Vlada Crne Gore
Ministarstvo javne uprave,
digitalnog društva i medija

STRATEGIJA

SAJBER BEZBJEDNOSTI 2022-2026.

Decembar 2021.

Lista skraćenica

ANB	Agencija za nacionalnu bezbjednost
AP	Akcioni plan
CIRT.ME	Tim za odgovor na računarsko bezbjednosne incidente u sajber prostoru Crne Gore
DZTP	Direkcija za zaštitu tajnih podataka
EK	Evropska komisija
EU	Evropska unija
KI	Kritična infrastruktura
KII	Kritična informatička infrastruktura
MJUDDM	Ministarstvo javne uprave, digitalnog društva i medija
MO	Ministarstvo odbrane
MPNKS	Ministarstvo prosvjete, nauke, kulture i sporta
MUP	Ministarstvo unutrašnjih poslova
MVP	Ministarstvo vanjskih poslova
NAC	Sjevernoatlantski savjet
NATO	Organizacija Sjevernoatlantskog ugovora
OEBS	Organizacija za evropsku bezbjednost i saradnju
UN	Ujedinjene nacije
UP	Uprava policije

SADRŽAJ

**** Smatra se da se svi izrazi u ovom dokumentu koji su vezani za zanimanja, a upotrijebljeni su u muškom gramatičkom rodu odnose bez diskriminacije i na žene.***

I UVOD

Paralelno sa digitalnom transformacijom društva, kriza izazvana pandemijom koronavirusa dovela je do porasta sajber napada i njegove proliferacije. Ovo je dodatno potcrtalo važnost adekvatne zaštite kritične infrastrukture i preduzimanja odlučnih koraka na planu sajber bezbjednosti, odnosno snaženja kapaciteta za sajber odbranu i odgovor na sajber kriminal.

Novi izazovi zahtijevaju ažuriranje postojećih mehanizama za odgovor na iste, ali i implementaciju inovativnih odgovora, posebno na planu upravljanja kriznim situacijama, snaženja svijesti i edukacije o značaju pitanja sajber bezbjednosti, te zaštite privatnosti i ličnih podatka.

Istovremeno, pojavom hibridnih prijetnji koje se u velikoj mjeri izvršavaju u vidu različitih vrsta sajber napada koji za cilj, između ostalog, mogu imati ostvarivanje ekonomskog ili političkog uticaja, narušavanje imidža ili reputacije kompanije, institucija, pa i samih država, sajber bezbjednost se sve više posmatra u širem kontekstu. Ova činjenica ukazuje na potrebu sveobuhvatnog pristupa, odnosno potrebu saradnje i sa drugim zainteresovanim stranama.

Procjenjuje se da će svjetsku ekonomiju u 2021. godini sajber kriminal "koštati" oko 6 triliona američkih dolara, što je duplo više u poređenju sa 2015. godinom, uz očekivanje da "troškovi" rastu 15% na godišnjem nivou dostižući blizu 10.5 triliona američkih dolara do 2025. godine[1].

Dodatno, u skladu sa indeksom vizuelnog umrežavanja- Cisco® (*Visual Networking Index - VNI*), tokom 2022. godine kreiraće se više IP "saobraćaja" nego tokom prethodne 32 godine od kada internet postoji[2]. Ovako povećana umreženost sa sobom neminovno je donijela i brojne sigurnosne izazove.

Uzimajući u obzir globalne trendove i pokazatelje, nameće se nužnost rapidnog djelovanja, ne samo na nacionalnom, imajući u vidu transnacionalnu prirodu sajber prijetnji, već i na međunarodnom planu.

Tako je Evropska unija utvrdila Višegodišnji finansijski okvir za period 2021-2027. kojim će se tokom narednih godina osigurati najveći iznos sredstava do sada od skoro 2 milijarde eura za oporavak od pandemije COVID-19 i realizaciju prioriteta EU, gdje sajber bezbjednost predstavlja "kamen temeljac digitalne i povezane Evrope"[3].

---

[1] Procjene Cybersecurity Ventures, vodećeg svjetskog istraživača u oblasti globalne sajber ekonomije.
[2] Izvor: https://cybersecurityventures.com/cybersecurity-almanac-2019/
[3] Izvor: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade.

Razumijevajući izmijenjen ambijent u kojem se države suočavaju sa sajber napadima i prijetnjama, te potrebu unapređivanja strateških okvira za odgovor na iste, Evropska komisija je u decembru 2020. godine predstavila novu Strategiju sajber bezbjednosti koja akcenat stavlja na neophodnost saradnje i povezivanja partnera širom svijeta kako bi se obezbijedila stabilnost i sigurnost u sajber prostoru, uz poštovanje i zaštitu osnovnih prava građana u Evropi.

Da je pitanje sajber bezbjednosti i siguran sajber prostor visoko na međunarodnoj agendi govori i podatak da su šefovi država i vlada država članica Organizacije Sjevernoatlantskog ugovora (NATO) 2016. godine na Samitu u Varšavi prepoznali sajber prostor kao četvrti domen operacija u kojem se moraju braniti na efekasan način kako to čine u vazduhu, na zemlji i moru. Dodatno, saveznici su se iste godine obavezali kroz Obećanje za sajber odbranu (*Cyber Defence Pledge*) da će im nacionalni prioritet biti unapređenje sajber odbrane mreža i infrastrukture i snaženje sposobnosti da efikasno odgovore na sajber napade i prijetnje koji su sve češće dio hibridnog ratovanja.

Nadgrađujući započete procese, na Samitu u Briselu, juna 2021. godine, saveznice su podržale nužnost aktivnog učešća Alijanse u pravcu odvraćanja, odbrane i suprotstavljanja sajber prijetnjama bilo tokom perioda mira, krize ili konflikta, i to na političkom, vojnom i tehničkom nivou, uz poštovanje međunarodnog prava[4]. Naročito, potvrđeno je da će se odluke o tome kada sajber napad može predstavljati osnov za pozivanje na član 5 Sjevernoatlantskog ugovora donositi od strane Sjevernoatlantskog savjeta (NAC) od slučaja do slučaja[5].

Tako je i Crna Gora kao članica NATO-a, Ujedinjenih nacija (UN), Organizacije za evropsku bezbjednost i saradnju (OEBS), Savjeta Evrope, i kao zemlja kandidat za članstvo u Evropskoj uniji, prepoznajući trendove i ispunjavajući svoje međunarodne obaveze, prethodnih godina a) potpisala i ratifikovala značajan broj međunarodnih konvencija[6], b) preduzela brojne strateške aktivnosti na planu usklađivanja nacionalnog zakonodavstva kako bi isto bilo na liniji savremenih i međunarodnih

[4] Više na: https://www.nato.int/cps/en/natohq/topics_78170.htm
[5] Izvor: https://www.nato.int/cps/en/natohq/news_185000.htm
[6] Crna Gora je donijela Zakon o potvrđivanju Konvencije o računarskom kriminalu Savjeta Evrope (Budimpeštanska konvencija), istovremeno ratifikovala dodatni Protokol o rasizmu i ksenofobiji (CETS 189), kao i Konvenciju o zaštiti djece od seksualne eksploatacije i seksualnog zlostavljanja (CETS 201). Nakon ratifikacije Crna Gora je uskladila svoje krivično zakonodavstvo sa odredbama ovih Konvencija, kao i sa Okvirnom odlukom Savjeta 2005/222/ o napadima na informacione sisteme i Okvirnom odlukom Savjeta 32000D0375 o suzbijanju dječije pornografije na internetu.

rješenja koja tretiraju pitanje sajber bezbjednosti, i c) učinila značajne transformacione i operativne napore na nacionalnom nivou u borbi protiv sajber napada.

Međutim, iako je kroz strateški okvir u oblasti sajber bezbjednosti Crne Gore napravljen značajan iskorak na planu dostizanja standarda i zahtjeva definisanih, prije svega od strane NATO-a i EU, prostor za dalji rad i unapređenje na ovom polju postoji.

Kako se krajem 2021. godine završava vremenski okvir trajanja Strategije sajber bezbjednosti Crne Gore 2018-2021, preduzete su aktivnosti na planu analize zakonodavnog i organizacionog okvira i postojećih mehanizama, i kroz konsultovanje akademske zajednice, privrede, civilnog sektora i ostale zainteresovane javnosti, i uz podršku međunarodnih eksperata definisana je nova, sveobuhvatna Strategija za period 2022-2026. godine čija vizija, strateški i operativni ciljevi su predstavljeni u nastavku dokumenta.

II METODOLOGIJA IZRADE STRATEGIJE

Strategija sajber bezbjednosti Crne Gore 2022-2026. godine (u daljem tekstu: Strategija) predstavlja interresorni dokument koji se odnosi na petogodišnji strateški period i usmjeren je na unapređenje ukupnih kapaciteta (zakonodavnih, operativnih, ljudskih, finansijskih i tehničkih) za adekvatan odgovor na izazove i prijetnje koje dolaze iz sajber prostora u/i izvan Crne Gore.

Prilikom izrade Strategije poštovani su kriterijumi strateškog planiranja definisani Uredbom o načinu i postupku izrade, usklađivanja i praćenja sprovođenja strateških dokumenata[7], kao i smjernice iz Metodologije razvijanja politika, izrade i praćenja sprovođenja strateških dokumenata[8].

Strategijom su utvrđeni strateški ciljevi, kao i operativni ciljevi za njihovo ostvarivanje.

Poštujući ***princip usklađenosti***, Strategija je pripremljena na liniji prioriteta i ciljeva krovnih strateških dokumenata Crne Gore koji tretiraju pitanja nacionalne bezbjednosti, odbrane i digitalizacije, a na liniji je i Programa rada Vlade za 2021. godinu.

Kao važan input pri izradi Strategije poslužile su sugestije i mišljenja zainteresovane javnosti prikupljeni tokom trajanja Javnog poziva organima, organizacijama, udruženjima i pojedincima da se uključe u početnu fazu pripreme Strategije, tokom aprila i maja 2021. godine, kada su organizovani i sastanci sa predstavnicima privrede, akademske zajednice, civilnog sektora i međunarodnih organizacija u Crnoj Gori[9].

Svi ključni rezultati proizašli iz dijaloga sa institucijama i zainteresovanom javnošću korišćeni su u kreiranju Strategije.

Nacrt Strategije prezentovan je javnosti u okviru procesa javne rasprave[10], kao i međunarodnim strateškim partnerima koji pružaju ekspertsku, tehničku i finansijsku podršku razvoju sajber bezbjednosti, čime je ispoštovan i ***princip transparentnosti***.

[7] Više na: https://www.gov.me/dokumenta/23c216b2-3eb7-453c-b0a7-3cdae9e9742e
[8] Više na: https://javnepolitike.me/wp-content/uploads/2020/11/Metodologija-razvijanja-politika-draft3-preview-22SEP20.pdf
[9] Više na: https://www.gov.me/clanak/javni-poziv-na-konsultacije-zainteresovane-javnosti-povodom-izrade-strategije-sajber-bezbjednosti-crne-gore-2022-2026 i https://www.gov.me/clanak/strategija-digitalne-transformacije-po-ugledu-na-najbolje-svjetske-prakse-nacrt-zakona-elektronski-dokument-izjednacen-sa-papirnim
[10] Javna rasprava organizovana je u periodu 11. oktobra – 15. novembra 2021. godine. Izvještaj o sprovedenoj javnoj raspravi dostupan je na linku: http://eusluge.euprava.me/eParticipacija/Docs/?Id=595

2.1. Pozicioniranje u strateškom okviru Crne Gore

Programom rada Vlade za 2021. godinu[11] kao peti ključni prioritet prepoznata je digitalna transformacija i u okviru nje aktivnosti na podizanju nivoa informacione bezbjednosti.

Strategija nacionalne bezbjednosti Crne Gore[12] kao strategijske nacionalne interese Crne Gore prepoznaje kontinuirano unapređenje sistema sajber odbrane, bezbjednosti i sigurnosti. Ostvarivanje strategijskih interesa Crne Gore doprinosi zaštiti vitalnih interesa, društvenom razvoju i ukupnom prosperitetu. Ostali važni interesi Crne Gore, čije promovisanje doprinosi zaštiti vitalnih i strategijskih interesa i jača otpornost društva na bezbjednosne izazove, rizike i prijetnje, podrazumljevaju, između ostalog - smanjenje stope kriminala sa težištem na visoko-tehnološkom i drugim vidovima organizovanog kriminala, kao i zaštitu kritičnih infrastruktura kroz podsticanje saradnje državnih institucija, civilnog i privatnog sektora, u cilju jačanja civilne spremnosti za odgovore na bezbjednosne izazove, rizike i prijetnje. Takođe, Strategija je kao bezbjednosnu prijetnju prepoznala i sajber i hirbridne prijetnje.

Strategija odbrane Crne Gore[13] dugoročno uređuje i usmjerava razvoj normativnih, doktrinarnih i organizacijskih rješenja u sistemu odbrane, kao i angažovanje i viziju razvoja odbrambenih resursa u odgovoru na savremene bezbjednosne izazove, rizike i prijetnje. Strategijom je definisan strateški cilj 1: Zaštita suvereniteta, teritorijalnog integriteta i nezavisnosti Crne Gore i operativni cilj 3 Unapređenje sistema sajber odbrane, bezbjednosti i sigurnosti, na koje se naslanja Strategija sajber bezbjednosti 2022-2026.

Pravci razvoja Crne Gore 2018-2021. godine[14] kroz oblast informaciono – komunikacione tehnologije **notiraju potrebu izrade propisa za zaštitu kritične informatičke infrastrukture.**

Nacrtom Strategije digitalne transformacije Crne Gore 2022-2026. kroz strateški cilj 1 planirano unaprjeđenje kapaciteta i sposobnosti za digitalnu transformaciju Crne Gor, a pratećim operativnim ciljem 3 - povećana pokrivenost i modernizacija

[11] Više na: https://www.gov.me/clanak/program-rada-vlade-crne-gore
[12] Više na: https://zakoni.skupstina.me/zakoni/web/dokumenta/zakoni-i-drugi-akti/522/1814-11450-00-38-18-1-4.pdf
[13] Više na: https://www.gov.me/dokumenta/08cb12b5-395e-4047-a1cd-ff884683b9e3
[14] Više na: https://www.gov.me/dokumenta/1a5fab12-ec7a-4f28-b1e9-83c9d0dadb79

elektronske komunikacione infrastrukture gdje će se razvoj IKT infrastrukture fokusirati na dostupnost, bezbjednost (sajber-bezbjednost) i redundantnost.

Nacrtom Strategije za digitalizaciju obrazovnog sistema 2022 - 2027. godine[15] definisan je razvoj i unapređenje digitalnih vještina i kompentencija kao strateški cilj 3, u okviru kojeg prepoznala operativni cilj 3 - Unapređenje bezbjednog korišćenja tehnologije u sistemu obrazovanja, dok je **pitanje edukacije i širenja svijesti o sajber bezbjednosti u javnom i privatnom sektoru obuhvaćeno Strategijom sajber bezbjednosti Crne Gore 2022-2026.**

2.2. Usklađenost sa EU strateškim okvirom

Prilikom izrade Nacrta Strategije sajber bezbjednosti Crne Gore 2022-2026. razmotren je strateški okvir Evropske unije koji tretira pitanje sajber bezbjednosti, kako bi pri formulisanju strateških ciljeva i daljih aktivnosti bili na liniji dugoročnih pravaca razvoja u ovoj oblasti.

