



CRNA GORA
Direkcija za zaštitu tajnih podataka

IZVJEŠTAJ O RADU
Direkcije za zaštitu tajnih podataka za 2023. godinu

Podgorica, februar 2024. godine

SADRŽAJ

UVOD	3
I NORMATIVNI POSLOVI	3
II DOZVOLE ZA PRISTUP TAJNIM PODACIMA	3
III MJERE ZAŠTITE TAJNIH PODATAKA	5
III-1 Fizičke mjere zaštite tajnih podataka	5
III-1 Informatičke mjere zaštite tajnih podataka	5
IV NATO I EU	6
IV-1. NATO	7
IV-2. EVROPSKA UNIJA	9
V MEĐUNARODNA SARADNJA	10
VI MEĐURESORSKA SARADNJA	12
VII SARADNJA SA NEVLADINIM ORGANIZACIJAMA	13
VIII OBUKE IZ OBLASTI TAJNIH PODATAKA	13
IX ORGANIZACIJA DIREKCIJE	14
X INFORMATIČKA BEZBJEDNOST I ODGOVOR NA RAČUNARSKE INCIDENTE	18
XI INSPEKCIJSKI NADZOR	24
XII BUDŽET I NABAVKE	25
XIII UPRAVLJANJE I UNUTRAŠNJA KONTROLA	26
XIV JAVNOST RADA	26

UVOD

Nadležnosti Direkcije za zaštitu tajnih podataka utvrđene su Zakonom o tajnosti podataka ("Službeni list Crne Gore", br. 14/08, 76/09, 41/10, 40/11, 38/12, 44/12, 14/13, 18/14, 48/15 i 74/20) i Uredbom o organizaciji i načinu rada državne uprave ("Službeni list Crne Gore", br. 49/22, 52/22, 56/22, 82/22, 110/22 i 139/22).

Izveštajem o radu Direkcije za zaštitu tajnih podataka obuhvaćen je pregled najvažnijih aktivnosti Direkcije u 2023. godini, u vezi sa: propisima iz oblasti tajnih podataka, izradom opštih akata Direkcije, izdavanjem dozvola za pristup tajnim podacima, NATO i EU sertifikata za pristup NATO i EU tajnim podacima, razmjenom tajnih podataka sa NATO i Evropskom unijom, obavezama koje proističu iz članstva u NATO, EU pregovorima za Poglavlje 31–Vanjska, bezbjednosna i odbrambena politika, aktivnostima na polju međunarodne saradnje, naročito u pogledu zaključivanja bilateralnih sporazuma o razmjeni i zaštiti tajnih podataka, bilateralne i regionalne saradnje, međuresorske saradnje i saradnje sa nevladinim organizacijama, obukama iz oblasti tajnih podataka i unapređenjem sistema obuke, stručnim osposobljavanjem i usavršavanjem službenika Direkcije, unutrašnjom organizacijom Direkcije i njenim funkcionisanjem, inspekcijским nadzorom nad sprovođenjem Zakona o tajnosti podataka i primjenom međunarodnih ugovora o razmjeni i zaštiti tajnih podataka, izvršenjem budžeta, sprovođenjem finansijskog upravljanja i kontrola i pružanjem obavještenja o radu Direkcije putem sredstava javnog informisanja.

I NORMATIVNI POSLOVI

Direkcija redovno učestvuje u davanju mišljenja na predloge zakona i podzakonskih akata koje su pripremali drugi organi, kao i mišljenja na predloge memoranduma i sporazuma o saradnji koji su uključivali odredbe o razmjeni i zaštiti tajnih podataka.

II DOZVOLE ZA PRISTUP TAJNIM PODACIMA

Dozvole za pristup tajnim podacima za fizička lica

Direkcija za zaštitu tajnih podataka, u skladu sa Zakonom, nadležna je za izdavanje dozvola za pristup tajnim podacima stepena tajnosti STROGO TAJNO, TAJNO i POVJERLJIVO.

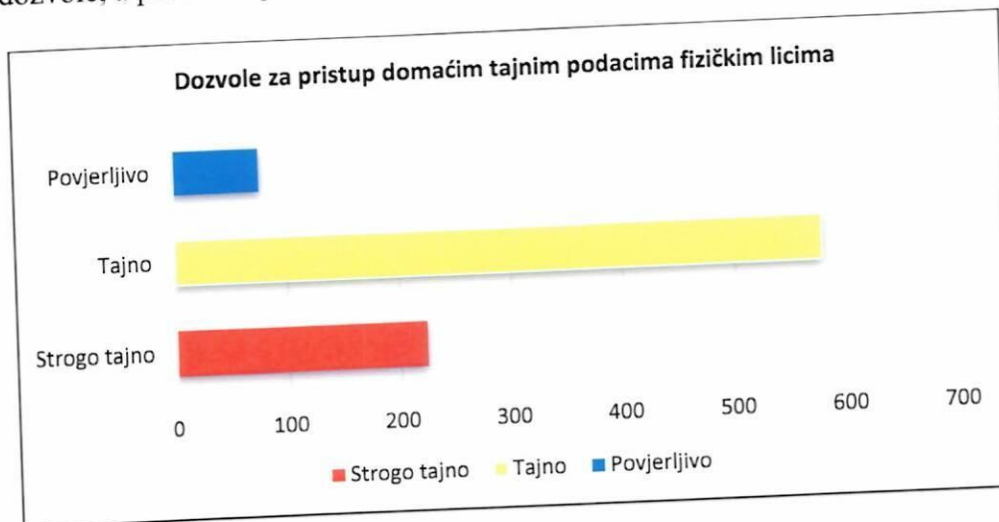
U 2023. godini, podnesena su 565 zahtjeva za izdavanje dozvola za pristup tajnim podacima, od čega je 222 zahtjeva za produženje važenja dozvole za pristup tajnim podacima, a 343 novih zahtjeva za izdavanje dozvola.

