ISSN 1314-3379

АСПЕКТИ НА КОМУНИКАЦИОННО-ИНФОРМАЦИОННОТО ОСИГУРЯВАНЕ НА ВОЕННОМОРСКИТЕ СИЛИ

Желязко Николов

COMMUNICATION AND INFORMATION SYSTEM SUPPORT FOR THE NAVY ASPECTS

Zhelyazko Nikolov

Abstract: *Nowadays improving the information environment is of growing importance not only for the Navy. It is well known that Communication and Information System is a crucial factor in effective command and control. That is why the progress in military communications is so important. In this article some current aspects of Bulgarian Naval Communication and Information System are overviewed.*

Keywords: *Communication and Information System, Navy.*

1. Въведение.

Нарастването на способностите на комуникационно-информационната система за осигуряване на ефективност на системата за командване и управление е проблем пред Военноморските сили с най-висок приоритет. Бурно променящата се информационна среда и факторите, които ѝ влияят допълнително усложняват тази задача, но въпреки това полаганите усилия водят до намирането и прилагането на определени актуални комуникационни решения. Така през последните години значителен брой мащабни проекти за осъвременяване на комуникационно-информационната система намериха своята успешна реализация. Освен това удовлетворяването на все по-високите потребности при воденето на информационен обмен включва съвкупност от активности, които неминуемо съсредоточават значителни системни усилия и тяхното планиране изисква регулярен преглед и оценка на извършеното. В настоящата разработка са представени някои аспекти на комуникационно информационното осигуряване на Военноморските сили [5,11,12].

2. Аспекти на комуникационно-информационното осигуряване на Военноморските сили.

Едно от предизвикателствата пред комуникационно-информационната система на Военноморските сили през последните две десетилетия е поддържането на необходимия темп на техническо обновяване за осигуряване на оперативна съвместимост с военноморските структури на Алианса. Несъмнено процесите по изпълнението на тази задача могат да бъдат отбелязани като успешно протичащи, но трябва да се отбележи и фактът, че те са съпроводени и с последствия, които в определени аспекти създават затруднения при адаптирането към съвременните реалности. Сред тях са динамично променящата се информационна среда, нарастването на дигиталната зависимост и разкриването на уязвимости в сферата на киберпространството [3,4,8,9,10,13,15,16]. Всичко това налага фокусирането върху постигането на адекватна на действителността киберсигурност.

Киберсигурност е състояние на обществото и държавата, при което чрез прилагане на комплекс от мерки и действия киберпространството е защитено от заплахи, свързани с неговите независими мрежи и информационна инфраструктура или които могат да нарушат работата им [6]. Според друг източник тя е състояние на киберпространството определяно от нивото на конфиденциалност, интегритет, достъпност и автентичност на информационните ресурси, системи и услуги. Киберсигурността се основава на ефективно изграждане и

поддържане на активни и превантивни мерки [7]. В този смисъл дейното търсене на решения при осигуряването на киберсигурност е от съществено значение не само в областта на военните телекомуникации. Тези решения биха могли да бъдат сведени, но не и ограничени до: повишаване на усилията при провеждането на адекватни на обстановката преглед и оценка на рисковете и заплахите по отношение на киберсигурността; обезпечаване на допълнителни способности за предотвратяване на киберзаплахи и инциденти; укрепване на капацитета за експертиза и реакция при кибератаки и тяхното възпиране. Усилията в тези направления освен да кореспондират на високата актуалност на проблема, трябва и да се фокусират върху провеждането на комплекс от организационни мероприятия, повишаването на квалификацията на личния състав за подобряване на нивото на мрежова и информационна сигурност и не на последно място в осигуряването на финансови средства за гарантиране на необходимите ресурси.

