцип розвитку», який визначає спрямованість концепції на інноваційний розвиток кожного елемента СЗІ та системи загалом, націлений на збільшення їх можливостей щодо виконання головних завдань за призначенням СЗІ; виходячи з цього пропонувані в роботі організаційні й технічні рішення передбачають постійний аналіз можливих загроз інформації, яка циркулює на об'єктах морської інфраструктури, та роботу «на запобігання» з метою ефективної нейтралізації нових загроз;

– принцип «задоволеності всіх учасників», який окреслює, що положення концепції повинні бути складені таким чином, щоб у період їх реалізації й завершення не погіршити становище інших систем, що забезпечують функціонування морської галузі; виходячи з цього принципу при розробці нової СЗІ передбачаються такі організаційно-керуючі та технічні рішення, які не створюють перешкод і завад нормальному функціонуванню інших систем СЗІ (наприклад, застосування безекіпажних морських систем не повинно ускладнювати організацію руху суден на захищених акваторіях);

– принцип «комплексності підходу», який полягає в необхідності розгляду можливостей реалізації концепції у всіх сферах життєдіяльності морської галузі; відповідність результатів роботи цьому принципу плануються забезпечувати шляхом застосування її результатів для захисту інформації не тільки при виконанні завдань морської галузі України (водний транспорт, видобувна та оборонна діяльність), а й для захисту інформації, яка циркулює при проведенні морської наукової й природоохоронної діяльності, освітньої й рекреаційної діяльності на морі.

З урахуванням вказаних загальних принципів формування концепцій і виходячи з сучасних завдань

СЗІ на ОМІ захищена система передачі даних повинна гарантувати:

- захист від несанкціонованого доступу;
- криптографічний захист інформації під час її передачі каналами зв'язку;
- контроль дотримання політики безпеки;
- керування комплексною СЗІ.

Досягнення визначеної мети передбачає вирішення наступних завдань:

- визначення можливих загрози інформації, що циркулює на об'єкті морської інфраструктури;
- розробка СЗІ, що циркулює на об'єкті морської інфраструктури.

Захищена інформаційна система передачі даних об'єкту морської інфраструктури являє собою розподілену мережу, до складу якої входять такі системи:

- система контролю доступу;
- система відеоспостереження та сигналізації (охоронна, пожежна);
- система засекреченого зв'язку;
- система керування та моніторингу надводної, підводної та повітряної обстановки на акваторіях, де розгорнуті об'єкти морської інфраструктури;
- пункт керування;
- апаратні складові інформаційної системи (безпілотні підводні, надводні, літальні апарати, стаціонарні апарати, засоби розвідки й контролю).

Принцип передачі даних у захищеній системі пропонується на основі протоколу IP, що забезпечить інформаційний обмін усіма видами інформації в мережах і має високий показник гнучкості, масштабованості й легкості взаємодії з іншими вузлами й системами зв'язку.

Для встановлення зв'язку між складовими мережі передачі даних може використовуватися комп'ютерна мережа з використанням різних каналів зв'язку (провідний, радіозв'язок, гідроакустичний).

Пропонована схема взаємодії між компонентами мережі наведена на рис. 1.

Характеристика умов і середовища експлуатації захищеної системи передачі даних. Робочі станції, сервери, пристрої мережевого обладнання та інші складові обчислювальної системи пункту управління повинні розміщуватись у захищеній будівлі, що розміщена в межах території, яка охороняється, та повинні мати джерела безперебійного живлення й цілодобову охорону.

Вхід до приміщення пункту управління варто здійснювати за службовими перепустками співробітників, які за своїми функціональними обов'язками мають відношення до робіт та/або обладнання в приміщенні пункту управління. Сервери системи, пристрої комутації, засоби криптографічного захисту інформації необхідно розмістити в окремому приміщенні (захищеній шафі), доступ до якого повинен бути наданий лише співробітникам, що здійснюють

експлуатацію й обслуговування зазначеного обладнання.