U 2023. godini, izdate su ukupno 879 dozvola za pristup tajnim podacima, od čega su 569 nove dozvole, dok je produžen rok važenja za 210 dozvola za pristup tajnim podacima.

Za pristup tajnim podacima stepena tajnosti **STROGO TAJNO** izdato je 224 dozvola, od čega je 106 novih dozvola, a produžen je rok važenja za 118 dozvola za pristup tajnim podacima.

Za pristup tajnim podacima stepena tajnosti **TAJNO** izdato je 578 dozvole, od čega je 389 novih dozvola, a produžen je rok važenja za 89 dozvola za pristup tajnim podacima.

Za pristup tajnim podacima stepena tajnosti **POVJERLJIVO** izdato je 77 dozvola, od čega su 74 nove dozvole, a produžen je rok važenja za 3 dozvola.



U 2023. godini, na zahtjev Nacionalnih bezbjednosnih organa (NSA) drugih država u kontinuitetu su procesuirane bezbjednosne provjere za strance koji su rođeni, živjeli, radili ili se školovali u Crnoj Gori, u skladu sa međudržavnim sporazumima.

Dozvole za pristup tajnim podacima za pravna lica

U 2023. godini, podnesen je jedan zahtjev za izdavanje dozvole za pristup tajnim podacima za pravno lice i izdata je jedna dozvola za pristup tajnim podacima za pravno lice.

Za pristup tajnim podacima za zaposlene u pravnom licu podneseno je 30 zahtjeva za izdavanje dozvole i 4 zahtjeva za produženje važenja dozvole za pristup tajnim podacima.

Prije izdavanja dozvole za pristup tajnim podacima zaposleni u državnim organima, kao i u pravnim licima u obavezi su da se edukuju o zaštiti i rukovanju tajnim podacima, odnosno bezbjednosnim pravilima i procedurama za zaštitu tajnih podataka, nakon čega pristupaju testiranju u elektronskoj aplikaciji. Testiranje se vrši neposredno prije izdavanja dozvole za pristup tajnim podacima i dozvola se izdaje nakon položenog E – testa.

III MJERE ZAŠTITE TAJNIH PODATAKA

III-1 Fizičke mjere zaštite tajnih podataka

Po pitanju fizičkih mjera zaštite tajnih podataka, Direkcija za zaštitu tajnih podataka je u 2023. godini, nastavila saradnju sa državnim organima i pravnim licima koja u vršenju zakonom utvrđenih poslova, odnosno izvršavanju ugovorenog posla postupaju sa tajnim podacima.

Sprovedene su konsultacije sa organima i pravnim licima u cilju njihovog upoznavanja sa obavezama koje je potrebno ispuniti u postupku prije izdavanja dozvole za pristup tajnim podacima po pitanju fizičkih mjera zaštite tajnih podataka i propisanih standarda u ovoj oblasti, procesuirani su zahtjevi za vršenje bezbjednosnje procjene ugroženosti i zahtjevi za pregled protiv prisluškivanja.

Nakon implementacije mjera zaštite tajnih podataka od strane organa i pravnih lica, Direkcija provjerava ispunjenost fizičkih mjera zaštite tajnih podataka u prostorijama namijenjenim za rad sa tajnim podacima.

U cilju ispunjavanja propisanih standarda iz oblasti fizičkih mjera zaštite tajnih podataka u toku 2023.godine, održani su sastanci i konsultacije sa predstavnicima Službe Predsjednika Crne Gore, Vrhovnog suda, Uprave za izvršenje krivičnih sankcija, Specijalnog državnog tužilaštva.

Direkcija je saradivala i sa predstavnicima pravnih lica, koje je u kontinuitetu upoznavala sa cjelokupnom procedurom za dobijanje dozvole za pristup tajnim podacima za pravno lice.

III-2 Informatičke mjere zaštite tajnih podataka

Informacioni sistem za razmjenu nacionalnih tajnih podataka

Direkcija za zaštitu tajnih podataka upravlja komunikaciono informacionim sistemom koji je sertifikovan za razmjenu nacionalnih tajnih podataka do i uključujući stepen tajnosti TAJNO. Korisnici sistema su Centralni registar Direkcije za zaštitu tajnih podataka i podregisti u Ministarstvu odbrane, Ministarstvu vanjskih poslova, Agenciji za nacionalnu bezbjednost i Stalnoj misiji Crne Gore pri NATO u Briselu.

Odjeljenje za informatičku zaštitu tajnih podataka tokom 2023. godine u kontinuitetu se bavilo unapređenjem i održavanjem informacionog sistema za razmjenu nacionalnih tajnih podataka.

