VLADA CRNE GORE
MINISTARSTVO JAVNE UPRAVE,
DIGITALNOG DRUŠTVA I MEDIJA

N a c r t

STRATEGIJA SAJBER BEZBJEDNOSTI CRNE GORE 2022-2026.

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:

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].

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.

[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.

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, b) preduzela brojne strateške aktivnosti na planu usklađivanja nacionalnog zakonodavstva kako bi isto bilo na liniji savremenih i međunarodnih 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.

**** 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.***

[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

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[6], kao i smjernice iz Metodologije razvijanja politika, izrade i praćenja sprovođenja strateških dokumenata[7].

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[8].

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 koji je trajao 20 dana, kao i međunarodnim strateškim partnerima koji pružaju ekspertsku, tehničku i finansijsku podršku razvoju sajber bezbjednosti, čime je ispoštovan i ***princip transparentnosti***.

2.1. 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 digilatlizacija društva otvara vrata zlonamjernim akterima,

[6] Više na: https://www.gov.me/dokumenta/23c216b2-3eb7-453c-b0a7-3cdae9e9742e
[7] Više na: https://javnepolitike.me/wp-content/uploads/2020/11/Metodologija-razvijanja-politika-draft3-preview-22SEP20.pdf
[8] 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

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[9].

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 bezbjednosti 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.

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[10].

Prema izvještajima Uprave za statistiku – Monstata o upotrebi informaciono-komunikacionih tehnologija u preduzećima i domaćinstvima za 2020. godinu[11], 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

[9] 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.

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

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

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.

Osnovu za analizu stanja činili su:

- ciljevi definisani prethodnim strategijama sajber bezbjedosti Crne Gore[12],
- izvještaji o njihovoj implementaciji,
- aktuelni zakonodavni okvir u ovoj oblasti,
- konsultacije sa zainteresovanom javnošću,
- preporuke dobijene od eksperata Savjeta Evrope i Svjetske banke, kao i međunarodnih partnera.

2.2. Lekcije koje smo naučili

- Monitoring sprovođenja Strategije i pratećih AP mora biti unaprijeđen kako bi omogućio pravovremeno identifikovanje prepreka na planu ispunjavanja planiranih aktivnosti u predviđenim rokovima i pružanje preporuka za njihovo prevazilaženje.
- Evaluacija Strategije treba da bude realizovana ne samo na kraju njenog životnog ciklusa, već i tokom njenog sprovođenja kako bi se provjerila aktuelnost i relevantnost postavljenih ciljeva i eventualno dala preporuka u pravcu ažuriranja Strategije i/ili AP ako izmijenjene okolnosti na nacionalnom i međunarodnom planu to zahtijevaju.
- Strateški ciljevi da bi bili održivi i ostvarljivi moraju biti postavljeni u skladu sa trendovima rasta sajber prijetnji i izazova, aktuelnom finansijskom situacijom, procjenom budućih finansijskih kapaciteta i resursa, razvojem novih tehnologija, prvenstveno 5G, kao i pretpostavkama o daljem toku COVID19 pandemije.

[12] Strategija sajber bezbjednosti Crne Gore 2013-2017: https://www.gov.me/dokumenta/ecc14807-fb3b-472f-8a9a-13de450ce0ed i Strategija sajber bezbjednosti 2018-2021: https://wapi.gov.me/download-preview/fa24a8c6-2241-4d6f-9297-328636b157e5?version=1.0

