ISSN 1314-3379

КОМУНИКАЦИОННО-ИНФОРМАЦИОННАТА СИСТЕМА НА ВМС В КОНТЕКСТА НА СЪВРЕМЕННИТЕ ИЗИСКВАНИЯ ЗА КИБЕРСИГУРНОСТ

Желязко Николов

NAVAL COMMUNICATION AND INFORMATION SYSTEM IN THE CONTEXT OF CYBERSECURITY TRENDS

Zhelyazko Nikolov

Abstract: *At the present time a great variety of challenges wield influence over Bulgarian Navy and of course over Communication and Information System. It is well known that Communication and Information System is a crucial factor in effective command and control and that is why the progress in military communications is so important to be examined. In this article some aspects of the development of Bulgarian Naval Communication and Information System are overviewed especially those related to Cybersecurity trends.*

Keywords: *Communication and Information System, cybersecurity.*

1. Въведение.

Приемането на Република България в Организацията на Северноатлантическия договор и произтичащите от това задължения на държавата към колективната система за сигурност поставиха нов хоризонт на предизвикателствата пред Военноморските сили. Едно от тях е необходимостта от адаптиране на системата за командване и управление към новите реалности, и по-специално на един от основните ѝ компоненти – комуникационно-информационната система.

Разработените през последните години национални концептуални и доктринални документи в сферата на отбраната осигуриха нормативна база за протичащите промени във военния ни флот. В Националната отбранителна стратегия [3] са посочени мисиите на въоръжените сили, а именно: отбрана, подкрепа на международния мир и сигурност, принос към националната сигурност в мирно време. Успешното изпълнение на задачите, които произтичат от тези мисии, от страна на Военноморските сили, съществено зависи от наличието на реални възможности за постигането на информационно превъзходство в процеса на командване и управление, както и от осъществяването на ефективно взаимодействие. Това може да бъде осигурено при използването на съвременна и функционална комуникационно-информационна система. Както е известно, тя представлява единен, интегриран организационно-технически комплекс от средства, методи, услуги и личен състав, организирани за поддържане на командването и управлението чрез добиване, обмен, съхранение, анализ, представяне и защита на информацията. По своята физическа същност комуникационно-информационната система е среда за функциониране на системата за командване и управление [6, 7].

В настоящия доклад е представен обзор на някои зависимости на системата по отношение на процеса на удовлетворяване на нарастващите изисквания за киберсигурност.

2. Комуникационно-информационната система на Военноморските сили в контекста на съвременните изисквания за киберсигурност.

Един от основните проблеми пред комуникационно-информационната система на Военноморските сили през последните години, който може да бъде определен като съществен в контекста на настоящата разработка е поетапното техническото обновяване на системата, с цел осигуряване на оперативна съвместимост в процеса на информационен обмен, както с останалите видове въоръжени сили, така и с Военноморските сили на НАТО и страните партньори. Несъмнено процесите по неговото решаване могат да бъдат отбелязани като успешно проведени, но те са съпроводени и с последствия, които в определени аспекти създават затруднения при адаптирането към съвременните реалности. Сред тях са нарастването на дигиталната зависимост и разкриването на уязвимости в новата среда на киберпространството. Всичко това налага фокусирането върху постигане на адекватна на динамичната действителност 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“ е записано в Закона за киберсигурност [2]. Според друг нормативен акт тя е състояние на киберпространството определяно от нивото на конфиденциалност, интегритет, достъпност, автентичност и отказоустойчивост на информационните ресурси, системи и услуги. Киберсигурността се основава на ефективно изграждане и поддържане на активни и превантивни мерки. [4]. Това дава основание да се твърди, че положителният отговор на въпроса „Отговаря ли комуникационно-информационната система на съвременните изисквания за киберсигурност?“ би бил допустим в настоящия момент с някои условности.

Може да се приеме, че предизвикателствата пред органите за управление на комуникационно-информационната система на Военноморските сили могат да бъдат сведени, но не и ограничени до:

- извършване на адекватни на обстановката преглед и оценка на рисковете и заплахите по отношение на киберсигурността;
- осигуряване на достатъчни човешки и технически ресурси за постоянно наблюдение на комуникационно-информационната система в киберпространството;
- обезпечаване на способности за предотвратяване на киберзаплахи и инциденти;
- укрепване на капацитета за експертиза и реакция при кибератаки и тяхното възпиране.