Ostale aktivnosti

Odjeljenje za informatičku zaštitu tajnih podataka kroz svoje svakodnevne aktivnosti u kontinuitetu se bavi aktivnostima na održavanju i unapređenju informacionih sistema u kojima se obrađuju tajni podaci, kao i računara i računarske opreme koju koriste zaposleni u Direkciji.

Imajući u vidu da je razvijena nova platforma za web prezentacije državnih organa, službenici DZTP sprovedli su aktivnosti na podizanju nove web prezentacije DZTP, kao i migraciji sadržaja sa stare web prezentacije.

Pored navedenih aktivnosti, Odjeljenje za informatičku zaštitu tajnih podataka u kontinuitetu sprovodi i aktivnosti u sklopu svojih nadležnosti koje se tiču upotrebe i distribucije kriptografskog materijala i akreditacije informacionih sistema u kojima se obrađuju tajni podaci.

Sistem za prenos NATO tajnih podataka - NS WAN

Razmjena tajnih podataka u elektronskoj formi između Centralnog registra Direkcije za zaštitu tajnih podataka, Ministarstva vanjskih poslova, Ministarstva odbrane (na lokacijama u Ministarstvu odbrane i Vazduhoplovno operativnom centru Vojske Crne Gore – VOC), kao i Stalne misije Crne Gore pri NATO u Briselu odvija se posredstvom NS WAN informacionog komunikacionog sistema. U saradnji sa NATO Agencijom za komunikacije i informacije (NATO Communication and Information Agency, NCIA) Odjeljenje za informatičku zaštitu tajnih podataka u kontinuitetu sprovodi aktivnosti na održavanju centralne CG lokacije ovog informacionog sistema.

Direkcija za zaštitu tajnih podataka - Odjeljenje za informatičku zaštitu tajnih podataka u saradnji sa Ministarstvom odbrane i Ministarstvom vanjskih poslova, usaglašava potrebne resurse za funkcionisanje ili unapređenje NS WAN informacionog sistema, na osnovu čega se svake godine generiše poseban ugovor za pružanje NCIA usluga za potrebe Crne Gore ("Service Support Package for Montenegro, SSP"). Ovaj ugovor za 2023. godinu (SSP 2023) direktor Direkcije za zaštitu tajnih podataka potpisao je u decembru 2023. godine.

Odjeljenje za informatičku zaštitu tajnih podataka u okviru svojih NDA (National Distribution Authority) nadležnosti u kontinuitetu se bavi rukovanjem kriptografskog materijala za potrebe ovog i drugih informacionih sistema u kojima se obrađuju tajni podaci.

IV NATO I EU

Najznačajnija dužnost Direkcije u vezi sa tajnim podacima NATO i EU je dužnost da kao bezbjednosni organ koordinira i sprovodi bezbjednosnu politiku NATO i EU u Crnoj Gori, u cilju obezbjeđivanja adekvatnog nivoa zaštite tajnih podataka (NSA - National Security Authority) i izdavanje NATO i EU sertifikata za pristup NATO i EU tajnim podacima.

U cilju adekvatne razmjene i zaštite NATO i EU tajnih podataka, ustanovljeni su i vode se Centralni registar NATO i EU tajnih podataka u Direkciji za zaštitu tajnih podataka i Podregistri tajnih podataka u Stalnoj misiji Crne Gore pri NATO i Stalnoj misiji Crne Gore pri EU u Briselu, kao i Komandi združenih snaga SHAPE u Monsu.

Podregistri tajnih podataka predstavljaju prvu tačku prijema NATO i EU tajnih podataka, odakle se tajni podaci distribuiraju Centralnom registru Direkcije za potrebe državnih organa u Crnoj Gori.

Distribucija tajnih podataka iz Centralnog registra prema državnim organima, korisnicima NATO i EU tajnih podataka, vrši se u okviru registara tajnih podataka uspostavljenih u državnim organima.

