Софка Хаџијевска Постоловска, PhD[1]
Наташа Тодоровска, PhD[2]
Мартин Симоновски, PhD[3]

UDC: 351.86:004.49.056

NEVOJA PËR SIGURI KIBERNETIKE NË PËRBALLIMIN E RREZIQEVE DHE KËRCËNIMEVE BASHKËKOHORE TË SIGURISË

ПОТРЕБАТА ОД САЈБЕР БЕЗБЕДНОСТ ВО СПРАВУВАЊЕТО СО СОВРЕМЕНИТЕ БЕЗБЕДНОСНИ РИЗИЦИ И ЗАКАНИ

THE NEED FOR CYBER SECURITY IN DEALING WITH MODERN SECURITY RISKS AND THREATS

Abstract

With the development of information technology and the mass use of the Internet as a global structure for business and as a new tool for politics, espionage, and military activities, the need to take measures to protect against the abuse of the opportunities offered by the Internet and the tools of information technology has become apparent. Cyberspace, or the Internet, is evolving into a global, interconnected network of systems and information that is transforming the behavior of governments, businesses, and citizens and opening up new markets with limitless opportunities for promotion and trade. On the other hand, this trend is followed by a continuous increase in cyber attacks on the critical infrastructure of states, which imposes the need to find an effective model for securing cyberspace from cyber attacks. Accordingly, the subject of this paper is an analysis of the need to create cybersecurity, timely, efficiently and comprehensively deal with modern risks and threats to security. Hence, the assumption is that dealing with contemporary risks and threats present in cyberspace depends on

[1] Министерство за одбрана, Email: sofka_hadzijevska@hotmail.com
[2] АУЕ – ФОН, Email: todorovskan@yahoo.com
[3] Email: martin.simonovski@yahoo.com

a comprehensive and efficient national cybersecurity strategy that involves the involvement of all stakeholders with precisely defined activities and fields of action, and its alignment with strategies at the international level.

Keywords: *cybersecurity, risks, threats, critical infrastructure, strategy.*

Вовед

Денес, како што технологиите, услугите, податоците и луѓето комуницираат на сè посложени начини, потенцијалната опасност од сајбер закани се помести надвор од традиционалните мрежи и компјутерски системи. Сајбер нападите врз националните критични инфраструктури може да имаат катастрофални влијанија врз еден или повеќе сектори и да произведат одредени нарушувања што може да влијаат и врз повеќе потсектори. Решителните противници постојано наоѓаат иновативни методи за искористување на ранливостите, па за да се остане чекор понапред, потребно е брз, поедноставен начин за развој, тестирање и користење на најсовремените решенија за сајбер безбедност.

Дигиталните закани денес се постојан предизвик не само за националната безбедност, туку и за меѓународната безбедност во целина. Праксата покажува дека постои одредена асиметрија помеѓу зголемениот дијапазон на дигитални закани и националните можности за отпорност. Токму ова асиметрија го зголемува ризикот од нарушувања на критичната инфраструктура, а зголемените активности на криминалните организации во дигиталната сфера додаваат уште еден слој на неизвесност.

Заканите и ризиците добиваат нов облик, па оттука хибридните закани со право може да се констатира дека се еден од главните фактори за загрозување на безбедноста. Хибридните закани вклучуваат разновидни активности, првенствено сајбер напади, ширење дезинформации, акти на саботажа и сл. Нивната цел е да го дестабилизираат, дезорганизираат и да го ослабат безбедносниот систем на една држава, вклучувајќи го тука и уништувањето на критичната инфраструктура.

Бидејќи достапноста, интегритетот, доверливоста и отпорноста на критичните инфраструктури и одговорот на сајбер заканите

се појавија како национални приоритети за сите развиени земји, потребно е добро планирање, координација и спроведување на активности за одговор со цел да се минимизира заканата, но и последиците кои би настанале. Тоа подразбира изготвување и развивање на сеопфатен план за управување со сајбер кризи кој е предуслов за целокупното управување со кризи. Всушност, националниот план за управување со сајбер кризи треба да обезбеди формален, фокусиран и координиран пристап кон реагирањето на заканите и ризиците што ќе обезбеди ефикасно функционирање на т.н. сајбер кризен менаџмент.