Сред значимите проекти, свързани с комуникационно-информационно осигуряване на Военноморските сили е и изграждането на мобилната мрежа за свръзка с подвижни обекти по разработения от Европейския институт за стандартизация в телекомуникациите стандарт TETRA (Terrestrial Trunked Radio). Този стандарт притежава характеристики на мобилна система с комерсиално приложение, но в същото време е предназначен да задоволява специфичните изисквания на държавни организации за сигурност и отбрана. Развърнатата военна мобилна мрежа на територията на страната се базира на стандартни Интернет протоколи, като тяхното сравнително широко разпространение спомага за лесното разширяване на системата и интегрирането ѝ с други системи, а това позволява развитието ѝ. Редно е да се отбележи ролята на TETRA мрежата за подобряването на условията и ефективността при воденето на ежедневния информационен обмен, но също и да се положат още усилия за използването на наличните възможности за разкриването на нови направления за развитие. Сред тях са разширяването на интеграцията с дружи мрежи, необходимостта от нарастване на капацитета по отношение на предаването на данни и използването на специализирани приложения.

Друг актуален аспект по отношение на комуникационно-информационното осигуряване на Военноморските сили е налагането на базирани на Интернет протоколи MHS (Message Handling System) приложения. Както е известно този вид работа се осигурява съгласно стандартизационно споразумения STANAG 4406, като направените нововъведения тук освен сигурност и повишена шумоустойчивост предоставят възможности за отчитане на конкретни особености в условията за разпространение на радиовълните. Безспорно сигурността все по-често се разглежда като високоприоритетен аспект на комуникациите изобщо, и в частност на MHS обмена. В днешно време производителите на военни системи за форматирани съобщения се придържат тясно към съвременните схващания в областта [14,17] и в тази посока трябва да се отбележи напредъкът на Военноморските сили в MHS обмена, включително в перспектива при новите многофункционални модулни патрулни кораби.

Нарастването на капацитета по отношение на киберсигурността, развитието на мобилните мрежови структури и налагането на базирани на Интернет протоколи MHS приложения са само малка част от предизвикателствата, свързани с усвояването на многофункционалните модулни патрулни кораби. През следващите години предстои интегрирането на тези нови платформи в единната комуникационно-информационна среда на Военноморските сили. Подобни високи амбиции основателно намират своята проекция и отговор във военно-образователната система, която на свой ред се приспособява към новите реалности. В този смисъл комуникационно-информационната система и реализирането на поставените пред нея цели са пряко обвързани с наличния научно-изследователски и академичен потенциал на Висшето военноморско училище „Н. Й. Вапцаров“. В този план категорично трябва да се отбележи, че се наблюдава стремеж за удовлетворяване на широк кръг изисквания, както по отношение на подготовката на курсанти, така и в работата по научни

проекти, предоставянето на материална база, включително тренажорни комплекси за тренировъчни дейности и учения [1,2].

3. Изводи.

Комуникационно-информационното осигуряване на Военноморските сили протича в динамично променяща се среда. Сред водещите фактори, които влияят на комуникационно-информационната система трябва да бъде посочен забележителният ръст на телекомуникационните технологии и нарастващото значение на сигурността в киберпространството. Едно от основните предизвикателства на хоризонта е усвояването на комуникационно-информационното оборудване на новите многофункционални модулни патрулни кораби. Този мрежово ориентиран технически комплекс обединява широк спектър от съвременни решения и неговата пълноценна интеграция в комуникационно-информационната среда на Военноморските сили е не само ключов приоритет, но и разкрива нови възможности и перспективи. Важна роля в подпомагането на тези процеси е отредена на военно-образователната система, както по отношение на подготовката на бъдещите кадри, така и при провеждането на научно-изследователска дейност в интерес на военния флот.

Използвана литература:

1. КАРАДЕНЧЕВА, А. Прилагане на компоненти от модела на Даниъл Голман за емоционална интелигентност в тренингите по лидерска подготовка за курсанти във ВВМУ „Н. Й. Вапцаров“. *Известия*, СУ-Варна, 2019, с. 13-22. ISSN 1314-3379. Available from: https://www.su-varna.org/izdanij/2019/MN_Proceedings_2019.pdf

2. КОРИТАРОВ, Т. Подходи в използването на безпилотни летателни системи в областта на морската индустрия и образование. *Известия*, СУ-Варна, 2021, с. 26-32. ISSN 1314-3379. Available from: https://www.su-varna.org/izdanij/2021/2021_Proceedings_Morski-nauki_final.pdf

3. КРЪСТЕВ, Д. Киберзащита на критичната информационна инфраструктура. *Сборник доклади „Логистиката и обществените системи”*, 2021, с. 159-165. НВУ „Васил Левски” ISSN 2738-8042.