IV-1. NATO

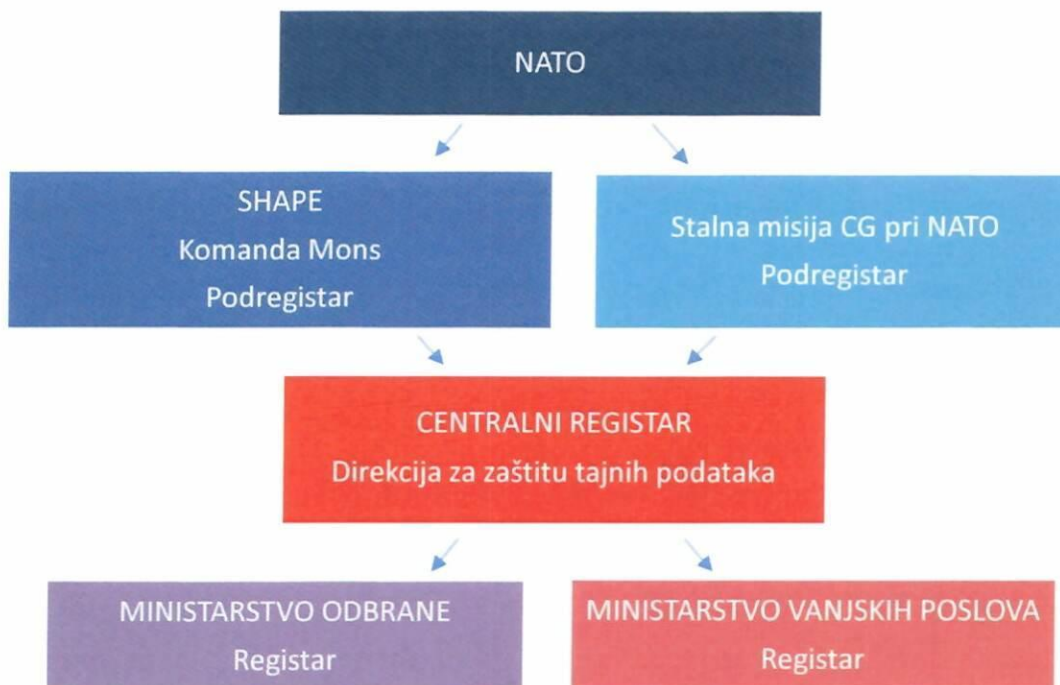
Pravni okvir za saradnju

Zakon o potvrđivanju Sporazuma između potpisnica Sjevernoatlantskog ugovora o bezbjednosti podataka ("Službeni list Crne Gore - Međunarodni ugovori", broj 12/17 od 07.12.2017), predstavlja pravni okvir za saradnju u oblasti uzajamne zaštite i čuvanja NATO tajnih podataka koji se dostavljaju Crnoj Gori i tajnih podataka koje Crna Gora dostavlja NATO-u i obezbjeđuje primjenu bezbjednosnih standarda i postupaka za razmjenu i zaštitu tajnih podataka.

Razmjena NATO tajnih podataka

Sa NATO se u kontinuitetu odvija razmjena tajnih podataka, koja je otpočela nakon upućivanja prvog kontigenta crnogorskih vojnika u mirovnu misiju ISAF u Avganistanu, a kasnije u misiju "Resolute Support" u Avganistanu.

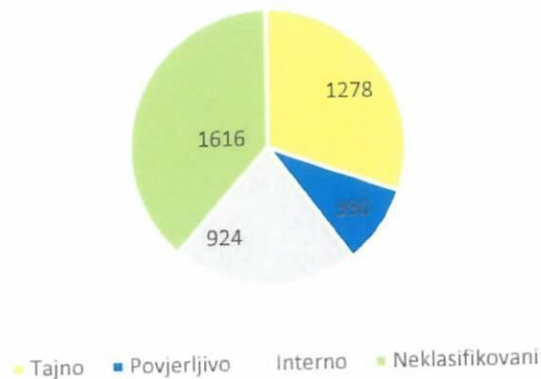
Pristupanjem Crne Gore NATO Savezu uveden je novi sistem elektronske razmjene NATO tajnih podataka NATO SECRET WAN AREA NETWORK (NS WAN) odobren od strane NATO Kancelarije za bezbjednost (NOS).



*šematski prikaz razmjene tajnih podataka sa NATO

U 2023. godini razmijenjeno je ukupno 4208 NATO tajnih podataka različitih stepena tajnosti, od čega 1278 stepena tajnosti TAJNO, 390 stepena tajnosti POVJERLJIVO, 924 stepena tajnosti INTERNO i 1616 neklasifikovanih podataka.

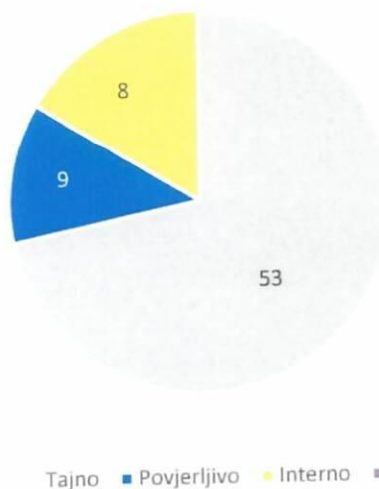
Razmjena NATO tajnih podataka po stepenima tajnosti



Razmjena nacionalnih tajnih podataka sa Stalnom misijom Crne Gore pri NATO u Briselu

Sa Stalnom misijom Crne Gore pri NATO u Briselu, u 2023. godini, razmijenjena su ukupno 70 tajna podataka različitih stepena tajnosti, od čega 53 stepena tajnosti TAJNO, 9 stepena tajnosti POVJERLJIVO i 8 stepena tajnosti INTERNO.

Razmjena domaćih tajnih podataka sa Misijom CG pri NATO



Sertifikati za pristup NATO tajnim podacima

Za pristup NATO tajnim podacima koji se prosleđuju Crnoj Gori, kao i za učešće na određenim NATO aktivnostima (konferencijama, sastancima, kursevima, obukama, vježbama,

radionicama i sl.) na kojima se razmatraju NATO tajni podaci, neophodno je posjedovanje NATO sertifikata.

U skladu sa Zakonom o potvrđivanju Sporazuma između potpisnica Sjevernoatlantskog ugovora o bezbjednosti podataka, Direkcija je organ nadležan za izdavanje NATO sertifikata za pristup NATO tajnim podacima i u 2023. godini izdala je 306 NATO sertifikata (NATO Personnel Security Clearance - NATO PSC).