Analizirana je implementacija odredbi **Direktive o mrežnoj i informacionoj bezbjednosti EU** (Network and Information Security Directive - NIS Direktiva)[16], koja predstavlja prvi pravni akt EU o sajber bezbjednosti koji je pružio pravne mjere za unapređenje ukupne sajber sigurnosti na nivou Evropske unije, sa fokusom na zaštiti kritične infrastrukture. Iako Crna Gora nije članica Evropske unije, odnosno ne postoji obaveza implementacije NIS Direktive, u prethodnom periodu smo prateći zahtjeve, odredili nadležni organ za informacionu bezbjednost, upostavili Nacionalni CIRT i jedinstvenu kontakt tačku za razmjenu informacija, donijeli Zakon o informacionoj bezbjednosti i Zakon o utvrđivanju i zaštiti kritične infrastrukture, kao i kreirali dvije strategije sajber bezbjednosti**, dok i novi strateški dokument o sajber bezbjednosti prati postavljeni pravni okvir u adresiranju mjera zaštite kritične informatičke infrastrukture.**

Uzeta je u obzir i nova **Strategija sajber bezbjednosti Evropske unije** 2020-2025 za digitalnu deceniju[17] predstavljena krajem 2020. godine, kojom su postaljeni prioriteti u pravcu izgradnje evropske otpornosti, autonomije, liderstva i operativnih kapaciteta u suočavanju sa kompleksnim prijetnjama po mrežne, informacione sisteme, kao i

[15] Više na: https://www.gov.me/clanak/program-javne-rasprave-o-nacrtu-strategije-za-digitalizaciju-obrazovnog-sistema-za-period-2022-2027-godine
[16] NIS Direktiva, jul 2016: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148
[17] Više na: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

unapređenja globalnog i otvorenog sajber prostora i međunarodne saradnje[18]. Strategijom se predlaže revizija NIS Direktive, odnosno donošenje **NIS 2 Direktive** i nove **Direktive o otpornosti kritičnih entiteta**, što je na liniji i prioriteta Evropske komisije da učini Evropu spremnom za digitalno doba.

Da bi Strategija bila usklađena sa pravnom tekovinom EU, njena izrada je planirana **Programom pristupanja Crne Gore Evropskoj uniji 2021-2023.[19]** koja predstavlja strateški dokument koji se prilagođava promjenama u okviru procesa revizije i razvoja pravne tekovine Evropske unije.

U okviru pregovaračkog procesa, 2013. godine Crna Gora je otvorila **PP24: Pravda, sloboda i bezbjednost**, a 2014. godine **PP 10: Informatičko društvo i mediji**.

U godišnjem **Izvještaju Evropske komisije za Crnu Goru 2021[20]**, u odnosu na PP24 konstatovano je da "*kapacitet Crne Gore u oblasti sajber-kriminala progresivno raste, ali i dalje nije dovoljno robustan da se suoči sa globalnim opasnostima u ovoj oblasti. Broj istraga slučajeva sajberkriminala porastao je sa četiri koliko ih je bilo 2019. godine na 19 tokom 2020. godine (protiv 22 fizička i jednog pravnog lica). Sudovi su 2020. godine imali u radu četiri predmeta sajberkriminala. Izrečene su dvije prvostepene osuđujuće presude, uključujući jednu sa zatvorskom kaznom. Nadležna policijska jedinica sada ima pet mjesta. Promjene u unutrašnjoj organizaciji policije omogućavaju sada zapošljavanje kadra koji nije iz policije na visoko-specijalizovanim funkcijama, kao što su stručnjaci za informacione tehnologije (IT).*" Istovremeno, u odnosu na PP10 notiran je pozitivan trend kada su u pitanju zakonodavne izmjene u dijelu informacione bezbjednosti[21].

Oslanjajući se na iznijete ocjene, **Strategija sajber bezbjednosti je kroz strateški, odnosno operativne ciljeve prepoznala dalje korake koje potrebno preduzeti na planu borbe protiv sajber kriminala.**

[18] Više na: https://digital-strategy.ec.europa.eu/en/library/first-implementation-report-eu-cybersecurity-strategy
[19] Više na: https://www.gov.me/en/documents/75fd43fa-de2e-4e70-9a1f-08e6fa224235
[20] Više na: http://www.euic.me/wp-content/uploads/2021/12/Prevod-Izvjestaja-za-Crnu-Goru-za-2021-godinu.pdf
[21] Više na: https://www.gov.me/dokumenta/b5f98cf5-f6a6-476b-9216-3133e67a8886

III ANALIZA STANJA

Očekujući da napadi na sajber prostor Crne Gore s godinama eksponencijalno rastu, postaju kompleksniji i s većim posljedicama po infrastrukturu, funkcionisanje javne uprave, naročito u dekadi digitalizacije društva, i građane - korisnike informaciono-komunikacionih tehnologija i e-servisa, kontinuirano su razvijani kapaciteti sajber odbrane, a strateški i zakonodavni okvir unapređivan. Pojava hibridnih prijetnji, koje sve više zamijenjuju konvencionalne metode ratovanja, sajber prostor postaje još više značajan, odnosno pogodan za kanalisanje široke lepeze hidbridnog ratovanja.

Drugim riječima, neminovna digitalizacija društva otvara vrata zlonamjernim akterima, koji u kontinuitetu pokušavaju da izvrše maliciozne sajber napade, radi ostvarenja različitih ciljeva.

U prethodnom periodu u Crnoj Gori je donijeto više zakona i podzakonskih akata koji su uspostavili mehanizme i postavili temelje za bezbjedniji sajber ambijent i zaštitu kritične infrastrukture[22].

Definisana je organizaciona struktura u oblasti sajber bezbjednosti, donijeta Strategija nacionalne bezbjednosti, Strategija odbrane Crne Gore, dvije Strategije o sajber bezbjednosti za periode 2013-2017. i 2018-2021. godine, Strategija sajber bezbjednosti Vojske Crne Gore 2019-2022, formiran nacionalni Tim za odgovor na računarsko bezbjednosne incidente u sajber prostoru Crne Gore (CIRT.ME) koji je postao član FIRST-a (*Forum of Incident Response and Security Teams*), uspostavljena organizaciona jedinica Ministarstva odbrane za sajber odbranu i odgovor na kompjuterske incidente, uspostavljena mreža CIRT-ova na nacionalnom i lokalnom nivou, unaprijeđeni kapaciteti sajber bezbjednosti u Agenciji za nacionalnu bezbjednost, kako u organizacionom tako i tehnološkom pogledu, reorganizovana i opremljena jedinica Uprave policije za borbu protiv visoko-tehnološkog kriminala, i obrazovan Savjet za informacionu bezbjednost.

[22] Usvojeni su, između ostalog, sledeći zakoni i podzakonski akti: Zakon o potvrđivanju Konvencije o računarskom kriminalu, Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o računskom kriminalu, Krivični zakonik, Zakon o krivičnom postupku, Zakon o informacionoj bezbjednosti, Zakon o Agenciji za nacionalnu bezbjednost, Zakon o određivanju i zaštiti kritične infrastrukture, Zakon o tajnosti podataka, Zakon o zaštiti podataka o ličnosti, Zakon o elektronskim komunikacijama, Zakon o elektronskoj trgovini, Zakon o elektronskom potpisu, Strategija sajber bezbjednosti Crne Gore 2013-2017, Strategija sajber bezbjednosti Crne Gore 2018-2021, Uredba o mjerama informacione bezbjednosti, Pravilnik o standardima informacione bezbjednosti, i sl.

Paralelno sa razvijanjem informacionih tehnologija i porastom njihove primjene, povećavao se i dijapazon prijetnji po sajber prostor, odnosno kritičnu infrastrukturu, nacionalne institucije, ekonomiju i građane.

Tako je u Crnoj Gori prepoznata tendencija rasta ICT sektora i oslanjanja javne uprave, preduzeća i građana na internet i informaciono-komunikacione tehnologije u cilju pružanja e-usluga, unapređenja procesa rada, otvaranja novih radnih mjesta i/ili ostvarivanja prihoda. U januaru 2021. godine, prema dostupnim podacima, u Crnoj Gori je bilo 477.300 internet korisnika, što je povećanje od 2.7%, odnosno 13.000, u periodu između 2020. i 2021. godine[23].

Prema izvještajima Uprave za statistiku – Monstata o upotrebi informaciono-komunikacionih tehnologija u preduzećima i domaćinstvima za 2020. godinu[24], utvrđeno je da u Crnoj Gori 98,8% anketiranih preduzeća koristi računare u svom poslovanju, od kojih 99,5% ima pristup internetu. Kada je riječ o internetu, anketa je pokazala da oko 84,5% preduzeća ima svoju veb prezentaciju, što je 4,5% više nego 2018. godine kada je donijeta druga Strategija sajber bezbjednosti 2018-2021. Takođe, da 80,3% anketiranih domaćinstava ima pristup internetu kod kuće, što je porast od 8,1% u odnosu na 2018. godinu, dok procenat onih koji su kupovali ili naručivali robu ili usluge iznosi 40,9%, što je za 13,9% više nego 2018. godine.

Istovremeno, sa prednostima koje je proces digitalizacije i oslanjanje na informaciono-komunikacionu infrastrukturu donijelo, protokom vremena indentifikovane su i prijetnje koje su do izražaja naročito došle sa pandemijom koronavirusa koja je zahvatila čitav svijet tokom 2020. godine. Prijetnje po dostupnost i integritet informaciono-komunikacione infrastrukture, privatnost i povjerljivost ličnih podataka uticale su na način posmatranja značaja sajber bezbjednosti, kao i sigurnosti sajber prostora i kritične infrastrukture i podstakle na analizu izmijenjenog ambijenta u kojem djeluje postojeći strateški i organizacioni okvir sajber bezbjednosti Crne Gore.

Posmatrajući dosadašnja dostignuća Crne Gore u domenu sajber bezbjednosti, prateći aktuelne trendove, identifikovani su određeni izazovi i nedvosmisleno utvrđeno da je ubrzan i sveobuhvatan razvoj sajber kapaciteta više nego neophodan. Ova Strategija će definisati smjernice daljeg razvoja, uzimajući u obzir sve aspekte: poziciju Crne Gore na međunarodnom planu, broj stanovnika, javni i privatni sektor i nivo ambicija koje želimo da dostignemo u sajber prostoru.

---

[23] Izvor: https://datareportal.com/reports/digital-2021-montenegro

[24] Više na: http://monstat.org/cg/page.php?id=459&pageid=457

***

Analiza postojećeg učinka u izgradnji sistema sajber bezbjednosti Crne Gore postavila je smjernice za pripremu strateških i operativnih ciljeva za Strategiju sajber bezbjednosti Crne Gore 2022-2026.

Osnovu za analizu stanja činili su:

- aktuelni međunarodni, evropski i nacionalni zakonodavni okvir u ovoj oblasti[25];
- analiza učinka prethodne strategije sajber bezbjedosti Crne Gore[26],
- konsultacije sa zainteresovanom javnošću,preporuke dobijene od eksperata Savjeta Evrope i Svjetske banke, kao i međunarodnih partnera,
- swot analiza.

Kroz dokument je predstavljen sveobuhvatan pregled trenutne situacije u oblasti sajber bezbjednosti, kao i glavni izazovi kojima će se baviti Strategija u narednom petogodišnjem periodu.

Analiza učinka prethodne Strategije

Nakon isteka četvorogodišnjeg perioda važenja Strategije sajber bezbjednosti 2018-2021, Završni izvještaj pokazao je da kada je riječ o edukaciji i regionalnoj i međunarodnoj saradnji, može se zaključiti da su strateški ciljevi ostvareni, ili uglavnom ostvareni. Svakako, to ne znači nužno da ove ciljeve ne treba dodatno nadgraditi i stepen njihove ostvarenosti povećati u okviru novog strateškog dokumenta. Na ovaj način se najefikasnije i dugoročno održivo obezbjeđuje adekvatno upravljanje sajber bezbjednošću u Crnoj Gori.

Na polju snaženja kapaciteta za sajber odbranu i partnerstva javnog i privatnog sektora, te zaštite podataka i jačanja međuinstitucionalne saradnje, dok je primjetan pozitivan trend, planiranje novih operativnih ciljeva i indikatora učinka ostaju preduslov kontinuiranog napretka u ovim oblastima.

Zaštita kritične informatičke infrastrukture i centralizacija sajber ekspertize i resursa notirane su kao oblasti u kojima nije ostvaren zadovoljavajući napredak u poređenju sa početnim vrijednostima iz 2018. godine, pa je u novom strateškom dokumentu potrebno posebnu pažnju posvetiti ovim strateškim ciljevima.

[25] Više na str. 8-10.
[26] Strategija sajber bezbjednosti 2018-2021: https://wapi.gov.me/download-preview/fa24a8c6-2241-4d6f-9297-328636b157e5?version=1.0

Naime, kada je u pitanju cjelokupni efekat tokom četiri godine, odnosno indikatori učinka, zabilježen je napredak kod njih 17 ili 61% (od ukupno 28 indikatora), dok 11 indikatora učinka nije ispunjeno.

Ključni izazovi

Proglašenje pandemije COVID19 u 2020. godini, koje uslovilo drugačiju prioritizaciju politika i pomjeranje fokusa na ulaganje u zdravstveni sistem i ekonomski oporavak, kao i kašnjenje sa usvajanjem Budžeta za 2021. godinu, koji postao operativan sredinom godine, usporilo je dinamiku ostvarenja postavljenih strateških ciljeva u drugoj polovini sprovođenja Strategije.

Nedovoljna sredstva opredijeljena u poslednje dvije godine realizacije Strategije, nisu omogućila nastavak trenda povećanja ulaganja u ljudske resurse i tehničke kapacitete.

Poseban izazov je nastao kada je CIRT iz Ministarstva javne uprave, krajem 2020. godine prešao u sastav Direkcije za zaštitu tajnih podataka, što se negativno odrazilo na njegovu funkcionalnost usled nedostatnih prostornih, tehničkih i kadrovskih kapaciteta, kao i realizaciju planiranih aktivnosti na snaženju kapaciteta za prevenciju i suzbijanje svih vrsta sajber napada u Crnoj Gori.

3.1. SWOT analiza

Snage

- članstvo u NATO, OEBS, UN, Sajvetu Evrope,
- iskustvo iz pregovaračkog procesa sa EU,
- finansijska i ekspertska podrška međunarodnih partnera,
- dobra komunikacija sa zainteresovanim stranama,
- relativno jeftina i kvalitetna radna snaga,
- dobra telekomunikaciona infrastruktura,
- postojanje zadovoljavajućeg pravnog i institucionalnog okvira.

Slabosti

- ne postoji posebna budžetska stavka za sprovođenje Strategije,
- nedostatak resursa (ljudskih, finansijskih, tehničkih),
- nedovoljna prepoznatljivost i razumijevanje značaja sajber bezbjednosti,
- učestale strukturne i kadrovske promjene na ekspertskom nivou,
- neusklađenost tržišta rada i tržišta obrazovanja,

Mogućnosti

- mogućnost pristupa međunarodnim fondovima,
- regulisan pravni i institucionalni okvir,
- usaglašavanje sa zahtjevima međunarodnih standarda u oblasti sajber bezbjednosti,
- efikasno korišćenje javno-privatnih partnerstava,
- bolja koordinacija sa privatnim sektorom i akademskom zajednicom.

Prijetnje

- nedovoljan priliv budžetskih sredstava,
- neharmonizovan pravni okvir,
- limitirana sredstva za ulaganje u infrastrukturu i tehnologiju,
- nedovoljna ulaganja u edukaciju i trening zaposlenih,
- slabi administrativni kapaciteti,
- odliv visoko kvalifikovanih ljudskih resursa.

Uočeni problemi

a) U Završnom izvještaju o sprovođenju prethodne Strategije sajber bezbjednosti kao glavni uzrok neispunjenja strateških ciljeva na zadovoljavajući način, prepoznat je finansijski faktor, kao i nedovoljno razvijena svijest o značaju ulaganja u sajber bezbjednost na najvišim upravljačkim nivoima.