Доступ до компонентів, що входять до захищеної системи передачі даних, та розміщені поза межами пункту управління, у тому числі на апаратних складових інформаційної системи (безпілотні підводні, надводні, літальні апарати, стаціонарні апарати, засоби розвідки та контролю) доцільно обмежити організаційними й фізичними заходами (окремі приміщення, захищені шафи, відсіки тощо).

Характеристики інформації, що обробляється:

- дані й програмні коди у вигляді файлів різних форматів, що містять інформацію, яка підлягає захисту: інформація про результати моніторингу підводної, надводної й повітряної обстановки; відомості про стан системи сигналізації, відеоспостереження й системи контролю доступу; алгоритми й режими роботи безпілотних апаратів; команди керування технічними засобами та управління захищеною системою передачі даних 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.

Характеристика персоналу захищеної системи передачі даних

Співробітники, які мають право доступу до пункту управління й приміщень (об'єктів), в яких розташовані складові системи й до обладнання захищеної системи передачі даних розподіляються на такі категорії:

- адміністратор безпеки (здійснює розподіл прав доступу та керування системою, контроль за функціонуванням);
- системний адміністратор (забезпечує працездатність апаратних засобів і прикладного програмного забезпечення системи);
- оператори системи (співробітники, які за встановленим порядком отримали допуск до роботи в системі, але не мають привілеїв щодо керування засобами захисту інформації).

Загрози інформації. Основними ймовірними загрозами інформаційним ресурсам системи передачі даних є такі:

- дії операторів (користувачів) системи при роботі в ній, що можуть призвести до порушення конфіденційності, цілісності, доступності інформаційних ресурсів автоматизованих систем (помилки в роботі або несанкціонований доступ);
- дії персоналу, який обслуговує технічні засоби системи або приміщень, в яких розташована компо-