- Ključni problemi pri ostvarivanju zacrtanih ciljeva prethodnih strategija bili su finansijske prirode, odnosno evidentirano je nedovoljno alociranje sredstava nadležnim resorima za jačanje kapaciteta za sajber odbranu kroz snaženje operativnih, ljudskih i tehničkih resursa.
- Interresorna saradnja treba da bude dodatno unaprijeđena kroz umrežavanje i kontinuirano usavršavanje službenika koji se bave pitanjima sajber bezbjednosti i/ili sprovođenjem aktivnosti iz AP, na svim nivoima, kako bi se smanjio „odliv“ stručnog kadra.
- Podizanje svijesti kod visoko-rukovodećeg kadra kako na nivou države, tako i ključnih državnih i privrednih institucija i organizacija o neophodnosti unapređenja sajber bezbjednosti u svim sferama i na svim pozicijama društva i njegove djelatnosti i razvoja.
- Uzimajući u obzir da Crna Gora spada u red zemalja sa manjom populacijom, što ukazuje i na limitiranu raspoloživost ljudskih resursa, potrebno je s jedne strane osmisliti modele interresornog djelovanja, kao i modele takve vrste saradnje u domenu privatno-javnog partnerstva.
- Pitanje širenja svijesti među građanima, kao najslabijim karikama u lancu sajber bezbjednosti, o važnosti sigurnog korišćenja informaciono-komunikacione tehnologije i dalje je aktuelno.
- Na osnovu analize trenutne organizacione strukture u oblasti sajber bezbjednosti, kao i analize položaja, kapaciteta i nadležnosti CIRT.ME, prepoznata je potreba formiranja posebnog organa nadležnog za sajber bezbjednost.
- Oblast zaštite kritične informatičke infrastrukture (KII) mora biti dodatno unaprijeđena, kroz a) utvrđivanje osnovnih mjera zaštite KII od sajber prijetnji, i b) preciziranje tijela koja će vršiti nadzor nad primjenom propisanih mjera.
- Osim pojedinačnih registra rizika po institucijama, nameće se potreba postavljanja osnovnih standarda za upravljanje rizicima, posebno u vezi sa zaštitom KII.
- Prethodnim strategijama, odnosno akcionim planovima realizovane su određene aktivnosti koje su bile usmjerene na izgradnju i dalje snaženje kapaciteta organa za sprovođenje zakona u oblasti sajber kriminala, međutim praksa je pokazala da pitanja eventualne izmjene pojedinih zakonskih rješenja, daljeg snaženja kapaciteta i saradnje organa za sprovođenje zakona i pravosuđa, kao i borbe protiv sajber kriminala, trebaju biti dodatno obrađena novom Strategijom.
- Edukacija o sajber bezbjednosti i sigurnom korišćenju ICT-a na različitim nivoima i u prilagođenim formama zavisno od ciljane javnosti, mora biti temelj strateškog odgovora na sajber izazove i prijetnje.
- Upravljanje kriznim situacijama mora biti prepoznato Strategijom na način da će se predvidjeti nadležni resori za sprovođenje analize postojećeg pravnog okvira za upravljanje u vanrednim situacijama kako bi se utvrdilo da li je potrebna njegova izmjena i/ili dopuna kako bi uključila i planiranje upravljanja kriznim situacijama izazvanim (zlo)upotrebom ICT i/ili sajber napadima u i/ili izvan Crne Gore.
- Međunarodna saradnja, kao i saradnja sa privatnim sektorom kroz javno-privatna partnerstva, akademskom zajednicom i civilnim sektorom mora biti dodatno unaprijeđena.

III VIZIJA, STRATEŠKI I OPERATIVNI CILJEVI

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

Vizija:

- Građani, operateri 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, utvrđeno je pet strateških ciljeva. Strateški ciljevi su utvrđeni analizom nedostataka i nedorečenosti iz prethodnog devetogodišnjeg perioda strateškog pristupa pitanju sajber bezbjednosti u Crnoj Gori. Kao takvi, predstavljaju namjeru da se uočeni izazovi prevaziđu i da se na izmijenjen sajber prostor i dijapazon sajber prijetnji po nacionalnu bezbjednost da rapidan i adekvatan odgovor.

Strateški i operativni ciljevi:

Strateški cilj 1: Unaprijeđeni kapaciteti za sajber odbranu i sistem upravljanja kriznim situacijama izazvanim sajber napadima/incidentima širih razmjera.

Operativni cilj 1*: Jačanje uticaja na najvećem upravljačkom nivou, u cilju obezbjeđivanja optimalnih finansijskih, organizacionih i ljudskih resursa za razvoj sajber kapaciteta.*
Operativni cilj 2*: Definisanje i uspostavljanje novog i održivog tijela za sajber bezbjednost na nacionalnom niovu.*
Operativni cilj 3*: Unaprjeđenje mehanizama za odgovor na incidente.*
Operativni cilj 4: *Nastavak razvoja vojnih sajber kapaciteta u cilju ispunjenja nacionalnih i NATO odbrambenih sposobnosti.*
Operativni cilj 5*: Definisanje osnovnih tehnoloških i operativnih principa za prevenciju sajber prijetnji i smanjenje rizika od istih.*
Operativni cilj 6: *Uspostavljanje baze talenata i volontera koji se bave sajber bezbjednošću.*
Operativni cilj 7*: Izvršena analiza i nadgradnja postojećeg sistema upravljanja kriznim situacijama u Crnoj Gori.*

Strateški cilj 2: Uspostavljen sistem zaštite kritične informatičke infrastrukture.