Na problem odgovoriće se kroz sledeći operativni cilj, kao i realizaciju aktivnosti navedenih u pratećem Akcionom planu za implementaciju Strategije:

Operativni cilj 1: Unapređenje ljudskih i finansijskih resursa.

b) U eri eksponencijanog rasta informacionih tehnologija na kojima se sve više oslanjaju krucijalni društveno ekonomski procesi svjedoci smo srazmjernog porasta sajber prijetnji i sofisticiranih vektora napada. U proteklom periodu pokazalo se da sajber napad čak i na najrazvijenije države u oblasti sajber bezbjednosti može uspješno da paralizuje esencijalne društvene funkcije. Tako na primjer napad kriptovirusom na zdravstveni sistem Velike Britanije 2017. godine za posledicu je imao otkazivanje operacija, pregleda pacijenata, kao i nedostupnost informacija, te prouzrokovao direktnu finansijsku štetu od preko 19 miliona eura tokom trajanja

napada, kao i finansijski trošak za oporavak sistema nakon napada od preko 73 miliona eura[27].

Crna Gora u proteklom periodu nije detektovala sajber napade koji za posledicu imaju prekide esencijalnih društveno ekonomskih procesa međutim usled transcedentalne prirode informacionih tehnologija svjesni smo postojanja velikog broja sofisticiranih sajber prijetnji kako u globalnom sajber prostoru, tako i u sajber prostoru Crne Gore. Prepoznato je da Crna Gora ne posjeduje adekvatne mehanizme za detektovanje sajber prijetnji, kao ni mehanizme za dovoljno brz odgovor, odnosno oporavak od sajber napada. Dodatno, nedostatak eksperata iz oblasti sajber bezbjednosti je prepoznat kao globalan problem, dok je u Crnoj Gori zbog ograničenih ljudskih resursa ovaj problem još izraženiji.

c) Sajber špijunaža je globalno prepoznat problem gdje se procjenjuje da je kompanijama/organizacijama koje imaju razvijene sajber sposobnosti neophodno u prosjeku više od 6 mjeseci za detektovanje malicioznih virusa specijalno dizajniranih u svrhe sajber šijunaže, dok kompanije/organizacije koje nemaju visok nivo sajber bezbjednosnih kapaciteta nijesu u stanju da detektuju postovanje ovih vrsta malicioznih virusa. Pretostavka je da se javna uprava Crne Gore takođe suočava sa ovom vrstom problema usled relativno limitiranih kapaciteta za sajber bezbjednost.

Na probleme pod b) i c) odgovoriće se kroz sledeće operativne ciljeve, kao i realizaciju aktivnosti navedenih u pratećem Akcionom planu za implementaciju Strategije:

Operativni cilj 2: Unapređenje mehanizama za odgovor na sajber incidente, i
Operativni cilj 7: Uspostavljen sistem zaštite kritične informatičke infrastrukture

d) Globalno poznata činjenica jeste da se u okviru generalne populacije osnovnom sajber bezbjednosnom higijenom i dobrom praksom sprječava 85% sajber napada. Na primjer, osobe koje koriste dvostruku autentifikaciju na mobilnim uređajima i/ili pri korišćenju online usluga imaju 10 puta manju šansu da budu kompromitovane iz prostog razloga što u cilju kompromitacije kod dvostruke autentifikacije potrebno je uložiti mnogo više napora, dok već postoji veliki broj korisnika koji ne koriste dvostruku autentifikaciju. U cilju dostizanja adekvatnog nivoa osnovne sajber bezbjednosne higijene neophodna je kontinuirana edukacija na svim nivoima društva. Analizom incidenata prijavljenih Nacionalnom CIRT-u primjetan je trend porasta sajber

[27] Više na: https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update

incidenata, od kojih je određen broj sasvim izvijesno mogao biti spriječen primjenom osnovne sajber higijene.

Na problem odgovoriće se kroz sledeći operativni cilj, kao i realizaciju aktivnosti navedenih u pratećem Akcionom planu za implementaciju Strategije:

Operativni cilj 3: Unapređenje mjera prevencije i edukacije o sajber bezbjednosti.

e) Na polju borbe protiv sajber kriminala primijećeni su problemi koji otežavaju krivično procesuiranje počinilaca sajber kriminala. U pojedinim situacijama praktično je nemoguće utvrditi odakle dolazi napad i ko stoji iza njega, ip adrese preko kojih se pokušava utvrditi lokacija mogu veoma lako da se fabrikuju, odgovor nadležnih organa drugih država može biti negativan u dijelu bilateralne/međunarodne saradnje u dijelu razmjene informacija. Crna Gora nema tehničku mogućnost, kao ni legislativni okvir za blokiranje sadržaja sa interneta, a koji mogu biti nedvosmisleno u okviru krivične sfere npr. dječija pornografija, govor mržnje, ucjenjivanje putem društvenih mreža, video materijali i drugo.

Na problem odgovoriće se kroz sledeći operativni cilj, kao i realizaciju aktivnosti navedenih u pratećem Akcionom planu za implementaciju Strategije:

Operativni cilj 4: Unapređenje odgovora na sajber kriminal

f) Analizom sprovođenja prethodne strategije je utvrđeno da nije ispunjena aktivnost koja se odnosi na implementaciju međunarodnih standarda za sajber bezbjednost što bi u značajnoj mjeri povećalo otpornost sistema na sajber napade i prijetnje. Takođe prepoznato je da Crna Gora svoje zakonodavstvo nije uskladila sa Opštom uredbom o zaštiti ličnih podataka – GDPR 2016/679 zbog čega se ne može smatrati da je omogućen nivo zaštite ličnih podataka i ostvarivanje prava na privatnost na način koji imaju građani Evropske unije.

Na problem odgovoriće se kroz sledeći operativni cilj, kao i realizaciju aktivnosti navedenih u pratećem Akcionom planu za implementaciju Strategije:

Operativni cilj 5: Osnažen i harmonizovan sistem zaštite podataka.

g) Globalno je prepoznat trend porasta aktivnosti na tzv. crnim tržištima gdje sajber kriminalci, hakeri, teroristi, kao i drugi maliciozni akteri na veoma efikasan način razmjenjuju informacije što im daje prednost u odnosu na legitimne entitete. Prepoznat je problem da ogranizacije veoma često imaju tendenciju da ne dijele informacije o sajber napadima na njihove sisteme i otkrivenim ranjivostima, na primjer usled rizika

od gubitka kredibiliteta, a samim tim i mogućih finansijskih gubitaka (što čest slučaj u bankarskom sektoru). Način za prevazilaženje ovog problema jeste jačanjem i izgradnjom međusobnog povjerenja. Ukoliko javna uprava se prepoznaje kao kredibilan partner, privatne i druge organizacije će uvidjeti benifite razmjene informacija koji prevazilaze pomenute rizike, i biti otvorenije za saradnju u ovoj oblasti ukoliko se obezbjedi obostrana razmjena informacija o sajber prijetnjama, ranjivostima, kao i dobrim praksama sajber zaštite. Na ovaj način stvoriće se dinamičan nacionalni okvir sajber zaštite.

Na problem odgovoriće se kroz sledeće operativne ciljeve, kao i realizaciju aktivnosti navedenih u pratećem Akcionom planu za implementaciju Strategije:

Operativni cilj 6: Razvoj i unapređenje saradnje s nacionalnim i međunarodnim partnerima.

IV VIZIJA, STRATEŠKI I OPERATIVNI CILJEVI, SA INDIKATORIMA

Strategija sajber bezbjednosti Crne Gore za period 2022-2026. naslanja se u značajnoj mjeri na politiku i viziju definisanu prethodnim strategijama.

Vizija:

- Građani, operatori kritičnih infrastruktura, privreda i javna uprava u Crnoj Gori zaštićeni u najvećoj mogućoj mjeri od negativnih aspekata sajber prijetnji i kriminala kroz kontinuiranu edukaciju o sigurnom korišćenju informaciono-komunikacionih tehnologija u svakodnevnom životu i poslovanju, „know-how“ razmjenu sa partnerima na nacionalnom, regionalnom i međunarodnom planu i implementaciju mjera zaštite kritične informatičke infrastrukture.
- Crna Gora ulaže u razvoj organizacionih, tehničkih i ljudskih kapaciteta, izgrađuje zakonodavni okvir u skladu sa međunarodnim standardima i postupa kao odgovoran partner na regionalnom i međunarodnom planu u oblasti sajber bezbjednosti.

Za ostvarivanje vizije, utvrđen je jedan strateški cilj i sedam operativnih ciljeva. Kao takvi, predstavljaju namjeru da se uočeni izazovi i problemi adresiraju i prevaziđu, te da se na izmijenjen sajber prostor i dijapazon sajber prijetnji po nacionalnu bezbjednost da rapidan i adekvatan odgovor.

STRATEŠKI CILJ 1:

Crna Gora u oblasti sajber bezbjednosti posjeduje održiv sistem za efikasno otkrivanje i odbranu od kompleksnih vektora sajber napada i prijetnji.

U eri digitalizacije koja sa sobom donosi brojne ekonomske i društvene benefite, drugu stranu „medalje“ predstavljaju sajber rizici. Stoga, osiguranje sajber prostora kroz aktivnosti usmjerene ka izgradnji kapaciteta za sajber odbranu postaje *conditio sine qua non* uspješnog procesa digitalizacije.

Operativni ciljevi, sa pratećim indikatorima:

Svi faktori uspješnosti razvoja sistema sajber bezbjednosti Crne Gore su adresirani sa 7 operativnih ciljeva i to:

Operativni cilj 1: Unapređenje ljudskih i finansijskih resursa

Kako bi se obezbjedio efiksan i funkcionalan mehanizam u oblasti sajber bezbjednosti koji će omogućiti otkrivanje i odbranu o sajber prijetnji i napada, neophodno je da postoji razvijena svijest na najvišem upravljačkom nivou u javnoj o značaju održivog alociranja potrebnih sredstava za snaženje operativnih, ljudskih i tehničkih resursa nadležnih resora za sajber bezbjednost.

Operativni cilj 1	**Unapređenje ljudskih i finansijskih resursa**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**	**Ciljna vrijednost do 2026.**
Procentualno povećanje budžetskih izdvajanja za razvoj sajber kapaciteta.	Nakon usvajanja budžeta za 2022. godinu vrijednost će biti definisana	10% uvećana budžetska izdvajanja u ANB, MO, MJUDDM, MVP, MUP, UP, Forenzičkom centru, DZZTP, CIRT u odnosu na budžetska izdvajanja u 2022. godini	20% uvećana budžetska izdvajanja u ANB, MO, MJUDDM, MUP, UP, MVP, Forenzičkom centru, DZZTP, CIRT u odnosu na budžetska izdvajanja u 2022. godini
Broj zaposlenih u MO, MJUDDM, MUP, MVP, UP, Forenzičkom centru, DZZTP i CIRT-u koji se bave pitanjima sajber bezbjednosti.	30	42	52

Operativni cilj 2: Efikasan mehanizam za odgovor na sajber incidente

Analizom trenutnog stanja, koja je izvršena na nivou Savjeta za informacionu bezbjednost i uz asistenciju strateških partnera, nameće se potreba temeljne reorganizacije Nacionalnog CIRT-a kako bi se postigla centralizacija sajber ekspertize, smanjio odliv stručnog kadra, i omogućio efiksaniji odgovor na sajber napade i zaštita kritične infomatičke infrastrukture.

Istovremeno, potrebno je omogućiti nastavak razvoja vojnih sajber kapaciteta u cilju ispunjenja nacionalnih i NATO odbrambenih sposobnosti. Odnosno, u domenu sistema odbrane, MO i VCG trebaju nastaviti sa razvojem sajber sposobnosti, posebno u dijelu podrške vojnih operacija. Za ostvarenje ovog cilja, potrebno je obezbijediti finansijske i ljudske resurse, koji će dovesti između ostalog do ispunjenja obaveza preuzetih članstvom u NATO. Sa druge strane, MO i VCG će usko sarađivati sa svim institucijama radi poboljšanja nivoa kolektivne odbrane. U tom kontkestu, sistem odbrane će biti otvoren da stavi svoje sajber kapacitete na raspolagnje svim zainteresovanim stranama, u skladu sa zakonom.

Sveobuhvatan pristup, tj. zajedničko djelovanje javne uprave, privatnog sektora i građana jedini je održivi način ostvarenja napretka u oblasti sajber bezbjednosti. Međusobna komunikacija i koordinacija aktivnosti ne bi trebala biti zasnovana na „ad hoc“ rješenjima i personalnoj osnovi. Potrebno je definisati jasniju podjelu uloga i odgovornosti i isticati značaj sistemskog pristupa. Stoga je združivanje resursa i postavljanje osnovnih principa djelovanja prilikom rješavanja sajber incidenata, posebno onih koji imaju uticaja na KII od velikog značaja.

Potrebno je definisanje i usvajanje osnovnih tehnoloških i organizacionih principa, kao osnove za efikasan mehanizam prevencije i odgovora na sajber incidente. Na ovaj način, kroz mehanizme kontrole primjene osnovnih principa, upravljanja rizicima i slično, će biti osnažena kolektivna sajber bezbjednost, odnosno sajber odbrana na nacionalnom nivou. **Inicijator za ostvarenje ovog operativnog cilja biće krovno tijelo – Agencija za sajber bezbjednost, kao pokretač i centralna tačka za sve zainteresovane strane.**

Operativni cilj 2	**Efikasan mehanizam za odgovor na sajber incidente**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**	**Ciljna vrijednost do 2026.**
Procenat uspješno riješenih sajber incidenata prijavljenih CIRT-u, odnosno Agenciji sa sajber bezbjednost	80%	85 %	90 %
Broj službenika za podršku vojnim operacijama u oblasti sajber bezbjednosti	12	16	20

Operativni cilj 3: Unapređenje mjera prevencije i edukacije o sajber bezbjednosti

Istraživanja su pokazala da 95% sajber bezbjednosnih incidenata su nastala kao rezultat ljudske greške[28]. Tim prije, osnovne tehnološke i operativne mjere za prevenciju sajber prijetnji moraju biti sastavni dio procesa edukacije u oblasti sajber bezbjednosti i dio nacionalnih aktivnosti usmjerenih ka podizanju svijesti među različitim ciljnim grupama (mladima, zaposlenima u javnoj upravi i široj javnosti).

Paralelno sa ovom Strategijom razvijena je i Strategija za digitalizaciju obrazovnog sistema koja pokriva isti vremenski period. Kako bi se izbjeglo preklapanje, sledeće aktivnosti biće tretirane Strategijom za digitalizaciju obrazovnog sistema:

- Utvrđivanje jasne procedure za obrazovno-vaspitne ustanove o postupanju u slučaju sajber incidenata;
- Kreiranje materijala za djecu na temu sajber bezbjednosti (infografici, video spotovi, izmjena postojeće aplikacije NetPrijatelji i sl);
- Pokretanje kampanje za upis studenata na studijske programe potrebne tržištu rada (IT i sajber bezbjednost);
- Kreiranje i akreditacija opšteg programa obuke o sajber bezbjednosti za sve zaposlene u obrazovno-vaspitnim ustanovama;
- Kreiranje i akreditacija specijalizovanog programa obuke o sajber bezbjednosti za nastavnike informatike;
- Kreiranje i akreditacija specijalizovanog programa obuke o sajber bezbjednosti za stručne službe (pedagoge i psihologe);
- Kreiranje i akreditacija specijalizovanog programa obuke o sajber bezbjednosti za rukovodioce obrazovno-vaspitnih ustanova;
- Kreiranje i akreditacija specijalizovanog programa obuke o sajber bezbjednosti za školske ICT koordinatore;
- Kreiranje gore pomenutih obuka kao samovodećih kurseva, koje bi osim kadru obrazovno-vaspitnih ustanova bile na raspolaganju i roditeljima;
- Kreiranje radionica za učenike za 4 uzrasne grupe koje bi se ustupile obrazovno-vaspitnim ustanovama;
- Kreiranje modula slobodnih aktivnosti koji nastavnici mogu uključivati u sve predmete osnovnog i opšteg srednje obrazovanja;

[28] Više na: https://accentconsulting.com/wp-content/uploads/2021/06/5-Cybersecurity-Stats-Infographic.pdf

- Kreiranje međupredmetne teme koji nastavnici mogu uključivati u mnoge predmete srednjeg stručnog obrazovanja;

O realizaciji navedenih aktivnosti, nadležni resor zadužen za prosvjetu, na polugodišnjem nivou izvještavaće Savjet za informacionu bezbjednosti.

