Crna Gora
Ministarstvo javne uprave

Prijedlog Akcionog plana za sprovođenje Strategije sajber bezbjednosti Crne Gore 2018-2021 za 2020. godinu, sa Izvještajem o realizaciji Akcionog plana za 2019. godinu

Podgorica, mart 2020. godine

Sadržaj

AKCIONI PLAN ZA IMPLEMENTACIJU STRATEGIJE SAJBER BEZBJEDNOSTI CRNE GORE 2018-2021 ZA 2020. GODINU *7*

I UVODNI REZIME *24*

II INFORMACIJE O VRIJEDNOSTIMA INDIKATORA UČINKA *26*

III REALIZACIJA MJERA PREMA STRATEŠKIM CILJEVIMA *27*

1. KAPACITETI ZA SAJBER ODBRANU 27
2. CENTRALIZACIJA SAJBER EKSPERTIZE I RESURSA 33
3. ZAŠTITA KRITIČNE INFORMATIČKE INFRASTRUKTURE 34
4. MEĐUINSTITUCIONALNA SARADNJA 35
5. ZAŠTITA PODATAKA 37
6. EDUKACIJA U OBLASTI SAJBER BEZBJEDNOSTI 39
7. SARADNJA JAVNOG I PRIVATNOG SEKTORA 42
8. REGIONALNA I MEĐUNARODNA SARADNJA 43

GRAFIČKI PRIKAZ REALIZACIJE MJERA IZ AKCIONOG PLANA *45*

FINANSIJSKI POKAZATELJI *45*

II TABELARNI PRIKAZ REALIZACIJE MJERA IZ AKCIONOG PLANA *46*

IV PREPORUKE ZA DALJE FAZE SPROVOĐENJA STARTEŠKOG DOKUMENTA *71*

V PREGLED DALJIH AKTIVNOSTI *72*

VI PREDLOG ZAKLJUČAKA *73*

AKCIONI PLAN ZA IMPLEMENTACIJU STRATEGIJE SAJBER BEZBJEDNOSTI CRNE GORE 2018-2021 ZA 2020. GODINU

STRATEŠKI CILJ: 1 **Kapaciteti za sajber odbranu**	**Vlada Crne Gore će nastaviti sa posvećenim radom na daljem jačanju sajber bezbjednosnih kapaciteta u smislu obezbjeđivanja adekvatnih ljudskih i finansijskih resursa, kao i drugih potreba neophodnih za efikasne i agilne sajber kapacitete institucija Crne Gore koje imaju za cilj da obezbijede siguran sajber prostor, omoguće podsticaj biznisa i u krajnjem doprinesu ekonomskom prosperitetu Crne Gore.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **procentualno povećanje trenutnog broja CIRT timova u odnosu na broj uspostavljenih i broj institucija koje trebaju da imaju CIRT timove.**	31 lokalni CIRT-a	Povećati broj lokalnih CIRT-ova za 30% u odnosu na početnu vrijednost	Povećati broj lokalnih CIRT-ova za 50% u odnosu na početnu vrijednost
Indikator učinka b) **Broj izrađenih analiza rizika u odnosu na broj institucija.**	Nosioci aktivnosti nemaju izrađenu analizu rizika	50% nosioca aktivnosti ima izrađenu analizu rizika	Svi nosioci aktivnosti izradili analizu rizika
Indikator učinka c) **Broj institucija koje imaju budžetska sredstva opredijeljena za sajber bezbjednost i broj institucija koje imaju trend povećanja godišnjeg budžeta za navedene potrebe.**		Povećanje budžetskih sredstava opredječjenih za sajber bezbjednost za 10% u odnosu na početnu vrijednost	Povećanje budžetskih sredstava opredječjenih za sajber bezbjednost za 20% u odnosu na početnu vrijednost
Indikator učinka d) **Izrađen izvještaj o minimalnom broju službenika za sajber bezbjednost.**	Ne postoji izvještaj	Izrađena analiza sa predlogom aktivnosti	Izrađen izvještaj

Aktivnost	Indikator rezultata	Nadležne institucije - nosioci aktivnosti	Datum početka	Datum ravršetka	Planirana sredstva	Izvor finansiranja
1.1. Uspostavljanje strukture lokalnih CIRT-ova, sa revizijom postojećeg stanja	Analiza postojećeg stanja	Ministarstvo javne uprave	I kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
1.2. Planiranje budžetskih sredstava opredijeljenih za sajber bezbjednost u okviru institucije koje su prepoznate kao nosioci	Broj institucija koje su izradile plan budžetskih sredstava opredijeljenih za sajber bezbjednost	Ministarstvo javne uprave Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	III kvartal	III kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
1.3. Uspostavljanje nove organizacione strukture Nacionalnog CIRT-a	Usvojen predlog strukture Nacionalnog CIRT-a	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka	I kvartal	III kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva

1.4. Uspostavljanje tehničkih kapaciteta NCIRT-a	1. Nabavljena oprema 2. Implementirani sistemi	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka	II kvartal	kontniuirano	Nisu potrebna dodatna sredstva	Budžet
1.5. Usklađivanje zakonske regulative u skladu sa planom reorganizacije NCIRT-a	1. Izmjene i dopune Zakona o informacionoj bezbjednosti 2. Izmjene i dopune Zakona o zaradama zaposlenih u javnom sektoru 3. Izmjene i dopune Uredbe o organizaciji l načinu rada državne uprave	Ministarstvo javne uprave Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	II kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
1.5. Analiza rizika	1. Formiran tim 2. Prikupljeni podaci 3. Pripremljen izvještaj	Ministarstvo javne uprave Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	II kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva

STRATEŠKI CILJ: 2 **Centralizacija sajber ekspertize i resursa**	**Vlada Crne Gore će preduzimati aktivnosti na centralizaciji i okupljanju ekspertize u oblasti sajber bezbjednosti kako bi se: ojačali kapa- citeti za adekvatan odgovor na sofisticirane sajber prijetnje po kritične infomatičke infra- strukture i druge bitne informacione sisteme; razumjeli rizici po sajber prostor Crne Gore; pružile adekvatne preporuke i unaprijedila sa- radnja sa privatnim i javnim sektorom.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Broj zaposlenih u Nacionalnom CIRT-u.**	U Nacionalnom CIRT-u zaposleno 4 osobe (sistematizovano 6 mjesta)	14 službenika u NCIRT	20 službenika u NCIRT
Indikator učinka b) **Usvojen pravilnik o unutrašnjoj organizaciji i sistematiza- ciji Ministarstva javne uprave (dva odjeljenja u CIRT).**	Ne postoje odsjeci u okviru Direkcije	Formirana dva odsjeka u okviru Direkcije	
Indikator učinka c) **Broj prostorija koje ispunjavaju minumum tehničkih karakteristika, u odnosu na broj predviđenih**	Ne postoji nijedna prostorija	Jedna specijalizovan prostorija za rad 10 osoba	Dvije specijalizovane prostorije
Indikator učinka d) **Broj organizovanih vježbi i uključenih aktera.**	Jedna vježba	Organizovane 2 vježbe	Organizovane 4 vježbe

Aktivnost	Indikator rezultata	Nadležne institucije - nosioci aktivnosti	Datum početka	Datum ravršetka	Planirana sredstva	Izvor finansiranja
2.1. Jačanje administrativnih kapaciteta NCIRT-a	Zaposleno 14 službenika	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka	III kvartal	kontinuirano	Nisu planirana sredstva	Budžet
2.2. Uspostavljanje Bezbjednosnog operativnog centra (CIRT SOC-a)	Nabavljena osnovna oprema za uspostavljanje CIRT SOC-a 1. obezbijeđen prostor 40m2 sa sistemom fizičke bezbjednosti 2. 4 TV/monitor 3. 6 računara 4. pristup SIEM rešenju	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka	II kvartal	kontinuirano	Nisu potrebna dodatna sredstva	Budžet
2.3. Nastavak razvoja mehanizama za zaštitu, monitoring, upravljanje ranjivostima, analizu i forenziku incidenata	Implementirana nova rješenja u institucijama , povećan nivo monitoringa, zaštite, upravljanja ranjivostima ili mehanizama za forenziku i analizu	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka Ministarstvo odbrane Agnecija za nacionalnu bezbjednost Ministarstvo unutrašnjih poslova Ministarstvo vanjskih poslova Ministarstvo pravde	Ikvartal	kontnuirano	Nisu potrebna dodatna sredstva	Budžet

STRATEŠKI CILJ: 3 **Zaštita kritične informatičke infrastrukture**	**Vlada Crne Gore će nastaviti da jača kapacitete za odbranu KII, a s obzirom da noseću ulogu na ovom polju ima nacionalni CIRT - on mora imati adekvatne resurse i alate kako bi na efikasan način mogao da razumije, analizira i odgovori na širok spektar prijetnji na ovom polju.** **Resursi državnih organa zaduženih za kontrolu bezbjednosti KII moraju biti adekvatni zadatku, odnosno državni organi moraju imati službenike koji razumiju prijetnje i rizike koji postoje za specifične KII koje pripadaju njihovom sektoru. Ljudski i tehnički resursi moraju biti ojačani u cilju efektivnog obavljanja ove funkcije.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Broj urađenih analiza u odnosu na broj KII, kao i kvalitet istih.**	Nema izrađenih analiza	Svi vlasnici identifikovanih KII imaju izrađene analize rizika	Svi vlasnici identifikovanih KII imaju izrađene analize rizika na godišnjem nivou
Indikator učinka b) **Usvojena Uredba o mjerama zaštite KII.**	Ne postoji uredba	Pripremljen nacrt uredbe	Usvojena uredba o Zaštiti kritične informatičke infrastrukture i njenoj zaštiti
Indikator učinka c) **Broj formalizovanih partnerstava sa nosiocima KII.**	Ne postoje formalizovana strateška partnerstva sa vlasnicima KII	Definisan model za razmjenu informacija i ekspertize	Formalizuje strateška partnerstva sa vlasnicima KII

Aktivnost	Indikator rezultata	Nadležne institucije - nosioci aktivnosti	Datum početka	Datum ravršetka	Planirana sredstva	Izvor finansiranja
3.1. Donošenje podzakonskih akata u vezi sa KI	1. Pripremljen predlog 2. Predlog usvojen	Ministarstvo unutrašnjih poslova	I kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
3.2.Opremljena specijalizovana prostorija za forenziku i analitiku	1. Obezbjeđena prostorija 2. nabavljeno 6 računara 4. instalirana open source rešenja za monitoring 5. nabavka alata za forenziku i analitiku	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka	III kvartal	kontinuirano	Nisu potrebna dodatna sredstva	Budžet
STRATEŠKI CILJ: 4 Međuinstitucionalna saradnja	**Prepoznata je potreba za jačanjem međuinstitucionalne saradnje, pri čemu će poseban akcenat biti stavljen na efikasnu i pravovremenu razmjenu informacija i najboljih praksi. U tom kontekstu, nadležne institucije će raditi na snaženju komunikacionih metoda kroz, između ostalog, organizovanje vježbi kriznog komuniciranja u slučaju sajber incidenata i napada većih razmjera. Vježbe će imati za cilj definisanje jasnih procedura komuniciranja u kriznim situacijama, kao i pravovremeno revidiranje istih.**					
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***			
Indikator učinka a) Broj imenovanih kontakt osoba, u odnosu na broj institucija.	31 kontakt osoba	Povećanje broja kontakt osoba za 30% u odnosu na početnu vrijednost	Povećanje broja kontakt osoba za 50% u odnosu na početnu vrijednost			

Indikator učinka b) **Aktivan registar sajber eksperata.**	Ne postoji registar	Napravljena tehnička specifikacija	Uspostavljen registar
Indikator učinka c) **Uspostavljena operativna platforma.**	Ne postoji platforma	Pripremljena tehnička specifikacija	Uspostavljena platforma
Indikator učinka d) **Formirana interresorna grupa.**	Ne postoji	Formirana grupa	Usvojen pravilnik o radu
Indikator učinka e) **Broj organizovanih vježbi na godišnjem nivou, dužina trajanja vježbi, kao i broj uključenih institucija.**	Jedna vježba	Organizovane 2 vježbe	Organizovane 4 vježbe
Indikator učinka f) **Definisan pravilnik i procedure razmjene informacija o sajber incidentima i komuniciranja između organa.**	Ne postoji pravilnik	Definisane procedure razmjene informacija o sajber incidentima i komunikacija između organa	Usvojen pravilnik

Aktivnost	Indikator rezultata	Nadležne institucije - nosioci aktivnosti	Datum početka	Datum ravršetka	Planirana sredstva	Izvor finansiranja
4.1. Platforma za razmjenu informacija	Operativna platforma	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka	III kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet/ Donacija
4.2. Interresorni operativni tim	Napravljen plan za odgovore na incidente koji imaju uticaj na veći dio sistema državnih organa. Plan treba da sadrži definisane uloge i raspoložive stručne i tehničke kapacitete po institucijama	Savjet za informacionu bezbjednost	II kvartal	III kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
4.3. Jačanje međuinstitucionalne saradnje	Broj Održanih zajedničke obuke, konferencije, sastanaka…	Ministarstvo javne uprave Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Nisu potrebna sredstva Donacije

4.4. Izmjene i dopune pravilnika o radu NCIRT-a	Unaprijeđen pravilnik u dijelu razmjene informacija i izvještavanja	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka	I kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva
STRATEŠKI CILJ: 5 **Zaštita podataka**	**Vlada Crne Gora će u cilju sprovođenja adekvatne zaštite važnog dijela informatičke infrastrukture jačati nacionalne kapacitete potrebne za sprovođenje bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci, kao i kapaciteti u oblasti kripto zaštite.**					
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***			
Indikator učinka a) **Izrada odgovarajućih pravnih akata i pratećih dokumenata od strane međuresorne radne grupe.**	Ne postoji pogovarajući pravni akt	Formirana radna grupa i izrađen predlog odgovarajućeg pravnog akta	Usvojen odgovarajući pravni akt			
Indikator učinka b) **Broj novozaposlenih informatičara u Direkciji za zaštitu tajnih podataka koji će se baviti akreditacijom komunikaciono-informacionih sistema i upravljanjem kripto materijalima.**	Dva zaposlena službenika	Zaposlena 3 službenika	Zaposlena 3 službenika			
Indikator učinka c) **Broj sistematizovanih radnih mjesta sa opisom poslova vezanih za informacionu bezbjednost tajnih podataka.**		Prepoznati radna mjesta i predložiti izmjene sistematizacije	Usvojena sistematizacija			
Indikator učinka d) **Broj sertifikovanih komunikaciono-informacionih sistema i sprovedenih internih revizija u cilju provjere implementacije standarda.**	Nema	Jedan sertifikovani sistem	Tri sertifikovana sistema			