Operativni cilj 1: *Izmjena i dopuna zakonskih rješenja u oblasti zaštite kritične informatičke infrastrukture.*
Operativni cilj 2: *Donošenje liste kritične informaticke infrastrukture.*
Operativni cilj 3: *Proširenje kadrovskih kapaciteta CIRT.ME i nabavka tehničke opreme sa ciljem uspostavljanja zaštite KII.*
Operativni cilj 4: *Usvojen set minimalnih tehnoloških i operativnih mjera koje su neophodne za zaštitu KII.*
Operativni cilj 5: *Unaprjeđena koordinacija u okviru javnog i privatnog sektora u cilju zaštite KII.*
Operativni cilj 5: *Uspostavljanje koordinacionog tijela za zaštitu kritične infrastrukture.*

Strateški cilj 3: Osnažen odgovor na sajber kriminal i harmonizovan sistem zaštite podataka.

Operativni cilj 1: *Izmjena i dopuna zakonskih rješenja u oblasti sajber kriminala.*
Operativni cilj 2: *Jačanje kapaciteta Uprave policije za odgovor na sajber kriminal.*
Operativni cilj 3: *Unapređenje procesa edukacije za zaposlene Ministarstva unutrašnjih poslova, Uprave policije i nosilaca pravosudnih funkcija.*
Operativni cilj 4*: Usklađen zakonodavni okvir sa Opštom uredbom Evropske unije o zaštiti podataka o ličnosti (GDPR).*

Strateški cilj 4: Unaprijeđen proces edukacije u oblasti sajber bezbjednosti u javnom i privatnom sektoru.

Operativni cilj 1: *Implementacija programa obrazovanja i obuka o sajber bezbjednosti i sigurnom korišćenju informaciono-komunikacionih tehnologija na svim nivoima obrazovanja.*
Operativni cilj 2: *Centralizacija i promocija edukativnih materijala i informacija o dostupnim programima i obukama.*
Operativni cilj 3: *Usvajanje osnovnih smjernica za sticanje i nadogradnju sajber vještina u javnom i privatnom sektoru.*
Operativni cilj 4: *Realizacija programa obuka za zaposlene u javnom i privatnom sektoru o sajber bezbjednosti.*

Strateški cilj 5: Ojačana javno-privatna partnerstva i međunarodna saradnja.

Operativni cilj 1: *Razvijanje novih institucionalnih i tematskih javno-privatnih partnerstava.*
Operativni cilj 2: *Unaprijeđeni i diversifikovani kanali komunikacije sa strateškim međunarodnim partnerima.*

3.1. Kapaciteti sajber odbrane i upravljanja kriznim situacijama

a) Kapaciteti sajber odbrane

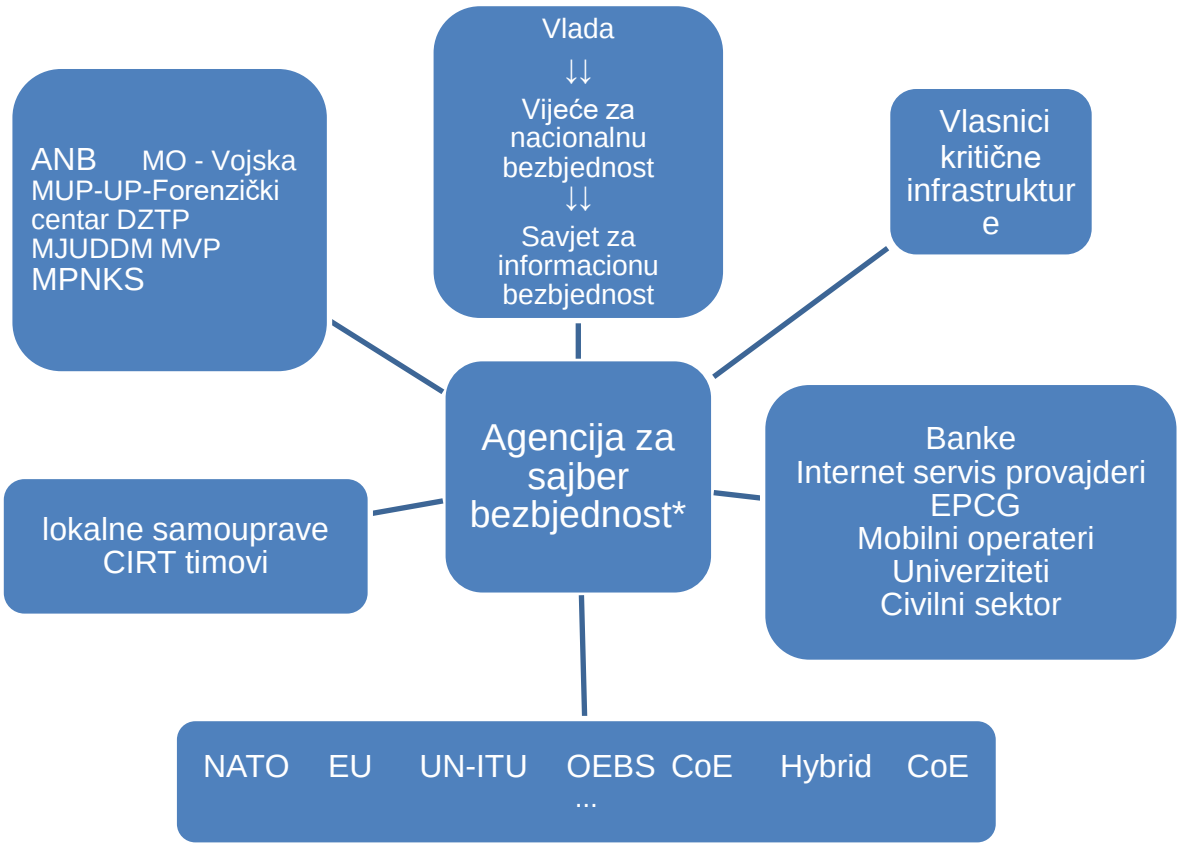
U eri digitalizacije koja sa sobom donosi brojne ekonomske i društvene benefite, drugu stranu „medalje“ predstavljaju sajber rizici. Stoga, osiguranje sajber prostora kroz aktivnosti usmjerene ka izgradnji kapaciteta za sajber odbranu postaje *conditio sine qua non* uspješnog procesa digitalizacije.