***

U narednom periodu biće neophodno nastaviti s planom obuka zaposlenih u javnoj upravi na lokalnom i centralnom nivou, kako bi se osnažila sajber bezbjednosna kultura. Dosadašnji napori učinjeni na ovom planu ukazali su na potrebu postojanja kontinuiteta edukacije među zaposlenima, ali i među novozaposlenima.

S tim u vezi, osim redovnih obuka koje će biti obezbijeđene zaposlenima od strane Uprave za kadrove, kreiraće se i obavezna online obuka o osnovnim pravilima i smjernicama za bezbjedno korišćenje naloga i informacionih sistema u svakodnevnom radu, sa pratećim testom, koju svako novozaposleno lice mora proći prije dobijanja e-mail adrese i upotrebe informacionog sistema državne uprave i/ili lokalne samouprave. Osim službenika i namještenika na lokalnom i centralnom nivou, odgovarajuću obuku moraće proći i funkcioneri.

Ujedno, potrebno je održati fokus generalne javnosti na značaju sajber bezbjednosti i potencijalnim prijetnjama koje dolaze iz sajber prostora kroz edukativne kampanje širenja svijesti i distribuciju edukativnih materijala iz oblasti sajber zaštite i bezbjednosti. Na ovaj način će se obezbijediti, u saradnji sa medijima, akademskom zajednicom, privatnim i civilnim sektorom, kao i međunarodnim partnerima, da se pitanje sajber kulture i investiranja u istu izdigne na potreban nivo.

Ovom zadatku će doprinijeti i centralizacija informacija o dostupnim obukama, programima obrazovanja na nacionalnom, regionalnom i međunarodnom planu, te edukativnih materijala na jednom mjestu – portalu CIRT.me.

Operativni cilj 3	**Unapređenje mjera prevencije i edukacije o sajber bezbjednosti**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**	**Ciljna vrijednost do 2026.**
Broj informacionih sistema nad kojima je izvršeno preventivno penetraciono testiranje	n/a	10	30
Procenat zaposlenih javnih službenika koji su prošli obuku na temu sajber bezbjednosti	1%	10%	15%

Operativni cilj 4: Poboljšanje odgovora na sajber kriminal

Sajber kriminal u eri sveopšte dostupnosti interneta predstavlja rastuću prijetnju koja zahtijeva uspostavljen pravni sistem, usklađen s međunarodnim standardima, snažne institucije, kao i interresornu i prekograničnu saradnju.

Crna Gora je zakonodavni okvir sprječavanja narušavanja funkcionisanja informaciono-komunikacionih tehnologija, sprovođenja istraga i rasvjetljavanja slučajeva računarskog, visoko-tehnološkog/sajber kriminala i sankcionisanja počinilaca, započela da uspostavlja reformom krivičnog zakonodavstva. Dodatno, Ustavom, konkretno članom 9 precizirala je da su potvrđeni i objavljeni međunarodni ugovori i opšteprihvaćena pravila međunarodnog prava sastavni dio unutrašnjeg pravnog poretka, da imaju primat nad domaćim zakonodavstvom, te da se neposredno primjenjuju kada odnose uređuju drugačije od unutrašnjeg zakonodavstva.

Godine 2009. Crna Gora je donijela Zakon o potvrđivanju Konvencije o računarskom kriminalu Savjeta Evrope (Budimpeštanska konvencija[29]), istovremeno ratifikovala dodatni Protokol o rasizmu i ksenofobiji (CETS 189), kao i Konvenciju o zaštiti djece od seksualne eksploatacije i seksualnog zlostavljanja (CETS 201), te započela implementaciju i usklađivanje nacionalnog pravnog okvira sa odredbama navedenih konvencija. Nakon ratifikacije Crna Gora je uskladila svoje krivično zakonodavstvo sa odredbama ovih Konvencija, kao i sa Okvirnom odlukom Savjeta 2005/222/ o napadima na informacione sisteme i Okvirnom odlukom Savjeta 32000D0375 o suzbijanju dječije pornografije na internetu.

Dosadašanja primjena zakonskih rješenja na planu borbe protiv sajber kriminala, odnosno sprovođenja efikasnih istraga i procesuiranja počinilaca krivičnih djela ukazala je na određene nedostatke i izazove koje adresira Strategija.

Prioritet u narednom periodu biće dat izmjenama i dopunama Krivičnog zakonika i Zakona o krivičnom postupku, 100% proširenju kapaciteta u Grupi za borbu protiv visokotehnološkog kriminala Uprave policije i specifičnim obukama na polju sajber kriminala, odnosno čuvanja, prepoznavanja i izuzimanja digitalnih dokaza za zaposlene Ministarstva unutrašnih poslova, Uprave policije i nosilaca pravosudnih funkcija. Izmjenama Krivičnog zakonika bi se išlo u pravcu sankcionisanja krivičnog djela koja se tiču širenja i prenošenja lažnih vijesti i dezinformacija, dok bi se izmjenama i dopunama Zakona o krivičnom postupku unaprijedio i olakšao istražni prostupak.

[29] Konvencija o sajber kriminalu, link: https://www.coe.int/en/web/cybercrime/the-budapest-convention

Dodatno, detektovano je da trenutno u Crnoj Gori ne postoji nadležno tijelo za analizu i gašenje internet stranica s kojih se vrše razna krivična djela, posebno krivična djela dječje pornografije, ksenofobije, terorizma, širenja vjerske i nacionalne mržnje, kao i krivična djela koja se tiču sive ekonomije. S tim u vezi, potrebno je razmotriti izmjenu postojećeg Zakona o elektronskim komunikacijama u dijelu omogućavanja preduzimanja aktivnosti na planu gašenja pomenutih internet stranica pod određenim uslovima. Dodatno, crnogorski ISP nemaju mogućnost gašenja subdomena, odnosno onemogućavanja pristupa stranicama na internetu sa kojih se vrše krivična djela.

Prevazilaženjem ovog izazova, crnogorske institucije bi mogle brzo i efikasno blokirati lažne profile na društvenim mrežama, bez da zavise od inostranih ISP.

Takođe, potrebno je obezbijediti adekvatne finansijske i tehnološke resurse, kao i periodične analize statistike o započetim/realizovanim istragama, trendova i rezultata sudskih postupaka.

Operativni cilj 4	**Poboljšanje odgovora na sajber kriminal**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**	**Ciljna vrijednost do 2026.**
Procenat procesuiranih krivičnih djela u oblasti visokotehnološkog kriminala i krivičnih djela učinjenih upotrebom informaciono komunikacionih tehnologija	25 %	30 %	35 %

Operativni cilj 5: Osnažen i harmonizovan sistem zaštite podataka

Paralelno sa povećanjem upotrebe ICT-a u svakodnevnom životu i poslovanju, došlo je do povećanja količine ličnih podataka i informacija dostupnih online, a koji su predmet potencijalne zloupotrebe. Izazovi na planu zaštite ličnih podataka postali su vidljiviji s proglašenjem pandemije uzrokovane koronavirusom, odnosno s većim oslanjanjem na e-usluge i servise za obavljanje svakodnevnih aktivnosti.

Zaštita ličnih podataka u Crnoj Gori se obezbjeđuje primjenom Ustava, ratifikovanih međunarodnih ugovora, kao i nacionalnog zakonodavstva, prije svega odredbi Zakona o zaštiti podataka o ličnosti i Zakona o slobodnom pristupu informacijama.

Adekvatnu nadzornu ulogu u oblasti zaštite ličnih podataka vrši Agencija za zaštitu ličnih podataka i slobodan pristup informacijama (u daljem tekstu: Agencija), čije administrativne kapacitete treba dodatno osnažiti kroz zapošljavanje novog kadra i edukaciju postojećeg u cilju daljeg unaprijeđenja proaktivnog djelovanja u oblasti zaštite ličnih podataka.

Kao zemlja kandidat za članstvo u Evropskoj uniji, Crna Gora će u narednom periodu morati da uskladi Zakon o zaštiti podataka o ličnosti sa pravnom tekovinom Evropske Unije, posebno sa Opštom uredbom o zaštiti ličnih podataka – GDPR 2016/679 čime će biti napravljeni novi iskoraci na planu ostvarivanja prava građana na privatnost i omogućen nivo zaštite ličnih podataka koji imaju građani EU.

Paralelno, budući da građani nisu još uvijek u dovoljnoj mjeri shvatili značaj zaštite podataka, kao i da podaci koje dobrovoljno ostavljaju u sajber prostoru mogu biti zloupotrijebljeni, biće neopodno intenzivirati napore na daljoj promociji i afirmisanju prava na zaštitu podataka, ali i nastaviti sa sprovođenjem aktivnosti na poboljšanju sistema za obradu tajnih podataka i sertifikaciju sistema.

Operativni cilj 5	**Osnažen i harmonizovan sistem zaštite podataka.**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**	**Ciljna vrijednost do 2026.**
Broj organizacija i njihovih komunikaciono informacionih sistema usklađenih sa standardima informacione bezbjednosti i sertifikovanih za obradu tajnih podataka	3	5	6

Operativni cilj 6: Razvoj i unapređenje saradnje s nacionalnim i međunarodnim partnerima

Javno-privatno partnerstvo

Evidentna je potrebna bliske saradnje javne uprave sa privatnim sektorom u oblasti sajber bezbjednosti. Vrsta takvih partnerstava može biti raznolika, od institucionalnih partnerstava na planu zaštite kritične infrastrukture imajući u vidu da ne mali dio KII pripada privatnom sektoru i razmjene informacija, znanja, iskustava i dobre prakse o sajber incidentima i prijetnjama, do ad hoc partnerstava na polju odgovora na kratkoročne izazove/prijetnje u oblasti sajber bezbjednosti kroz fokusirano djelovanje i

snaženja kulture sajber bezbjednosti kroz edukativne kampanje, obuke, radionice, konferencije i sl, kreiranje kanala i platformi za informisanje o dostupnim obrazovnim programima i edukativnim materijalima za različite ciljne grupe i namjene.

Javno-privatna partnerstva mogu biti tematska i vremenski određena. Tako će biti potrebno podsticti snaženje partnerstava na planu istraživanja i razvoja u domenu sajer bezbjednosti, uspostavljanja nacionalne baze sajber eksperata i platforme za njihovo okupljanje, razmjenu informacja i saradnju, kao i u svim drugim segmentima gdje je koordinacija svih segmenata društva neophodna u cilju pravovremenog i efikasnog odgovora na izazove u sajber domenu.

U prethodnom periodu napravljeni su značajni iskoraci na polju uspostavljanja javno-privatnh partnerstava, i snaženja sajber bezbjednosnog ekosistema. Postojeće platforme (kao što je NTP Crna Gora) treba u narednom periodu dodatno afirmisati kao lokacije gdje se privatni i javnih sektor okuplja, obezbjeđuje obuke, realizuje radionice, takmičenja, vježbe, razmjenjuje know-how i ekspertizu i podstiče saradnju na polju istraživanja i razvoja u oblasti sajber bezbjednosti, edukacije i usavršavanja zaposlenih.

Dodatno, snaženjem postojećih javno-privatnih partnertava i iniciranjem novih, osim zaštite kritične informatičke infrastrukture, širenja svijesti o sajber bezbjednosti, razmjene znanja i informacija, te podsticanja istraživanja i razvoja, može se doprinijeti i snaženju nacionalnih kapaciteta za sajber bezbednost kroz udruživanje ekspertize, iskustva i znanja s kojom raspolažemo, kao i pokretanje inicijativa kojima će se podstaći veći broj ljudi da postanu profesionalci iz oblasti sajber bezbednosti.

Međunarodna saradnja

Saradnja je nezaobilazan element svih dosadašnjih strategija sajber bezbjednosti Crne Gore budući da ista ne podrazumijeva pojedinačnu, sektorsku odgovornost, već udruženo djelovanje svih nadležnih aktera.

Kako je sajber bezbjednost međunarodni izazov, da bi se obezbijedio potreban nivo bezbjednosti međunarodna saradnja je neophodna. Tako je Crna Gora ratifikovala brojne međunarodno obavezujuće konvencije, postala članica UN-a, OEBS-a, NATO-a, FIRST-a, pridružila se inicijativama i platformama za snaženje kapaciteta za sajber odbranu i na putu članstva u EU preduzela brojne aktivnosti na izgradnji i uskađivanju nacionalnog zakonodavstva za pravnom tekovinom EU o oblasti sajber bezbjednosti.

Tako je Crna Gora postala i članica Evropskog centra izvrsnosti za suprotstavljanje hibridnim prijetnjama, pristupila NATO Centru izvrsnosti za kooperativnu sajber odbranu u Talinu, Republika Estonija, učestvovala u brojnim zajedničkim međunarodnim vježbama, obukama, na sastancima, forumima, konferencijama.

U predstojećem periodu biće nastavljene aktivnosti na polju daljeg snaženja saradnje s organizacijama čiji smo član, kao i pristupanja i promocije novih kanala komunikacije, saradnje i partnerstava na međunarodnom planu.

Operativni cilj 6	**Razvoj i unapređenje saradnje s nacionalnim i međunarodnim partnerima**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**	**Ciljna vrijednost do 2026.**
Procenat međunarodnnih konferencija, obuka i vježbi na kojima je Crna Gora uzela učešće	60 %	70 %	75%

Operativni cilj 7: Uspostavljen sistem zaštite kritične informatičke infrastrukture.

U cilju uspostavljanja zakonodavnog okvira kojim će se obezbijediti zaštita kritične infrastrukture (KI), Crna Gora je donijela Zakon o određivanju i zaštiti kritične infrastrukture koji je stupio na snagu 3. januara 2020. godine.

Istim je definisano da kritična infrastruktura obuhvata sisteme, mreže, objekte, odnosno njihove djelove koji se nalaze na teritoriji Crne Gore, čiji prekid funkcionisanja, odnosno prekid isporuka roba ili usluga preko tih sistema, mreža, objekata, odnosno njihovih djelova može imati ozbiljne posljedice po nacionalnu bezbjednost, zdravlje i život ljudi, imovinu, životnu sredinu, bezbjednost građana, ekonomsku stabilnost, odnosno vršenje djelatnosti od javnog interesa.

U skladu sa Zakonom zaštita kritične infrastrukture utvrđena je kao “skup aktivnosti i mjera koje imaju za cilj da spriječe nastanak poremećaja u radu, oštećenje ili uništenje kritične infrastrukture u slučaju prijetnje, obezbijede funkcionisanje i otpornost kritične

infrastrukture u slučaju poremećaja u radu ili oštećenja i spriječe nastanak posljedica poremećaja u radu, odnosno oštećenja ili uništenja kritične infrastrukture”[30].

Za sektore KI u kojima se vrši određivanje KI prepoznati su: energetika, saobraćaj, snabdijevanje vodom, zdravstvo, finansije, elektronske komunikacije, informaciono-komunikacione tehnologije, zaštita životne sredine, funkcionisanje državnih organa, kao i druge oblasti od javnog interesa.