4. КРЪСТЕВ, Д. Актуални проблеми на киберсигурността в корабоплаването. *Сборник доклади „Логистиката и обществените системи”*, 2021, с. 140-149. НВУ „Васил Левски” ISSN 2738-8042.

5. ДОКТРИНА ЗА КОМУНИКАЦИОННО-ИНФОРМАЦИОННАТА СИСТЕМА НА ВЪОРЪЖЕНИТЕ СИЛИ – НП-06. *Министерство на отбраната на Република България*, 2012.

6. ЗАКОН ЗА КИБЕРСИГУРНОСТ, *обн. ДВ, бр. 94*, 2018.

7. НАЦИОНАЛНА СТРАТЕГИЯ ЗА КИБЕРСИГУРНОСТ „КИБЕРУСТОЙЧИВА БЪЛГАРИЯ 2020“, *Министерски съвет на Република България, 2016.*

8. DIMITROV N., Ch. ALEXANDROV, M. TODOROV. Cyber Security Analysis of Maritime Surveillance Systems, *21-st Annual General Assembly IAMU AGA21* – Proceedings of the International Association of Maritime Universities, IAMU Conference, pp. 463 – 471, Egypt, 2021.

9. GRANCHAROVA, V. Challenges To The Multimodal Transport Networks Based On Sustainable Growth In The Volume Of Containerized Cargoes. *Pedagogika-Pedagogy*, 2021, Volume 93, Number 7s, p. 53-64 . ISSN 1314–8540 (Online) ISSN 0861–3982 (Print). Available from: https://doi.org/10.53656/ped21-7s.04chal

10. GRANCHAROVA, V. The challenge of building greenfield terminals. *Journal of Marine Technology and Environment*. 2014, Year VI I, Vol. II/2014, p. 33-36. ISSN 1844 – 6116. Available from: https://issuu.com/jmte/docs/jmte-vol.2-2014

11. AJP-3.10. Allied Joint Doctrine for Information Operations. *NATO Standardization Office*, 2015.

12. AJP-6. Allied Joint Doctrine for Communication and Information System. *NATO Standardization Office*, 2017.

13. HYBRID WARFARE – NEW THREATS, COMPLEXITY, AND 'TRUST' AS THE ANTIDOTE [online]. 2021 [Accessed 23 June 2023]. Available from: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

14. MILITARY MESSAGING (MMHS) OVER SMTP [online]. 2023 [Accessed 23 June 2023]. Available from: https://www.isode.com/whitepapers/mmhs-over-smtp.html

15. NORTH ATLANTIC TREATY ORGANIZATION. Cyber Defence [online]. 2022. [Accessed 23 June 2023]. Available from: https://www.nato.int/cps/en/natohq/topics_78170.htm

16. NORTH ATLANTIC TREATY ORGANIZATION. NATO's Cyber Security Centre [online]. 2022. [Accessed 23 June 2023]. Available from: https://www.ncia.nato.int/what-we-do/cyber-security.html

17. RHODE-SCHWARZ MMHS STANAG 4406 – BASED MILITARY MESSAGE HANDLING SYSTEM [online]. 2011 [Accessed 23 June 2023]. Available from: https://cdn.rohde-schwarz.com/pws/dl_downloads/dl_common_library/dl_brochures_and_datasheets/pdf_1/MMHS_bro_en.pdf

За контакти:
доц. д-р Желязко Кирилов Николов
ВВМУ „Н. Й. Вапцаров"
e-mail: zhelyazko_nikolov@abv.bg