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 odbranu, uz navođenje operativnih ciljeva iz njihovih domena čija realizacija će imati prioritet u radu tokom narednog petogodišnjeg perioda, kako bi se na kraju ciklusa Strategije dostigao i postavljeni strateški cilj.

Strateški cilj 1: Unaprijeđeni kapaciteti za sajber odbranu i sistem upravljanja kriznim situacijama izazvanim sajber napadima/incidentima širih razmjera.

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.[13]

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 .me domenu, tj. 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.

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

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

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 za saber bezbjednost u okviru koga bi funkcionisao CIRT.ME.

Direkcija za zaštitu tajnih podataka

Direkcija će i u narednom periodu nastaviti da 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.

Shodno zadanim ciljevima i akcionim planovima prethodne Strategije Agencija je realizovala sljedeće aktivnosti:

- Agencija je vršila planiranje budžetskih sredstava opredijeljenih za sajber bezbjednost na godišnjem nivou.
- U organizacionoj strukturi Agencije su opredijeljena radna mjesta koja pokrivaju oblast sajber bezbjednosti kako kroz tehnički dio odgovora na incidentne situacije tako i analitičku obradu podataka.
- Radni tim je izvršio analizu rizika i unaprijeđen je Registar rizika sa predlozima za reakciju i kontrolne mehanizme.
- U prethodnom periodu Agencija je intezivno radila na jačanju tehničkih kapaciteta u oblasti sajber bezbjednost, izvršena je nabavka i implementacija novih tehničkih sredstava koja su doprinijela boljoj zaštiti i bezbjednosti IK sistema Agencije.
- Tokom prethodnih godina službenici Agencije pohađali su više obuka, konferencija, seminara i drugih vidova edukacije iz oblasti sajber bezbjednosti. Službenici Agencije su imali redovne obuke na temu “security awareness”
- Kako bi na što bolji i efikasniji način odgovorili na incidentne situacije, Agencija je kontinuirano održavala kvalitetnu saradnju i razmjenu informacija sa ključnim institucijama na polju sajber bezbjednosti, kako u javnom tako i privatnom sektoru. Aktivno je učestvovala u rješavanju incidentnih situacija, kroz pružanje pomoći kako u tehničkim kapacitetima tako i u profesionalnim i stručnim.
- Predstavnik Agencije u Savjetu za informacionu bezbjednost je aktivno učestvovao u procesu inteziviranja i unapređenja saradnje između ključnih institucija.
- Agencija u kontinuitetu radila na unapređenju prostorija, računarske opreme i sistema za prenos, obradu i čuvanje tajnih podataka označenih stepenima tajnosti -“Povjerljivo”, “Tajno” i “Strogo Tajno”.
- Agencija je u kontinuitetu ostvarivala uspješnu saradnju sa institucijama i službama partnerskih zemalja na polju sajber bezbjednosti koja podrazumijeva obostranu razmjenu informacija, podataka i iskustava. Službenici Agencije su bili redovni učesnici na konferencijima i seminarima u organizaciji OEBS-a i NATO-a.

Podizanje svjesnosti o značaju sajber bezbjednosti kod menadžmenta i donosioca odluka, kao i kod ne-tehničkog osoblja je bio najveći izazov, prevashodno kako bi se opredijelila finansijska sredstva potrebna za unapređenje kadrovskog i tehničkog potencijala.

Usvajanje i implementacija međunarodnih standarda iz oblasti sajbera je bila neophodnost obzirom na obaveze Agencije koje su proizašle nakon pristupanja Crne Gore NATO-u.