Na osnovu sektorskih kriterijuma koje donosi Vlada na temelju prethodno izvršenih analiza rizika od strane resora nadležnih za navedene sektore, i međusektorskih kriterijuma definisanih predmetnim Zakonom, operatori KI procjenjuju koji sistemi, mreže, objekti, odnosno njihovi djelovi koje oni koriste, odnosno kojima upravljaju predstavljaju KI u određenom sektoru KI, o čemu dostavljaju obavještenje ministarstvu nadležnom za taj sektor. Na osnovu obavještenja, resorna ministarstva utvrđuju da li su ispunjeni kriterijumi i sačinjavaju predloge za određivanje KI za te sektore i dostavljaju Ministarstvu unutrašnjih poslova koji objedinjene predloge svih resora dostavlja Vladi kako bi se odredila KI.

Operatori KI su u obavezi da izrade bezbjednosni plan za zaštitu KI i da za isti pribave saglasnost Ministarstva unutrašnjih poslova koji za te potrebe formira Komisiju. Takođe, u obavezi su da imaju lice za zaštitu KI, odnosno koordinatora koji između ostalog ima položen stručni ispit za zaštitu KI, čiji program i način polaganja je propisalo Ministarstvo unutrašnjih poslova.

Zaštita KI vrši se primjenom fizičke i tehničke zaštite, na način i pod uslovima propisanim Zakonom o zaštiti lica i imovine. Način zaštite kritične informatičke infrastrukture (KII) i način zaštite KI koju koriste organ državne uprave nadležan za poslove odbrane, policijske poslove, Vojska Crne Gore i ANB, vršiće se u skladu sa posebnim zakonom. Isti su oslobođeni obaveze izrade bezbjednosnog plana i određivanja koordinatora.

Zakonom o informacionoj bezbjednosti 2016. godine definisano je da KII čine informacioni sistemi organa čijim bi se prekidom rada ili uništenjem ugrozili život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa. Mjere zaštite KII propisuje organ državne uprave nadležan za informaciono društvo.

[30] Izvor: https://me.propisi.net/zakon-o-odredjivanju-i-zastiti-kriticne-infrastrukture/

U slučaju nastanka poremećaja u radu, odnosno oštećenja ili uništenja KI rukovođenje i koordinaciju preduzima koordinacioni tim obrazovan u skladu sa Zakonom o zaštiti i spašavanju.

U narednom periodu potrebno je pristupiti izmjeni regulative, kako bi i sistemi za registrovanje domena i DNS sistem bili definisani kao kritični sistemi, na šta upućuje NIS direktiva EU, kao i da bi prepoznali i sektor operatora usluga registracije domena i sistema upravljanja domenima i obezbijedili potrebno usklađivanje postojećih zakona u oblasti zaštite KI i KII.

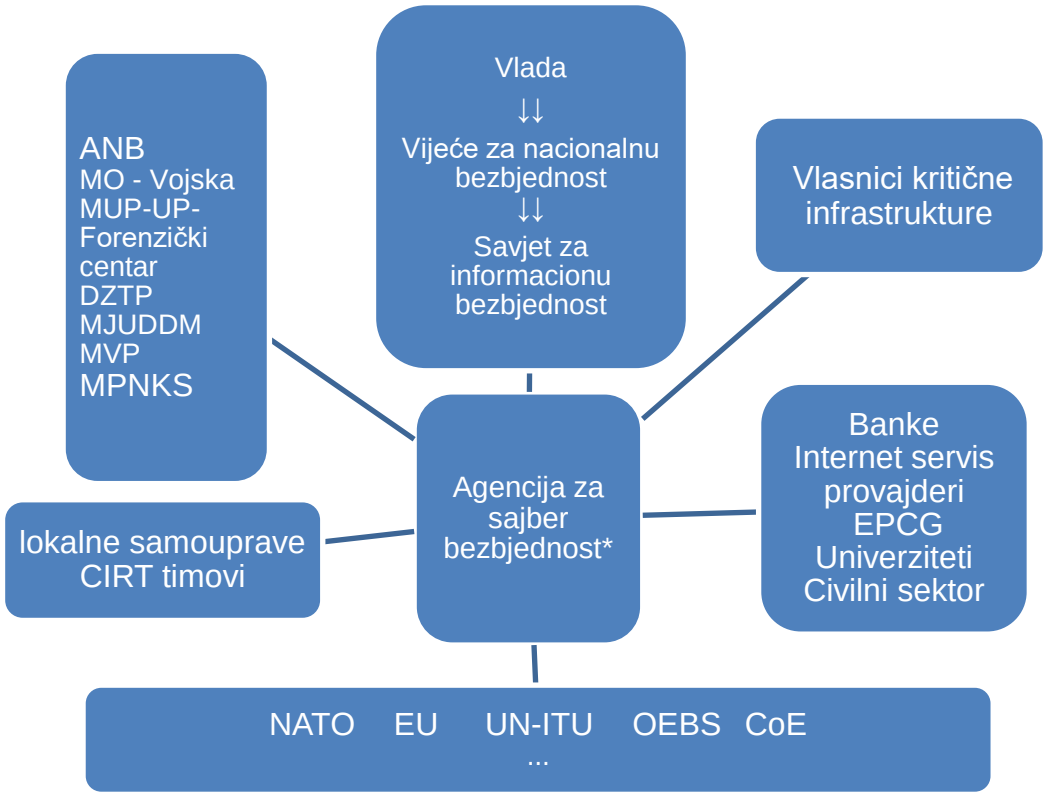
Operativni cilj 7:	**Uspostavljen sistem zaštite kritične informatičke infrastrukture**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**	**Ciljna vrijednost do 2026.**
Procenat kritičnih informacionih sistema koji imaju implementirane sve zakonski propisane tehničke mjere zaštite	n/a	30%	85%
Broj zaposlenih službenika u CIRT-u	6 službenika	16 službenika	24 službenika

V INSTITUCIONALNI OKVIR ZA SPROVOĐENJE STRATEGIJE

Protekle decenije Crna Gora je uspostavila organizacionu strukturu u oblasti sajber bezbjednosti i prepoznala organe državne uprave nadležne za navedenu oblast, strateško planiranje i realizaciju politika definisanih prethodnim strategijama sajber bezbjednosti.

U nastavku je predstavljen šematski prikaz organizacione strukture, kao i aktivnosti koje su nadležni organi državne uprave preduzeli na planu snaženja kapaciteta za sajber bezbjednost, uz navođenje aktivnosti čija realizacija će imati prioritet u radu tokom narednog petogodišnjeg perioda, kako bi se na kraju ciklusa Strategije dostigao i postavljeni strateški cilj.

Šema 1: *Prikaz organizacione strukture u oblasti sajber bezbjednosti*



** U sklopu Agencije bi funkcionisao CIRT.ME.*

Savjet za informacionu bezbjednost

Radi unaprjeđenja mjera informacione bezbjednosti, kao i praćenja rada i predlaganja aktivnosti CIRT-u na uspostavljanju sistema zaštite od računarskih i bezbjednosnih incidenata na internetu, Vlada Crne Gore je na osnovu Zakona o informacionoj bezbjednosti donijela Odluku o obrazovanju **Savjeta za informacionu bezbjednost** (u daljem tekstu: Savjet).

Savjet čine predstavnici organa državne uprave nadležnog za unutrašnje poslove, organa državne uprave nadležnog za poslove odbrane, organa državne uprave nadležnog za poslove pravosuđa, organa uprave nadležnog za informaciono društvo, organa uprave nadležnog za vanjske poslove, organa uprave nadležnog za tajne podatke i Agencije za nacionalnu bezbjednost, a po potrebi i predstavnici drugih organa i institucija. Zadaci Savjeta, definisani su njegovim aktom o obrazovanju.[31]

Dosadašnje fukcionisanje Savjeta ukazalo je na neophodnost izmjene Odluke o obrazovanju na način da se i formalno predvidi mogućnost da se po potrebi, radi razmatranja određenih pitanja i podsticanja saradnje, na sjednice Savjeta mogu pozivati i predstavnici privatnog sektora, akademske zajednice i civilnog sektora.

Takođe, potrebno je korigovati i dio koji se odnosi na zadatke Savjeta kako bi se prepoznalo da Savjet prati sprovođenje nove Strategije za period 2022-2026. i akcionih planova za njenu implementaciju.

Tim za odgovor na računarsko bezbjednosne incidente u sajber prostoru Crne Gore – CIRT.ME

CIRT je tim za odgovor na računarsko bezbjednosne incidente u sajber prostoru Crne Gore. Formiran je 2012. godine kao dio zajedničkog projekta Vlade Crne Gore i Međunarodne telekomunikacione unije.

U skladu sa Zakonom o tajnosti podataka i Zakonom o informacionoj bezbjednosti vrši funkciju zaštite od računarskih bezbjednosnih incidenata na Internetu i drugih rizika u vezi sa informacionom bezbjednošću.

Takođe, predstavlja centralnu kontakt tačku na nacionalnom i međunarodnom nivou za sve računarske bezbjednosne incidente u kojima se jedna od strana u incidentu nalazi u Crnoj Gori (odnosno, ako je u crnogorskom IP adresnom prostoru).

U periodu od osnivanja, zaključno sa junom 2021. godine, konstatovan je porast broja incidenata prijavljenih CIRT-u, što govori u prilog neophodnosti daljeg snaženja kapaciteta ovog tijela za odgovor na novonastale okolnosti.

[31] https://www.gov.me/dokumenta/5b254c61-683f-45fa-8925-30d2df8ecb63

Statistika CIRT-a o prijavljenim incidentima u periodu 2012-jun 2021.

Godina	Napad na web sajtove i IS	Prevare putem Interneta	Zloupotreba profila na društvenim mrežama	Neprikladan sadržaj na Internetu	Malver	Ostali (Uznemiravanje, Ucjene, Krađa identiteta i sl.	Ukupno
2012	3	2	-	1		-	6
2013	5	3	10	-	1	3	22
2014	5	6	20	5		6	42
2015	6	17	37	19	17	36	132
2016	18	20	36	14	50	25	163
2017	91	18	34	9	368	12	532
2018	13	68	50	6	363	37	537
2019	19	70	79	11	387	38	604
2020	25	84	90	15	383	44	641
2021 ***01.01-15.06***	12	38	48	7	167	23	295

Do novembra 2020. godine CIRT se nalazio u Ministarstvu javne uprave, a od novembra u skladu za izmjenama i dopunama Zakona o tajnosti podatka, u Direkciji za zaštitu tajnih podataka (DZTP).

U prethodnom periodu nije postignuta puna funkcionalnost rada CIRT-a (kadrovski, tehnički i smještajni kapaciteti), sa čim u vezi je u narednom periodu neophodno definisati uspostvljanje novog tijela – Agencije za sajber bezbjednost u okviru koje bi funkcionisao CIRT.ME.

Direkcija za zaštitu tajnih podataka

Direkcija se bavi edukacijom i sprovođenjem aktivnosti iz svojih nadležosti, kao i intenzivnom saradnjom sa međunarodnim partnerima u cilju informisanja i unapređenja svojih kapaciteta iz oblasti sertifikacije klasifikovanih informacionih sistema, TEMPEST zaštite i rukovanja kripto materijalima, kao i unapređenjem i daljom implementacijom informacionog sistema za razmjenu domaćih tajnih podataka.

Agencija za nacionalnu bezbjednost

Agencija za nacionalnu bezbjednost je shodno nadležnostima usmjerenim prvenstveno na zaštitu nacionalnih interesa i bezbjednosti, osim Zakonom o ANB, kroz strateška dokumenta, kako Nacionalnu strategiju za sajber bezbjednost, tako i prethodne Strategije za sajber bezbjednost, prepoznata kao jedna od ključnih institucija na polju zaštite sajber prostora Crne Gore. Kroz zakon o ANB su definisane nadležnosti Agencije prije svega u prikupljanju i obradi podataka koji su od značaja za nacionalnu bezbjednost, kao i nadležnosti kontraobavještajne zaštite štićenih objekata i ličnosti.

Planirane obaveze pred ANB-om u narednom strateškom petogodišnjem periodu su:

- Imajući u vidu narastajuće APT (Advanced Persistent Threat) prijetnje po nacionalnu sajber bezbjednost i potrebu da se izazovima uspješno odgovori u što kraćem roku Agencija će nastaviti da radi na podizanju kadrovskih, tehničkih i analitičkih kapaciteta i sposobnosti, prije svega kroz izmjenu organizacije i sistematizacije radnih mjesta u cilju povećanja broja zaposlenih na poslovima sajber bezbjednosti kao i implementaciji savremenih rješenja i izbora opreme u skladu sa standardima ISO 27001 i EU i NATO standardima.
- Kointinuirano će unapređivati Registar rizika sa rizicima iz oblasti sajber bezbjednosti u skladu sa usvojenom Strategijom upravljanja rizicima kroz postavljanje odgovarajućih kotrola u clju reakcije na rizike i njihovu mitigaciju. Dostizanje ovih operativnih ciljeva mora biti praćeno i pravovremenim i adekvatnim planiranjem budžetskih sredstava.
- Agencija će u kontinuitetu raditi na obezbjeđivanju adekvatnih prostorija, računarske opreme i sistema za prijem, obradu i čuvanje tajnih podataka označenih stepenima tajnosti “Povjerljivo”, “Tajno” i “StrogoTajno”.
- Kroz opredijeljene kadrovske i tehničke potencijale Agencija će participirati u radu Savjeta za informacionu bezbjednost i operativnih timova za odgovore na sajber incidente i učestvovati u rješavanju incidenata koji ugrožavaju nacionalne interese i bezbjednost u skladu sa svojim nadležnostima.
- Kako je zaštita štićenih ličnosti i objekata jedna od nadležnosti rada Agencije, djelatnosti u tom dijelu će podrazumijevati i aktivnosti vezane za njihovu sajber bezbjednost.
- Zaštita sopstvene i nacionalne KI je jedna od prioritetnih aktivnosti Agencije.

- Na međunarodnom planu aktivnosti Agencije će se ogledati u razmjeni podataka, informacija i iskustava sa partnerskim službama NATO i drugih zemalja u skladu sa smjernicama Vlade, kroz ostvarivanje bilateralne i multilateralne saradnje.
- Službenici Agencije će nastaviti da pohađaju obuke, konferencije, seminare druge vidove edukacije iz oblasti sajber bezbjednosti.

Ministarstvo odbrane

Nakon pridruživanja Crne Gore NATO savezu, Ministarstvo odbrane i Vojska Crne Gore su uložili značajne napore na unaprijeđenju informacione bezbjednosti, posebno izgradnji kapaciteta za sajber odbranu, u skladu sa nacionalnim i NATO strateškim ciljevima. U tom kontekstu, napravljene su izmjene organizacionih struktura unutar MO i VCG, čime je jasno prepoznata potreba jačanja sajber kapaciteta u domenu odbrane. Dodatno, uložena su značajna sredstva u domenu primjene tehnoloških rješenja i nadogradnje znanja stručnog kadra, čime su unaprijeđeni mehanizmi prevencije sajber prijetnji i za odgovore na sajber incidente.

Krajem 2019. godine, usvojena je Strategija sajber bezbjednosti Vojske Crne Gore 2019-2022. godine, koja je fokusirana na dostizanje specifičnih ciljeva u domenu zaštite informaciono-komunikacionih sistema MO i VCG i definisanje okvira za razvoj sajbera u domenu vojnih operacija. MO i VCG će nastaviti da nadograđuju postojeće i razvijaju nove sajber sposbnosti, kako bi obezbijedili kapacitete za sajber odbranu, u skladu sa nacionalnim i NATO strateškim ciljevima.