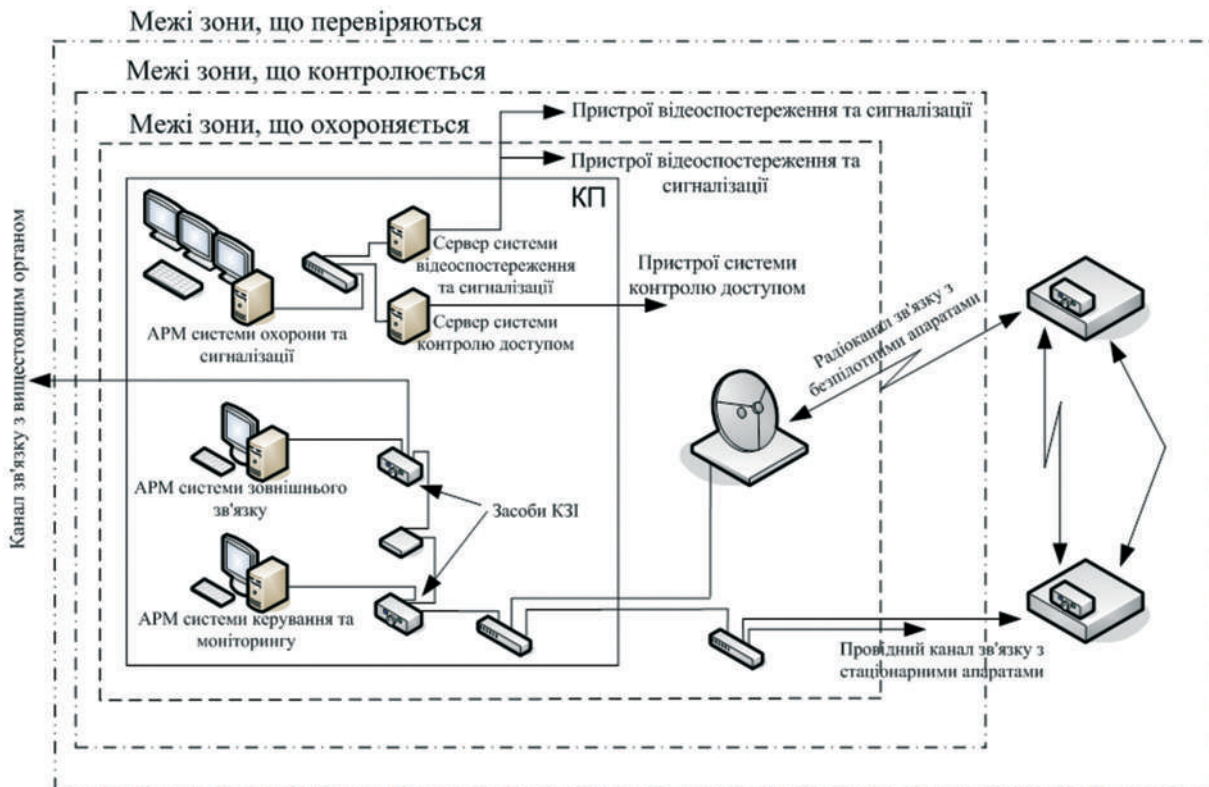


Рис. 1. Схема взаємодії між компонентами мережі передачі інформації, яка циркулює на об'єктах морської інфраструктури

ненти системи, що можуть спричинити втрати інформації, яка підлягає захисту шляхом крадіжки носіїв інформації або їх пошкодження;

– дії персоналу, який обслуговує технічні засоби системи або приміщень, у яких розташована компоненти системи, що можуть призвести до порушення спостережності інформаційних ресурсів і доступності програмно-апаратних засобів (виведення з ладу компонентів системи);

– дії зловмисників з поза меж контрольованої території, що стануть причиною витоку інформації технічними каналами та втрати апаратних складових системи (безпілотні апарати).

Вимоги щодо технічного захисту інформації.

Для забезпечення конфіденційності, цілісності, доступності інформації, що циркулює, обробляється, зберігається складовими інформаційної системи об'єкта морської інфраструктури й передається каналами зв'язку, варто впровадити комплекс заходів з організаційного, технічного й криптографічного захисту інформації.

Також необхідне вжиття організаційних заходів внутрішньооб'єктового режиму на об'єкті морської інфраструктури. Для організації розмежування фізичного доступу співробітників до різних зон такого об'єкта повинна бути створена система контролю доступу, яка складатиметься з тривірневого розподілу зон доступу, які відокремлені одна від одної пристроями пропуску (замки, турнікети, пункти пропуску). Для визначення системою контролю доступу прав співробітників на доступ до однієї із зон доцільно передбачити електронні перепустки (посвідчення з електронними чипами), за допомогою електронного коду яких можна налагоджувати систему на пропуск їх власників до різних приміщень або об'єктів наземних, прибережних, морських територій (акваторій), які підлягають охороні. По периметру приморського об'єкта й на внутрішніх об'єктах, які містять відомості, що потребують захисту (пункти управління, спеціальні сховища, стаціонарні морські споруди, вибухо- й пожежо-небезпечні об'єкти) необхідно встановлювати системи сигналізації й відеоспостереження, лінії яких повинні підключатися до пристроїв (моніторів) на пункті управління (АРМ системи охорони й сигналізації).

До телекомунікаційної мережі передачі даних, що призначена для обробки інформації з обмеженим доступом, висуваються підвищені вимоги щодо її надійності й забезпечення конфіденційності інформації. Захист інформації в таких системах здійснюється засобами технічного й криптографічного захисту [20], що запобігає несанкціонованому доступу до інформації й програмного забезпечення, за допомогою якого відбувається керування системою, порушенню її цілісності, достовірності, перехопленню у відкритих каналах зв'язку, а також витоку технічними каналами.