Aktivnost	Indikator rezultata	Nadležne institucije - nosioci aktivnosti	Datum početka	Datum ravršetka	Planirana sredstva	Izvor finansiranja
5.1. Jačanje institucionalnih kapaciteta potrebnih za implementaciju informaciono - komunikacionih sistema u kojima se obrađuju tajni podaci stepena tajnosti „INTERNO“	Implementiran jedan novi sistem	Ministarstvo javne uprave Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet
5.2. Unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za obradu tajnih podataka	Izrađeni odgovarajući pravni akti i prateća dokumenata od strane međuresorne radne grupe	Direkcija za zaštitu tajnih podataka	I kvartal	II kvartal	Nisu potrebna dodatna sredstva	Nisu potrebna sredstva
5.3. Obuke po pitanju implementacije standarda informacione bezbjednosti (sertifikovani implementator, interni revizor ili eksterni revizor)	Sertifikovano minimum po jedan službenik iz institucija	Ministarstvo javne uprave Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet

5.4. Stvaranje uslova za prijem i čuvanje podataka označenih stepenima tajnosti “Povjerljivo”, “Tajno” i “Strogo Tajno”	3 institucije koje imaju potrebu da vrše razmjenu tajnih podataka su obezbijedili adekvatne prostorije, računarsku opremu ili sistem (u slučaju da je potreban) za prijem, obradu i čuvanje tajnih podataka.	Ministarstvo javne uprave Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	III kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet
5.5. Donošenje pravnog akta o imenovanju savjetnika za informacionu bezbjednost	Izrada odgovarajućeg pravnog akta; Donošenje pravnog osnova za imenovanje lica koja bi bila zadužena za poslove informacione bezbjednosti i predstavljala kontakt tačke u institucijama za akreditaciju informacionih sistema ili implementaciju standarda informacione bezbjednosti.	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Ministarstvo vanjskih poslova Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Nisu potrebna sredstva
5.6. Prepoznati ključne institucije u kojima treba urgentno uraditi penetraciono testiranje	Prepoznate ključne institucije u kojima treba urgentno uraditi penetraciono testiranje	Savjet za informacionu bezbjednost	III kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Nisu potrebna sredstva

STRATEŠKI CILJ: 6 **Edukacija u oblasti sajber bezbjednosti**	**Nadležni državni organi u cilju najbolje sajber bezbjednosne prakse će informisati o najnovijim sajber prijetnjama i preduzimati aktivnosti na edukaciji građana i organizacija u pogledu mehanizmima zaštite u sajber prostoru. Potrebni su održivi, kontinuirani i koordinirani napori kako bi se postigle šire promjene ponašanja i kako bi osigurali da sve ciljne grupe, javni i privatni sektor, kao i pojedinačni građanin, razumiju rizike i prijetnje koje postoje u sajber prostoru.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Broj održanih konferencija/radionica/obuka i gostovanja u obrazovnim emisijama.**		5 konferencija/obuka/gostovanja u emisijama	10 konferencija/obuka/gostovanja u emisijama
Indikator učinka b) **Broj objavljenih sadržaja na portalu CIRT.ME i broj ažuriranih materijala.**	Ažuriranje informacija na mjesečnom nivou	Ažuriranje informacija na portalu na nedeljnom nivou	Ažuriranje informacija na portalu na dnevnom nivou
Indikator učinka c) **Broj obučenih nastavnika po predhodno utvrđenom programu obuke.**	Definasan program obuke	Obučeno 250 nastavnika	Obučeno 500 nastavnika
Indikator učinka e) **Broj održanih radionica, takmičenja, debati itd, kao i broj djece koji je obuhvaćen aktivnostima.**	Definisan plan aktivnosti	Održane radionice 1.000 učenika	Održane radionice 2.000 učenika

Aktivnost	Indikator rezultata	Nadležne institucije - nosioci aktivnosti	Datum početka	Datum ravršetka	Planirana sredstva	Izvor finansiranja
6.1. Edukacija državnih službenika i namještenika na temu sajber bezbjednosti	Edukovano 50 službenika	Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet/Donacije
6.2. Obuke za zaposlene koji rade na polju sajber bezbjednost u okviru Nacionalnog CIRT-a i lokalnih CIRT-ova, mreži državnih organa	Broj specijalističkih obuka	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka Ministarstvo odbrane Agnecija za nacionalnu bezbjednost Ministarstvo unutrašnjih poslova Ministarstvo vanjskih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet/Donacije
6.3. Podizanje svijesti građana o bezbjednom korišćenju interneta	1. Izrada i promovisanje brošura, izrada publikacija, pisanje članaka i gostovanje u emisijama u edukativne svrhe 2. Ažuriranje materijala na portalu CIRT-a iz oblasti sajber bezbjednosti	Ministarstvo javne uprave	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet / Donacije

STRATEŠKI CILJ: 7 **Saradnja javnog i privatnog sektora**	**Vlada Crne Gore će i u narednom periodu nastaviti sa posvećenim radom u cilju podrške, kako u odgovoru na incidente, tako i u dijeljenju informacija i zajedničke inicijative u partnerstvu sa privatnim sektorom. Dakle, jedino visok stepen komunikacije, saradnje i integracije može biti efikasan način da se razumije i na pravi način odgovori na potrebe i izazove privatnih kompanija, a u cilju preduzimanja neophodnih mjera kako bi se postigao dovoljan stepen bezbjednosti.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka b) **Definisan pravilnik za proceduru razmjene informacija o sajber incidentima i komuniciranja između javnog i privatnog sektora.**	Ne postoji pravilnik	Definsane procedure	Usvojen pravilnik

Aktivnost	**Indikator rezultata**	**Nadležne institucije - nosioci aktivnosti**	**Datum početka**	**Datum ravršetka**	**Planirana sredstva**	**Izvor finansiranja**
71. Unapređenje saradnje sa privatnim sektorom i akademskom zajednicom	1. Broj uspostavljenih partnerstava sa privatnim sektorom i akademskom zajednicom, 2. Broj zajedničkih učešća na događajima u oblasti sajber bezbjednosti 3. Izrada pravilnika i procedura za razmjenu informacija o sajber incidentima	Savjet za informacionu bezbjednost Ministarstvo javne uprave Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebana dodatna sredstva	Budžet/Donacije
7.2. Unaprijeđenje zakonskih preduslova za jačanja saradnje sa privatnim sektorom, a u cilju podizanja nivoa kolektivne prevencije sajber prijetnji	Izmjene i dopune Zakona o informacionoj bezbjednosti I drugih akata, gdje će se jasno definisati nivo saradnje između institucije odgovorne za sajber bezbjednost na nacionalnom nivou i privatnog sektora	Ministarstvo javne uprave Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebana sredstva	Budžet/Donacije

STRATEŠKI CILJ: 8 **Regionalna i međunarodna saradnja**	**Vlada Crne Gore će nastaviti sa regionalnim i međunarodnim aktivnostima i vršiti svoj uticaj ulaganjem u partnerstva koja oblikuju globalnu evoluciju sajber prostora na način koji unaprjeđuje i širi ekonomske i bezbjednosne interese i poboljšava kolektivnu bezbjednost.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Broj održanih obuka, konferencija, seminara, vježbi, sastanaka i biće kvalitativnog karaktera.**	Jedna vježba na godišnjem nivou	Tri održane obuke/konferencije/seminara/vježbi/sastanaka	Šest održanih obuka/konferencija/seminara/vježbi/sastanaka
Indikator učinka b) **Broj sklopljenih partnerstava, potpisanih ugovora i memoranduma.**	Ne postoji nijedan	Jedan memorandum	Dva memoranduma

Aktivnost	**Indikator rezultata**	**Nadležne institucije - nosioci aktivnosti**	**Datum početka**	**Datum završetka**	**Planirana sredstva**	**Izvor finansiranja**
8.1. Unapređenje saradnje sa međunarodnim organizacijama i CERT/CIRT-ovima na regionalnom i međunarodnom nivou	Učestvovanje/organizacija tri konferencije, radionice, okrugla stola…	Savjet za informacionu bezbjednost Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	I kvartal	IV kvartal	Nisu potrebna sredstva	Budžet/Donacije

8.2. Jačanje bilateralne i multilateralne saradnje na polju sajber bezbjednosti	Broj realizovanih aktivnosti (kursevi, radionice, konferencije, vježbe i drugo)	Ministarstvo javne uprave Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet/Donacije
8.3. Jačanje saradnje sa NATO, OEBS i drugim međunarodnim organizacijama	Broj učešća na redovnim događajima u organizaciji NATO, OEBS i drugih međunarodnih organizacija (Sastanci komiteta, bordova, radnih grupa, konferencije, obuke, seminari, radionice i drugo)	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka Agencija za nacionalnu bezbjednost Ministarstvo vanjskih poslova Ministarstvo odbrane	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	Budžet/Donacije
8.4. Izrada pravilnika i procedura za razmjenu informacija o sajber incidentima	Pripremljen predlog pravilnika i procedura za razmjenu informacija o sajber incidentima	Ministarstvo javne uprave Direkcija za zaštitu tajnih podataka	II kvartal	IV kvartal	Nisu potrebna sredstva	Nisu potrebna sredstva

I UVODNI REZIME

Strategija sajber bezbjednosti Crne Gore (u daljem tekstu Strategija) je najviši državni strateški dokument kojim se uređuje sistem sajber bezbjednosti u Crnoj Gori. Vlada Crne Gore (u daljem tekstu Vlada), na sjednici održanoj 21. decembra 2017. godine, donijela je Strategiju koja obuhvata period od 2018. do 2021. godine.

Uredbom Vlade o načinu i postupku izrade, usklađivanja i praćenja sprovođenja strateških dokumenta propisano je da Strategija mora imati izrađen Akcioni plan, koji definiše aktivnosti za sprovođenje strategije ili programa u cilju postizanja utvrđenih strateških i operativnih ciljeva.

Akcioni plan za sprovođenje Strategije sajber bezbjednosti Crne Gore 2018-2021 za 2019. godinu (u daljem tekstu Akcioni plan), Vlada je usvojila na sjednici održanoj 4. aprila 2019. godine.

U Strategiji je jasno definisana vizija, nacionalna organizaciona struktura, strateški ciljevi, a Akcioni plan sadrži jasnu podjelu aktivnosti koje treba realizovati.

Prilikom izrade Strategije korišćene su preporuke vodećih međunarodnih organizacija na polju sajber bezbjednosti (NATO, ENISA). Jedna od ključnih preporuka međunarodnih subjekata je da Strategiju treba razvijati u okviru životnog ciklusa koji treba da sadrži sledeće faze:

1. Razvoj
2. Implementacija
3. Evaluacija
4. Prilagođavanje Strategije

Imajući u vidu gore navedene faze, cilj ovog dokumenta je da izvrši evaluaciju Strategije osvrćući se na realizovane aktivnosti iz postojećeg Akcionog plana. Ministarstvo javne uprave pripremilo je predmetni izvještaj na osnovu podataka dobijenih o strane nosilaca realizacije pojedinih aktivnosti određenih Akcionim planom.

Izvještaj sadrži pregled aktivnosti predviđenih Akcionim planom za 2019. godinu, na osnovu kojih će Vlada i šira javnost imati uvid u napredak i buduće aktivnosti za postizanje ciljeva u prioritetnim oblastima.

Akcioni plan definiše aktivnosti za sprovođenje sledećih strateških ciljeva:

1. Kapaciteti za sajber odbranu
2. Centralizacija sajber ekspertize i eksperata
3. Zaštita kritične informatičke infrastrukture
4. Međuinstitucionalna saradnja
5. Zaštita podataka
6. Edukacija u oblasti sajber bezbjednosti
7. Saradnja javnog i privatnog sektora
8. Regionalna i međunarodna saradnja

Navedeni strateški ciljevi predstavljaju kombinaciju bezbjednosnih interesa i odgovora Crne Gore na izazove, rizike i prijetnje definisane u Strategiji, a čija implementacija kroz mjere i aktivnosti u Akcionom planu predstavlja prioritet u periodu na koji se odnosi ovaj dokument, kako bi Strategija bila dosledno implementirana.

Uvidom u status realizacije Akcionog plana za implementaciju Strategije evidentna je intenzivna aktivnost nadležnih institucija u ispunjavanju zacrtanih ciljeva kojim su, do sada, uspješno implementirali veći dio aktivnosti utvrđenih Akcionim planom.

Aktivnost 2.2. nije realizovana u 2019. godini iz razloga što je nacrtom zakona o tajnim podacima predviđeno je da se Nacionalni CIRT tim izmjesti u Direkciju za zaštitu tajnih podataka, te potrebe da se u 2020 godini Zakon o informacionoj bezbjednosti uskladi sa navedenom odredbom Zakona o zaštiti tajnih podataka, kao i da se nakon navedenih izmjena u roku od 2 mjeseca izmjene aktovi o sistematizacijama Ministarstva javne uprave i Direkcije za zaštitu tajnih podataka.

Aktivnost 4.1. nije realizovana zbog Izmjene plana javnih nabavki za 2019. godinu iz razloga hitnosti, sredstva za ovu aktivnost su preusmjerena. Budžetom za 2020. godinu, planirana su sredstva za ovu aktivnost

II INFORMACIJE O VRIJEDNOSTIMA INDIKATORA UČINKA

Kapaciteti za sajber odbranu: u okviru ovog strateškog cilja radilo se na uspostavljanju lokalnih CIRT-ova i planirano povećanje broja lokalnih timova/kontakt osoba su premašene. U dijelu koji se odnosi na broj urađenih analiza ostvarena je vrijednost od 50%. Pripremljen je predlog organizacione šeme i broja službenika koji bi se bavili sajber bezbjednošću.

Centralizacija sajber ekspertize i resursa: Broj službenika u okviru CIRT-a nije povećan na 14. Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave, u okviru Direkcije za informatičku bezbjednost i odgovor na kompjuterske incidente (u okviru koje je i Nacionalni CIRT) sistematizovano je 8 radnih mjesta (popunjeno 6). Takođe, u okviru Direkcije za informatičku bezbjednost i odgovor na kompjuterske incidente (CS/NCIRT) nisu formirana dva odjeljenja sa jasno podijeljenim nadležnostima iz razloga što je Nacrtom zakona o tajnim podacima predviđeno je da se Nacionalni CIRT tim izmjesti u Direkciju za zaštitu tajnih podataka. U 2020. godini potrebno je u Direkciji za zaštitu tajnih podataka obazbijediti prostor za nacionalni CIRT, kao i specijalizovane prostorije.

Zaštita kritične informatičke infrastrukture: Vlada Crne Gore je na 139. sjednici na prijedlog Ministarstva unutrašnjih poslova usvojila Predlog zakona o određivanju i zaštiti kritične infrastrukture. Ministarstvo unutrašnjih poslova je formiralo je Radnu grupu za sprovođenje zakona o određivanju i zaštiti kritične infrastrukture i izradu podzakonskih akata.