Ministarstvo javne uprave, digitalnog društva i medija

Uredbom o organizaciji i načinu rada državne uprave propisano je da Ministarstvo javne uprave, digitalnog društva i medija između ostalog vrši poslove uprave koji se odnose na: predlaganje i sprovođenje utvrđene politike u oblasti uspostavljanja i razvoja informacionog društva; pripremu predloga zakona i drugih propisa iz oblasti informacionog društva; pružanje stručne pomoći u primjeni informaciono-komunikacionih tehnologija u organima državne uprave; uspostavljanje okvira za upravljanje informacionim sistemima organa državne uprave i državnih organa u skladu sa međunarodnim standardima; uspostavljanje tehnološke i bezbjednosne informatičke infrastrukture u organima državne uprave i državnim organima; kao i utvrđivanje tehničkih i drugih pravila upotrebe informacionokomunikacionih tehnologija u organima državne uprave i državnim organima.

Kao resor nadležan za informaciono-komunikacionu infrastrukturu i informacionu sigurnost državne uprave, u narednom periodu kako bi se dodatno zaštitila IK infrastruktura, ažuriraće se procedura otvaranja novih naloga (e-mail adresa) i odobravanja pristupa državnim informacionim sistemima kako bi se predvidjela i obavezna obuka o sigurnom korišćenju interneta i ICT za svakog novog zaposlenog državnog službenika i namještenika. Dodatno, u saradnji sa Upravom za kadrove, razviće se specifični programi obrazovanja za zaposlene u javnoj upravi na državnom i lokalnom nivou, kao i za funkcionere.

Uprava policije

U okviru nadležnosti Uprave policije spada preduzimaje mjera i radnja u dijelu izvršavanja naredbi nadležnih sudova, kojom prilikom koriste uniformisane digitalne forenzičke alate i uređaje za izvršavanje istih, a koji su validirani od nadležnih naučnih institucija koje se bave digitalnim dokazima.

U narednom periodu Uprava policije će nastaviti sa jačanjem ljudskih i tehničkih kapaciteta u oblasti sajber bezbjednosti i borbe protiv sajber kriminala, a u okviru čega je planirano 100% povećanje ljudskih resursa, kao i nastavak edukacije službenika.

Forenzički centar

U cilju unapređenja, a kako bi se dodatno poboljšala zaštita podataka u Forenzičkom centru, trenutno se realizuje projekat implementacije LIMS sistema (A Laboratory Information Management System)[32] koji će predstavljati Intranet mrežu, dakle četvrtu (privatnu) mrežu u samom Forenzičkom centru.

Implementacijom ovakve Intranet mreže unutar centra, odnosno LIMS sistema, izvršiće se potpuni transfer svih podataka sa postojećeg na novo hardversko i softversko rješenje koje će biti u potpunosti fizički izolovano i zaštićeno u okviru same institucije, te koje će dakle osim slobodnog transfera svih podataka unutar Forenzičkog centra doprinijeti i fizičkoj zaštiti podataka od strane bilo kakvog pokušaja sajber napada iz spoljašnjeg svijeta putem Interneta.

Kako ulaganja u nova hardverska i softverska rješenja, a sve zbog unapređenja procesa rada Forenzičkog centra, nisu na zadovoljavajućem nivou, u predstojećem periodu biće neophodno opredijeliti potrebna sredstva za unapređenje sigurnosti računarskih sistema iznutra.

[32] Projekat se relizacije kroz donaciju ICITAP organizacije.

Osim ulaganja u nova hardverska i softverska rješenja, mora se obezbijediti i da Forenzički centar ima dovoljno ljudskih kapaciteta da sprovodi digitalnu forenziku i adekvatno istražuje sajber kriminalne aktivnosti u Crnoj Gori.

VI FINANSIJSKI OKVIR

Strategija sajber bezbjednosti Crne Gore odnosno njene pojedinačne aktivnosti finansiraće se iz budžeta i donatorskih sredstava.

Kroz Akcioni plan za 2022-2023. godinu, za postizanje svih operativnih ciljeva predviđen je utrošak u ukupnom iznosu od 3.577.000,00 EUR. Sledećim Akcionim planovima za preostale godine sprovođenja Strategije definisaće se preostala finansijska sredstva.

Budžetom za 2022. godinu predviđena su finansijska sredstva za implementaciju Strategije sajber bezbjednosti, srazmjerno definisanim aktivnostima i neophodnim finansijskim resursima za realizaciju istih.

IZNOS IZ BUDŽETA	3.435.000,00 EUR
IZNOS IZ DONACIJA:	97.000,00 EUR
UKUPAN IZNOS POTREBNIH SREDSTAVA ZA 2022-2023.	**3.532.000,00 EUR**

VII MONITORING, IZVJEŠTAVANJE I EVALUACIJA

4.1. Monitoring

Vlada je na osnovu člana 13a stav 1 Zakona o informacionoj bezbjednosti donijela Odluku o obrazovanju Savjeta za informacionu bezbjednost (u daljem tekstu: Savjet) čiji zadaci su utvrđeni aktom o njegovom obrazovanju kojim je između ostalog definisana obaveza Savjeta da prati, odnosno vrši monitoring sprovođenja Strategije i akcionih planova za njenu implementaciju.

Nadležni organi državne uprave prepoznati Strategijom – *Agencija za nacionalnu bezbjednost, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Uprava policije, Direkcija za zaštitu tajnih podataka, CIRT.ME, Ministarstvo prosvjete, nauke, kulture i sporta, Ministarstvo javne uprave, digitalnog društva i medija, Ministarstvo vanjskih poslova* - imaju obavezu da Savjetu na polugodišnjem nivou dostavljaju podatke u vezi sa dinamikom realizacije aktivnosti koje su definisane akcionim planovima. Na osnovu prikupljenih i obrađenih podataka, te analize, Savjet će inicirati i predložiti mjere nadležnim organima državne uprave za dalje unapređenje implementacije Strategije, odnosno realizacije aktivnosti i o svom radu informisati Vladu na godišnjem nivou, a po potrebi i češće.

4.2. Izvještavanje

Nosioci aktivnosti iz Strategije, odnosno AP – gore navedeni nadležni organi državne uprave, dužni su da tokom trajanja implementacije Strategije, najkasnije do kraja januara tekuće godine, dostave Ministarstvu javne uprave, digitalnog društva i medija (MJUDDM) podatke o stepenu realizovanosti aktivnosti iz AP za prethodnu godinu.

MJUDDM je zaduženo da objedini podatke i pripremi **godišnje Izvještaje o sprovođenju AP** koje dostavlja na mišljenje Savjetu za informacionu bezbjednost. Na osnovu mišljenja Savjeta, MJUDDM pristupa finalizaciji Izvještaja koje dostavlja Vladi tokom prvog kvartala tekuće godine za prethodnu godinu.

Izvještaji će biti pripremani u skladu sa Metodologijom razvijanja politika, izrade i praćenja sprovođenja strategijskih dokumenata (u daljem tekstu: Metodologija), i poslužiće za identifikovanje “uskih grla” i zastoja u realizaciji aktivnosti i davanje preporuka za njihovo prevazilaženje. Po usvajanju na Vladi, ukoliko se ukaže potreba, MJUDDM će izvršiti ažuriranje AP najkasnije do kraja aprila tekuće godine.

MJUDDM je zaduženo da pripremi i **Završni izvještaj o realizaciji Strategije** na osnovu podataka dostavljenih od strane nadležnih organa državne uprave o stepenu ostvarenosti operativnih i strateških ciljeva u periodu trajanja strateškog dokumenta, kao i aktivnosti iz AP u poslednjoj godini sprovođenja Strategije (2026), uz osvrt na uočene izazove koji su obilježili implementaciju Strategije, planirana i utrošena sredstva, i preporuke za naredni ciklus Strategije.

Završni izvještaj pratiće formu definisanu Metodologijom i biće dostavljen Savjetu na razmatranje i davanje mišljenja. Nakon dobijenog mišljenja i finalizacije Završnog izvještaja, čiji sastavni dio će činiti i rezultati ex post evaluacije, MJUDDM će isti u I kvartalu 2027. godine dostaviti na usvajanje Vladi Crne Gore.

4.3. Evaluacija

Tokom perioda trajanja Strategije, izvršiće se dvije evaluacije, i to: srednjeročna i ex post evaluacija.

Srednjeročna evaluacija će se realizovati u prvom kvartalu 2024. godine, primjenom kombinovane metode (spoljni evaluator i nadležni generalni direktorat u MJUDDM). Ovo iz razloga što će u predstojeće dvije godine, po usvajanju “Sajber paketa” – revidirane NIS Direktive i Direktive o otpornosti kritičnih entiteta, države članice EU biti u obavezi da mandatorne odredbe iz direktiva transponuju u nacionalna zakonodavstva. Kako Crna Gora kao zemlja kandidat za članstvo u EU, preduzima pravovremeno aktivnosti na usklađivanju zakonodavstva sa pravnom tekovinom Evropske unije, srednjeročna evaluacija će imati za cilj da a) analizira usvojene direktive i u odnosu na iste b) provjeri njihovu usklađenost sa definisanim strateškim i operativnim ciljevima, kao i aktivnostima iz Strategije, odnosno AP, te c) da preporuke u pravcu eventualnog ažuriranja Strategije i/ili planiranja novih aktivnosti kroz AP kojima bi se indentifikovale potrebne izmjene i dopune nacionalnog zakonodavstva u predmetnim oblastima.

Po završetku perioda na koji je donijeta Strategija, biće izvršena **ex post evaluacija** takođe primjenom kombinovanog metoda, čime će se obezbijediti veći stepen objektivnosti. Rezultati evaluacije kojima će se procijeniti relevantnost, efikasnost i efektivnost javne politike

U budžetu MJUDDM biće planirana sredstva za srednjeročnu evaluaciju koja će se obezbijediti kroz usvajanje Zakona o Budžetu za 2024. godinu u iznosu od 10.000 EUR, dok će sredstva za ex post evaluaciju u iznosu od 10.000 EUR biti planirana kroz Zakon o Budžetu za 2027. godinu.

ANEKS: Definicije i termini

Analiza rizika - razmatranje mogućih opasnosti i konvencionalnih, odnosno hibridnih prijetnji radi procjene mogućih posljedica poremećaja u radu ili mogućeg prekida funkcionisanja kritične infrastrukture, njenog oštećenja, odnosno uništenja.

Domen – Domen locira organizaciju ili drugi entitet na internetu sa jedinstvenim imenom koje je registrovano u autorizovanim institucijama, tzv. domen registratorima.

Informaciona bezbjednost - stanje povjerljivosti, cjelovitosti i dostupnosti podatka.

Internet – globalna računarska mreža, koja pruža razne informacione i komunikacione kapacitete, a koja se sastoji od međusobno povezanih računarskih mreža koristeći standardizovane komunikacione protokole.

KII – Kritična informatička infrastruktura obuhvata informacione sisteme kojima upravljaju operatori kritične infrastrukture, čijim bi se prekidom rada ili uništenjem ugrozili život, zdravlje, bezbjednost građana i funkcionisanje države i od čijeg funkcionisanja zavisi vršenje djelatnosti od javnog interesa.

Mjere informacione bezbjednosti - opšta pravila kojima se obezbjeđuje osnovna zaštita podataka na fizičkom, tehničkom i organizacionom nivou.

Odgovor na incident – aktivnosti koje se odnose na odgovor na kratoročne, direktne efekte nekog incidenta, a takođe mogu podržati kratoročni oporavak.

Operatori kritične infrastrukture - državni organi, organi državne uprave, organi lokalne samouprave, organi lokalne uprave i službe obrazovane u skladu sa zakonom kojim se uređuje lokalna samouprava, privredna društva i druga pravna lica koji koriste, odnosno upravljaju sistemima, mrežama, objektima, odnosno njihovim djelovima koji su određeni kao kritična infrastruktura.

Sajber bezbjednost – zaštita sistema, povezanih na internetu (uključujući hardver, softver i povezanu infrastrukturu), podataka na njima i usluga koje oni pružaju, od neovlašćenog pristupa, štete ili zloupotrebe. Ovo uključuje štetu prouzrokovanu namjerno od strane operatora sistema, ili slučajno, kao rezultat neizvršenja bezbjednosnih procedura ili štete koja je proizvod manipulacije.

Sajber incident – događaj koji zapravo ili potencijalno predstavlja prijetnju računaru, uređaju koji je povezan putem interneta ili mreže - ili podatke obrađivane, čuvane ili prenijete na tim sistemima - što može zahtijevati odgovor sa ciljem ublažavanje posljedica.

Sajber kriminal – krivična djela zavisna od sajbera (krivična djela koja se mogu izvršiti samo upotrebom ICT uređaja, gdje su uređaji i sredstvo za izvršenje krivičnih djela i meta krivičnih djela); ili krivična djela potpomognut sajberom (krivična djela koja mogu biti počinjenja bez ICT uređaja, poput finansijskih prevara, ali se značajno mijenjaju korišćenjem ICT-a u smislu razmjera i dometa).

Sajber odbrana – princip implementiranja bezbjednosnih mjera za jačanje bezbjednosti mreže ili sistema kako bi bili otporniji na napade.

Sajber otpornost – sposobnost sistema i organizacija da izdrže sajber incidente i oporave se od štete u slučaju istih.

Sajber prijetnja - sve što može ugrožavati bezbjednost ili izazvati štetu na informacionim sistemima i internet konektovanim uređajima (uključujući hardver, softver i prateću infrastrukturu) podatke o njima i uslugama koje pružaju prvenstveno putem sajber sredstava.

Sajber prostor – međusobno povezana mreža informatičke infrastrukture koja uključuje internet, telekomunikacione mreže, računarske sisteme, internet povezane uređaje i ugrađene procesore, i kontrolere. Može se odnositi i na virtuelni svijet ili domen kao doživljeni fenomen ili apstraktni koncept.

Upravljanje incidentima – upravljanje i koordinacija aktivnosti za istraživanje i sanaciju, stvarnih ili potencijalnih neželjenih sajber događaja, koji mogu ugroziti ili uzrokovati štetu na sistemu ili mreži.

Crna Gora
Ministarstvo javne uprave,
digitalnog društva i medija

AKCIONI PLAN
STRATEGIJE SAJBER BEZBJEDNOSTI CRNE GORE 2022-2026, ZA PERIOD 2022-2023.

Podgorica, decembar 2021. godine

AKCIONI PLAN
STRATEGIJE SAJBER BEZBJEDNOSTI CRNE GORE 2022-2026, ZA PERIOD 2022-2023.

Akcioni plan Strategije sajber bezbjednosti Crne Gore 2022-2026, za period 2022-2023. predstavlja dvogodišnji akcioni plan koji je će biti usvojen istovremeno sa strateškim dokumentom.

Akcioni plan je pripremljen u skladu sa Metodologijom razvijanja politika, izrade i praćenja sprovođenja strateških dokumenata, i njegovu strukturu čine 5 strateških ciljeva sa operativnim ciljevima, i to:

Strateški i operativni ciljevi:

Strateški cilj 1: Crna Gora u oblasti sajber bezbjednosti posjeduje održiv sistem za efikasno otkrivanje i odbranu od kompleksnih vektora sajber napada i prijetnji

Operativni cilj 1: Unapređenje ljudskih i finansijskih resursa
Operativni cilj 2: Efikasan mehanizam za odgovor na sajber incidente
Operativni cilj 3: Unapređenje mjera prevencije i edukacije o sajber bezbjednosti u javnom i privatnom sektoru
Operativni cilj 4: Poboljšanje odgovora na sajber kriminal
Operativni cilj 5: Osnažen i harmonizovan sistem zaštite podataka
Operativni cilj 6: Razvoj i unapređenje saradnje s nacionalnim i međunarodnim partnerima
Operativni cilj 7: Uspostavljen sistem zaštite kritične informatičke infrastrukture.

Svi operativni ciljevi sadrže indikatore učinka uz prateće vrijednosti gdje je iste bilo moguće detektovati. Definisane su konkretne aktivnosti za svaki operativni cilj, indikatori rezultata, rokovi, nosioci i izvori finansiranja. Važno je napomenuti da su zbog budžetskih ograničenja iskazane budžetske potrebe u nekim slučajevima manje od realnih, uz pretenziju da se kroz donacije prevaziđu eventualna ograničenja.