Управувањето со сајбер кризите вклучува различни актери на регионално, национално и меѓународно ниво, а дејствувањето може да биде на техничко, оперативно и на стратешко ниво подобрувајќи ја соработката и координацијата меѓу сите релевантни засегнати страни.

1. Осврт на потребата од сајбер безбедност

Интензивниот и брз технолошки напредок, ја наметна потребата на државите да бидат во чекор со сајбер заканите за да можат да го одбранат својот сајбер простор. Како врвен приоритет на националните влади се истакнува потребата за изнаоѓање законски решенија и регулативи за справување со сајбер заканите, предвидување и спречување на нападите врз сајбер просторот, соработка со приватниот сектор и безбедносните експерти, обука на државните безбедносни кадри, изнаоѓање соодветен одговор на нападите и брзо враќање во функција на нападнатите системи и мрежи (Славевски, 2015: 7-9).

Сајбер нападите како глобална безбедносна закана предизвикуваат огромни импликации не само врз поединци или врз системите на една компанија, туку и врз комплетниот безбедносен систем на една држава, со можност за предизвикување кризи од пошироки размери. Посебен акцент се става врз најновите индустриски напади, кои се сметаат за најголеми сајбер закани и воедно претставуваат едни од најголемите глобални закани

Критичната инфраструктура како поим означува елемент, систем или дел од систем лоциран во одредена држава, чии основни функции и значење се поддршка на виталните општествени функции, здравјето, безбедноста, економската и социјалната

благосостојба, а чие нарушување или деструкција би имало огромни последици врз самата држава поради неможноста да се одржат тие функции (Бакрески и др., 2017:17).

Бидејќи инфраструктурните мрежи се меѓусебно зависни, односно заемно влијаат една на друга и имаат комплексни врски, нарушувањето на нивното функционирање може да предизвика огромни материјални и човечки загуби во општествата, па дури и да доведе до крах на системите.

Критичната информатичка инфраструктура е онаа што се базира на критичната инфраструктура поврзана со информатичката технологија. Нападите од неовластени лица на ваквата информатичка инфраструктура претставуваат сериозна закана за безбедноста на државата, поради што стабилната и безбедна критична информатичка инфраструктура треба да биде приоритет на секоја современа држава и нејзина основна стратешка цел.

Основен столб на сајбер безбедноста претставува, пред сè, безбедноста на комуникациите, која опфаќа мерки и контрола, преземени заради спречување неавторизиран пристап на лица до информациите што произлегуваат од комуникациите и да се обезбеди автентичност на таквите комуникации. Комуникациската безбедност вклучува криптозаштита, безбедност на трансмисијата, безбедност на емисија, безбедност на мрежите и физичка безбедност на материјалите за безбедност на комуникациите (Дончев, 2007:34).

Критичната инфраструктура како комплексна и меѓусебно структурно поврзана целина е од големо значење за непреченото функционирање на државата. Таа е јасна дијалектика и синергија што ги поврзува индустрискиот сектор, комуникациските системи, енергетскиот сектор и другите сектори, системи и мрежи што се од големо значење за државата бидејќи со неа се обезбедува потребната стабилност (Бакрески и др., 2017:9).

Оттука, секое нарушување или прекин на работата на одредени сектори или системи може да предизвика сериозни последици, во однос на загрозување на безбедноста на државата, националната економија, економскиот развој и просперитет, како и на стабилноста на енергетскиот сектор. Секое нарушување или прекинот на работата на само еден од наведените сектори може да предизвика сериозни последици врз другите критични сектори и на тој начин да се наруши хармонијата, а безбедноста на државата да биде доведена во прашање.

2. Сајбер безбедноста и меѓународната заедница

Сајбер заканите за критичната инфраструктура, која сè повеќе е подложена на софистицирани сајбер упади, претставуваат нови ризици за безбедноста на државата. Поради тоа, голем број држави изготвуваат стратегии за сајбер безбедност и ги приспособуваат казнено-правните регулативи за да останат во чекор со брзиот и интензивен развиток на информатичката технологија и придружните алатки, како и заради обезбедување соодветен степен на заштита од ваквите злоупотреби. Освен на национално ниво, и меѓународните организации, пред сè ООН, НАТО и ЕУ, активно ја следат оваа проблематика, при што преземаат соодветни активности за сузбивање на негативните предизвици.