Međuinstitucionalna saradnja: Izmjenom plana javnih nabavki za 2019. godinu sredstva koja su planirana za izradu registra i platforme za razmjenu informacija, preusmjerena na druge pozicije, iz razloga hitnosti, te je iz navedenih razloga ova aktivnosti nisu nerealizovane i planirane su budžetom za 2020. godinu. Institucije koje imaju predstavnike u Savjetu za informacionu bezbjednost su delegirale članove u Operativnom radnom timu. Odluka o obrazovanju Operativnog radnog tima biće usvojena na prvoj sjednici Savjeta za informacionu bezbjednost u 2020. godini. Ministarstvo javne uprave je u IV kvartalu, u saradnji sa DCAF-om i u okviru projekta „Unapređenje upravljanja sajber bezbjednošću na Zapadnom Balkanu“ organizovalo tri CompTIA obuke za predstavnike nacionalnog i lokalnih CIRT-ova

Zaštita podataka: U skladu sa predviđenim rokom, Direkcija je Pravilnikom o unutrašnjoj organizaciji i sistematizaciji predvidjela novo radno mjesto u Odjeljenju za informatičku zaštitu tajnih podataka i u aprilu 2018. godine zaposlila novog informatičara koji će se baviti akreditacijom komunikaciono-informacionih sistema i upravljanjem kripto materijalima. Agencija za nacionalnu bezbjednost je izvršila nabavku opreme koja će omogućiti neophodne preduslove za sertifikaciju sistema za obradu tajnih podataka do nivoa TAJNO. Agencija posjeduje sertifikovane službenike za rad na ovim sistemima.

Edukacija u oblasti sajber bezbjednosti: Ministarstvo prosvjete je realizovalo radionice za oko 2.600 učenika i 530 nastavnika u cilju podizanja svijesti o bezbjednom korišćenju interneta, koje takođe obilježava Dan sigurnog internet svake godine u obrazovno-vaspitnim ustanovama.

Saradnja javnog i privatnog sektora: Definisan je način razmjene informacija dok se u narednoj godini očekuje definisanje procedura za razmjenu informacija između državnih organa i ključnih institucija iz privatnog sektora.

Regionalna i međunarodna saradnja: U prethodnom periodu Ministarstvo javne uprave je organizovalo tri vježbe/konferencije zna kojima su učestvovali predstavnici privatnog sektora i akademske zajednice.

IZVJEŠTAJ O REALIZACIJI MJERA IZ AKCIONOG PLANA ZA IMPLEMENTACIJU STRATEGIJE SAJBER BEZBJEDNOSTI 2018-2021, za 2019. GODINU

III REALIZACIJA MJERA PREMA STRATEŠKIM CILJEVIMA

Akcioni plan sadrži 8 ciljeva i 24 aktivnosti i mjere. Realizovano je 15 aktivnosti, u toku je realizacija još sedam aktivnosti, dok dvije aktivnosti nisu realizovane. Mjere iz Akcionog plana su realizovane samostalno ili u saradnji sa ključnim institucijama iz oblasti sajber bezbjednosti.

Implementacija Strategije predstavlja složen proces čiju realizaciju otežava činjenica da se radi o vrlo kompleksnoj oblasti kod koje je teško predvidjeti probleme u realizaciji ciljeva. Na osnovu navedene analize realizovanih aktivnosti koje su prikazane ovim Izvještajem, evidentirano je da su odgovorni organi, do sada, uspješno implementirali veći dio aktivnosti utvrđenih Akcionim planom. Ipak, treba imati u vidu da je veliki broj aktivnosti neophodno sprovoditi u kontinuitetu kako bi se osigurao konstantan razvoj sajber bezbjednosti u Crnoj Gori.

1. KAPACITETI ZA SAJBER ODBRANU

1.1. Uspostavljanje strukture lokalnih CIRT-ova sa revizijom postojećeg stanja

- Indikator rezultata: Analiza postojećeg stanja; Formiranje lokalnih CIRT-ova u organima lokalne samouprave
- Nadležna institucija: Ministarstvo javne uprave
- Datum početka: I kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna sredstva
- Izvor finansiranja: Nisu potrebna sredstva
- **Status realizacije: Realizovano**

U skladu sa aktivnostima Ministarstvo javne uprave je pokrenulo proceduru za uspostavljanje lokalnih CIRT timova u organima lokalne samouprave. Obaveza formiranja lokalnih CIRT timova ili određivanja kontakt osobe u institucijama jeste u cilju uspostavljanja sistema zaštite od računarskih bezbjednosnih incidenata na internetu i koji će neposredno sarađivati sa Nacionalnim CIRT-om.

U 2019 godini formirano je 20 lokalnih timova, što zbirno čini cifru od ukupno formiranih 80 lokalnih timova koja sarađuju sa članovima Nacionalnog CIRT-a vezano za pitanja zaštite od računarskih bezbjednosnih incidenata na internetu.

1.2. Planiranje budžetskih sredstava opredijeljenih za sajber bezbjednost u okviru institucija koje su prepoznati kao nosioci

- Indikator rezultata: Broj institucija koje su izradile plan budžetskih sredstava opredijeljenih za sajber bezbjednost
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: III kvartal
- Datum završetka: III kvartal
- Planirana sredstva: Nisu potrebna sredstva
- Izvor finansiranja: Nisu potrebna sredstva
- **Status realizacije: Realizovano**

Budžetom Ministarstva javne uprava za 2020. godinu planirana je konsolidacija mreže ODU kao i sredstva za godišnje licence za SIEM i WAF sisteme. U smislu podizanja stepena bezbjednosti, opredjeljena su sredstva za hardversku infrastrukturu u DC.

Kao i za 2019. godinu, Ministarstvo odbrane i Vojska Crne Gore su budžetom za 2020. godinu izdvojili posebna sredstva za razvoj sajber kapaciteta (hardver, softver, obuke) i zaštitu komunikacija, što predstavlja više od polovine budžeta za investiranje u te namjene.

Ministarstvo vansjkih poslova je opredijelilo određena budžetska sredstva u cilju finansiranja aktivnosti iz domena sajber bezbjednosti iz redovnih budžetskih sredstava.

Ministarstvo pravde je planom budžetskih sredstava za 2020. godinu definisalo nabavku stavki: Licence za softvere – bezbjednosne: DAM za registre i licence za radne stanice i licence za firewall, kao i nadogradnja softverskih rješenja i nabavka potrebne HW opreme u cilju povećanja sajber bezbjednosti i zaštite kritične infrastrukture ministarstva. Planirana sredstva su dobijena Zakonom o budžetu za 2020. godinu.

U skladu sa zadatkom, Direkcija za zaštitu tajnih podataka izradila je predlog budžeta za fiskalnu 2020.godinu, a predlogom budžeta obuhvaćene su i stavke koje su namijenjene za sajber bezbjednost. Planirana su sredstva za obuke službenika u NATO školi za kriptografiju (Latina, Italija), kao i posjete važnim događajima iz oblasti sajber bezbjednosti koje su u nadležnosti DZTP (NDA konferencija, BSAB sastanci, itd.). Takođe, predviđena su sredstva za nastavak projekta nadogradnje postojećeg informacionog sistema za razmjenu domaćih podataka sa stepena tajnosti POVJERLJIVO na stepen TAJNO.

Takođe, i Agencija za nacionalnu bezbjednost izvršila je planiranje budžetskih sredstava opredijeljenih za sajber bezbjednost.

1.3. Jačanje administrativnih kapaciteta zaduženih za sajber bezbjednost

- Indikator rezultata: Izrađena analiza trenutnog stanja sa predlogom sistematizacije
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: II kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna sredstva
- Izvor finansiranja: Nisu potrebna sredstva
- **Status realizacije: Realizovano**

Vlada Crne Gore je na sjednici od 19.09.2019. godine utvrdila Zakon o izmjenama i dopunama Zakona o tajnosti podataka kojima je definisano da je nadležnost nacionalnog CIRT-a povjerena Direkciji za zaštitu tajnih podataka, s obavezom da se sa ovim Zakonom uskladi Zakon o informacionoj bezbjednosti. Kroz rad komisije za hibridne prijetnje i sajber grupe prepoznate su potrebe da se nacionalni CIRT proširi na najmanje 12 službenika.

Ministarstvo vanjskih poslova je uradilo analizu trenutnog stanja u Odjeljenju za upravljanje informacionim sistemima, kao i procjenu optimalnog broja službenika zaduženih za sajber bezbjednost. Analizom je utvrđeno da je u Odjeljenju trenutno angažovano samo dva službenika na poslovima: primjene informaciono komunikacionih tehnologija (ICT) u Ministarstvu i diplomatsko-konzularnim predstavništvima; održavanja, administriranja i razvoja cjelokupne informatičke strukture; upravljanja i koordiniranja projektima koji sadrže informatičku komponentu; kontinuiranog praćenja i primjene novih tehnologija i rješenja u cilju povećanja kvaliteta rada i jačanja interakcije sa partnerima i zainteresovanim stranama; projektovanja, razvoja i administracije, održavanja i dokumentovanja računarskih programa, računarske mreže i opreme, kao i administracije, ažuriranja i obuke za korišćenje postojećih aplikativnih rješenja (informacionog sistema, podsistema i portala); sprovođenja i uvođenja međunarodnih standarda za upravljanje bezbjednošću informacija, uspostavljanja mjera i procedura koje se odnose na zaštitu podataka i informacionih sistema, kao i zaštićene i efikasne elektronsku komunikaciju između Ministarstva i diplomatsko-konzularnih predstavništva. Na osnovu pomenute analize, procjena je da je za tekuću godinu neophodno angažovanje minimum jednog službenika na poslovima jačanja sajber bezbjednosti. Napominjemo da je kadrovsko jačanje Odjeljenja kontinuirana aktivnost i da je potrebno zapošljavanje dodatnih kadrova.

Analizom trenutnog stanja u Ministarstvu pravde, koja pokazuje da u ministarstvu postoje dva službenika/načelnika koji se pored svojih osnovnih nadležnosti bave i sajber bezbjednošću. Iz analize se vidi da je na nivou Direktorata za IKT pravosuđa potreban jedan službenik za sajber bezbjednost, koji bi bio prva kontakt osoba za komunikaciju sa nacionalnim CIRT-om u slučaju incidenta. Međutim, zbog optimizacije radnih mjesta na nivou državne uprave, ministarstvo će u sklopu postojećih sistematizovanih radnih mjesta u Direktoratu za IKT pravosuđa dodati nadležnosti i obaveze jednom od službenika, koje se odnose na sajber bezbijednost.

Direkcija za zaštitu tajnih podataka realizovala je aktivnost broj 1.3. tokom 2018.godine. Pravilnikom o unutrašnjoj organizaciji i sistematizaciji predviđeno je novo radno mjesto u Odjeljenju za informatičku zaštitu tajnih podataka i u aprilu 2018.godine zapošljen je novi informatičar koji se bavi akreditacijom komunikaciono-informacionih sistema i upravljanjem kripto materijalima. Direkcija nije imala dodatnih aktivnosti tokom 2019.godine.

Agencija za nacionalnu bezbjednost ulaže značajne napore u cilju stvaranja administrativnih kapaciteta za borbu protiv sajber kriminala i špijunaže, koji uz terorizam i organizovani kriminal, postaje najveći bezbjednosni izazov današnjice. Iz navedenog razloga, Agencija je izvršila analizu trenutnog stanja na osnovu koje će planirati naredne korake u suprotstavljanju izazovima ove vrste. Na osnovu analize je procijenjeno da je potrebno povećati broj službenika koji će se baviti ovom problematikom pa je i napravljen predlog za povećanjem broja radnih mjesta. I ne samo navedeno, krajem godine izvršen je prijem službenika koji će raditi na poslovima informacione i sajber bezbjednosti.

Ministarstvo odbrane je Pravilnikom o unutrašnjoj organizaciji i sistematizaciji koji je usvojen u martu 2019. godine formiralo Odsjek za sajber odbranu i odgovore na kompjuterske incidente i izvršilo popunu predviđenih pozicija. Vojska Crne Gore je Odlukom o organizacijsko-formacijskoj strukturi iz 2019. godine u okviru Generalštaba predvidjela Odsjek za bezbjednost informacija i sajber zaštitu. Osim navedenog, u okviru Čete veze i elektronskog ratovanja predviđene su formacijske pozicije koje će biti fokusirane na sajber

odbranu. Na ovaj način, Ministarstvo odbrane i Vojska Crne Gore će stvoriti preduslove za izgradnju adekvatnih kapaciteta za sajber odbranu, prateći nacionalne i partnerske (NATO) ciljeve.

1.4. Jačanje tehničkih kapaciteta institucija zaduženih za sajber bezbjednost

- Indikator rezultata: Implementirani sistemi za zaštitu; Nabavljena oprema
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: II kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet
- **Status realizacije: Realizovano**

Ministarstvo javne uprave je sprovelo aktivnosti u cilju jačanja bezbjednosnog okvira, odnosno sajber zaštite, za informacione sisteme i mrežu organa državne uprave. Zamjena komunikacione opreme u cilju pouzdanijeg protoka podataka ka serverima u data centru i segmentacije mreže uz pomoć kojih je dodatnom konfiguracijom moguće ograničen pristup između različitih mreža unutar mreže državnih organa.

U cilju prevencije prijetnji koje dolaze sa interneta unaprijeđenje su funkcionaknosti postojećeg sistema zaštite. Na ovaj način smo omogućeno je efikasnije detektovanje malicioznih aktivnosti, prevencija pristupa malicioznim sajtovima ili aplikacijama i druge bezbjezbjedonosne kontrole. Ovaj uređaj je ključan za skeniranje HTTPS saobraćaja. Dio procesorske snage uređaja oslobođen je preraspodjelom polisa i upgradom sistemskog softvera. Ipak ovaj uređaj performansama posjeduje limite jer ne zadovoljava potrebu filtriracije kompletnog HTTPS saobraćaja. Iz navedenog razloga budžetom za 2020 godinu predviđena su finansijska sredstva za nabavku novog uređaja adekvatne skalabilnosti.

Stepen informacione bezbjednosti dodatno je poboljšan, budući da su unapređenje funkcionalnosti postojećeg sistema za prevenciju od DDoS i drugih napada.

Dodano je unaprijeđen stepen bezbjednosti kroz Implementaciju antivirusne zaštite sa antivirusnom konzolom koja omogućava kontrolu i administraciju antivirusnog rješenja se jednog mjesta nad svim korisnicima unutar mreže državnih organa, a ogleda se između ostalog u redovom update-u baze sa definicijama i skeniranju radnih stanica.

Izvšrena je nabavka i implementacija aplikativnog firewall-a koji je dizajniran je specifično da zaštiti web portale od cyber napada koji dolaze spolja. Glavna funkcija je sposobnost analize svakog HTTP zahtjeva (predstavljaju način komunikacije između krajnjeg korisnika i web aplikacije) na aplikativnom nivou i omogućili potpunu dekripciju SSL/TLS saobraćaja. Ovaj alat omogućava funkcionalnosti koji nemaju drugi sistemi za zaštitu sistemi u obrani protiv napada preko interneta. Osim toga, većina komunikacije, pogotovo web aplikacijama, danas je kriptovana, što predstavlja dodatni problem za takve uređaje. Implementirana je funkcionalnost keširanja pristupa portalu Vlade, koji omogućava brži odziv portala i tjuniranje je u toku. Dalja implementacija ovog rješanja se radi u kontinuitetu. Trenutno se iza ovog uređaja nalazi portal Vlade, portal Predsjednika države i portal elektronske uprave.

Implementiran je još jedan od ključnih savremenih specijalizovanih alata - sistem za upravljanje sigurnosti informacija i događaja (SIEM), i funkcija mu je da analizira i koreliše (povezuje događaj sa korisnikom ili uređajem) svaki događaj koji se javlja unutar mreže državnih organa, gdje događaj predstavlja svaku prijavu, odjavu ,pristup datotekama, upit baza podataka itd. Sposoban je da dostavi detaljnu listu bezbednosnih rizika i kršenja usklađenosti. Glavna prednost rješenja je detekcija svih događaja, koji mogu biti rizični, a zatim mogućnost da se ti događaji analiziraju. Alat otkriva maliciozne pristupe kao što je botnet ili bilo koja vrsta skenera i slično.