Takođe, u slučajevima gdje nije bilo moguće navesti tačne iznose za realizaciju pojedinačnih aktivnosti od strane određenih resora, navedena je okvirna kumulativna procjena potrebnih sredstava.

Prilikom izrade Akcionog plana uvažene su u mjeri mogućeg preporuke dobijene kroz izještaje eksperata Savjeta Evrope i Svjetske banke, i definisane aktivnosti čijom implementacijom će date preporuke biti operacionalizovane i doprinijeti unapređenju stanja u oblasti sajber bezbjednosti Crne Gore.

Akcioni plan je donijet za period do kraja 2023. godine, i može se revidirati ukoliko se takva potreba prilikom njegove implementacije pojavi.

Nosioci aktivnosti će na polugodišnjem nivou informisati Savjet za informacionu bezbjednosti o realizaciji aktivnosti iz AP, a na godišenjem nivou Ministarstvo javne uprave, digitalnog društva i medija, i u skladu sa dobijenim preporukama dalje prilagođavati svoje postupanje.

Strateški cilj I:	**Crna Gora u oblasti sajber bezbjednosti posjeduje održiv sistem za efikasno otkrivanje i odbranu od kompleksnih vektora sajber napada i prijetnji**		
Operativni cilj 1	**Unapređenje ljudskih i finansijskih resursa**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**	**Ciljna vrijednost do 2026.**
Procentualno povećanje budžetskih izdvajanja za razvoj sajber kapaciteta.	Nakon usvajanja budžeta za 2022. godinu vrijednost će biti definisana	10% uvećana budžetska izdvajanja u ANB, MO, MJUDDM, MVP, MUP, UP, Forenzičkom centru, DZZTP, CIRT u odnosu na budžetska izdvajanja u 2022. godini	20% uvećana budžetska izdvajanja u ANB, MO, MJUDDM, MUP, UP, MVP, Forenzičkom centru, DZZTP, CIRT u odnosu na budžetska izdvajanja u 2022. godini
Broj zaposlenih u MO, MJUDDM, MUP, MVP, UP, Forenzičkom centru, DZZTP i CIRT-u koji se bave pitanjima sajber bezbjednosti.	35	42	52

Aktivnost koja utiče na realizaciju operativnog cilja 1	Indikator rezultata	Nadležna institucija	Datum početka	Planirani datum završetka	Sredstva planirana za sprovođenje aktivnosti	Izvor finansiranja
1.1. Učešće članova Vlade na sjednicama Savjeta za informacionu bezbjednost	Na najmanje dvije godišnje sjednice Savjeta za informacionu bezbjednost učešće uzeli članovi Vlade.	Savjet za informacionu bezbjednost	I kvartal 2022.	Kontinuirano	Nisu potrebna sredstva	-
1.2. Izrada godišnje Informacije o potrebnim budžetskim sredstvima za unaprjeđenje sajber bezbjednosti.	Vlada je usvojila informacije i podržala kroz zaključke izdvajanje sredstava za unaprijeđenje sajber bezbjednosti	Savjet za informacionu bezbjednost MJUDDM ANB MO DZTP MUP UP Forenzički centar MVP	II kvartal 2022.	Kontinuirano	Nisu potrebna sredstva	-
1.3. Izmjene Pravilnika o unutrašnjoj organizaciji i sistematizaciji radnih mjesta kako bi se obezbijedilo povećanje broja zaposlenih u institucijama obuhvaćenih godišnjom Informacijom planiranom kroz aktivnost 1.2	Izmijenjeni Pravilnici	Institucije prepoznate godišnjom Informacijom o potrebnim budžetskim sredstvima za unaprjeđenje sajber bezbjednosti (aktivnost 1.2)	I kvartal 2023.	II kvartal 2023	Nisu potrebna sredstva	-

1.4. Popunjavanje radnih mjesta u skladu sa izmjenjenim pravilnicima u institucijama obuhvaćenih godišnjom Informacijom planiranom kroz aktivnost 1.2.	Popunjena radna mjesta u skladu sa izmjenjenim pravilnicima	Institucije prepoznate godišnjom Informacijom o potrebnim budžetskim sredstvima za unaprjeđenje sajber bezbjednosti (aktivnost 1.2)	III kvartal 2023.	kontinuirano	60.000,00 € na godišnjem nivou	Budžet

Operativni cilj 2	**Efikasan mehanizam za odgovor na sajber incidente**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**	**Ciljna vrijednost do 2026.**
Procenat uspješno riješenih sajber incidenata prijavljenih CIRT-u, odnosno Agenciji sa sajber bezbjednost	80 %	85 %	90 %
Broj službenika za podršku vojnim operacijama u oblasti sajber bezbjednosti	12	16	20

Aktivnost koja utiče na realizaciju operativnog cilja 2	**Indikator rezultata**	**Nadležna institucija**	**Datum početka**	**Planirani datum završetka**	**Sredstva planirana za sprovođenje aktivnosti**	**Izvor finansiranja**
2.1. Izmjene i dopune Zakona o informacionoj bezbjednosti i Zakona o tajnosti podataka radi stvaranja zakonskih preduslova za formiranje novog tijela – Agencije za sajber bezbjednost	Usvojeni zakoni o izmjenama i dopunama Zakona o informacionoj bezbjednosti i Zakona o tajnosti podataka	MO DZTP MJUDDM	I kvartal 2022.	IV kvartal 2022.	Nisu potrebna sredstva	-

2.2. Izmjene Uredbe o organizaciji i načinu rada državne uprave u pravcu osnivanja novog organa uprave – Agencije za sajber bezbjednost	Usvojena Izmjena Uredbe	MO DZTP MJUDDM	III kvartal 2022	IV kvartal 2022	Nisu potrebna sredstva	-
2.3. Izrada i usvajanje Pravilnika o unutrašnjoj organizaciji i sistematizaciji Agencije za sajber bezbjednost	Usvojen Pravilnik o unutrašnjoj organizaciji i sistematizaciji Agencije za sajber bezbjednost	Agencija za sajber bezbjednost	IV kvartal 2022.	I kvartal 2023.	Nisu potrebna sredstva	-
2.4. Popunjavanje minimum 50% radnih mjesta planiranih u skladu sa Pravilnikom	Popunjeno 50% radnih mjesta u skladu sa Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Agencije za sajber bezbjednost.	Agencija za sajber bezbjednost	II kvartal 2023.	IV kvartal 2023.	*	Budžet
2.5. Nabavka i implementacija tehničke opreme u skladu sa zaključcima iz Informacije o potrebi fomiranja novog organa uprave – Agencije za sajber bezbjednosti koju je usvojila Vlada.	Izvršena nabavka i implementacija tehničke opreme	Agencija za sajber bezbjednost	II kvartal 2023.	IV kvartal 2023.	1.300.000,00€	Budžet
2.6. Izmjena Zakona o informacionoj bezbjednosti u cilju definisanja načina upravljanja kriznim	Izmijenjen Zakon o informacionoj bezbjednosti.	MJUDDM DZTP MO	I kvartal 2022.	IV kvartal 2022.	Nisu potrebna sredstva	-

* Dok se ne realizuje aktivnost 1.7. nije moguće definisati potrebna sredstva za realizaciju aktivnosti 1.8.

situacijama izazvanim sajber prijetnjama.						
2.7. Priprema Pravilnika o upravljanju kriznim situacijama izazvanim sajber prijetnjama.	Usvojen Pravilnik	MJUDDM DZTP MO	I kvartal 2023.	IV kvartal 2023.	Nisu potrebna sredstva	-
2.8. Priprema Pravilnika o bližem načinu uspostavljanja zaštite od računarskih bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema, kao i koordinacije prevencije i zaštite	Usvojen Pravilnik	MJUDDM DZTP	I kvartal 2022	I kvartal 2022	Nisu potrebna sredstva	-
2.9. Formiranje interresornog operativnog tima za koordinaciju odgovora na sajber incidente	Formiran interresorni operativni tim sa koordinaciju odgovora na sajber incidente	MJUDDM Savjet za informacionu bezbjednost	I kvartal 2022.	I kvartal 2022.	20.000,00€ na godišnjem nivou[2]	Budžet
2.10. Učešće na sjednicama Savjeta za informacionu bezbjednost predstavnika privatnog sektora i akademske zajednice	Na najmanje dvije sjednice Savjeta za informacionu bezbjednost učešće uzeli predstavnici privatnog sektora i akademske zajednice.	Savjet za informacionu bezbjednost	I kvartal 2022.	Kontinuirano	Nisu potrebna sredstva	-
2.11. Ažuriranje liste lokalnih CIRT-ova	Ažurirana lista	DZTP	I kvartal 2022.	IV kvartal 2023.	Nisu potrebna sredstva	-

[2] Sredstva za isplatu novčanih naknada po osnovu rada u interresornom operativnom timu snosice institucije čiji zaposleni su određeni za članove u ovom timu.

2.12. Uspostavljanje tehničkih kapaciteta CIRT-a	1. Nabavljena oprema 2. Nabavljeni sistemi 3. Implementirani sistemi	DZTP	II kvartal 2022.	IV kvartal 2023.	300.000,00€	Budžet
2.13. Implementacija mehanizama za zaštitu, monitoring sajber prijetnji, upravljanje ranjivostima, analizu i forenziku sajber incidenata	Implementiran SEIM (eng. Security Event Information System) sistem za monitoring, upravljanje ranjivošću	DZTP	I kvartal 2022.	II kvartal 2023. god	200.000,00€	Budžet
2.14. Opremljena specijalizovana prostorija za forenziku i analitiku	1. Obezbjeđena prostorija 2. Nabavljeno 6 računara 3. Nabavljena kontrola pristupa 4. Instalirana open source rešenja za monitoring	DZTP	I kvartal 2022.	II kvartal 2022.	30.000,00€	Budžet
2.15. Promovisanje sajta CIRT-a	1. Postavljanje banera na sajtovima ANB, MUP, UP, MPNKS, MVP, MO, MZ, sajtu Zajednice opština Crne Gore, sajtovima lokalnih samouprava, sajtovima obrazovnih ustanova u Crnoj Gori, sajtu PKCG. 2. Promovisanje na društvenim mrežama	DZTP	II kvartal 2022.	III kvartal 2023.	1.000,00€ godišnje	Budžet

2.16. Redovno planiranje i ažuriranje Registra rizika	Ažuriran Registar rizika sa rizicima iz oblasti sajber bezbjednosti	ANB MJUDDM MO MUP MVP DZTP	2022.	kontinuirano	Nisu potrebna sredstva	-
2.17. Verifikovan predlog novog organizacionog okvira koji će biti integrisan u Sistematizaciju MO i Organizacijsko-formacijskoj strukturi VCG (OFS), sa ciljem unaprjeđenja sajber komandovanja u domenu vojnih operacija.	Usvojen predlog novog organizacionog okvira i integrisan u Sistematiziju i OFS, u skladu sa NATO ciljevima sposobnosti.	MO i VCG	I kvartal 2022.	IV kvartal 2022.	Nisu potrebna sredstva	-
2.18. Nabavka i implementacija novih tehnoloških rješenja neophodnih za zaštitu statičkih i pokretnih informaciono-komunikacionih sistema MO i VCG, u cilju sajber podrške vojnim operacijama.	Izvršena nabavka i implementacija hardvera i softvera koji je neophodan za funkcionisanje Bezbjednosno-operativnog centra MO i VCG (SOC MO i VCG) i mobilnog CIRT-a (Deployable CIRT).	MO	II kvartal 2022.	IV kvartal 2023.	300.000,00€	Budžet
2.19. Nastavak programa sticanja ekspertskih vještina iz oblasti sajber odbrane	Obezbijeđen trening program za minimum 12 sajber eksperta iz MO i VCG	MO	II kvartal 2022.	IV kvartal 2023.	30.000,00€	Budžet/Donacije

2.20. Formiranje vojne rezerve za sveobuhvatnu sajber odbranu.	Alocirana organizaciona struktura za sajber rezervu, definisani zadaci, kao i akcioni plan za dvije godine od dana njegovog formiranja.	MO	I kvartal 2023.	IV kvartal 2023.	15.000,00€	Budžet
2.21. Izvođenje sveobuhvatnih sajber vježbi	Izvedena minimum jedna sajber vježba (tehničkog ili koordinacionog karaktera).	MO i VCG u saradnji s zainteresovanim stranama	I kvartal 2023.	IV kvartal 2023.	10.000,00€	Budžet
Operativni cilj 3	**Unapređenje mjera prevencije i edukacije o sajber bezbjednosti**					
Indikator učinka	**Početna vrijednost**		**Ciljna vrijednost do 2024.**		**Ciljna vrijednost do 2026.**	
Broj informacionih sistema nad kojima je izvršeno preventivno penetraciono testiranje	n/a		10		30	
Procenat zaposlenih javnih službenika koji su prošli obuku na temu sajber bezbjednosti	1%		10%		15%	
Aktivnost koja utiče na realizaciju operativnog cilja 3	**Indikator rezultata**	**Nadležna institucija**	**Datum početka**	**Planirani datum završetka**	**Sredstva planirana za sprovođenje aktivnosti**	**Izvor finansiranja**
3.1. Izrada vodiča za osnovne tehnološke i operativne mjere za prevenciju sajber prijetnji.	Izrađen vodič za osnove tehnološke i operativne mjere za prevenciju sajber prijetnji, sa kojim su upoznate sve zainteresovane strane	Agencija za sajber bezbjednost Savjet za informacionu bezbjednost	I kvartal 2023.	IV kvartal 2023.	10.000,00 €	Donacije

3.2. Izrada informacije o ključnim institucijama i IT sistemima u kojima neophodno uraditi penetraciono testiranje (PEN test)	Izrađena informacija	MJUDDM DZTP	II kvartal 2022.	IV kvartal 2022.	Nisu potrebna sredstva	-
3.3. PEN testiranje u institucijama, odnosno na sistemima prepoznatim u informaciji iz 5.2.	Realizovana PEN testiranja na 10 informacionih sistema	MJUDDM DTZP	I kvartal 2023.	IV kvartal 2023.	50.000,00€	Budžet
3.4. Nabavka opreme u cilju unapređenje prevencije i odbrane internet mreže i sertifikacije sistema za razmjenu klasifikovanih podataka do nivoa INTERNO, Ministarstva vanjskih poslova i Diplomatsko-konzularnih predstavništava (DKP) Crne Gore u svijetu	Zaštita komunikacione mreže između MVP-a i DKP (ukupno 38 predstvaništava) kao i njihova sertifikacija u skladu sa standardom ISO:27001, koji bi se koristili za razmjenu klasifikovanih podataka MVP-DKP do nivoa INTERNO.	MVP	I kvartal 2022.	IV kvartal 2023.	400.000,00€	Budžet, donacije
3.5. Izrada analize potrebnih sajber obuka u javnom sektoru	Izrađena analiza potrebnih sajber obuka na godišnjem nivou.	DZTP MJUDDM UzK	I kvartal 2022.	II kvartal 2022.	Nisu potrebna sredstva	
3.6. Donošenje Programa stručnog osposobljavanja i usavršavanja državnih i lokalnih službenika i namještenika u oblasti sajber bezbjednosti	Donijet Program	MJUDDM - UzK	II kvartal 2022.	IV kvartal 2022.	Nisu potrebna sredstva	-
3.7. Realizacija obuka prema Programu stručnog	Realizovano najmanje 4 obuke na	UzK	I kvartal 2023.	IV kvartal 2023.	2.000,00 €	Budžet

osposobljavanja i usavršavanja državnih i lokalnih službenika i namještenika	lokalnom i centralnom nivou i obuhvaćeno namjanje 100 zaposlenih.					
3.8. Izrada analize potrebnih sajber obuka u privatnom sektoru	Izrađena analiza potrebnih sajber obuka na godišnjem nivou.	DZTP MJUDDM	I kvartal 2022.	II kvartal 2022.	Nisu potrebna sredstva	-
3.9. Organizacija obuka za zaposlene na poslovima informacione sigurnosti u privatnom sektoru	Realizovane najmanje dvije obuke i obuhvaćeno minimum 20 zaposlenih na poslovima informacione bezbjednosti u privatnom sektoru	DZTP MUP MJUDDM	I kvartal 2022.	IV kvartal 2023.	Nisu potrebna sredstva	-
3.10. Donošenje novog ili izmjena i dopuna postojećeg pravnog akta kojim bi se predvidjela obaveza za zaposlene u javnom sektoru, a koji su korisnici e-mail servisa MJUDDM, da polože online test o osnovama bezbjednog korišćenja ICT-a, a prije dobijanja pristupa IT sistemima javne uprave u nadležnosti MJUDDM.	Donijet novi ili izmjenjen i dopunjen postojeći pravni akt.	MJUDDM	I kvartal 2022.	III kvartal 2023.	Nisu potrebna sredstva	-