Određeni ciljevi proistekli iz akcionih planova prethonih strategija nijesu realizovani iz sledećih razloga:

- Kašnjenje usvajanja budžeta za 2021. se negativno odrazilo na aktivnosti planiranja i trošenja opredijeljenih sredstava.
- Zbog Covid 19 pandemije obim međuinstitucionalne saradnje u vidu zajedničkih programa obuke je bio na nižem nivou nego prethodnih godina.

Agencija za nacionalnu bezbjednost je u sklopu svoje nadležnosti i definisanih obaveza Akcionim planom Strategije sajber bezbjednosti, za 2021. godinu, a u skladu

sa trenutnom situacijom i realizovanim aktivnostima drugih nosilaca aktivnosti, realizovala većinu planiranih ciljeva i nastaviće da kontinuirano radi na ostvarivanju svih aktivnosti koje nijesu realizovane.

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 kontrola u cilju 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 međunerodnom 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.
- U planu je da se poveća broj službenika na obukama koje omogućavaju sertifikaciju po pitanju implementacije standarda informacione bezbjednosti (*sertifikovani implementator, interni revizor, eksterni revizor*).

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, a u okviru čega je planirano 100% povećanje ljudskih resursa.

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)[14] 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

[14] Projekat se relizacije kroz donaciju ICITAP organizacije.

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.

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.

b) Upravljanje nacionalnim kriznim situacijama

U Strategiji nacionalne bezbjednosti Crne Gore iz 2018. godine navodi se da krizno upravljanje predstavlja "koordinisanu upotrebu elemenata diplomatske, informacione, vojne i ekonomske moći u kompleksnom bezbjednosnom okruženju, kako bi se preduprijedila kriza, spriječila eskalacija sukoba u oružani konflikt i savladala neprijateljstva, u slučaju njihovog pojavljivanja", da će "Crna Gora prepoznati stanje krize, kao jedno od stanja nacionalne bezbjednosti, i razviti sistem kriznog upravljanja kompatibilan NATO sistemu" i "nakon uspostavljanja sistema kroz vježbe kriznog upravljanja, na nacionalnom nivou i u okviru NATO sistema za odgovore na krize, periodično će se provjeravati sistem kriznog upravljanja, kapaciteti i sposobnosti Crne Gore da odgovori na razlicite bezbjednosne izazove, rizike i prijetnje[15]."

Programom rada Vlade Crne Gore za 2021. godinu, u III kvartalu predviđeno je utvrđivanje Predloga zakona o kriznom upravljanju. U cilju izrade Predloga zakona, Ministarstvo odbrane je obrazovalo interresornu radnu grupu.

Rad interresorne radne grupe bio je fokusiran na definisanju pojma krize, događaja koje mogu izazvati krizu, kao i identifikovanja organa za upravljanje krizama i njihove nadležnosti u tim situacijama. Posebna pažnja posvećena je mogućoj koliziji Predloga zakona sa Ustavom i važećim zakonima Crne Gore, naročito u oblasti unutrašnjih poslova i odbrane.

U skladu sa međunarodnom i NATO definicijom krize, radna grupa je utvrdila da je pojam krize veoma širok i da on obuhvata situacije koje mogu nastati u miru (epidemije, prirodne nepogode, terorizam, itd.), u ratnom ili vanrednom stanju, ali i situacije koje su posljedica kriza u državama članicama Sjevernoatlantskog saveza.

Takođe, zaključeno je da je postupanje i koordinacija u velikom broju navedenih situacija već propisana propisima Crne Gore[16].

[15] Izvor – Strategija nacionalne bezbjednosti Crne Gore.

[16] Ustav Crne Gore, Zakon o odbrani, Zakon o Vojsci Crne Gore, Zakon o upotrebi jedinica Vojske Crne Gore u međunarodnim snagama i učešću pripadnika operativne jedinice za zaštitu i spašavanje, policije i zaposlenih u organima državne uprave u mirovnim misijama i drugim aktivnostima u inostranstvu, Zakon o vojno-obavještajnim i bezbjednosnim poslovima, Zakon o unutrašnjim poslovima, Zakon o zaštiti i spašavanju, Zakon o osnovama obavještajno bezbjednosnog sektora Crne Gore, Uredba o organizaciji i načinu rada državne uprave, itd.

Uzimajući u obzir propise koji posredno uređuju oblast kriznog upravljanja, a ne definišu pojam krize, jedinstveni sistem upravljanja krizama i koordinaciju između organa i tijela koji postupaju u slučajevima kriza, radna grupa je zaključila da bi donošenje novog zakona, bez izmjene gore navedenih zakona, moglo dovesti do konfuzije u njegovoj primjeni i neefikasnosti u postupanjima organa u kriznim situacijama.