Sistem je integrisan sa alatom koji daje preporuke za otklanjanje mogućih rizika i na taj način se može proaktivno dijelovati u cilju zaštite računarskih resursa na mreži. Radi se o programskom alatu koji se koristi za postupke provjere ranjivosti koji se provode u svrhu određivanja sigurnosnih nedostataka testiranih računara i mreža.

Implementirano je i alat za provjere ranjivosti koji putem skeniranja portova (portscan) odnosno sondiranjem otvorenih portova računara iz pojedinog IP raspona, dolazi do informacija o pokrenutim servisima.

Za sigurnost podataka unaprijeđen je backup rješenje koje koristimo za backup aktivnog direktorijuma, mejla i portala Vlade. Backup se radi na nivou baze i aplikacije. Implementiran je sistem dnevnog ikrementalnog backupa i nedeljnog full backupa sa periodom čuvanja podataka. Takođe se radi o savremenom alatu.

Sva implementiran riješenja nalaze se u Gartnerovom dijagramu kao liderska riješenja, a ujedno se I nalaze na NATO listama.

Tokom 2019. godine, Ministarstvo odbrane i Vojska Crne Gore implementirali su 4 napredna sistema za zaštitu informaciono-komunikacionih sistema (IKS), monitoring, analizu i forenziku sajber incidenata.

Ministarstvo pravde je u posjedu odgovarajućih uređaja na svim lokacijama. Direktorat za IKT je u 2019. godini sproveo niz redovnih aktivnosti, koje u velikoj mjeri smanjuju ranjivost postojećih sistema ministarstva, u sajber prostoru, izvršen je update firewall-a Fortigate i kupljene su licence za tekuću godinu za sve lokacije Ministarstva pravde. Web aplikativni firewall je update-ovan u okviru nabavke pomenutih licenci. U toku je implementacija deep inspection funkcije na firewall-u kojom će se onemogućiti zaobilaženje firewall polisa od strane korisnika koji pristupaju raznim web sadržajima. U sklopu tog procesa potrebno je izvršiti export sertifikata sa firewall-a i njegovo importovanje na svim radnim stanicama Ministarstva pravde. Takođe, započeta je realizacija implementacije rješenja za backup definisanih podataka sa svih radnih stanica. Nadalje, Akcionim planom Strategije IKT pravosuđa 2016-2020.god. započeta je realizacija dvije ključne mjere koje se tiču povećanja nivoa sajber bezbjednosti na nivou pravosuđa: nabavka i implementacija Log management sistema i nabavka i implementacija sistema za prevenciju gubitka podataka.

Ministarstvo vanjskih poslova je, u saradnji sa Ministarstvom javne uprave, a u skladu sa preporukom Savjeta za informacionu bezbjednost Crne Gore, održanom 19. jula 2019. godine koja se odnosi na unaprjeđenje nivoa stepena sajber bezbjednosti, instaliralo interni sofisticirani firewall sistem, čime je značajno unaprijeđena bezbjednost informacionih sistema i njihovih korisnika.

Direkcija za zaštitu tajnih podataka je, u skladu sa prethodno izvršenom procjenom trenutnog stanja tehničkih kapaciteta, za 2019.godinu planirala realizaciju projekta nadogradnje postojećeg informacionog sistema za razmjenu domaćih tajnih podataka sa stepena tajnosti POVJERLJIVO na stepen TAJNO. Izvršena je nabavka opreme neophodne za realizaciju projekta i započete su aktivnosti na implementaciji novog sistema. Planirano je

da se novi sistem stavi u produkciju i certifikuje za obradu tajnih podataka u prvom kvartalu 2020. godine.

U prethodnom periodu Agencija je intezivno radila na jačanju tehničkih kapaciteta u oblasti sajber bezbjednost. Iz tog razloga je i izvršena nabavka i implementacija novih tehničkih sredstava koja su doprinijela boljoj zaštiti i bezbjednosti IK sistema Agencije. Takođe je izvršeno i godišnje produženje licenci za softversku i hardversku opremu u cilju postizanja kontinuiranog tehničkog održavanja i upgrade-a postojeće opreme. Agencija će nastaviti da kontinuirano radi na nabavci i implementrianju novih hardverskih i softverskih rješenja u cilju jačanja otpornosti i zaštite informacionih sistema koje koristi. Odabir opreme i softvera se vrši u skladu sa propisima koji propisuju oblast tajnih podataka kao i u skladu sa setom standarda ISO 27001.

1.5. Analiza i audit ICT sistema

- Indikator rezultata: Formiran tim; Prikupljeni podaci; Pripremljen izvještaj
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: III kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna sredstva
- Izvor finansiranja: Nisu potrebna sredstva
- **Status realizacije: Djelimično realizovano**

Ministarstvo javne uprave u sklopu redovnih aktivnosti sprovodi pojedine mjere kontrole i audit sistema u cilju procjene bezbjednosti i analize rizika.

Ministarstvo odbrane i Vojska Crne Gore su počeli reviziju važećih procedura, što podrazumijeva sprovođenje analize i ažuriranje procedura u cilju potpune primjene standarda iz oblasti informacione bezbjednosti.

U Ministarstvu pravde je urađena djelimična realizacija ove mjere, u sklopu projekta implementacije standarda MEST ISO 27001:2014. Audit SW rješenja nije rađen.

Direkcija za zaštitu tajnih podataka nije imala realizovanih aktivnosti kada je ovaj zadatak u pitanju.

Nakon implementacije novih hardverskih i softverskih rješenja Agencija za nacionalnu bezbjednost je izvršila internu kontrolu ICT sistema i audit sistema. Kontrola i audit sistema je aktivnost koju Agencija kontinuirano sprovodi u cilju procjene bezbjednosti i analize rizika po sopstveni IKS.

1.6. Analiza rizika

- Indikator rezultata: Formiran tim; Prikupljeni podaci; Pripremljen izvještaj
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: III kvartal

- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna sredstva
- Izvor finansiranja: Nisu potrebna sredstva
- **Status realizacije: Realizovano**

Ministarstvo javne uprave redovno vrši analiziranje rizika u mreži državnih organa, koji se dalje tretiraju kroz pripremu mjesta za umanjenje rizika kako kroz nabavku specijalizovane opreme i alata u narednoj godini a tako i kroz obuke zaposlenih i jačanje kapaciteta.

Na bazi sprovedene analize rizika iz 2018. godine, Ministarstvo odbrane i Vojska Crne Gore su napravili Analizu rizika za 2019. godinu, koja je pokazala da su prethodno prepoznati rizici značajno umanjeni.

Ministarstvo pravde je u sklopu implementacije standarda MEST ISO 27001:2014, odradilo i analizu rizika informacionih sistema Ministarstva pravde. Izrađen je plan tretiranja rizika koji sadrži listu kontrola, odnosno organizacionih i tehničkih mjera koje treba preduzeti za ublažavanje, odnosno eliminisanje svakog identifikovanog rizika. Urađena je „Politika informacione bezbjednosti informacionog sistema pravosuđa“. Urađen je Plan za nastavak poslovanja informacionog sistema Ministarstva pravde u kojem su definisane sve neophodne procedure u slučaju javljanja kriznih/vanrednih situacija: timovi za upravljanje/oporavak, backup procedure i off site lokacija, nivoi komunikacije,...

Direkcija za zaštitu tajnih podataka je nakon nadogradnje postojećeg informacionog sistema za razmjenu domaćih tajnih podataka planirala je i certifikaciju istog. Proces certifikacije informacionog sistema za tajne podatke obuhvata analizu rizika i očekuje se njena izrada u I kvartalu 2020. godine.

Agencija za nacionalnu bezbjednost kontinuirano vrši analizu i procjenu rizika ne samo za Agenciju već i drugih štićenih objakata u skladu sa Zakonom. Ovaj proces će se i dalje obavljati kontinuirano.

2. CENTRALIZACIJA SAJBER EKSPERTIZE I RESURSA

2.1. Jačanje administrativnih kapaciteta CIRT-a

- Indikator rezultata: Zaposleno 10 službenika
- Nadležna institucija: Ministarstvo javne uprave
- Datum početka: II kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet
- **Status realizacije: Djelimično realizovano**

Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave, u okviru Direkcije za informatičku bezbjednost i odgovor na kompjuterske incidente (u okviru koje je i Nacionalni CIRT) sistematizovano je 8 radnih mjesta (popunjeno 6).

2.2. Jačanje organizacionih kapaciteta CIRT-a

- Indikator rezultata: Sistematizovana dva odsjeka(odgovor na incidente, tehničkog karakrtera i odsjek za strateške pravce, politike i preventivu)
- Nadležna institucija: Ministarstvo javne uprave

- Datum početka: II kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet
- **Status realizacije: Nije realizovano**

Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave, u okviru Direkcije za informatičku bezbjednost i odgovor na kompjuterske incidente (CS/NCIRT) nisu formirana dva odjeljenja sa jasno podijeljenim nadležnostima iz razloga što je nacrtom zakona o tajnim podacima predviđeno je da se Nacionalni CIRT tim izmjesti u Direkciju za zaštitu tajnih podataka, te potrebe da se u 2020 godini Zakon o informacionoj bezbjednosti usladi sa navedenom odredbom Zakona o zaštiti tajnih podataka, kao i da se nakon navedenih izmjena u roku od 2 mjeseca izmjene aktovi o sistematizacijama Ministarstva javne uprave i Direkcije za zaštitu tajnih podataka.

2.3. Uspostavljanje Bezbjednosnog operativnog centra (GSOC)

- Indikator rezultata: Nabavljena osnovna oprema za uspostavljanje GSOC-a (obezbijeđen prostor 40m2,TV/monitor, 6 računara, SIEM rešenje, nabavljena oprema za kontrolu pristupa)
- Nadležna institucija: Ministarstvo javne uprave
- Datum početka: II kvartal
- Datumzavršetka: IV kvartal
- Planirana sredstva: 114.900 €
- Izvor finansiranja: Budžet
- **Status realizacije: Djelimično realizovano**

Obezbijeđena je prostorije u Ministarstvu javne uprave i nabavljeno je dio novih računara za zaposlene. Implementirano je SIEM rješenje. Neophodno je raditi na obezbjeđivanju sistema za skladištenje logova i monitoring mreže organa državne uprave u Ministarstvu javne uprave. U 2020. godini potrebno je u Direkciji za zaštitu tajnih podataka obazbijediti prostor za nacionalni CIRT.

3. ZAŠTITA KRITIČNE INFORMATIČKE INFRASTRUKTURE

3.1. Uredba o zaštiti kritične informatičke infrastrukture

- Indikator rezultata: Pripremljen predlog; Predlog usvojen
- Nadležna institucija: Ministarstvo javne uprave
- Datum početka: II kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna sredstva
- Izvor finansiranja: Nisu potrebna sredstva
- **Status realizacije: Djelimično realizovano**

Vlada Crne Gore je na 139. sjednici na prijedlog Ministarstva unutrašnjih poslova usvojila Predlog zakona o određivanju i zaštiti kritične infrastrukture. Ministarstvo unutrašnjih poslova je formiralo je Radnu grupu za sprovođenje zakona o određivanju i zaštiti kritične infrastrukture i izradu podzakonskih akata.

3.2. Opremljena specijalizovana prostorija

- Indikator rezultata: Obezbijeđena prostorija: Nabavljeno 6 računara; Nabavljena kontrola pristupa; Instaliran open source rešenja za monitoring
- Nadležna institucija: Ministarstvo javne uprave
- Datum početka: II kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet
- **Status realizacije: Djelimično realizovano**

Obezbijeđena je prostorija u Ministarstvu javne uprave, instalirana oprema za kontrolu pristupa i video nadzor. Potrebno je dodatno i obezbijediti računare. U 2020. godini u skladu sa izmjenama organizacionog okvira i potrebno je obazbijediti prostor za nacionalni CIRT u Direkciji za zaštitu tajnih podataka.

4. MEĐUINSTITUCIONALNA SARADNJA

4.1. Platforma za razmjenu informacija

- Indikator rezultata: Operativna platforma
- Nadležna institucija: Ministarstvo javne uprave
- Datum početka: III kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: 14.000 €
- Izvor finansiranja: Budžet
- **Status realizacije: Nije realizovano**

Izmjenom plana javnih nabavki za 2019. godinu sredstva sa ove pozicije su preusmjerena na druge pozicije, iz razloga hitnosti, te je iz navedenih razloga ova aktivnost ostala nerealizovana i planirana je budžetom za 2020. godinu.

4.2. Interresorni operativni tim

- Indikator rezultata: Formiran operativni tim
- Nadležna institucija: Savjet za informacionu bezbjednost
- Datum početka: II kvartal
- Datum završetka: III kvartal
- Planirana sredstva: Nisu potrebna sredstva
- Izvor finansiranja: Nisu potrebna sredstva
- **Status realizacije: Realizovano**

Instutucije koje imaju predstavnike u Savjetu za informacionu bezbjednost su delegirale članove u Operativnom radnom timu. Odluka o obrazovanju Operativnog radnog tima biće usvojena na prvoj sjednici Savjeta za informacionu bezbjednost u 2020. godini.

4.3. Jačanje međuinstitucionalne saradnje

- Indikator rezultata: Održane 3 zajedničke obuke, konferencije, sastanka

- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: I kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Sredstva iz donacija
- Izvor finansiranja: Nisu potrebna sredstva; Donacije
- **Status realizacije: Realizovano**

Ministarstvo javne uprave je u IV kvartalu, u saradnji sa DCAF-om i u okviru projekta „Unapređenje upravljanja sajber bezbjednošću na Zapadnom Balkanu“ organizovalo tri CompTIA obuke za predstavnike nacionalnog i lokalnih CIRT-ova, koje su držali sertifikovani predavači.

U dijelu jačanja međuinstitucionalne saradnje Ministarstvo odbrane daje doprinos razvoju sajber i informacione bezjbednosti kroz prisustvo u Savjetu za informacionu bezbjednost. Takođe, kao jedna od aktivnosti iz AP za implementaciju Strategije sajber bezbjednosti Crne Gore 2018-2021, za 2019. godinu, je bila formiranje Radnog tima za unapređenje propisa neophodnih za sprovođenje sertifikacije komunikaciono-informacionih sistema i procesa za tajne podatke, u okviru kojeg su 3 predstavnika Ministarstva odbrane i Vojska Crne Gore.

Krajem 2019. godine u okviru projekata jačanja sajber kapaciteta u Crnoj Gori, koji sprovodi Ambasada Velike Britanije, Ministarstvo odbrane i Vojska Crne Gore su u saradnji sa Ministarstvom javne uprave (Nacionalni CIRT) kao koordinatorom aktivnosti, organizovali 3 kursa iz oblasti sajber bezbjednosti (CompTIA).