3.11. Donošenje on-line obuke o sigurnom korišćenju informaciono - komunikacionih tehnologija u javnoj upravi, sa online testom, za zaposlene u javnoj upravi, a koji su korisnici e-mail servisa MJUDDM	Definisana online obuka, sa online testom	MJUDDM DZTP	III kvartal 2022.	IV kvartal 2022.	10.000,00 €	Donacija
3.12. Implementacija online obuka o sigurnom korišćenju ICT u javnoj upravi, sa testom od strane zaposlenih u javnoj upravi, a koji su korisnici e-mail servisa MJUDDM.	Svi zaposleni u javnoj upravi, a koji su korisnici e-mail servisa MJUDDM prošli online obuku, i položili online test.	MJUDDM	I kvartal 2023.	Kontinuirano	Nisu potrebna sredstva	-
3.13. Podizanje svijesti o bezbjednom korišćenju interneta	1. Izrada i promovisanje minimum po jedne brošure/publikacije, pisanje članaka i gostovanje u emisijama u edukativne svrhe; 2. Ažuriranje materijala na portalu CIRT-a iz oblasti sajber bezbjednosti. 3. Realizovana minimum jedna promotivna aktivnost/kampanja	DZTP MPNKS	I kvartal 2022.	IV kvartal 2023.	14.000,00€ (godišnje)	Budžet

	tokom mjeseca sajber bezbjednosti.					
3.14. Organizovanje specijalizovnog treninga iz oblasti sajber diplomatije za visoki-rukovodi kadar MVP, ANB, MJUDDM i MO	Organizovana minimum dva specijalizovana treninga za minimum 10 predstavnika navedenih resora na pozicijama visokog rukovodnog kadra.	MJUDDM	III kvartal 2022.	IV kvartal 2023.	10.000,00€	Donacija
3.15. Unapređenje sajta CIRT-a i platforma za razmjenu informacija	1. Sajt CIRT-a sadrži objedinjene edukativne materijale i informacije o dostupnim programima i obukama o sajber bezbjednosti 2. Operativna platforma za razmjenu informacija	DZTP	II kvartal 2022.	III kvartal 2023.	30.000,00€ za 2023.	Budžet/donacije

Operativni cilj 4	**Poboljšanje odgovora na sajber kriminal**		
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**	**Ciljna vrijednost do 2026.**
Procenat procesuiranih krivičnih djela u oblasti visokotehnološkog kriminala i krivičnih djela učinjenih upotrebom informaciono komunikacionih tehnologija	25%	30 %	35 %

Aktivnost koja utiče na realizaciju operativnog cilja 4	Indikator rezultata	Nadležna institucija	Datum početka	Planirani datum završetka	Sredstva planirana za sprovođenje aktivnosti	Izvor finansiranja
4.1. Izmjene i dopune Zakona o krivičnom postupku	- Formirana Radna grupa za izmjenu i dopunu Zakona o krivičnom postupku; - Donijet Predlog Zakona o izmjenama i dopunama Zakona o krivičnom postupku;	UP MPLJMP	II kvartal 2022.	III kvartal 2023.	Nisu potrebna sredstva	-
4.2. Izmjene Krivičnog zakonika Crne Gore kako bi se prepoznalo i sankcionisalo krivično djelo kreiranja i širenja lažnih vijesti i dezinformacija na internetu	- Formirana Radna grupa; - Donijet Predlog izmjena Krivičnog zakonika Crne Gore	UP MPLJMP	II kvartal 2022.	III kvartal 2023.	Nisu potrebna sredstva	-
4.3. Izmjena postojećeg Zakona o elektronskim komunikacijama, radi prepoznavanja tehničkih mogućnosti za gašenje/blokiranje subdomena, odnosno, onemogućavanje pristupa stranicama na internetu, a sa kojih se vrše krivična djela ili koja krše odredbe Krivičnog zakonika Crne Gore.	- Formirana Radna grupa; - Donijet Predlog izmjena.	MER UP	II kvartal 2022.	III kvartal 2023.	Nisu potrebna sredstva	-

4.4. Organizovanje obuka za službenike MUP, UP i nosioce pravosudnih funkcija	Organizovane minimum dvije obuke godišnje	MUP UP Centar za obuku u sudstvu i državnom tužilaštvu	I kvartal 2022.	IV kvartal 2023.	10.000,00€	Budžet/donacije
Operativni cilj 5	**Osnažen i harmonizovan sistem zaštite podataka.**					
Indikator učinka	**Početna vrijednost**	**Ciljna vrijednost do 2024.**			**Ciljna vrijednost do 2026.**	
Broj organizacija i njihovih komunikaciono informacionih sistema usklađenih sa standardima informacione bezbjednosti i sertifikovanih za obradu tajnih podataka	3	5			6	
Aktivnost koja utiče na realizaciju operativnog cilja 5	**Indikator rezultata**	**Nadležna institucija**	**Datum početka**	**Planirani datum završetka**	**Sredstva planirana za sprovođenje aktivnosti**	**Izvor finansiranja**
5.1 Unapređenje propisa neophodnih za sprovođenje sertifikacije komunikaciono-informacionih sistema za obradu tajnih podataka	Usvojene unapređene verzije Uredbe o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka i Pravilnika o certifikovanju komunikaciono-informacionih sistema i procesa za obradu tajnih podataka	MO DZTP	I kvartal 2022.	III kvartal 2022.	Nisu potrebna sredstva	-

5.2 Identifikacija komunikaciono-informacionih sistema (KIS) za obradu tajnih podataka koje je neophodno sertifikovati	Identifikovane institucije koje imaju potrebu za uspostavljanje sistema za obradu tajnih podataka i napraviljena lista	DZTP	II kvartal 2022.	III kvartal 2022.	Nisu potrebna dodatna sredstva	-
5.3 Obuke od značaja za usklađivanje i reviziju poslovanja u skladu sa standardima informacione bezbjednosti (sertifikovani implementator, interni revizor, eksterni revizor)	1. Utvrđena lista službenika koji trebaju da prođu sertifikaciju i obuke 2. Izrađen plan sertifikacije i obuka	1. MJUDDM 2. Savjet za informacionu bezbjednost	II kvartal 2022.	III kvartal 2023.	Nisu potrebna dodatna sredstva	-
5.4 Usklađivanje organa državne uprave i njihovih komunikaciono-informacionih sistema sa standardima informacione bezbjednosti	1. Utvrđena lista IKT sistema u organima državne uprave koji imaju usglašene sisteme sa standradima informacione bezbjednosti 2. Povećanje za 10% godišnje u odnosu na listu	MJUDDM	I kvartal 2022.	IV kvartal 2023.	Nisu potrebna dodatna sredstva	-
5.5. Usklađivanje Zakona o zaštiti podataka o ličnosti sa rješenjima iz Opšte uredbe o zaštiti ličnih podataka – GDPR 2016/679	Usvojen Zakon o izmjenama i dopunama Zakona o zaštiti podataka o ličnosti.	MUP	II kvartal 2022.	IV kvartal 2023.	Nisu potrebna sredstva	-
Operativni cilj 6	**Razvoj i unapređenje saradnje s nacionalnim i međunarodnim partnerima**					

Indikator učinka	Početna vrijednost	Ciljna vrijednost do 2024.	Ciljna vrijednost do 2026.
Procenat međunarodnnih konferencija, obuka i vježbi na kojima je Crna Gora uzela učešće	60 %	70 %	75%

Aktivnost koja utiče na realizaciju operativnog cilja 6	Indikator rezultata	Nadležna institucija	Datum početka	Planirani datum završetka	Sredstva planirana za sprovođenje aktivnosti	Izvor finansiranja
6.1. Priprema Memoranduma o saradnji s privatnim sektorom	Usaglašen tekst najmanje dva Memoranduma o saradnji	MJUDDM DZTP MO	II kvartal 2022.	IV kvartal 2023.	Nisu potrebna sredstva	-
6.2. Potpisivanje Memoranduma o saradnji s privatnim sektorom	Potipisana najmanje dva MoS	MJUDDM DZTP MO	III kvartal 2022.	IV kvartal 2023.	Nisu potrebna sredstva	-
6.3. Formiranje zajednice sajber eksperata iz javnog i privatnog sektora	Formirana mreža sajber eksperata iz privatnog i javnog sektora, kao i akademske zajednice, sa ciljem razmjene informacija, znanja, dobrih praksi i organizovanja zajedničkih aktivnosti.	DZTP	I kvartal 2023.	IV kvartal 2023.	Nisu potrebna sredstva	-
6.4. Učešće na vježbama u organizciji NATO, EU,	Učešće minimum 15 predstavnika Crne	ANB MO	I kvartal 2022.	Kontinuirano	50.000,00€	Budžet

OEBS-a i drugih međunarodnih partnera.	Gore na minimum dvije godišnje međunarodne vježbe (Cyber Coalition, Locked Shiled; CMX, i sl).	MJUDDM MUP				
6.5. Inteziviranje participacije u NATO CCD COE	1. Učešće na minimum dvije aktivnosti u organizaciji CCD COE. 2. Shodno MoU između Ministarstva odbrane i CCD COE, upućen predstavnik Crne Gore na rad u CCD COE.	MO	I kvartal 2022.	IV kvartal 2023.	170.000,00€ (dvije godine)	Budžet
6.6. Povećan angažman Crne Gore u okviru platformi međunarodnih organizacija (OEBS; SE i sl) za razmjenu informacija, znanja i dobrih praksi.	Minimum 8 događaja, predavanja i obuka u okviru platformi međunarodnih organizacija na kojima predstavnici Crne Gore uzeli učešće.	ANB MO MJUDDM MUP	I kvartal 2022.	IV kvartal 2023.	15.000,00€	Budžet/donacije
6.7. Inteziviranje bilateralnih aktivnosti na polju sajber bezbjednosti	Minimum dvije institucije su planom bilateralne saradnje konkretizovali minimum 1 aktivnost koja će doprinijeti nadogradnji iskustva, znanja, razmjeni informacija i slično u	ANB MO MJUDDM MUP MVP MPNKS MPLJMP UP	I kvartal 2022.	IV kvartal 2023.	Nisu potrebna sredstva	-

	oblasti sajber bezbjednosti					
Operativni cilj 7:	**Uspostavljen sistem zaštite kritične informatičke infrastrukture**					
Indikator učinka	**Početna vrijednost**		**Ciljna vrijednost do 2024.**		**Ciljna vrijednost do 2026.**	
Procenat kritičnih informacionih sistema koji imaju implementirane sve zakonski propisane tehničke mjere zaštite	n/a		30%		85%	
Broj zaposlenih službenika u CIRT-u	6 službenika		16 službenika		24 službenika	
Aktivnost koja utiče na realizaciju operativnog cilja 7	**Indikator rezultata**	**Nadležna institucija**	**Datum početka**	**Planirani datum završetka**	**Sredstva planirana za sprovođenje aktivnosti**	**Izvor finansiranja**
7.1. Izmjena Zakona o informacionoj bezbjednosti i Zakona o određivanju i zaštiti kritične infrastrukture	Donijeti zakoni o izmjeni Zakona o informacionoj bezbjednosti i Zakona o određivanju i zaštiti kritične infrastrukture kako bi se kroz jedno zakonsko rješenje tretiralo pitanje zaštite kritične i kritične informatičke infrastrukture	MUP MJUDDM	I kvartal 2022.	IV kvartal 2022.	Nisu potrebna sredstva	-

7.2. Utvrđivanje predloga liste kritične informatičke infrastrukture	Utvrđen predlog liste kritične informatičke infrastrukture	MJUDDM	I kvartal 2022.	IV kvartal 2022.	Nisu potrebna sredstva	-
7.3. Određivanje kritične informatičke infrastrukture od strane Vlade Crne Gore na osnovu objedinjenih međusektorskih i sektorskih predloga	Određena kritična informatička infrastruktura od strane Vlade Crne Gore u skladu s Zakonom o utvrđivanju i zaštiti kritične infrastrukture	MUP	IV kvartal 2022.	I kvartal 2023.	Nisu potrebna sredstva	-
7.4 Izrada analize o potrebi donošenja podzakonskog pravnog akta o bližem načinu zaštite kritične informatičke infrastrukture	Izrađena analiza.	MJUDDM MUP	I kvartal 2023.	IV kvartal 2023.	Nisu potrebna sredstva	-
7.5. Jačanje administrativnih kapaciteta CIRT-a	Zaposleno 6 novih službenika	DZTP	I kvartal 2022.	III kvartal 2023.	50.000,00€	Budžet
7.6. Uspostavljanje bezbjednosnog operativnog centra (CIRT SOC-a) u cilju monitoringa kritične informatičke infrastrukture	Nabavljena osnovna oprema za uspostavljanje CIRT SOC-a 1. obezbijeđen prostor oko 50m2 2. video zid 3. 6 računara 4. SIEM rešenje 5. nabavljena oprema za kontrolu pristupa	DZTP	I kvartal 2022.	III kvartal 2023.	300.000,00€	Budžet

	6. opremljena prostorija 7. nabavljeno i implemetirano SIEM rešenje					
7.7. Organizovanje obuke za vlasnike KII	Organizovana minimum jedna obuka godišnje za vlasnike KII.	DZTP MJUDDM	I kvartal 2022.	IV kvartal 2023.	50.000,00€	Budžet/donacije
7.8. Učešće u radu koordinacionog tijela za zaštitu kritične infrastrukture.	Imenovan predstavnik MJUDDM i CIRT-a u koordinacionom tijelu za zaštitu KI.	MUP	I kvartal 2022.	III kvartal 2022.	Nisu potrebna sredstva	-

Napomene:

Prilikom izrade Akcionog plana uzete su u obzir aktivnosti iz Akcionog plana za implementaciju prethodne Strategije, za 2021. godinu koje su se realizovale u kontinuitetu, kao i djelimično realizovane i nerealizovane aktivnosti, na način što su inkorporirane u novi Akcioni plan.

Kada je riječ o sredstvima planiranim za sprovođenje aktivnosti, za one aktivnosti gdje neće biti potrebno obezbjeđivanje dodatnih sredstava, stavljena je oznaka „nisu potrebna sredstva“.

U koloni koja se odnosi na izvore finansiranja, pored sredstava koja će biti obezbjeđena kroz Budžet, jedan dio sredstava biće obezbjeđen kroz donatorska sredstva tradicionalnih partnera – Ambasade Velike Britanije u Crnoj Gori, Ambasade SAD, kao i međunarodnih organizacija – SE, OEBS i UN.

Aktivnosti koje se odnose na obrazovne i nastavne programe iz oblasti sajber bezbjednosti nijesu dio Akcionog plana iz razloga što su iste dio Strategije za digitalizaciju obrazovnog sistema za period 2022-2027. godine i akcionog plana za njeno sprovođenje.