Uporedna praksa i iskustva partnerskih država dala su dodatna saznanja, ali i otvorila nova sporna pitanja za koje Ministarstvo odbrane smatra da ih je potrebno riješiti prije početka izrade konačnog teksta Predloga zakona.

Prepoznata je potreba da Ministarstvo odbrane obrazuje interresornu radnu grupu koja će pripremiti analizu propisa Crne Gore koji uređuju postupanja u situacijama koje mogu izazvati krizu i predložiti rješenja za cjelovito i jedinstveno normativno uređenje ove oblasti[17], na način kojim će se obezbijediti i prepoznavanje upravljanje krizama u slučajevima kada je njihov uzrok sajber napad/incident, odnosno (zlo)upotreba informaciono-komunikacionih tehnologija od strane aktera u i/ili van Crne Gore.

****

Na osnovu predstavljenih nadležnosti organa državne uprave u oblasti sajber bezbjednosti, uočenih izazova u implementaciji strateških ciljeva iz prethodnih strategija i indentifikovanih aktivnosti koje treba realizovati u narednom, petogodišnjem periodu, kroz prateće akcione planove, formulisani su operativni ciljevi navedeni u nastavku. Njihovim ostvarenjem osiguraće se i ispunjavanje postavljenog strateškog cilja.

Strateški cilj 1: Unaprijeđeni kapaciteti za sajber odbranu i sistem upravljanja kriznim situacijama izazvanim sajber napadima/incidentima širih razmjera.

***Operativni cilj 1**: Jačanje uticaja na najvećem upravljačkom nivou, u cilju obezbjeđivanja optimalnih finansijskih, organizacionih i ljudskih resursa za razvoj sajber kapaciteta.*
***Operativni cilj 2**: Definisanje i uspostavljanje novog i održivog tijela za sajber bezbjednost na nacionalnom niovu.*
***Operativni cilj 3**: Unaprjeđenje mehanizama za odgovor na incidente.*
***Operativni cilj 4:** Nastavak razvoja vojnih sajber kapaciteta u cilju ispunjenja nacionalnih i NATO odbrambenih sposobnosti.*
***Operativni cilj 5**: Definisanje osnovnih tehnoloških i operativnih principa za prevenciju sajber prijetnji i smanjenje rizika od istih.*
***Operativni cilj 6:** Uspostavljanje baze talenata i volontera koji se bave sajber bezbjednošću.*
***Operativni cilj 7**: Izvršena analiza i nadgradnja postojećeg sistema upravljanja kriznim situacijama u Crnoj Gori.*

Prvim strateškim ciljem su definisani operativni ciljevi koji treba da unaprijede mehanizme upravljanja sajber bezbjednošću u Crnoj Gori, što predstavlja osnov za prevazilaženje izazova iz prethodnog perioda, kako i osnov za ubrzani razvoj koji će pratiti procese digitalizacije i uticati na jačanje sajber otpornosti na sve više pristune

[17] Preuzeto sa: https://www.gov.me/dokumenta/97e83986-decc-41cb-b43d-c46bf553a191

hibridne prijetnje. Fokus će biti na podizanju svijesti o važnosti zaštite sajber prostora na najvišem upravljačkom nivou, što je osnov za obezbjeđenje adekvatnih sredstava za investiranje u tehnologiju, ljude i motivaciju odgovornih ljudi u lancu sajber odbrane.

Analizom trenutnog stanja, koja je izvršena na nivou Savjeta za informacionu bezbjednost i uz asistenicju strateških partnera, nameće se potreba temeljne reorganizacije Nacionalnog CIRT-a. U tom smislu date su preporuke, odnosno okvir za novu organizaciju koja će u narednom periodu biti sposobna da u skladu sa nivoom ambicija i prijetnji odgovori raznovrsnim izazovima. Strategija će posebno biti usmjerena na ostvarenje ovog cilja, jer snažno vjerujemo da je to jedini način da se dugoročno obezbijede održivi mehanizmi za vođenje brige o kolektivnoj sajber bezbjednosti i zaštiti KI, odnosno KII.

Paralelno sa gore navedenim aktivnostima, sveobuhvatan pristup, tj. zajedničko djelovanje javne uprave, privatnog sektora i građana je jedini održivi način ostvarenja napretka u ovoj oblasti. 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. U tom smislu, potrebno je unaprijediti koordinaciju i saradnju svih zainteresovanih strana, otklanjanjem zakonskih barijera u dijelu razmjene informacija. Stoga je združivanje resursa i postavljanje osnovnih principa djelovanja prilikom rješavanja sajber incidenata, posebno onih koji imaju uticaja na KII od velikog značaja.