Засоби й заходи захисту інформації повинні бути спрямовані на протидію загрозам інформації, яка циркулює в інформаційно-телекомунікаційній системі об'єкта морської інфраструктури, а саме способи, методи, механізми захисту інформації від [23]:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали;

– несанкціонованих дій і несанкціонованого доступу до інформації, що можуть провадитися шляхом підключення до апаратури й ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін.;

– спеціального впливу на інформацію, що може здійснюватися шляхом формування полів і сигналів з метою порушення цілісності інформації або руйнування СЗІ.

Всі програмні апаратні й апаратно-програмні засоби, що будуть застосовуватися для реалізації системи інформаційної безпеки, повинні мати відповідний експертний висновок за результатами проведеної державної експертизи [22].

Вимоги до криптографічного захисту інформації. Побудову захищеної системи передачі даних необхідно впроваджувати за допомогою засобів шифрування трафіку IP-мереж відповідного рівня таємності, центру генерації ключових даних, централізованої системи керування (АРМ адміністратора) й кінцевого обладнання обробки інформації (безпілотні апарати, абонентські пункти зв'язку) [19].

IP-шифратори забезпечують шифрування й контроль цілісності потоків мережних IP-пакетів, що передаються через них між складовими системи.

Пристрої генерації ключових даних призначені для генерації, зберігання й розподілу ключових даних. Розподілення ключів має здійснюватись двома методами: передачею мережею шифрованого зв'язку й/або на носіях ключових даних [19].

Централізована система керування (АРМ адміністратора) призначена для управління мережею, налагодження параметрів конфігурації, моніторингу та протоколювання подій, перегляду статистичної інформації.

Засоби КЗІ й кінцеве обладнання можуть застосовуватися на стаціонарних і рухомих об'єктах. Вони повинні мати резервні джерела живлення й надійні (дублюючі) канали зв'язку.

Система криптографічного захисту інформації з використанням апаратних і програмних засобів (IP-шифраторів) буде забезпечувати:

– збереження конфіденційності інформації за допомогою засобів шифрування;

– здійснення контролю цілісності інформації за допомогою контрольної суми повідомлення або електронного цифрового підпису;

– гарантування отримання інформації в необхідні часові строки.

Ключові дані повинні складатися із послідовного набору символів, що формуються за допомогою пристроїв генерації ключових даних [19].

Необхідно забезпечити надійний захист самої системи захисту інформації від модифікації для унеможливлення зменшення криптостійкості системи загалом. Ключову інформацію, яка міститься на окремих складових інформаційної системи, доцільно знищувати в автоматичному режимі в разі несанкціонованого доступу до них (фізичного або програмного).

Для відновлення роботи СЗІ після можливих збоїв вона необхідно здійснювати періодичне збереження критичних параметрів роботи.

Засоби криптографічного захисту інформації, що встановлені в сегменти інформаційної системи, повинні використовувати єдину ключову зону в межах контрольованої території. Для передачі даних за межі контрольованої зони (до вищих органів, штабів, міністерств, адміністрацій) варто застосовувати іншу ключову зону (ключову документацію, криптоалгоритм). Для спільної роботи різних ключових зон необхідно створити вузол їх спряження й розподілу повідомлень між адресатами (концентратор), який має перебувати на території, що охороняється.

Під час побудови СЗІ доцільно забезпечити відсутність гальванічного з'єднання внутрішньої системи й ліній зв'язку, які виходять за межі контрольованої зони. Провідні тракти відкритої інформації (від абонента, або пристрою передачі інформації до апаратури шифрування) повинні бути обладнані системою сигналізації на випадок пошкодження або підключення сторонніх пристроїв.

Для захисту інформації під час її передачі каналами зв'язку всі апаратні складові інформаційної системи (безпілотні підводні, надводні, літальні апарати, засоби розвідки й контролю, пункти управління та ін.) варто використовувати засоби шифрування (ІР-шифратори). Вказані засоби повинні встановлюватися в апаратах у розрив лінії між пристроєм збору й накопичення даних і каналотворюючим обладнанням (супутниковий модем, роутер, обладнання ущільнення, радіостанція та ін.). Пристрої криптографічного захисту інформації (апаратура засекречування) мають забезпечувати якісну роботу незалежно від вибраного виду зв'язку (супутниковий зв'язок, мобільний зв'язок, Wi-Fi, кабельна мережа, тощо).