U skladu sa preporukama NATO sačinjen je spisak pozicija na nacionalnom nivou i lica na tim pozicijama koja imaju pristup posebnoj grupi NATO tajnih podataka (NATO sensitive informations), kao i spisak ovlašćenih lica i njihovih zamjenika u Direkciji i Stalnoj misiji Crne Gore pri NATO u Briselu ovlašćenih za prijem i dostavu NATO COSMIC/ATOMAL podataka.

NATO NOS inspeksijska kontrola

NATO tajni podaci prosljeđeni Crnoj Gori čuvaju se u Centralnom registru Direkcije, koriste u skladu sa propisanim bezbjednosnim standardima i podliježu redovnoj kontroli NATO Kancelarije za bezbjednost (NOS).

U Direkciji je tokom 2023.godine, kontinuirana praćena realizacija preporuka i korektivnih mjera iz Izvještaja o izvršenom inspeksijskom nadzoru u 2022.godini, nad sprovođenjem mjera zaštite NATO tajnih podataka u Crnoj Gori u organima gdje je izvršen nadzor od strane NATO - Kancelarije za bezbjednost.

Pored kontrole od strane NATO Kancelarije za bezbjednost (NOS), NATO tajni podaci koji se dostavljaju državnim organima na korišćenje podliježu i inspeksijskoj kontroli Direkcije za zaštitu tajnih podataka.

IV-2. EVROPSKA UNIJA

Pravni okvir za saradnju

Sporazum o bezbjednosnim procedurama za razmjenu i zaštitu tajnih podataka zaključen između Crne Gore i Evropske Unije (septembra 2010. godine) i Bezbjednosni aranžmani za implementaciju Sporazuma (iz februara 2011. godine) predstavljaju pravni okvir za saradnju u oblasti tajnih podataka i obezbjeđuju primjenu standarda prilikom razmjene i zaštite tajnih podataka iz oblasti zajedničke vanjske, bezbjednosne i odbrambene politike.

EU PREGOVORI

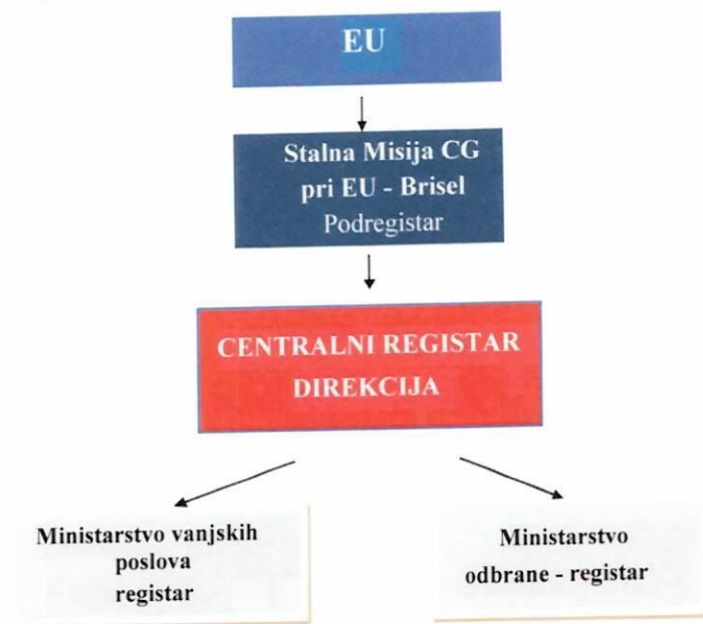
Poglavlje 10 – Informatičko društvo i mediji

Službenik Odjeljenja za informatičku zaštitu tajnih podataka je od septembra 2022.godine, učestvovao u radu Radne grupe za pripremu i vođenje pregovora o pristupanju Crne Gore Evropskoj uniji za oblast pravne tekovine Evropske unije.

Poglavlje 31 – Vanjska, bezbjednosna i odbrambena politika

Službenik Odjeljenja za zaštitu tajnih podataka, kao član radne grupe za Poglavlje 31 – Vanjska, bezbjednosna i odbrambena politika, aktivno je učestvovao u radu sjednica, u cilju realizacije obaveza koje proističu iz Programa pristupanja Crne Gore Evropskoj uniji (PPCG).

Razmjena EU tajnih podataka



Za pristup EU tajnim podacima koji se prosleđuju Crnoj Gori, kao i za učešće u misijama EU i drugim aktivnostima, neophodno je posjedovanje EU sertifikata (EU PSC).

U skladu sa Sporazumom o bezbjednosnim procedurama za razmjenu i zaštitu tajnih podataka zaključenim između Crne Gore i Evropske Unije, Direkcija je organ nadležan za izdavanje EU sertifikata za pristup EU tajnim podacima i u 2023. godini izdala je 5 EU sertifikata.

V MEĐUNARODNA SARADNJA

U izvještajnom periodu, u okviru međunarodne saradnje, aktivnosti Direkcije za zaštitu tajnih podataka realizovale su se kroz bilateralnu i multilateralnu saradnju.