Во 2010 година Генералното собрание на ООН донесе Резолуција за сајбер безбедност, која го нагласува сајбер криминалот како главен предизвик за безбедноста на национално и на глобално ниво и потребата од преземање заеднички напори за заштита на критичната информатичка инфраструктура (Бакревски и Милошевска, 2021:165-166).

Во Новиот стратегиски концепт на НАТО и Декларацијата донесена на Самитот на НАТО во Чикаго 2012 година е утврдено дека сајбер нападите се сè пософистицирани и затоа потребата од креирање ефективна сајбер-одбрана е една од најприоритетните задачи на НАТО. Изнаоѓањето ефективен одговор мора да се обезбеди со интензивна координација, со што ќе се придонесе за зајакнување на отпорноста на системот на одбрана. Комплексноста на сајбер заканите наметнува низа предизвици во делот на предвидување на капацитетите и начините за справување со нив, што во голема мера може да предизвикаат контрадикторни ситуации во однос на меѓународното право, како и дел од човековите права (http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en).

Во 2008 година во Талин, Естонија, е формиран НАТО - Центар за кооперативна сајбер одбрана, кој има статус на меѓународна воена организација со мисија за зголемување на способноста, соработката и размената на информации помеѓу НАТО, земјите-членки и земјите-партнери во областа на сајбер-одбрана, врз основа на образование, истражување и развој, научени лекции и консултации.

НАТО Центарот за кооперативна сајбер одбрана се стреми да биде главен извор на експертиза во областа на соработката на сајбер одбраната, со акумулирање, создавање и ширење знаења за сродни прашања во рамките на НАТО, земјите-членки и земјите-партнери. НАТО-Центарот се фокусира на подобрување на практичната соработка помеѓу земјите кои ги спонзорира, креирајќи мрежни одбранбени вежби во реално време и други слични симулации, овозможувајќи им на учесниците да воспостават национална координација и рамка на соработка за да ги практикуваат и да ги тестираат можностите што им се потребни за да одговорат на реалните сајбер напади (https://ccdcoe.org/).

Идејата за неопходноста од развој на сајбер безбедноста како нераскинлив дел од колективните безбедносни системи, продолжува и на наредните самити на НАТО, со посебен акцент на сајбер одбраната. Имено, нападите од сајбер-сферата станаа дел од задачата на колективната одбрана на НАТО и земјите-членки се обврзаа на сајбер-одбрана, односно да го развијат и зајакнат целосниот спектар на националните можности за компјутерска одбрана (Бакревски и Милошевска, 2021: 172).

Стратегијата за сајбер безбедност од 2013 година на Европската комисија и Високиот претставник за надворешни работи и безбедносна политика на ЕУ претставува прв сеопфатен документ на Европската Унија за оваа област (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013:2).

Стратегијата ги опфаќа внатрешниот пазар, правдата, внатрешните работи и сајбер простор, од аспект на надворешната политика. Стратегијата е проследена со законодавниот предлог да се зајакне безбедноста на информатичките системи на ЕУ, за што се претпоставува дека ќе го поттикне економскиот раст во однос на растот на довербата во купувањето на интернет.

Во Стратегијата за сајбер безбедност на ЕУ јасно е предвидена визијата на Европската Унија, т.е. „обезбедување силна и ефективна заштита и промоција на правата на граѓаните за да ја направи онлајн-средината на ЕУ најбезбедна во светски рамки“, за чие остварување е предвидено исполнување на пет стратегиски приоритети: постигнување сајбер отпорност, драстично намалување на сајбер криминалот, развој на сајбер безбедносна политика и способностите поврзани со Заедничката безбедносна и одбранбена политика, развој на индустриските и технолошки ресурси за

сајбер безбедност и воспоставување кохерентна меѓународна политика на сајбер простор на ЕУ и промовирање на основните вредности на ЕУ (Славевски, 2015:7-9).

Новата Стратегија за сајбер безбедност на ЕУ за дигиталната декада има за цел да обезбеди глобален и отворен интернет со силна заштита за справување со ризиците за безбедноста и за основните човекови права и слободи во Европа. Следејќи го напредокот постигнат во рамките на претходните стратегии, таа содржи конкретни предлози за распоредување на три главни инструменти - регулаторни, инвестициски и политички инструменти, за справување со три области на дејствување на ЕУ: отпорност, технолошки суверенитет и лидерство; градење оперативен капацитет за спречување, одвраќање и одговор; и унапредување на глобален и отворен сајбер-простор. ЕУ е посветена на поддршка на оваа стратегија преку значително ниво на инвестиции во дигиталната транзиција на ЕУ во следните седум години и на тој начин сајбер безбедноста мора да се интегрира во сите сфери на дигитализацијата, како дел од новите технолошки и индустриски политики и агендата за закрепнување (https://digital-strategy.ec.europa.eu/en/policies /cybersecurity-strategy).