Predstavnici Ministarstva pravde su učestvovali na regionalnoj sajber konferenciji, kao i prisustvovali nizu radionica i prezentacija na temu sajber bezbjednosti u organizaciji Ministarstva javne uprave i Ministarstva odbrane. Predstavnik Ministarstva pravde je ujedno i član Savjeta za informacionu bezbjednost, na čijim sastancima se operativno prati stanje bezbjednosti na nivou mreže organa državne uprave, tj. kritične informatičke infrastrukture, te razmjenjuju aktuelne informacije i podaci od značaja za ovaj segment. Takođe, predstavnik Ministarstva pravde je član Radnog tima za pripremu predloga Akcionog plana za uspostavljanje politike IT bezbjednosti u domenu standarda ISO 27002

Direkcija za zaštitu tajnih podataka ima delegiranog predstavnika u Savjetu za informacionu bezbjednost, Interresornoj komisiji za suprotstavljanje hibridnim prijetnjama i Radnoj grupi za sajber bezbjednost. Na inicijativu Direkcije za zaštitu tajnih podataka formiran je interresorni Radni tim za unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za tajne podatke. Takođe, službenici Direkcije za zaštitu tajnih podataka redovno učestvuju u radnim timovima i prisustvuju raznim sastancima i konferencijama na temu sajber bezbjednosti.

Kako bi na što bolji i efikasniji način odgovorili na incidentne situacije, Agencija za nacionalnu bezbjednost konstantno održava kvalitetnu saradnju i nesmetanu razmjenu informacija između ključnih institucija na polju sajber bezbjednosti. Tokom prethodnog perioda kroz razmjenu iskustava i informacija, kao i organizovanjem zajedničkih sastanaka i obuka, Agencija je kontinuirano radila na unapređenju saradnje sa drugim državnim organima i organima uprave i nastaviće saradnju ubuduće.

5. ZAŠTITA PODATAKA

5.1. Jačanje institucionalnih kapaciteta potrebnih za sertifikaciju informaciono-komunikacionih sistema u kojima se obrađuju tajni podaci

- Indikator rezultata: Implementiran jedan novi sistem
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: I kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet
- **Status realizacije: Realizovano**

Ministarstvo javne uprave nije korisnik ovog sistema i nije sprovodilo aktivnosti vezano za realizaciju ove mjere.

Ministarstvo odbrane/Vojska Crne Gore su izvršili nabavku dijela opreme za implementaciju posebnog sistema.

Ministarstvo pravde nije sprovodilo aktivnosti vezano za realizaciju ove mjere. Službenici Direktorata za IKT pravosuđa nisu pohađali obuke koje se tiču sertifikacije informacionih sistema za obradu tajnih podataka. Trenutno, Ministarstvo pravde nije korisnik ovog sistema, ali je planiralo da bude u narednom periodu.

Direkcija za zaštitu tajnih podataka izvršila je nabavku opreme neophodne za nadogradnju postojećeg informacionog sistema za razmjenu domaćih tajnih podataka sa stepena tajnosti POVJERLJIVO na stepen TAJNO i započete su aktivnosti na implementaciji novog sistema. Planirano je da se novi sistem stavi u produkciju i certifikuje za obradu tajnih podataka do kraja I kvartala 2020. godine. Direkcija u kontinuitetu radi na jačanju svojih kapaciteta kao organ nadležan za certifikaciju sistema u kojima se obrađuju tajni podaci.

Agencija za nacionalnu bezbjednost je izvršila nabavku opreme koja će omogućiti neophodne preduslove za sertifikaciju sistema za obradu tajnih podataka do nivoa TAJNO. Agencija posjeduje sertifikovane službenike za rad na ovim sistemima.

5.2. Unapređenje propisa neophodnih za sprovođenje sertifikacije komunikaciono-informacionih sistema i procesa za obradu tajnih podataka

- Indikator rezultata: Izrađeni odgovarajući pravni akti i prateća dokumenta od strane međuresorne radne egrupe
- Nadležna institucija: Direkcija za zaštitu tajnih podataka
- Datum početka: I kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna sredstva
- Izvor finansiranja: Nisu potrebna sredstva
- **Status realizacije: Djelimično realizovano**

Interresorni Radni tim za unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za tajne podatke formalno je kreiran u martu 2019. godine, na inicijativu Direkcije za zaštitu tajnih podataka. Članovi Radnog tima se redovno sastaju i sprovode aktivnosti na unapređenju propisa. Imajući u vidu da je Zakon o izmjenama i dopunama Zakona o tajnosti podataka u skupštinskoj proceduri i da se očekuje njegovo usvajanje, procedura za usvajanje izmjena i dopuna Uredbe o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka, koja proizilazi iz navedenog Zakona, ne može se pokrenuti do završetka ovog postupka. Tek nakon usvajanja izmjena i dopuna Uredbe, moguće je usvajanje Pravilnika o certifikovanju komunikaciono-informacionih sistema i procesa za obradu tajnih podataka i drugih pratećih dokumenata.

Shodno gore navedenim rokovima i procedurama, radni tim nije bio u mogućnosti da izvrši svoj zadatak u prvobitno propisanom roku – do kraja 2019.godine. Direkcija za zaštitu tajnih podataka tim povodom inicirala je izmjenu Rješenja o formiranju Radnog tima za unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za tajne podatke i propisala novi rok za izvršenje zadataka – do kraja II kvartala 2020.godine.

5.3. Obuke po pitanju implementacije standarda informacione bezbjednosti (sertifikovani implementator, interni revizor ili eksterni revizor)

- Indikator rezultata: Sertifikovano 10 službenika
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: I kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet
- **Status realizacije: Realizovano**

U sklopu aktivnosti koje obuhvataju reviziju važećih procedura iz oblasti informacione bezbjednosti, dva službenika Ministarstvo odbrane su prošli kurs za Internog revizora za ISO 27001 (Sistem menadžmenta bezbjednošću informacija).

Ministarstvo pravde je u sklopu projekta implementacije standarda MEST ISO 27001:2014 izvršilo obuke: 3 službenika posjeduju sertifikat Risk manager – ISO 31000:2018; 3 službenika posjeduju Certified data protection officer – General data protection regulation; 2 službenika posjeduju Lead implementer for information security management systems ISO/IEC 27001:2013; 2 službenika posjeduju Internal auditor for information security management systems ISO/IEC 27001:2013; 10 službenika je prošlo jednodnevnu obuku za ISO 27001.

Tri službenika Direkcije za zaštitu tajnih podataka prošli su obuku i dobili sertifikat za ISO/IEC 27001:2013 eksternog revizora.

Trenutno dva pripadnika Agencije za nacionalnu bezbjednost posjeduju sertifikate iz oblasti primjene standarda informacione bezbjednosti. Agencija planira sertifikaciju još jednog lica tokom naredne godine.

5.4. Donošenje pravnog akta o imenovanju savjetnika za informacionu bezbjednost

- Indikator rezultata: Izrada odgovarajućeg pravnog akta; Donošenje pravnog osnova za imenovanje lica koja bi bila zadužena za poslove informacione bezbjednosti i predstavljala kontakt tačke u institucijama za akreditaciju informacionih sistema ili implementaciju standarda informacione bezbjednosti
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: I kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna sredstva
- Izvor finansiranja: Nisu potrebna sredstva
- **Status realizacije: Djelimično realizovano**

Ministarstvo javne uprave će u izmjenama akta o sistematizaciji koje će prijedložiti Vladi na usvjanje, a u skladu sa usklađivanjem sa Zakonom o tajnosti podataka, u 2020 godini, sadržati propisivanje nadležnosti u opisu poslova za pojedina radna mjesta.

Predlogom Pravilnika o unutrašnjoj organizaciji i sistematizaciji Ministarstva odbrane, koji će se usvojiti u prvoj polovini 2020. godine, u opisu poslova za pojedina radna mjesta, prepoznate su nadležnosti koje se tiču primjene standrada iz oblasti informacione bezbjednosti.

Mogućnost imenovanja savjetnika za informacionu bezbjednost se razmatra u okviru Savjeta za informacionu bezbjednost, a tema je pokrenuta i u okviru Radnog tima za unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za tajne podatke kroz predlog nove Uredbe o bližim uslovima i načinu sprovođenja informatičkih mjera zaštite tajnih podataka (ovlašćena lica za upravljanje bezbjednošću sistema).

U Ministarstvu pravde na snazi je optimizacija postojećeg broja sistematizovanih mjesta u Direktoratu za IKT pravosuđa, tako da Ministarstvo pravde planira izmjenu Pravilnika o sistematizaciji, kojim će se postojećem službeniku u Direkciji za informatičku infrastrukturu i bezbjednost podataka dodati zaduženja za poslove informacione bezbjednosti, kao i za poštovanje GDPR uredbe.

U Agenciji za nacionalnu bezbjednost postojećom sistematizacijom predviđena su sajetnička mjesta koja su popunjena službenicima koji se bave ovom problematikom.

6. EDUKACIJA U OBLASTI SAJBER BEZBJEDNOSTI

6.1. Edukacija državnih službenika i namještenika na temu sajber bezbjednosti

- Indikator rezultata: Edukovano 50 službenika
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: I kvartal
- Datum završetka: IV kvartal

- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet; Donacije
- **Status realizacije: Realizovano**

Ministarstvo javne uprave ulaže kontinuirani napor u organizaciju različitih događaja iz oblasti sajber bezbjednosti. Od početka godine organizovan je veći broj događaja kojima je prisustvovao veći broj službenika.

Ministarstvo odbrane je tokom juna 2019. godine sprovelo “security awareness” program koji je podrazumijevao predavanja na temu sajber prijetnji i polaganje “pilot testa” svjesnosti na sajber prijetnje. Na osnovu rezultata napravljen je detaljan izvještaj, iz kojeg se mogao zaključiti nivo svjesnosti kod zaposlenih. U toku je razvoj web platforme i informativnog portala (biće operativni u martu 2020. godine), a planiran kontinuitet u sprovođenju predavanja.

Iz Ministarstva pravde službenik Direktorata za IKT pravosuđa i bezbjednost podataka je pohađao i uspješno završio kurs Certified Ethical Hacker (CEHv10) (CS6154).

Predstvanici Ministarstva vanjskih poslova uzeli su učešće na obuci „International Cyber Shield“, u Ankari, u organizaciji Ministarstva transporta i infrastrukture Republike Turske i Uprave za informacione i komunikacione tehnologije Republike Turske, uz podršku ITU Kancelarije za Evropu u okviru Regionalne inicijative ITU za Evropu i učestvovali na obuci na temu sajber bezbjednosti u organizaciji DCAF Ženevskog centra za bezbjednost sektora uprave koja je održana u Podogrici. Dodatno, u saradnji sa Ambasadom SAD u Podgorici uspostavljena je saradnja sa američkim partnerskim službama u cilju sprovođenja edukacije državnih službenika u oblasti sajber bezbjednosti.

U 2019. godini, službenici Direkcije za zaštitu tajnih podataka su pohađali sledeće obuke: tri službenika pohađala su obuku za SINA Core sisteme koji se koriste za razmjenu tajnih podataka, dva službenika su pohađala obuku za GDPR, dva službenika pohađala su obuku za korišćenje DKMI sistema za razmjenu kripto ključeva, jedan službenik pohađao je obuku CompTIA Linux +, dva službenika pohađala su obuku CompTIA Security+.

Kako bi na što bolji i efikasniji način odgovorili na incidentne situacije, pripadnici Agencije za nacionalnu bezbjednost su pohađali više obuka i konferencija čiji je cilj bio stručno usavršavanje kadrova koje rade na rješavanju incidenata. Pored učestvovanja, pripadnici Agencije su održali i više predavanja za zaposlene u državnoj administraciji u cilju njihove edukacije iz ove oblasti.

6.2. Obuke za zaposlene koji rade na polju sajber bezbjednosti u okviru Nacionalnog CIRT-a i lokalnih CIRT-ova

- Indikator rezultata: Obezbijediti 10 obuka
- Nadležna institucija: Ministarstvo javne uprave
- Datum početka: I kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet; Donacije
- **Status realizacije: Realizovano**

Ministarstvo javne uprave je u januaru, u saradnji sa DCAF-om (The Geneva Centre for the Democratic Control of Armed Forces), organizovalo „Regional TRANSITS I training for

CERTs“. Cilj vježbe bio je da okupi predstavnike glavnih aktera u crnogorskom sajber prostoru kako bi, između ostalog, unaprijedili saradnju, povećali nivo svijesti o sajber prijetnjama i razvili što bolju koordinaciju na ovom polju.

U novembru je održana TRANSITS II obuka. Takođe u saradnji sa DCAF-om, u četvrtom kvartalu su održane osnovne CompTIA obuke koje su održali sertifikovani predavači. Održane su 3 nezavisne obuke.

Takođe, predstavnici Ministarstva javne uprave su prethodnom periodu učestvovali i na:

- OSCE cyber/ICT security training – Sarajevo, Bosna i Hercegovina
- ITU Cyber Drill – Bukurest, Rumunija
- iPROCEEDS - Save the Date_4th annual Symposium on Cybersecurity Awareness – Bukurest, Rumunija
- Study Visit on Protection of Critical Information Infrastructure as a key priority of the Cybersecurity – Tallin, Estonija
- OSCE Sub-regional training on cyber/ICT security in Skopje, North Macedonia
- međunarodnoj sajber vježbi 2019 u Ankari, Turskoa;
- FIRST Fusion Training 5-7 marta. 2019. godine, Skoplje, Makedonija;
- planskoj vježbi za CMX19, 21.-25. januara 2019. godine, Stavanger, Norveska;
- Sub-regionalnom treningu o ulozi informatičkih i komunikacionih tehnologa (IKT) u kontekstu regionalne i međunarodne sigurnosti 23-24 maj. 2019. godine, Sarajevo, Bosna i Hercegovina
- Simpozijumu o podizanju svijestiu oblasti sajber bezbjednosti, Bukurešt, Rumunija

6.3. Podizanje svijesti građana o bezbjednom korišćenju interneta

- Indikator rezultata: Edukacija djece, nastavnog kadra, školskih pedagoga i psihologa; Izrada i promovisanje brošura, izrada publikacija, pisanje članaka i gostovanje u emisijama u edukativne svrhe; Ažuriranje materijala na portalu CIRT-a iz oblasti sajber bezbjednosti
- Nadležna institucija: Ministarstvo javne uprave, Ministarstvo prosvjete
- Datum početka: I kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet; Donacije
- **Status realizacije: Realizovano**

Ministarstvo javne uprave u kontinuitetu radi na podizanju svijesti kada je bezbjedno korišćenje interneta u pitanju kroz objavu sigurnosnih savjeta, objavu članaka i gostovanja u medijima.

U decembru 2019. godine potpisan je Sporazum o saradnji u realizaciji edukativne kampanje „Digitalna pismenost i zaštita djece i mladih na internetu“. Potpisnici sporazuma su Ministarstvo javne uprave, Ministarstvo sporta, Ministarstvo unutrašnjih poslova i Uprava policije. Kampanja će se sprovoditi na način, da se djeci i mladima kroz edukativne radionice i razne panel diskusije približi šta podrazumijeva elektronsko nasilje, kako ga prepoznati, koji oblici elektronskog nasilja postoje, koje posljedice može imati elektronsko nasilje, koje su preventivne mjere koje djeca I mladi mogu preduzeti kako ne bi bili žrtva elektronskog nasilja, kome se mogu obratiti za pomoć.