Direkcija za zaštitu tajnih podataka, 28. avgusta 2023. godine, bila je predsjedavajuća na XIII SEENSA konferenciji održanoj u Ohridu, uz operativnu i finansijsku podršku Direktorata za zaštitu tajnih podataka Republike Makedonije (NSA), kao domaćina i Regionalnog Centra za saradnju (RCC) sa sjedištem u Sarajevu.

Akcentat XIII SEENSA susreta, dat je na obezbjeđivanju platforme za razgovore na visokom nivou i razmjenu informacija o pitanjima od zajedničkog interesa vezanim za rad nacionalnih organa u okviru sjeverno-istočne Evrope.

Cilj XIII SEENSA Konferencije bio je da se istraže načini za zajedničku edukaciju, izgradnju kapaciteta i inicijative za obuku za unapređivanje regionalne bezbjednosne saradnje.

Takođe, u okviru pomenute inicijative održana je i redovna godišnja konferencija direktora Nacionalnih bezbjednosnih organa Jugoistočne Evrope. Budući da je Crna Gora bila predsjedavajuća SEENSA konferencije 2023. godine, 13. Konferencija je održana u Ohridu 28. avgusta. Učesnici su imali priliku da razgovaraju o bezbjednosnim uticajima na Jugoistočnu Evropu sa fokusom na cyber bezbjednost i evropske integracije kao i o budućoj saradnji u ovom formatu. Na konferenciji je dogovoreno i da 2024. godine predsjedavajuća SEENSA konferencije bude Bugarska.

U okviru multilateralne saradnje direktor Direkcije za zaštitu tajnih podataka učestvovao je kao panelista na Bezbjednosnoj konferenciji u organizaciji Marshall centra, koja je takođe organizovana u avgustu u Ohridu. Učesnici su imali priliku da razmjene iskustva i iniciraju jačanje međunarodne i regionalne saradnje u oblasti zaštite tajnih podataka.

U cilju jačanja i intenziviranja bilateralne saradnje Direkcija za zaštitu tajnih podataka je nastavila rad na usaglašavanju sporazuma o razmjeni i zaštiti tajnih podataka sa Rumunijom, Republikom Hrvatskom, Republikom Srbijom i započela pregovore na usaglašavanju sporazuma sa Državom Izrael i Ukrajinom.

U okviru međunarodne saradnje realizovane su posjete od strane kolega iz Republike Sjeverne Makedonije, Slovenije i Bosne i Hercegovine.

U okviru saradnje sa NATO, Direktor Direkcije za zaštitu tajnih podataka u oktobru 2023. godine učestvovao je na redovnom godišnjem sastanku NATO bezbjednosnog komiteta koji je održan u Briselu, NATO HQ, na nivou direktora Nacionalnih bezbjednosnih organa.

Predstavnik Odjeljenja za informatičku zaštitu tajnih podataka učestvovao je od 19. - 20. oktobra 2023. godine u Briselu, na sastanku Security Committee in CIS Security format, koji okuplja predstavnike država članica NATO.

Direkcija za zaštitu tajnih podataka je u okviru SAA nadležnosti (Security Accreditation Authority) učestvovala na sastanku međunarodnog BICES akreditacionog tijela (BICES Accreditation Board, BSAB) u Bratislavi od 08. - 10. novembra 2023. godine.

U periodu od 11. do 15. septembra 2023. godine u Cirihu je održana 37. godišnja Multinacionalna radna grupa u oblasti industrijske bezbjednosti (MISWIG). Učesnici, među kojima je bila i predstavnica Direkcije za zaštitu tajnih podataka, imali su priliku da nastave rad na značajnim pitanjima koja se odnose na MISWIG pravila i procedure, aranžmanima za međunarodni prenos tajnih podataka, opreme i/ili komponenata, pitanjima koja se odnose na učešće i uticaj stranaca u vlasničkoj strukturi kao i drugim pitanjima od značaja u oblasti industrijske bezbjednosti. Na pomenutoj konferenciji Crna Gora je po prvi put uzela učešće kao formalna članica Multinacionalne radne grupe u oblasti industrijske bezbjednosti (MISWIG).

Direkcija takođe ima i kontinuiranu regionalnu i međunarodnu saradnju u oblasti sajber bezbjednosti.

U okviru bileteralne saradnje, u izvještajnom periodu, Direkcija za zaštitu tajnih podataka bila je domaćin kolegama iz NSA Sjeverne Makedonije, Bosne i Hercegovine i Slovenije a sve sa ciljem razmjene iskustava, dobrih praksi i planiranih aktivnosti po pitanju ove vrste saradnje.

U cilju jačanja saradnje u oblasti sajber bezbjednosti CIRT kontinuirano saraduje sa ključnim međunarodnim institucijama kao što su: FIRST, ITU, NATO, OEBS, DCAF, KISA, RCC, Savjet Evrope.

VI MEĐURESORSKA SARADNJA

U izvještajnom periodu, Direkcija za zaštitu tajnih podataka je imala kontinuiranu međuresorsku saradnju koja se u najvećoj mjeri odnosila na implementaciju propisa o tajnosti podataka, realizaciju mjera zaštite tajnih podataka i rješavanje zahtjeva za izdavanje dozvola za pristup tajnim podacima.