На 6 јуни 2025 година, Советот на Европската Унија усвои ревидиран План за сајбер безбедност преку Препораката на Советот COM (2025). Оваа ажурирана рамка, позната како План за сајбер безбедност на ЕУ, опишува како ЕУ, нејзините земји – членки и назначените координативни тела ќе се подготват и заеднички ќе управуваат со големи сајбер инциденти. Ги заменува упатствата од 2017 година и означува значаен пресврт кон оперативно усогласување во услови на растечки сајбер закани што влијаат на критичната инфраструктура и прекуграничните системи (https://eur-lex.europa.eu/eli/C/2025/3445/oj).

3. Сајбер - безбедноста и Република Северна Македонија

Досега Република Северна Македонија не била изложена на посериозни сајбер напади, но како приоритет се наметнува потребата од преземање превентивни мерки за справување со ваков тип закани. Освен тоа, потребно е да се вршат континуирани анализи и истражувања на новите трендови во областа на сајбер безбедноста, а вработените во институциите од безбедносниот систем да ги следат светските текови. Информатиката и безбедноста се исклучително

флуидни и сеопфатни области кои бараат мултидисциплинарен пристап при нивно проучување, истражување на сите новитети во овие области, со крајна цел следење на инвентивните *modus operandi* на лицата што вршат криминални активности од оваа област.

Земајќи ги предвид заканите и ризиците за сајбер простор, неопходно е креирање на национална стратегија за сајбер безбедност за да се обезбеди соодветна заштита на сајбер просторот, за унапредување на неговата безбедност, како и заштита на критичната инфраструктура, заштита на податоците од државните институции и пред сè нивните класифицирани информации, податоците на бизнис-заедницата и на граѓаните воопшто.

Република Северна Македонија следејќи ги меѓународните трендови презема иницијатива за изработка на стратегија за сајбер безбедност, со цел унапредување на својата сајбер безбедност и спречување на ризиците и заканите за нејзиниот сајбер простор.

Врз основа на досегашните анализи, а во смисла на практичната потреба, донесена е Национална стратегија за сајбер безбедност 2018-2022, која Владата на Република Северна Македонија ја усвои на 107 седницата одржана на 11.12.2018 година.

Имајќи ја предвид посветеноста на РСМ во спроведувањето на идејата за целосна дигитална трансформација на државата, Владата на Република Северна Македонија ги донесе Стратегијата за сајбер безбедност 2025 - 2028 година и Националната развојна стратегија (НРС) за 2024-2044 година кои се меѓусебно тесно поврзани преку комплементарните цели за одржлив, безбеден и отпорен развој.

Двете стратегии ги делат заедничките принципи на инклузивност, одржливост, дигитална трансформација и отпорност на современите закани (https://mdt.gov.mk/mk-MK/regulativa/strategija-za-sajber-bezbednost).

Стратегијата за сајбер безбедност 2025 - 2028 на Република Северна Македонија е стратешки документ, чија цел е преку широк спектар на мерки и активности да обезбеди услови за координиран национален одговор на предизвиците во поглед на сајбер безбедноста, како и превенција од сајбер инциденти и напади преку изградба на отпорна дигитална инфраструктура и човечки капацитети.

Истовремено, со членството на Република Северна Македонија во НАТО, се наметна потребата од донесување на Стратегија

за сајбер одбрана, во согласност со условите од членот 3 од Северно-Атланскиот Договор според кој земјите треба да ги одржуваат и развиваат индивидуалните и колективните капацитети, со цел да се справат со предизвиците и заканите во сајбер просторот.