U aprilu 2019. godine u organizaciji Biznis akademije Vijesti uz podršku Ministarstva javne uprave i Ministarstva prosvjete, održana je konferencija za mlade o zaštiti od interbnet nasilja pod nazivom „Nasilje je za slabe“. Događaj je imao za cilj podizanje svijesti mladih o vršnjačkom nasilju, sa akcentom na internet nasilje. U okviru konferencije održana su dva panela: prvi se odnosio na načine prevencije i zaštite na tehničkom nivou, a na drugom se, iz ugla psihologa i maldih, govorilo o tome kako se suočavatio sa eventualnim problemima ove vrste.

U sklopu ove aktivnosti, Ministarstvo prosvjete je u toku godine održalo jednodnevne radionice za 1.500 učenika osnovnih i srednjih škola, kao i jednodnevne radionice za 280 nastavnika.

6.4. Unapređenje informacionog sistema u obrazovanju

- Indikator rezultata: Nadograđen modul za pedagoško-psihološke službe u Informacionom sistemu obrazovanja (MEIS) u cilju evidencije sajber nasilja kod djece školskog uzrasta i implementacija u svim osnovnim i srednjim školama
- Nadležna institucija: Ministarstvo prosvjete
- Datum početka: II kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet; Donacije
- **Status realizacije: Realizovano**

Ministarstvo prosvjete je ovu aktivnost realizovalo u potpunosti. Informacioni sistem obrazovanja Crne Gore nadograđen je modulom za evidenciju rada pedagoško-psiholoških službi u cilju evidencije sajber nasilja kod djece školskog uzrasta i implementiran je u svim osnovnim i srednjim školama.

7. SARADNJA JAVNOG I PRIVATNOG SEKTORA

7.1. Unapređenje saradnje sa privatnim sektorom i akademskom zajednicom

- Indikator rezultata: Broj uspostavljenih partnerstava sa privatnim sektorom i akademskom zajednicom; Broj zajedničkih učešća na događajima u oblasti sajber bezbjednosti
- Nadležna institucija: Savjet za informacionu bezbjednost, Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: I kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet; Donacije
- **Status realizacije: Realizovano**

Ministarstvo javne uprave je u prethodnom periodu ostvarilo saradnju sa više renomiranih privatnih kompanija iz Crne Gore na čiji poziv je učestvovala na zajedničkim obukama, vježbama i konferencijama. U cilju pronalaženja modela za bržu i efikasniju razmjenu informacija, u saradnji sa EKIP-om, uspostavljena je saradnja sa ISP-ovima.

U maju je održana je regionalna „Cyber Security“ konferencija pod pokroviteljstvom Ministarstva javne uprave Crne Gore na temu „Jačanje nacionalne sajber bezbjednosti u kontekstu suprotstavljanja hibridnim prijetnjama na bazi uspostavljenih standarda NATO i EU na globalnom nivou“. Cilj konferencije bio je da pruži uvid u uspostavljanje, održavanje i unapređenje informacione bezbjednosti, zaštite od hibridnih prijetnji na nacionalnom nivou, kao i zaštite kritične infrastrukture u kompanijama i institucijama, kroz informisanje i edukaciju o načinima prevencije, otkrivanja, odbrane, kao i saniranja posljedica od sajber napada.

Ministarstvo odbrane preko Savjeta za informacionu bezbjednost nastoji da ostvari bližu komunikaciju sa privatnim sektorom i akademskom zajednicom. Realizovana su i dva pilot projekta u saradnji sa Elektrotehničkom školom "Vaso Aligrudić", a odnosili su se na razvoj internih aplikacija.

Ministarstvo pravde u sklopu implementacije Akcionog plana Strategije IKT pravosuđa 2016-2020. godine imalo je tokom 2019. godine intezivnu saradnju sa privatnim sektorom, koja se odnosila na realizaciju mjera koje se odnose na implementaciju SW/HW rješenja na novou cijelog pravosuđa, sa ciljem implementacije jednistvenog informacionog sistema pravosuđa(ISP). Nadalje, sa akademskom zajednicom su uspostavili saradnju u dijelu edukacije službenika pravosuđa, koja se odnosi na specijalistička znanja i vještine neohodne u procesu uspostavjanja navedenog jedinstvenog ISP-a. Predstavnik Ministarstva pravde je učestvovao kao panelista na regionalnoj GDPR konferenciji u Podgorici, na kojoj je i sajber segment bio u fokusu.

Preko Savjeta za informacionu bezbjednost pokrenute su aktivnosti za saradnju sa privatnim sektorom i akademskom zajednicom. Direkcija za zaštitu tajnih podataka nije imala realizovanih aktivnosti kada je ovaj zadatak u pitanju.

Agencija za nacionalnu bezbjednost je u prethodnom periodu ostvarila značajnu saradnju sa više renomiranih privatnih kompanija iz Crne Gore na čiji poziv je učestvovala na zajedničkim obukama, vježbama i konferencijama. Takođe je nastavljena dobra saradnja u pogledu razmjena informacija i iskustava sa privatnim kompanijama koje su pružaoci usluga u oblasti telekomunikacija, interneta, hostinga i dr. Predstavnik Agencije u Savjetu za informacionu bezbjednost aktivno učestvuje u daljem definisanju procedura za razmjenu informacija između državnih organa i ključnih institucija iz privatnog sektora.

8. REGIONALNA I MEĐUNARODNA SARADNJA

8.1. Unapređenje saradnje sa međunarodnim organizacijama i CERT/CIRT-ovima na regionalnom i međunarodnom nivou

- Indikator rezultata: Učestvovanje/organizacija tri konferencije, radionice, okrugla stola…
- Nadležna institucija: Savjet za informacionu bezbjednost, Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Agencija za nacionalnu bezbjednost, Direkcija za zaštitu tajnih podataka, Ministarstvo vanjskih poslova
- Datum početka: I kvartal
- Datum završetka: IV kvartal
- Planirana sredstva: Nisu potrebna dodatna sredstva
- Izvor finansiranja: Budžet; Donacije
- **Status realizacije: Realizovano**

U cilju jačanja saradnje na regionalnom i međunarodnom nivou predstavnici Ministarstva javne uprave su učestvovali na sajber vježbama, obukama, konferencijama koje su imale za cilj jačanje kapaciteta tima za odgovor na incidentne situacije.

Ministarstvo javne uprave je delegiralo predstavnika za nacionalnu CB8 kontakt tačku OEBS-a .

U cilju jačanja saradnje na regionalnom i međunarodnom nivou predstavnici Ministarstva javne uprave su učestvovali na sajber vježbama, obukama, konferencijama koje su imale za cilj jačanje kapaciteta tima za odgovor na incidentne situacije. U okviru ove aktivnosti predstavnici CIRT-a učestvovali su na:

- tehničkom kolokvijumu u Ljubljani, Slovenija
- „Cyber Conference“, Podgorica
- Western Balkan 6 Digital Summit – Beograd, Srbija
- radionici Povezivanje i izgradnja kapaciteta CIRT-ova na zapadnom Balkanu, Budva

Podrškom Velike Britanije, koja je posebno fokusirana na jačanje sajber kapaciteta u Crnoj Gori, predstavnici Ministarstva odbrane i Vojska Crne Gore su učestvovali na 3 planske konferencije i završnoj NATO vježbi „Cyber Coalition 19“. Osim toga, Crna Gora je u maju 2019. godine organizovala Glavnu plansku konferenciju za navedenu NATO vježbu, koja je okupila preko 100 sajber eksperata iz zemalja koje su članice NATO i partnerskih zemalja.

Predstavnici Ministarstva odbrane i Vojska Crne Gore su kroz saradnju sa SAD (Komanda SAD za Evropu i kroz „state partnership program“) tokom 2019. godine učestvovali na 4 međunarodna seminara „Cyber Endeavor“ i organizovali „tabletop“ vježbu na temu odgovora na sajber incidente, u kojoj su učestvovali i predstavnici Nacionalnog CIRT-a i ANB.

Ističemo posjetu tima sajber eksperata iz SAD, sačinjenog od predstavnika Sajber komande SAD i predstavnika Komande SAD za Evropu, koji su tokom oktobra i novembra boravili u Crnoj Gori sa ciljem sprovođenja zajedničkih aktivnosti u sistemima Ministarstva odbrane i Vojska Crne Gore (monitoring mreže, analiza incidenata, forenzika i različiti vidovi obuka).

Predstavnici Ministarstva vanjskih poslova su učestvovali na različitim bilateralnim i multilateralnim forumima gdje je tema, između ostalih, i sajber bezbjednost. Takođe, Ministarstvo vanjskih poslova je, preko Misije Crne Gore pri NATO, aktivno uključeno u sve rasprave i odluke o politici sajber odbrane NATO, i redovno učestvuje na sastancima radnih tijela NATO posvećenih sajber bezbjednosti. S tim u vezi, Crna Gora je drugi put učestvovala na vježbi upravljanja kriznim situacijama u NATO-u (CMX 2019) koja je održana od 9. do 15. maja 2019. godine, a koja je imala u značajnom dijelu i sajber komponentu. Ovo je bila prilika da se sagleda postojeći sistem odgovora na krizne situacije i provjeri njegova kompatibilnost s NATO-om, ali i da se identifikuju nedostaci koje je potrebno otkloniti u narednom periodu..

Predstavnici Ministarstva pravde su učestvovali na regionalnoj sajber konferenciji, kao i prisustvovali nizu radionica i prezentacija na temu sajber bezbjednosti u organizaciji Ministarstva javne uprave i Ministarstva odbrane.

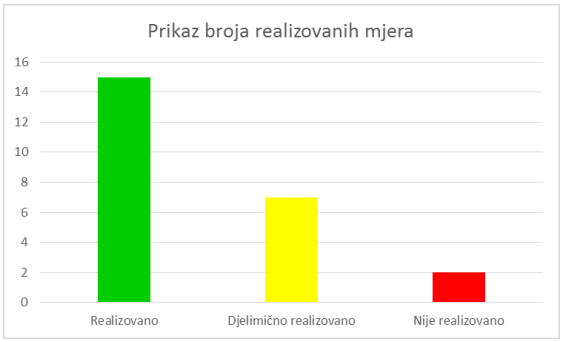
Kada je u pitanju regionalna i međunarodna saradnja, Direkcija je tokom 2019. godine sprovela niz aktivnosti: predstavnici Direkcije za zaštitu tajnih podataka učestvovali su na godišnjoj NDA (National Distribution Authority) konferenciji koja okuplja NDA tijela iz država članica NATO; predstavnici Direkcije za zaštitu tajnih podataka prisustvovali su BSAB

sastanku koji okuplja SAA (Security Accreditation Authority) tijela iz država članica NATO; potpisan je sporazum o razmjeni i uzajamnoj zaštiti tajnih podataka sa Makedonijom; prisustvo sastanku SEENSA radne grupe na temu drafta Sporazuma o uzajmnoj zaštiti tajnih podataka koji bi mogle da koriste članice SEENSA u pregovorima; učešće Direkcije na sastanku NATO Bezbjednosnog komiteta održanog u Varšavi.

Predstavnici Agencije su u saradnji sa partnerskim službama učestvovali na konferencijama, okruglim stolovima i studijskim posjetama sa regionalnim i međunarodnim organizacijama. Takođe su učestvovali i u aktivnostima u organizaciji Ministarstva javne uprave.

GRAFIČKI PRIKAZ REALIZACIJE MJERA IZ AKCIONOG PLANA

Od 24 planirane mjere i aktivnosti realizovano je 15, u toku je realizacija još sedam aktivnosti, dok dvije aktivnosti nisu realizovane. Mjere iz Akcionog plana su realizovane samostalno ili u saradnji sa ključnim institucijama iz oblasti sajber bezbjednosti. Iz navedenog se može zaključiti da postoji visok nivo posvećenosti državnih organa u realizaciji mjera i aktivnosti iz Akcionog plana, i da su ostvareni značajni rezultati.



FINANSIJSKI POKAZATELJI

Finansijska sredstva za realizaciju mjera iz Akcionog plana planiraju su u okviru redovnih ciklusa planiranja budžeta od strane nosioca mjera i ostvaruju se kroz budžet ili donacije.

II TABELARNI PRIKAZ REALIZACIJE MJERA IZ AKCIONOG PLANA

STRATEŠKI CILJ: 1 **Kapaciteti za sajber odbranu**	**Vlada Crne Gore će nastaviti sa posvećenim radom na daljem jačanju sajber bezbjednosnih kapaciteta u smislu obezbjeđivanja adekvatnih ljudskih i finansijskih resursa, kao i drugih potreba neophodnih za efikasne i agilne sajber kapacitete institucija Crne Gore koje imaju za cilj da obezbijede siguran sajber prostor, omoguće podsticaj biznisa i u krajnjem doprinesu ekonomskom prosperitetu Crne Gore.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Procentualno povećanje trenutnog broja CIRT timova u odnosu na broj uspostavljenih i broj institucija koje trebaju da imaju CIRT timove.**	31 lokalni CIRT-a	Povećati broj lokalnih CIRT-ova za 30% u odnosu na početnu vrijednost Ostvarena vrijednost: 80 lokalnih timova	Povećati broj lokalnih CIRT-ova za 50% u odnosu na početnu vrijednost
Indikator učinka b) **Broj izrađenih analiza rizika u odnosu na broj institucija.**	Nosioci aktivnosti nemaju izrađenu analizu rizika	50% nosioca aktivnosti ima izrađenu analizu rizika Ostvarena vrijednost: 50%	Svi nosioci aktivnosti izradili analizu rizika
Indikator učinka c) **Broj institucija koje imaju budžetska sredstva opredijeljena za sajber bezbjednost i broj institucija koje imaju trend povećanja godišnjeg budžeta za navedene potrebe.**		Povećanje budžetskih sredstava opredječjenih za sajber bezbjednost za 10% u odnosu na početnu vrijednost Ostvarena vrijednost: 10%	Povećanje budžetskih sredstava opredječjenih za sajber bezbjednost za 20% u odnosu na početnu vrijednost
Indikator učinka d) **Izrađen izvještaj o minimalnom broju službenika za sajber bezbjednost.**	Ne postoji izvještaj	Izrađena analiza sa predlogom aktivnosti Ostvarena vrijednost: napravljen predlog	Izrađen izvještaj

RB	Aktivnost	Ključne tačke (podaktivnosti)	Institucije odgovorne za sprovođenje aktivnosti na vrijednost	Indikator rezultata i postignuta vrijednost	Planirani datum početka	Planirani datum završetka	Izvor finansiranja aktivnosti	Status realizacije	Preporuke u narednom periodu sprovođenja
1.1.	Uspostavljanje strukture lokalnih CIRT timova	Uspostavljanje lokalnih CIRT timova / određivanje kontakt osoba	Ministarstvo javne uprave	1. analiza postojećeg stanja 2. formiranje lokalnih CIRT-ova u organima lokalne samouprave	I kvartal	Kontinuirano	Redovna sredstva iz budžeta	**Realizovano**	Redovno ažuriranje liste
1.2.	Planiranje budžetskih sredstava opredijeljenih za sajber bezbjednost u okviru institucija koje su prepoznati kao nosioci	Za efikasno funkcionisanje u okviru institucija koje su prepoznate kao nosioci sajber bezbjednosti moraju postojati opredijeljena budžetska sredstva za sajber bezbjednost	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Broj institucija koje su izradile plan budžetskih sredstava opredijeljenih za sajber bezbjednost	III kvartal	III kvartal	Redovna sredstva iz budžeta	**Realizovano**	Nastaviti na obezbjeđivanju finansijskih sredstava opredijeljenih za sajber bezbjednost