Saradnja sa Ministarstvom odbrane odvijala se po pitanju sprovođenja bezbjednosnih provjera za vojna lica i službenike Ministarstva za koje su podneseni zahtjevi za izdavanje dozvola za pristup tajnim podacima, kroz realizaciju obuka o bezbjednosnoj kulturi, tajnosti podataka i informatičkoj zaštiti tajnih podataka, davanju mišljenja i sugestija na sporazume o saradnji u oblasti odbrane u dijelu koji se odnosi na tajne podatke, finansijske poslove i unutrašnju reviziju, izdavanje dozvola za pristup tajnim podacima, učešće na sastancima i sl.

Saradnja sa Agencijom za nacionalnu bezbjednost odvijala se po pitanju sprovođenja bezbjednosnih provjera za lica za koja su podneseni zahtjevi za izdavanje dozvola za pristup tajnim podacima, NATO i EU sertifikata, vršenja bezbjednosnih provjera za strance po zamolnicama drugih država, izrade bezbjednosnih procjena ugroženosti, pregleda protiv prisluškivanja i pregleda od kompromitujućeg elektromagnetnog zračenja-TEMPEST mjerenja.

Saradnja sa Ministarstvom finansija odvijala se kroz podnošenje zahtjeva za dodjelu budžetskih sredstava za 2024. godinu i pripremu Nacrta budžeta Direkcije za zaštitu tajnih podataka za 2024. godinu, realizaciju budžeta i dostavljanje izvještaja o primicima, izdacima i ugovorenim obavezama, dostavljanje godišnjeg izvještaja o aktivnostima na sprovođenju i unaprijeđenju upravljanja i kontrola, dostavljanje zahtjeva za preusmjeravanje odobrenih sredstava po programima i pojedinim izdacima, dostavljanje Plana javnih nabavki, Izvještaja o javnim nabavkama.

Saradnja sa Agencijom za sprječavanje korupcije odvijala se po pitanju obaveza koje proizilaze iz Plana integriteta i izveštavanje Agencije o njegovom sprovođenju u 2023. godini, te je shodno tome sačinjen Izvještaj o sprovođenju Plana integriteta Direkcije. Sačinjena je Metodologija za procjenu primjene antikorupcijskih mjera Direkcije za zaštitu tajnih podataka i popunjen je Upitnik za procjenu efektivnosti i efikasnosti Plana integriteta.

Saradnja sa Agencijom za zaštitu ličnih podataka i slobodan pristup informacijama odvijala se kroz zaštitu ličnih podataka, dostavljanje podataka za potrebe vođenja informacionog sistema pristupa informacijama i ponovne upotrebe informacija.

Saradnja sa Upravom za ljudske resurse odvijala se kroz realizaciju obuka na temu „Tajnost podataka i informatička zaštita tajnih podataka“, zatim kroz učešće zaposlenih na obukama koje realizuje Uprava za kadrove u okviru Programa stručnog osposobljavanja. Saradnja se odvijala i kroz izradu Kadrovskog plana (planiranju broja zaposlenih, promjenama u kadrovskoj strukturi i drugim pitanjima upravljanja kadrovima, u skladu sa budžetskim sredstvima), vođenja i ažuriranja kadrovskog informacionog sistema (KIS) i dr.

I u ovom izvještajnom periodu, kontinuirano se saradivalo sa Privrednom komorom Crne Gore, Ministarstvom ekonomskog razvoja i Ministarstvom vansjnih poslova, kroz aktivnosti na izradi Uputstva o postupku provjere ispunjenosti uslova za učešće privrednih subjekata registrovanih u Crnoj Gori i izdavanje potvrde za učešće u nabavkama za potrebe Sjeverno-Atlantskog Saveza. U tom smislu je održan okrugli sto za privredne subjekte, gdje su pored predstavnika Direkcije, učešće uzeli i predstavnici pomenutih državnih organa.

Predstavnik Odjeljenja za informatičku zaštitu tajnih podataka, učestvovao je od avgusta 2023. godini u radu Operativnog tima za suprotstavljanje sajber napadima kao njegov član.

Direkcija je na svojoj internet stranici objavljivala informacije koje zahtijevaju proaktivni pristup, vodeći računa o zaštiti ličnih podataka i podataka koji su označeni stepenom tajnosti.

VII SARADNJA SA NEVLADINIM ORGANIZACIJAMA

Direkcija za zaštitu tajnih podataka saradivala je sa nevladinim organizacijama kroz rješavanje podnijetih zahtjeva za slobodan pristup informacijama, kao i kroz pripremu, podnošenje Izvještaja i izvoda iz informacionog sistema Agenciji za sprječavanje korupcije, u vezi zahtjeva za slobodan pristup informacijama.

VIII OBUKE IZ OBLASTI TAJNIH PODATAKA

U cilju stručnog usavršavanja državnih službenika i namještenika i unapređenja znanja iz oblasti tajnih podataka, Direkcija za zaštitu tajnih podataka u saradnji sa Upravom za kadrove realizovala je u kontinuitetu seminare na temu „Tajnost podataka i informatička zaštita tajnih podataka“, za zaposlene u organima državne uprave.