Strategija predviđa definisanje i usvajanje osnovnih tehnoloških i organizacionih principa, kao osnovu za upostavljanje mehanizama prevencije i odgovora na sajber incidente. Na ovaj način, kroz mehanizme kontrole primjene osnovnih smjernica, upravljanja rizicima i slično, će biti osnažena kolektivna sajber bezbjednost, odnosno sajber odbrana na nacionalnom nivou. Inicijator za ostvarenje ovog operativnog cilja bi trebalo biti krovno tijelo nadležno za sajber bezbjednost, kao pokretač i centralna tačka za sve zainteresovane strane.

Na kraju, svi akteri na nacionalnom nivou su svjesni izazova koji raspoloživost ljudskih kapaciteta predstavlja. Po uzoru na najbolje prakse, osmislićemo model okupljanja svih sajber eksperata i mladih talenata na nacionalnom nivou, uključujući akademsku zajednicu i privatni sketor, koji su nam potrebni kao dio širih ljudskih resursa. Na ovaj način, osnažićemo interesovanje za domen sajber bezbjednosti, povjerenje između svih zainteresovanih strana, što će kroz usklađivanje zakonske regulative ojačati i ukupne kapacitete za sajber odbranu.

3.2. Zaštita 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"[18].

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.

Operateri 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.

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

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.

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.

***

Na osnovu navedenog zakonskog okvira i uočenih izazova na planu njegove implementacije, u cilju dostizanja drugog strateškog cilja:

Strateški cilj 2: Uspostavljen sistem zaštite kritične informatičke infrastrukture.

definisani su sledeći operativni ciljevi:

Operativni cilj 1: *Izmjena i dopuna zakonskih rješenja u oblasti zaštite kritične informatičke infrastrukture.*
Operativni cilj 2: *Donošenje liste kritične informaticke infrastrukture.*
Operativni cilj 3: *Proširenje kadrovskih kapaciteta CIRT.ME i nabavka tehničke opreme sa ciljem uspostavljanja zaštite KII.*
Operativni cilj 4: *Usvojen set minimalnih tehnoloških i operativnih mjera koje su neophodne za zaštitu KII.*
Operativni cilj 5: *Unaprjeđena koordinacija u okviru javnog i privatnog sektora u cilju zaštite KII.*
Operativni cilj 5: *Uspostavljanje koordinacionog tijela za zaštitu kritične infrastrukture.*

3.3. Sajber kriminal i zaštita podatka

a) 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[19]), 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.

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.

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.

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

b) Zaštita podatka

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.

***

Na liniji uočenih izazova i nedostataka u oblasti odgovora na sajber kriminal i zaštite podataka, u pravcu dostizanja strateškog cilja:

Strateški cilj 3: Osnažen odgovor na sajber kriminal i harmonizovan sistem zaštite podataka.

prepoznati su sledeći operativni ciljevi:

> ***Operativni cilj 1:*** *Izmjena i dopuna zakonskih rješenja u oblasti sajber kriminala.*
> ***Operativni cilj 2:*** *Jačanje kapaciteta Uprave policije za odgovor na sajber kriminal.*
> ***Operativni cilj 3:*** *Unapređenje procesa edukacije za zaposlene Ministarstva unutrašnjih poslova, Uprave policije i nosilaca pravosudnih funkcija.*
> ***Operativni cilj 4****: Usklađen zakonodavni okvir sa Opštom uredbom Evropske unije o zaštiti podataka o ličnosti (GDPR).*

3.4. Edukacija

Istraživanja su pokazala da 95% sajber bezbjednosnih incidenata su nastala kao rezultat ljudske greške[20]. Tim prije, edukacija o sajber bezbjednosti mora biti dio nacionalnih aktivnosti usmjerenih ka podizanju svijesti među različitim ciljnim grupama (mladima, zaposlenima u javnoj upravi i široj javnosti).

a) Edukacija zaposlenih i učenika u obrazovno-vaspitnim ustanovama

U periodu za nama se mnogo radilo na edukaciji učenika i nastavnika u sferi sajber bezbjednosti, kroz sporadične kampanje, godišnje obilježavanje Dana sigurnog interneta, pojedinačne radionice koje su same škole organizovale, vršnjačke radionice i sl.

Kako bi se kontinuirano dala podrška školama i djeci na temu sajber bezbjednosti, u okviru Portala za nastavnike (www.skolskiportal.edu.me) kreirana je posebna stranica posvećena bezbjednosti djece na internetu na kojoj se može naći veliki broj materijala, priprema za čas, kvizova, aplikacija, smjernica, istraživanja itd.

Potrebno je još mnogo toga učiniti, i to sistemski, kako bi se pokrile sve obrazovno-vaspitne ustanove i što veći procenat zaposlenih i učenika.