1.3.	Jačanje administrativnih kapaciteta zaduženih za sajber bezbjednost	Analiza trenutnog stanja i procjena optimalnog broja službenika zaduženih za sajber bezbjednost	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Izrađena analiza trenutnog stanja sa predlogom sistematizacije	II kvartal	IV kvartal	Redovna sredstva iz budžeta	**Realizovano**	Nastaviti na obezbjeđivanju ljudskih resursa u institucijama zaduženim za sajber bezbjednost
1.4.	Jačanje tehničkih kapaciteta institucija zaduženih za sajber bezbjednost	Analiza trenutnih i planiranih tehničkih kapaciteta; Nabavka opreme	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih	1. Implementirani sistemi za zaštitu 2. Nabavljena oprema	II kvartal	IV kvartal	Nisu potrebna sredstva	**Realizovano**	Nabavka opreme u skladu sa izrađenom analizom

			podataka Ministarstvo vanjskih poslova						
1.5.	Analiza i audit ICT sistema		Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	1. Formiran tim 2. Prikupljeni podaci 3. Pripremljen izvještaj	III kvartal	IV kvartal	Nisu potrebna sredstva	**Djelimično realizovano** Nisu sve institucije realizovale ovu aktivnost Novi rok IV kvartal 2020. god.	Intenziviranje aktivnosti
1.6.	Analiza rizika		Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo	1. Formiran tim 2. Prikupljeni podaci 3. Pripremljen izvještaj	II kvartal	III kvartal	Nisu potrebna sredstva	**Realizovano**	

			unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova						
STRATEŠKI CILJ: 2			**Vlada Crne Gore će preduzimati aktivnosti na centralizaciji i okupljanju ekspertize u oblasti sajber bezbjednosti kako bi se: ojačali kapa- citeti za adekvatan odgovor na sofisticirane sajber prijetnje po kritične infomatičke infra- strukture i druge bitne informacione sisteme; razumjeli rizici po sajber prostor Crne Gore; pružile adekvatne preporuke i unaprijedila sa- radnja sa privatnim i javnim sektorom.**						
Centralizacija sajber ekspertize i resursa									
INDIKATORI UČINKA			***Polazne vrijednosti***		***Vrijednost na sredini sprovođenja Strategije***		***Vrijednosti u poslednjoj godini sprovođenja Strategije***		
Indikator učinka a) **Broj zaposlenih u Nacionalnom CIRT-u.**			U Nacionalnom CIRT-u zaposleno 4 osobe (sistematizovano 6 mjesta)		14 službenika u NCIRT Ostvarena vrijednost: 6		20 službenika u NCIRT		

Indikator učinka b) **Usvojen pravilnik o unutrašnjoj organizaciji i sistematiza- ciji Ministarstva javne uprave (dva odjeljenja u CIRT).**			Ne postoje odsjeci u okviru Direkcije		Formirana dva odsjeka u okviru Direkcije Ostvarena vrijednost: nije realizovano				
Indikator učinka c) **Broj prostorija koje ispunjavaju minumum tehničkih karakteristika, u odnosu na broj predviđenih**			Ne postoji nijedna prostorija		Jedna specijalizovan prostorija za rad 10 osoba Ostvarena vrijednost: nije realizovano		Dvije specijalizovane prostorije		
Indikator učinka d) **Broj organizovanih vježbi i uključenih aktera.**			Jedna vježba		Organizovane 2 vježbe Ostvarena vrijednost: organizovane tri vježbe		Organizovane 4 vježbe		
RB	Aktivnost	Ključne tačke (podaktivnosti)	Institucije odgovorne za sprovođenje aktivnosti na vrijednost	Indikator rezultata i postignuta vrijednost	Planirani datum početka	Planirani datum završetka	Izvor finansiranja aktivnosti	Status realizacije	Preporuke u narednom periodu sprovođenja
2.1.	Jačanje administrativnih kapaciteta CIRT-a	Povećanje broja službenika CIRT-a kroz izmjene Pravilnika o unutrašnjoj organizaciji i sistematizaciji	Ministarstvo javne uprave Ministarstvo odbrane	Zaposleno 10 službenika	II kvartal	IV kvartal	Budžet nadležnih institucija	**Djelimično realizovano** U prethodnom periodu, u CIRT-u je zaposlena jedna osoba (ukupno 6 službenika)	Dalje jačanje administrativnih kapaciteta CIRT tima i povećanje broja službenika
2.2.	Jačanje organizacionih kapaciteta CIRT-a	U okviru CIRT-a sistematizovaće se dva odjeljenja:	Ministarstvo javne uprave	Sistematizovana dva odsjeka (odgovor na incidente, tehničkog	II kvartal	IV kvartal	Nisu potrebna sredstva	**Nije realizovano**	Aktivnost nije realizovana shodno Planu

		odjeljenje za odgovor na incidente, tehničkog karaktera i odjeljenje za strateške pravce, politike i preventivu		karaktera i odsjek za strateške pravce, politike i preventivu)				Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Ministarstva javne uprave u okviru CIRT-a povećan je broj službenika, međutim aktivnost nije realizovana budući da nisu formirana dva odjeljenja sa jasno podijeljenim nadležnostima.	optimizacije javne uprave,
2.3.	Uspostavljanje Bezbjednosnog operativnog centra (GSOC)		Ministarstvo javne uprave	Nabavljena osnovna oprema za uspostavljanje GSOC-a 1. obezbjeđen prostor 40m2 2. 4 TV/monitor 3. 6 računara 4. SIEM rešenje 5. nabavljena oprema za kontrolu pristupa	II kvartal	IV kvartal	114.900 €	**Djelimično realizovano** Obezbijeđen je prostor u Ministarstvu javne uprave, monitori i kontorla pristupa. Nisu nabavljeni računari	Nacrtom zakona o tajnim podacima predviđeno je da se Nacionalni CIRT tim izmjesti u Direkciju za zaštitu tajnih podataka. Potrebno je obezbijediti nove protorije u Direkciji za zaštitu tajnih podataka i nabaviti opremu.

STRATEŠKI CILJ: 3 **Zaštita kritične informatičke infrastrukture**	**Vlada Crne Gore će nastaviti da jača kapacite- te za odbranu KII, a s obzirom da noseću ulogu na ovom polju ima nacionalni CIRT - on mora imati adekvatne resurse i alate kako bi na efi- kasan način mogao da razumije, analizira i odgovori na širok spektar prijetnji na ovom polju. Resursi državnih organa zaduženih za kontrolu bezbjednosti KII moraju biti adekvatni zadatku, odnosno državni organi moraju imati službenike koji razumiju prijetnje i rizike koji postoje za specifične KII koje pripadaju njihovom sektoru. Ljudski i tehnički resursi moraju biti ojačani u cilju efektivnog obavljanja ove funkcije.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Broj urađenih analiza u odnosu na broj KII, kao i kvalitet istih.**	Nema izrađenih analiza	Svi vlasnici identifikovanih KII imaju izrađene analize rizika Ostvarena vrijednost: izrađena analiza rizika sistema	Svi vlasnici identifikovanih KII imaju izrađene analize rizika na godišnjem nivou
Indikator učinka b) **Usvojena Uredba o mjerama zaštite KII.**	Ne postoji uredba	Pripremljen nacrt uredbe Ostvarena vrijednost: pripremljen nacrt	Usvojena uredba o Zaštiti kritične informatičke infrastrukture i njenoj zaštiti
Indikator učinka c) **Broj formalizovanih partnerstava sa nosiocima KII.**	Ne postoje formalizovana strateška partnerstva sa vlasnicima KII	Definisan model za razmjenu informacija i ekspertize Ostvarena vrijednost:	Formalizuje strateška partnerstva sa vlasnicima KII

RB	Aktivnost	Ključne tačke (podaktivnosti)	Institucije odgovorne za sprovođenje aktivnosti na vrijednost	Indikator rezultata i postignuta vrijednost	Planirani datum početka	Planirani datum završetka	Izvor finansiranja aktivnosti	Status realizacije	Preporuke u narednom periodu sprovođenja
3.1.	Uredba o zaštiti kritične informatičke infrastrukture	Donošenje regulative koja treba da definiše procedure komunikacije između vlasnika KII i nadležnih institucija, kao i osnovne tehničke i organizacione mjere koje vlasnici KII moraju da ispune	Ministarstvo javne uprave	1. Pripreljmljen predlog 2. Predlog usvojen	II kvartal	IV kvartal	Nisu potrebna sredstva	**Djelimično realizovano** Vlada Crne Gore je na 139. sjednici na prijedlog Ministarstva unutrašnjih poslova usvojila Predlog zakona o određivanju i zaštiti kritične infrastrukture. Ministarstvo unutrašnjih poslova je formiralo je Radnu grupu za sprovođenje zakona o određivanju i zaštiti kritične infrastrukture i izradu podzakonskih akata. Pripremljeni predlog uredbe usaglasiti sa Zakonom	Intenziviranje aktivnosti

3.2.	Opremljena specijalizovana prostorija	Izvršiti analizu rizika po informacione sisteme u okviru nadležnosti ključnih institucija	Ministarstvo javne uprave	1. Obezbjeđena prostorija 2. nabavljeno 6 računara 3. nabavljena kontrola pristupa 4. instalirana open source rešenja za monitoring	II kvartal	IV kvartal	Redovna sredstva iz budžeta / Moguća donatorska sredstva	**Djelimično realizovano** Obezbijeđen je prostor u Ministarstvu javne uprave, monitori i kontorla pristupa. Nisu nabavljeni računari	Na osnovu odrađene analize i preporuka održavati postojeće i razvijati nova IT rješenja
STRATEŠKI CILJ: 4 **Međuinstitucionalna saradnja**			**Prepoznata je potreba za jačanjem međuinstitucionalne saradnje, pri čemu će poseban akcenat biti stavljen na efikasnu i pravovremenu razmjenu informacija i najboljih praksi. U tom kontekstu, nadležne institucije će raditi na snaženju komunikacionih metoda kroz, između ostalog, organizovanje vježbi kriznog komuniciranja u slučaju sajber incidenata i napada većih razmjera. Vježbe će imati za cilj definisanje jasnih procedura komuniciranja u kriznim situacijama, kao i pravovremeno revidiranje istih.**						
INDIKATORI UČINKA			***Polazne vrijednosti***		***Vrijednost na sredini sprovođenja Strategije***		***Vrijednosti u poslednjoj godini sprovođenja Strategije***		
Indikator učinka a) **Broj imenovanih kontakt osoba, u odnosu na broj institucija.**			31 kontakt osoba		Povećanje broja kontakt osoba za 30% u odnosu na početnu vrijednost Ostvarena vrijednost: 109 kontakt osoba		Povećanje broja kontakt osoba za 50% u odnosu na početnu vrijednost		

Indikator učinka b) **Aktivan registar sajber eksperata.**	Ne postoji registar	Napravljena tehnička specifikacija Ostvarena vrijednost:	Uspostavljen registar
Indikator učinka c) **Uspostavljena operativna platforma.**	Ne postoji platforma	Pripremljena tehnička specifikacija Ostvarena vrijednost:	Uspostavljena platforma
Indikator učinka d) **Formirana interresorna grupa.**	Ne postoji	Formirana grupa Ostvarena vrijednost: formirana grupa	Usvojen pravilnik o radu
Indikator učinka e) **Broj organizovanih vježbi na godišnjem nivou, dužina trajanja vježbi, kao i broj uključenih institucija.**	Jedna vježba	Organizovane 2 vježbe Ostvarena vrijednost: organizovane dvije vježbe	Organizovane 4 vježbe
Indikator učinka f) **Definisan pravilnik i procedure razmjene informacija o sajber incidentima i komuniciranja između organa.**	Ne postoji pravilnik	Definisane procedure razmjene informacija o sajber incidentima i komunikacija između organa	Usvojen pravilnik

RB	Aktivnost	Ključne tačke (podaktivnosti)	Institucije odgovorne za sprovođenje aktivnosti na vrijednost	Indikator rezultata i postignuta vrijednost	Planirani datum početka	Planirani datum završetka	Izvor finansiranja aktivnosti	Status realizacije	Preporuke u narednom periodu sprovođenja
4.1.	Platforma za razmjenu informacija	Definisanje modela za razmjenu informacija iz oblasti sajber bezbjednosti (o sajber incidentima, načinima komuniciranja u slučaju sajber napada itd.) između državnih organa	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Operativna platforma	III kvartal	IV kvartal	Nisu potrebna sredstva	**Nije realizovano** Izmjenom plana javnih nabavki za 2019. godinu sredstva su preusmjerena na druge pozicije, a ova aktivnost je planirana budžetom za 2020. godinu.	Intenzivirati aktivnosti na izradi pravilnika/protokola o međusobnoj razmjeni

4.2.	Interresorni operativni tim		Savjet za informacionu bezbjednost	Formiran operativni tim	II kvartal	III kvartal	Nisu potrebna sredstva	**Realizovano**	
4.3	Jačanje međuinstitucionalne saradnje		Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	Održane 3 zajedničke obuke, konferencije, sastanaka...	I kvartal	IV kvartal	Sredstva iz donacija	**Realizovano**	

STRATEŠKI CILJ: 5 **Zaštita podataka**	**Vlada Crne Gora će u cilju sprovođenja adekvatne zaštite važnog dijela informatičke infrastrukture jačati nacionalne kapacitete potrebne za sprovođenje bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci, kao i kapaciteti u oblasti kripto zaštite.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Izrada odgovarajućih pravnih akata i pratećih dokumenata od strane međuresorne radne grupe.**	Ne postoji pogovarajući pravni akt	Formirana radna grupa i izrađen predlog odgovarajućeg pravnog akta Ostvarena vrijednost: formirana radna grupa i izrađen predlog	Usvojen odgovarajući pravni akt
Indikator učinka b) **Broj novozaposlenih informatičara u Direkciji za zaštitu tajnih podataka koji će se baviti akreditacijom komunikaciono-informacionih sistema i upravljanjem kripto materijalima.**	Dva zaposlena službenika	Zaposlena 3 službenika Ostvarena vrijednost: 3 službenika	Zaposlena 3 službenika
Indikator učinka c) **Broj sistematizovanih radnih mjesta sa opisom poslova vezanih za informacionu bezbjednost tajnih podataka.**		Prepoznati radna mjesta i predložiti izmjene sistematizacije Ostvarena vrijednost:	Usvojena sistematizacija

Indikator učinka d) **Broj sertifikovanih komunikaciono-informacionih sistema i sprovedenih internih revizija u cilju provjere implementacije standarda.**			Nema		Jedan sertifikovani sistem Ostvarena vrijednost: jedan sertifikovan sistem		Tri sertifikovana sistema		
RB	Aktivnost	Ključne tačke (podaktivnosti)	Institucije odgovorne za sprovođenje aktivnosti na vrijednost	Indikator rezultata i postignuta vrijednost	Planirani datum početka	Planirani datum završetka	Izvor finansiranja aktivnosti	Status realizacije	Preporuke u narednom periodu sprovođenja
5.1.	Jačanje institucionalnih kapaciteta potrebnih za sertifikaciju informaciono - komunikacionih sistema u kojima se obrađuju tajni podaci		Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	Implementirana jedan novi sistem	I kvartal	IV kvartal	Nisu potrebna sredstva	**Realizovano** Do kraja prvog kvartala 2019. godine očekuje se formalno kreiranje i početak rada radne grupe na unapređenju propisa.	Ubrzati rad na unapređenju propisa za sprovođenje sertifikacije komunikaciono-informacionih sistema i procesa

5.2.	Unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za obradu tajnih podataka	Formiranje međuresorne radne grupe za unapređenje propisa / Unapređenje propisa za sprovođenje sertifikacije komunikaciono-informacionih sistema i procesa	Direkcija za zaštitu tajnih podataka	Izrađeni odgovarajući pravni akti i prateća dokumenata od strane međuresorne radne grupe	I kvartal	IV kvartal	Nisu potrebna sredstva	**Djelimično realizovano** S obzirom na to da je Zakon o izmjena i dopunama Zakona o tajnosti podataka u Skupštinskoj proceduri, radni tim nije bio u mogućnosti da izvrši svoj zadatak u prvobitno propisanom roku – do kraja 2019.godine. Direkcija za zaštitu tajnih podataka tim povodom inicirala je izmjenu Rješenja o formiranju Radnog tima za unapređenje propisa neophodnih za sprovođenje certifikacije komunikaciono-informacionih sistema i procesa za tajne podatke i propisala novi rok za izvršenje zadataka – do kraja II kvartala 2020.godine.	