Апаратура криптографічного захисту інформації має бути сертифікована Державною службою спеціального зв'язку й захисту інформації України [21] й повинна давати змогу будувати мережі засекреченого зв'язку для передачі конфіденційної інформації й інформації, що становить державну таємницю. Налагодження, управління, перевірку конфігурування ІР-шифраторів доцільно здійснювати за допомогою

АРМ адміністратора й за допомогою мобільного АРМ (ноутбук) при обслуговуванні безпілотних апаратів, для яких необхідно передбачити відповідний інтерфейс і до яких повинен бути виключений несанкціонований доступ.

У разі необхідності передачі аналогових сигналів перед апаратурою криптографічного захисту інформації необхідно встановлювати прилади перетворення аналогового сигналу в цифровий.

Система криптографічного захисту інформації повинна забезпечувати засекречений зв'язок між сегментами системи один з одним і між апаратними сегментами інформаційної системи приморського об'єкта з пультом керування. Контроль й управління в СЗІ має здійснюватись з командного пункту, який розташовується на контрольованій території й де розміщено апаратуру контролю й комутації.

Система криптографічного захисту інформації на базі ІР-шифраторів буде забезпечувати захист від:

- несанкціонованого доступу до інформації, що циркулює в мережі, і службової інформації керування системою;
- модифікації програмного забезпечення терміналів апаратури засекречування;
- коректування (спотворення) інформації, яка зберігається у файлах терміналів апаратури засекречування, або інформації, що передається каналами зв'язку;
- спроб видачі себе за клієнта інформаційної мережі інших приладів шляхом крадіжки носіїв ключової інформації;
- перехоплення функцій керування інформаційною системою зловмисниками з інших місць, окрім командного пункту;
- несанкціонованого отримання конфіденційної інформації або службових даних методами аналізу паразитних електромагнітних випромінювань;
- несанкціонованого отримання конфіденційної інформації або службових даних через встановлення спеціальних програмно-апаратних пристроїв у сегменти інформаційної системи.

Також система захисту повинна забезпечувати:

- блокування управління з ПЕОМ до повного завершення ідентифікації користувача;
- розподіл повноважень і доступ до ресурсів між користувачами, адміністраторами й технічним персоналом за допомогою особистого пароля й електронного ключа;
- шифрування інформації, що передається каналами зв'язку, з використанням криптоалгоритмів і ключової інформації з гарантованою стійкістю;
- звірку контрольної суми або електронного цифрового підпису після сенсу передачі даних;
- прозорість взаємодії ПЕОМ і каналотворюючої апаратури (модеми, роутори тощо) і відсутність обмежень на використання спеціального програмного забезпечення.

ВИСНОВКИ. 1. Ефективно вирішувати завдання щодо захисту інформації, яка циркулює в інформаційних системах, можна лише шляхом створення в їх складі комплексних систем захисту інформації, що поєднують організаційні, інженерні заходи, а також технічні й криптографічні засоби захисту. 2. Метою створення комплексної системи захисту інформації є забезпечення захисту інформації, що обробляється, передається й зберігається в системі від несанкціонованого доступу, порушення її цілісності, конфіденційності, несанкціонованої модифікації й знищення, а та-

кож гарантування доступності інформації для авторизованих користувачів. 3. Реалізація функцій захисту досягається через використання об'єднаних в єдину систему систем охорони, криптографічних засобів захисту, а також шляхом виконання спеціальних організаційних, інженерних і технологічних заходів із захисту інформації. 4. Захист інформації в розподілених інформаційних системах є складною системною задачею, яка вимагає застосування комплексу інженерно-технічних, криптографічних, апаратно-програмних й організаційних заходів захисту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