Националната стратегија за сајбер безбедност ја препознава сајбер одбраната како автономна и специфична гранка во поширокиот концепт на сајбер безбедноста. Исто така, согласно Законот за одбрана, сајбер одбраната се перципира како дел од одбраната на државата. Законот ја дефинира одбраната на државата како систем за одбрана на независноста и територијалниот интегритет, како и заштита на животите на граѓаните и нивниот имот од надворешен напад. Ова вклучува изградба на ефикасен систем на национална одбрана, подготовка и ангажирање на релевантни сили и средства и учество во колективниот одбранбен систем на НАТО (Стратегија за сајбер одбрана, 2020:1-2).

Conclusion

Potential threats can manifest themselves through a wide range of phenomena, such as the proliferation of weapons of mass destruction, international terrorism, unequal distribution of wealth, organized crime, while the process of globalization further increases the effect of current threats with direct consequences in terms of demand for energy resources, climate change, urbanization, unequal demographic trends and the resulting socio-economic consequences. All of these potential threats pose a security risk to critical infrastructures, which are susceptible to the effects of the attack.

With the development of society, threats and risks take on a new form, and unconventional threats are slowly coming to the forefront. Modern risks and threats are interconnected and cannot be considered separately. On the contrary, they multiply and reach enormous proportions, and most often receive the epithet of hybrid threats.

The definition of hybrid threats most often refers to military actions, but can also be applied to non-military actions that include techniques that combine both cyber and traditional aspects. That is why states are increasingly paying attention to the development of cybersecurity, and when it comes to the legal and political aspects of cybersecurity, a trend has been observed for an increasing number of countries to adopt their own national cybersecurity strategies. In this

way, legal regulation of the area of operation of critical information infrastructure is carried out, establishing cybersecurity as a priority for national security. In fact, as an imperative of modern society, finding new strategies and unique programs that will respond to security challenges, risks, and threats in a timely and efficient manner, and will enable users of information technology to live in a world that is constantly changing. There are different approaches to solving cybersecurity problems, but all agree and mostly emphasize the continuous education of information technology users, raising awareness of the need for protection, and building an information security culture.

In recent years, many countries have reformed or established cybersecurity institutions, including cyber incident response teams, cyber forensic capacities, and specialized departments within the security services.

When it comes to the Republic of North Macedonia, through the achievement of the strategic goals of the Cyber Security Strategy, the protection and promotion of national interests in and through cyberspace is enabled, and then greater economic growth and prosperity of citizens, to strengthen national capacities in the national security of the state in general, and efficient and effective management of critical infrastructure.

However, sovereign states often cannot independently protect critical infrastructure, so more intensive international cooperation is necessary, where the role of the UN, NATO and the European Union will come to the fore, to develop joint early warning systems and increase the interoperability of civilian and military capacities to protect the proper functioning of institutions and secure infrastructure, including energy resources. To this end, cooperation between NATO and the European Union should enable complementarity in the implementation of measures to improve the resilience of capacities in the long term. In the end, it can be concluded that cybersecurity is an important part not only of the national security of states, but also of collective security systems and international security. To this end, cybersecurity strategies adopted at the national and international levels provide not only the legal, but also the operational framework for achieving the set goals, which are to take effective measures for early intervention and dealing with modern risks and threats.

Рецензенти:
Проф. д-р Стефан Буџакоски
Проф. д-р Татијана Ашталкоска Балоска

Користена литература:

1. Бакрески, О., Милошевска, Т., и Алчески, Ѓ. (2017). *Заштита на критична инфраструктура.* Скопје: Комора на Република Македонија за приватно обезбедување;

2. Бакрески, О. и Милошевска, Т. (2021). *Безбедноста на информациите и критичната инфраструктура.* Скопје: Дирекција за безбедност на класифицирани информации;

3. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. (2013). Brussels: EUROPEAN COMMISSION;

4. Дончев, А. (2007). Современи безбедносни системи. Скопје: ФОН универзитет;

5. Стратегија за сајбер одбрана. (2020), Скопје: Министерство за одбрана на Република Северна Македонија;

6. Славевски, С. (2015). *Меѓународните организации и сајбер-безбедноста*. Скопје:Штит;

7. The EU's Cybersecurity Strategy for the Digital Decade. (2020). Brussels: EUROPEAN COMMISSION;

8. http://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en;

9. https://ccdcoe.org/;

10. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy;

11. https://eur-lex.europa.eu/eli/C/2025/3445/oj;

12. https://mdt.gov.mk/mk-MK/regulativa/strategija-za-sajber-bezbednost.