5.3.	Obuke po pitanju implementacije standarda informacione bezbjednosti (sertifikovani implementator, interni revizor ili eksterni revizor)		Ministarstvo javne uprave Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde	Sertifikovano 10 službenika	I kvartal	IV kvartal	Nisu potrebna dodatna sredstva	**Realizovano**	

5.4.	Donošenje pravnog akta o imenovanju savjetnika za informacionu bezbjednost			Izrada odgovarajućeg pravnog akta Donošenje pravnog osnova za imenovanje lica koja bi bila zadužena za poslove informacione bezbjednosti i predstavljala kontakt tačke u institucijama za akreditaciju informacionih sistema ili implementaciju standarda informacione bezbjednosti.	III kvartal	IV kvartal	Nisu potrebna sredstva	**Djelimično realizovano** Većina institucija nije realizovala ovu aktivnost i prenosi se u 2020. godinu Novi rok je IV kvartal 2020. god.	Intenzivirati aktivnosti

STRATEŠKI CILJ: 6 **Edukacija u oblasti sajber bezbjednosti**	**Nadležni državni organi u cilju najbolje sajber bezbjednosne prakse će informisati o najnovijim sajber prijetnjama i preduzimati aktivnosti na edukaciji građana i organizacija u pogledu mehanizmima zaštite u sajber prostoru. Potrebni su održivi, kontinuirani i koordinirani napori kako bi se postigle šire promjene ponašanja i kako bi osigurali da sve ciljne grupe, javni i privatni sektor, kao i pojedinačni građanin, razumiju rizike i prijetnje koje postoje u sajber prostoru.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Broj održanih konferencija/radionica/obuka i gostovanja u obrazovnim emisijama.**		5 konferencija/obuka/gostovanja u emisijama Ostvarena vrijednost: 5	10 konferencija/obuka/gostovanja u emisijama
Indikator učinka b) **Broj objavljenih sadržaja na portalu CIRT.ME i broj ažuriranih materijala.**	Ažuriranje informacija na mjesečnom nivou	Ažuriranje informacija na portalu na nedeljnom nivou Ostvarena vrijednost: ažuriranje po potrebi	Ažuriranje informacija na portalu na dnevnom nivou
Indikator učinka c) **Broj obučenih nastavnika po predhodno utvrđenom programu obuke.**	Definasan program obuke	Obučeno 250 nastavnika Ostvarena vrijednost: 530 nastavnika	Obučeno 500 nastavnika
Indikator učinka e) **Broj održanih radionica, takmičenja, debati itd, kao i broj djece koji je obuhvaćen aktivnostima.**	Definisan plan aktivnosti	Održane radionice 1.000 učenika Ostvarena vrijednost: 2.600 učenika	Održane radionice 2.000 učenika

RB	Aktivnost	Ključne tačke (podaktivnosti)	Institucije odgovorne za sprovođenje aktivnosti na vrijednost	Indikator rezultata i postignuta vrijednost	Planirani datum početka	Planirani datum završetka	Izvor finansiranja aktivnosti	Status realizacije	Preporuke u narednom periodu sprovođenja
6.1.	Edukacija državnih službenika i namještenika na temu sajber bezbjednosti	Organizovanje/učešće na obukama, konferencijama, vježbama, sastancima, forumima, seminarima, radionicama	Ministarstvo javne uprave u saradnji sa ključnim institucijama iz oblasti sajber bezbjednosti	Edukovano 50 službenika	I kvartal	Kontinuirano	Redovna sredstva iz budžeta	**Realizovano**	Nastaviti sa edukacijom državnih službenika i namještenika na temu sajber bezbjednosti
6.2.	Obuke za zaposlene koji rade na polju sajber bezbjednost u okviru Nacionalnog CIRT-a i lokalnih CIRT-ova		Ministarstvo javne uprave	Obezbjediti 10 obuka	I kvartal	IV kvartal		**Realizovano**	

6.3.	Podizanje svijesti građana o bezbjednom korišćenju interneta	Edukacija djece, nastavnog kadra, školskih pedagoga i psihologa / Izrada i promovisanje brošura, izrada publikacija, pisanje članaka i gostovanje u emisijama u edukativne svrhe / Ažuriranje materijala na portalu CIRT-a iz oblasti sajber bezbjednosti	Ministarstvo javne uprave Ministarstvo prosvjete	1. Edukacija djece, nastavnog kadra, školskih pedagoga i psihologa 2. Izrada i promovisanje brošura, izrada publikacija, pisanje članaka i gostovanje u emisijama u edukativne svrhe 3. Ažuriranje materijala na portalu CIRT-a iz oblasti sajber bezbjednosti	I kvartal	Kontinuirano	Redovna sredstva iz budžeta	**Realizovano**	Organizovati bolju promociju portala CIRT.ME; izraditi promotivne materijale; nastaviti sa održavanjem radionica
6.4.	Unapređenje informacionog sistema u obrazovanju		Ministarstvo prosvjete	Nadograđen modul za pedagoško-psihološke službe u Informacionom sistemu obrazovanja (MEIS) u cilju evidencije sajber nasilja kod djece školskog uzrasta i implementacija u svim osnovnim i srednjim školama	II kvartal	IV kvartal	Nisu potrebna dodatna sredstva	**Realizovano**	

STRATEŠKI CILJ: 7	**Vlada Crne Gore će i u narednom periodu nastaviti sa posvećenim radom u cilju podrške, kako u odgovoru na incidente, tako i u dijeljenju informacija i zajedničke inicijative u partnerstvu sa privatnim sektorom. Dakle, jedino visok stepen komunikacije, saradnje i integracije može biti efikasan način da se razumije i na pravi način odgovori na potrebe i izazove privatnih kompanija, a u cilju preduzimanja neophodnih mjera kako bi se postigao dovoljan stepen bezbjednosti.**		
Saradnja javnog i privatnog sektora			
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka b) **Definisan pravilnik za proceduru razmjene informacija o sajber incidentima i komuniciranja između javnog i privatnog sektora.**	Ne postoji pravilnik	Definsane procedure Ostvarena vrijednost: definisan način za razmjenu informacija	Usvojen pravilnik

RB	Aktivnost	Ključne tačke (podaktivnosti)	Institucije odgovorne za sprovođenje aktivnosti na vrijednost	Indikator rezultata i postignuta vrijednost	Planirani datum početka	Planirani datum završetka	Izvor finansiranja aktivnosti	Status realizacije	Preporuke u narednom periodu sprovođenja
7.1.	Uspostavljanje saradnje sa privatnim sektorom (ISP, banke, ...) i akademskom zajednicom	Formalizovanje saradnje sa privatnim sektorom u vidu definisanja procedura za razmjenu informacija, organizovanje zajedničkih vježbi, konferencija, obuka, sastanaka	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Broj uspostavljenih partnerstava sa privatnim sektorom i akademskom zajednicom, Broj zajedničkih učešća na događajima u oblasti sajber bezbjednosti	I kvartal	IV kvartal	Redovna sredstva iz budžeta	**Realizovano**	Jačanje saradnje sa privatnim sektorom i akademskom zajednicom

STRATEŠKI CILJ: 8 **Regionalna i međunarodna saradnja**	**Vlada Crne Gore će nastaviti sa regionalnim i međunarodnim aktivnostima i vršiti svoj uticaj ulaganjem u partnerstva koja oblikuju globalnu evoluciju sajber prostora na način koji unaprjeđuje i širi ekonomske i bezbjednosne interese i poboljšava kolektivnu bezbjednost.**		
INDIKATORI UČINKA	***Polazne vrijednosti***	***Vrijednost na sredini sprovođenja Strategije***	***Vrijednosti u poslednjoj godini sprovođenja Strategije***
Indikator učinka a) **Broj održanih obuka, konferencija, seminara, vježbi, sastanaka i biće kvalitativnog karaktera.**	Jedna vježba na godišnjem nivou	Tri održane obuke/konferencije/seminara/vježbi/sastanaka Definisan plan aktivnosti: četiri	Šest održanih obuka/konferencija/seminara/vježbi/sastanaka
Indikator učinka b) **Broj sklopljenih partnerstava, potpisanih ugovora i memoranduma.**	Ne postoji nijedan	Jedan memorandum Definisan plan aktivnosti: jedan	Dva memoranduma

RB	Aktivnost	Ključne tačke (podaktivnosti)	Institucije odgovorne za sprovođenje aktivnosti na vrijednost	Indikator rezultata i postignuta vrijednost	Planirani datum početka	Planirani datum završetka	Izvor finansiranja aktivnosti	Status realizacije	Preporuke u narednom periodu sprovođenja
8.1.	Unapređenje saradnje sa međunarodnim organizacijama i CERT/CIRT-ovima na regionalnom i međunarodnom nivou	Organizacija konferencija, okruglih stolova, radionica, studijskih posjeta sa regionalnim i međunarodnim organizacijama	Ministarstvo javne uprave Ministarstvo odbrane Ministarstvo unutrašnjih poslova Ministarstvo pravde Ministarstvo prosvjete Agencija za nacionalnu bezbjednost Direkcija za zaštitu tajnih podataka Ministarstvo vanjskih poslova	Učestvovanje/organizacija tri konferencije, radionice, okrugla stola...	I kvartal	IV kvartal	Redovna sredstva iz budžeta	**Realizovano**	

IV PREPORUKE ZA DALJE FAZE SPROVOĐENJA STARTEŠKOG DOKUMENTA

Sajber bezbjednost i zaštita integriteta sajber prostora Crne Gore predstavlja zajedničku odgovornost i zahtijeva blisku i koordinisanu saradnju svih subjekata, od pojedinca, preko državnih i nedržavnih aktera, mehanizmima nacionalnog sistema bezbjednosti i mehanizmima međunarodne saradnje.

Strategijom je prepoznato osam ciljeva, čija je realizacija detaljnije definisana kroz pojedinačne zadatke postojećeg Akcionog plana.

Uvidom u status realizacije Akcionog plana za implementaciju Strategije evidentna je intenzivna aktivnost nadležnih institucija u ispunjavanju zacrtanih ciljeva kojim su, do sada, uspješno implementirali veći dio aktivnosti utvrđenih Akcionim planom.

Aktivnosti 2.2.i 4.1. nisu realizovana u 2019. godini shodno Planu optimizacije javne uprave, kao i izmjeni plana javnih nabavki i kao takve naći će se u Akcionom planu za 2020. godinu

Preporuke za dalje faze sprovođenja strateškog dokumenta po ciljevima su:

STRATEŠKI CILJ 1: Jačanja kapaciteta za sajber odbranu

- redovno ažurirati listu lokalnih CIRT timova/kontakt osoba
- na osnovu izrađene analize stanja i procjene budžetom predvidjeti sredstva za zapošljavanje službenika zaduženih za sajber bezbjednost
- nabaviti opremu u skladu sa izrađenom analizom

STRATEŠKI CILJ 2: Centralizacija sajber ekspertize i resursa

- shodno izrađenoj analizi predložiti izmjene Pravilnika o unutrašnjoj organizaciji i sistematizaciji sa ciljem da se u CIRT-u sistematizuju dva odjeljenja (odjeljenje tehničkog karaktera i odjeljenje za strateške pravce, politiku i preventive) kao i popuniti upražnjena mjesta

STRATEŠKI CILJ 3: Zaštita kritične informatičke infrastrukture

- intenzivirati aktivnosti na donošenju Uredbe o kritičnoj informatičkoj infrastrukturi i načinu njene zaštite
- ažurirati postojeću listu kritične informatičke infrastrukture

STRATEŠKI CILJ 4: Međuinstitucionalna saradnja

- implementirati platformu za razmjenu informacija

STRATEŠKI CILJ 5: Zaštita podataka

- usvojiti pravne propise za sertifikaciju komunikaciono-informacionih sistema

STRATEŠKI CILJ 6: Edukacija u oblasti sajber bezbjednosti

- organizovati pet događaja (konferencije, radionice, seminare, obuke…) za edukaciju državnih službenika i namještenika

V PREGLED DALJIH AKTIVNOSTI

Implementacija Strategije predstavlja složen proces čiju realizaciju otežava činjenica da se radi o vrlo kompleksnoj oblasti kod koje je teško predvidjeti probleme u realizaciji ciljeva. Na osnovu navedene analize realizovanih aktivnosti koje su prikazane ovim Izvještajem, evidentirano je da su odgovorni organi, do sada, uspješno implementirali veći dio aktivnosti utvrđenih Akcionim planom. Ipak, treba imati u vidu da je veliki broj aktivnosti neophodno sprovoditi u kontinuitetu kako bi se osigurao konstantan razvoj sajber bezbjednosti u Crnoj Gori.

Prilikom izrade Akcionog plana za 2020. godinu, obuhvaćene su aktivnosti koje nisu u potpunosti realizovane ili se realizuju u kontinuitetu. Na ovaj način se najefikasnije i dugoročno održivo obezbjeđuje adekvatno upravljanje sajber bezbjednošću u Crnoj Gori.

Na izradi Predloga akcionog plana učestvovali su predstavnici sledećih institucija: Ministarstvo javne uprave, Ministarstvo odbrane, Ministarstvo unutrašnjih poslova, Ministarstvo pravde, Ministarstvo prosvjete, Ministarstvo vanjskih poslova, Agencija za nacionalnu bezbjednost i Direkcija za zaštitu tajnih podataka