Усилията в тези направления трябва да кореспондират на високата актуалност на проблема и да се фокусират от една страна върху провеждане на комплекс от организационни мероприятия и повишаване на квалификацията на личния състав за подобряване на нивото на мрежова и информационна сигурност, а от друга - в осигуряването на финансови средства за гарантиране на необходимите технически ресурси.

Друг важен елемент, който гарантира ефективна работа на системата за командване и управление е военноморската критична инфраструктура. Известно е, че кибератаките притежават сравнително висок потенциал за въздействие и нанасяне на щети върху нея чрез налични уязвимости на софтуерно базираните системи за управление. Съвременната информационна война показва, че организирани кибератаки могат да бъдат инициирани и от терористични организации и това дава основание при

изграждането на способности за противодействие да се разглежда един по-широк кръг от вероятни източници на заплахи, средства и методи за въздействие [1,10]. Освен това и фактът, че все по-ясно се наблюдава тясна обвързаност на информационните мрежи с обекти на военноморската критична инфраструктура, като например стационарни компоненти на мобилната мрежа по стандарт TETRA; радиорелейни мрежи на системата за наблюдение; логистични хранилища и дори пристанища, води до необходимостта от решаване на проблема за тяхната адекватна киберзащита и устойчивост [5, 8, 9].

И в този случай активността за решаване на въпроса следва да бъде ориентирана към нарастване на капацитета за експертиза. Важна стъпка за повишаване на възможностите в сферата на киберсигурността е подготовката на курсанти във Висшето военноморско училище „Н. Й. Вапцаров“ по специализация „Кибероперации“. Това ще позволи в краткосрочна перспектива да се разчита на квалифицирани специалисти на длъжности не само в комуникационно-информационната система на Военноморските сили, но и във видовете въоръжени сили.

3. Изводи.

Ефективната работа на системата за командване и управление в национален план осигурява ясна индикация, че комуникационно-информационната система се е адаптирала към съвременната динамична информационна среда. От друга страна, успешното участие на Военноморските сили в учения и мисии в съюзен формат е показател, че изискванията за оперативна съвместимост на КИС са изпълнени във всички нейни аспекти – техническа, семантична и организационна. Въпреки това, на този етап трябва да се търси решение на проблема за извършване на адекватната оценка на рисковете и заплахите в киберпространството. Това ще позволи своевременно изграждане и поддържане на необходимите способности са осигуряване на киберсигурност и предотвратяване на киберзаплахи и инциденти. Едно от ключовите решения, макар и с отложен във времето резултат е обучението на висококвалифицирани специалисти във Висшето военноморско училище „Н. Й. Вапцаров“. Разбира се, не бива да се пренебрегва и обстоятелството, че справянето с разглеждания проблем допълнително се усложнява от ролята на финансовия фактор, който поставя Военноморските сили пред предизвикателството да удовлетворяват нарастващите изисквания за наличието на способности по отношение на киберсигурността в условията на дефицит на средствата за придобиването и поддържането им.

Използвана литература:

1. Анева, А. Ислямска държава и прекрояването на официалните граници. Военен журнал, година 122, бр. 2, с. 137-143, София, Министерство на отбраната, 2015, ISSN 2534-8388.

2. Закон за киберсигурност, обн. ДВ, бр. 94 от 13.11.2018.

3. Национална отбранителна стратегия. Министерство на отбраната, София, 2016.

4. Национална стратегия за киберсигурност „Киберустойчива България 2020“, Министерски съвет на Република България, София, 2016.

5. Grancharova V., V. Vasilev. Safety and reliability in port. IV International Scientific “Conference modern ports - problems and decisions”, p. 14-17, Poland, 2012, ISBN 978-966-7716-69-1.

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

7. Naval Command and Control – NDP-6. Headquarters United States Marine Corps, Washington, DC 20380-0001, 1995.

8. https://euagenda.eu/upload/publications/untitled-145478-ea.pdf - 10.10.2020.

9.https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector – 10.10.2020.

10.https://www.researchgate.net/publication/341589395_CYBER_TERRORISM_A_CASE_STUDY_OF_ISLAMIC_STATE – 10.10.2020.

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