Neophodno je kreirati radionice za učenike osnovnih i srednjih škola, kao i obuke za nastavnike, pedagoge, psihologe, rukovodioce škola. Sa kreiranjem samovodećih obuka, obuke mogu pohađati i roditelji. Sa ciljanim kampanjama (gostovanjima stručnjaka iz ove oblasti) i radionicama, potrebno je dosegnuti što veći procenat djece školske dobi kako bi prevenirali da postanu sajber žrtve. Takođe ih treba i zainteresovati za zanimanja iz ove oblasti. Djeca mogu usvajati osnovne vještine sajber sigurnosti jednako brzo kao što osvajaju nove tehnologije, samo je potrebno pravilno ih usmjeravati.

Potrebno je kontinuirano raditi na podizanju svijesti kod djece, koja su u fokusu pažnje kada je obrazovanje u pitanju, a takođe i kod nastavnika, stručnih saradnika i roditelja. Takođe, zbog nedovoljnog broja stručnjaka iz ove oblasti, ovu temu je potrebno više uključiti u obrazovni sistem: na opštem nivou znanja za sve učenike i na specijalizovanom nivou za one koji svoju buduću profesiju vide u sajber bezbjednosti.

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;

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

- 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;

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

b) Osnaživanje nastavnih planova i programa na svim nivoima

Sajber bezbjednost se već kao tema obrađuje u nekim obaveznim i izbornim predmetima u osnovnim i srednjim školama (informatika, zdravi stilovi života, socijalne mreže i globalizacija i dio su nekoliko predmeta u stručnim obrazovnim programima iz oblasti elektrotehnike i IT), ali se samo na jednom obrazovnom programu stručnog usmjerenja izučava kao poseban predmet. Ipak, potreba je mnogo veća.

Nastavnici bi, već od nižih razreda osnovne škole, trebali uključiti osnove sajber bezbjednosti u svoje svakodnevne planove i programe. Kako nastavnici u svoje nastavne planove i programe uključuju više obrazovnih alata na internetu (tu potrebu je dodatno podstakla pandemija), oni mogu istovremeno podučavati učenike svih uzrasta osnovnim vještinama sajber sigurnosti i podsticati ih da i sami postanu stručnjaci za sajber sigurnost.

Strategijom za digitalizaciju obrazovnog sistema biće, s tim u vezi, realizovane sledeće aktivnosti:

- Kreiranje modula slobodnih aktivnosti koji nastavnici mogu uključivati u sve predmete osnovnog i opšteg srednje obrazovanja;
- 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 izjvještavaće Savjet za informacionu bezbjednosti.

c) Edukacija zaposlenih u javnoj upravi i kampanja širenja svijesti među generalnom populacijom

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.

***

Stoga, da bi se dostigao strateški cilj:

Strateški cilj 4: Unaprijeđen proces edukacije u oblasti sajber bezbjednosti u javnom i privatnom sektoru

biće neophodno planirati i realizovati aktivnosti koje će omogućiti realizaciju sledećih operativnih ciljeva:

> ***Operativni cilj 1:*** *Implementacija programa obrazovanja i obuka o sajber bezbjednosti i sigurnom korišćenju informaciono-komunikacionih tehnologija na svim nivoima obrazovanja.*
> ***Operativni cilj 2:*** *Centralizacija i promocija edukativnih materijala i informacija o dostupnim programima i obukama.*
> ***Operativni cilj 3:*** *Usvajanje osnovnih smjernica za sticanje i nadogradnju sajber vještina u javnom i privatnom sektoru.*
> ***Operativni cilj 4:*** *Realizacija programa obuka za zaposlene u javnom i privatnom sektoru o sajber bezbjednosti.*

3.5. Javno-privatno partnerstvo i međunarodna saradnja

a) 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.

b) 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.

***

Uvažavajući realnost da je pitanje sajber bezbjednosti međunarodnog karaktera, te da osim napora na nacionalnom nivou od strane javnog sektora zahtjeva i uključivanje privatnog sektora, te saradnju na međunarodnom nivou, postavljen je strateški cilj:

Strateški cilj 5: Ojačana javno-privatna partnerstva i međunarodna saradnja

koji će biti dostignut u predstojećem petogodišnjem period kroz realizaciju definisanih operativnih ciljeva:

> ***Operativni cilj 1:*** *Razvijanje novih institucionalnih i tematskih javno-privatnih partnerstava.*
> ***Operativni cilj 2:*** *Unaprijeđeni i diversifikovani kanali komunikacije sa strateškim međunarodnim partnerima.*

IV 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 poslednjem kvartalu 2023. 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 za 2024-2025. godinu 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