- [1] **Аверчиков, В. И.** Аудит информационной безопасности: учеб. Пособие / В. И. Аверченков. — Брянск : БГТУ, 2005. — 269 с.
- [2] **Антопольский, А. Б.** Информационные ресурсы России : научно-методическое пособие / А. Б. Антопольский. — Москва : Либерия, 2004. — 423 с.
- [3] Безекіпжна військово-морська техніка – стан та оснащення ВМС ЗС України / В. С. Блінцов, О. М. Киричук, О. В. Красних, С. В. Яким'як // «Наука і оборона», 2012. — № 4. — С. 61–64.
- [4] **Дергаусов, М. М.** Украина – держава морская / М. М. Дергаусов. — Д. : Изд-во «Донецчина», 2000. — 269 с.
- [5] **Домарев, В. В.** Безопасность информационных технологий: Системный подход / Домарев В. В. — К. : ООО «ТИД «ДС», 2004. — 992 с.
- [6] Захист інформації. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97. — [Чинний від 1998.01.01]. — [Електронний ресурс] / Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. — Режим доступу : http://www.dstszi.gov.ua/dstszi/control/uk/publish/article.jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38934&cat_id=38836.
- [7] **Кормич, В. А.** Інформаційна безпека України: організаційно-правові основи : навч. посібник / В. А. Кормич. — К. : Кондор, 2004. — 384 с.
- [8] **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.
- [9] **Литвиненко, О. В.** Інформаційна безпека Європи: Консп. Лекцій / О. В. Литвиненко. — К. : КНУ ім. Т. Шевченка, 1999. — 61 с.
- [10] **Макаренко, В.** Правове регулювання захисту конфіденційної інформації, що є власністю держави: становлення, розвиток, проблемні питання / В. Макаренко // Право України. — 2006. — № 1. — С. 132–135.
- [11] Украина – держава морская : монография / Ю. В. Макогон, А. Ф. Лысый, Г. Г. Гаркуша, А. В. Грузан // под ред. Ю. В. Макогона. — Донецк : ДонНУ, 2010. — 393 с.
- [12] Міжнародне право : навч. посібник / за ред. М. В. Буроменського. — К. : Юрінком Інтер, 2005. — 336 с.
- [13] НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
- [14] **Почепцов, Г. Г.** Коммуникативные технологии двадцатого века / Г. Г. Почепцов. — М. : Рефл-бук; К. : Ваклер, 2000. — 352 с.
- [15] **Рабинович, П. М.** Основы общей теории права и государства : [посіб. для студ. спец-ті «Правознавство»] / П. М. Рабинович. — К., 1994. — 236 с.
- [16] **Рач, В. А.** Принципи формування концепцій / В. А. Рач // «Вісник Державної служби України». — К., 2000. — № 3. — С. 93–95.
- [17] Стратегія розвитку морських портів України на період до 2038 року: [Затверджено розпорядженням Кабінету Міністрів України від 11 липня 2013 р. N 548-р.]. — К. : Кабінет Міністрів України, 2013. — 7 с.
- [18] 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.
- [19] Веб-сайт ТОВ «ІТ» [Електронний ресурс]. — Режим доступу: www.iit.com.ua.
- [20] Веб-сайт ТОВ «Трител» [Електронний ресурс]. — Режим доступу: www.tritel.ua.
- [21] Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-002-99. [Електронний ресурс]. — Режим доступу : <http://www.dsszzi.gov.ua/dstszi/doccatalog/document?id=117620>.
- [22] Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України № 100 «Про затвердження положення про державну експертизу в сфері криптографічного захисту інформації». [Електронний ресурс]. — Режим доступу : <http://zakon4.rada.gov.ua/laws/show/z0651-08>.
- [23] Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003-05. [Електронний ресурс]. — Режим доступу : http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=46074&cat_id=38835.

© В. С. Блінцов, П. В. Майданюк

Надійшла до редколегії 19.01.2016

Статтю рекомендує до друку член редколегії ЗНП НУК
д-р техн. наук, проф. К. В. Кошкін