Unaprijeđen je sistem obuke iz oblasti tajnih podataka na način što je, u okviru TAIEX instrumenata tehničke podrške, uspostavljena elektronska aplikacija za E-trening, koja pruža mogućnost državnim službenicima za lakšim i savremenijim edukovanjem u ovoj oblasti. Ovaj oblik edukacije primijenjuje se na sva lica prije izdavanja dozvole za pristup tajnim podacima.

Stručno osposobljavanje i usavršavanje službenika Direkcije

U Upravi za ljudske resurse u izvještajnom periodu, zaposleni su pohađali sljedeće obuke: zaštita ličnih podataka, Rezolucija 1325 žene, mir i bezbjednost, izrada i upravljanje projektima finansiranim iz EU fondova, Informatička zaštita podataka, Cloud servisi za skladištenje podataka i produktivniji rad, Sajber bezbjednost, Google paket besplatnih alata, Pregovaračka struktura Crna Gora i Evropska unija, izrada Kadrovskog plana, finansijsko upravljanje i kontrole, Samoprocjena unutrašnjih kontrola, upravljanje rizicima, mobing.

U okviru Mreže za ljudske resurse realizovano je učešće na radionicama: Uloga vrhovne državne revizije u kontroli zakonitosti i uspješnosti rada javnog sektora, Zadovoljstvo zaposlenih u državnoj upravi, Upravljanje ljudskim resursima-novi standardi i modeli.

Službenici Odjeljenja za informatičku zaštitu tajnih podataka učestvovali su na NDA konferenciji na kojoj učestvuju predstavnici NDA iz država članica NATO u Varšavi od 8. do 12. maja 2023. godine.

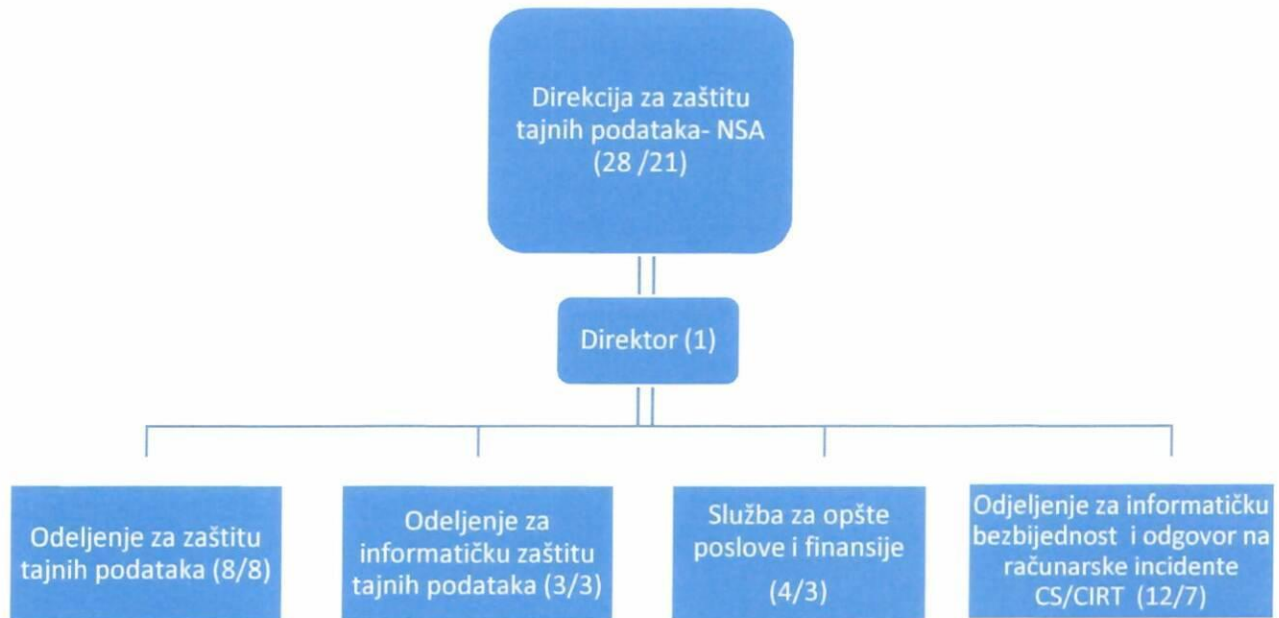
U periodu od 17. do 21. juna 2023. godine u NCIA centru za obuku u Portugalu službenik Direkcije pohađao je obuku za upravljanje kripto materijalima (004 Crypto administration course).

U okviru Programa stručnog osposobljavanja Uprave za kadrove u 2023. godini, sa predavačima iz DZTP kontinuirano su se organizovale obuke na temu tajnosti podataka i informatičke zaštite tajnih podataka, za potrebe zaposlenih u Ministarstvu odbrane i Vojsci Crne Gore.

IX ORGANIZACIJA DIREKCIJE

Vlada Crne Gore na sjednici održanoj 11.06.2021. godine., utvrdila je Pravilnik o unutrašnjoj organizaciji i sistematizaciji Direkcije za zaštitu tajnih podataka, koji je stupio na snagu 25. 06.2021. godine.

U skladu sa Pravilnikom, Direkcija vrši poslove iz svoje nadležnosti u okviru četiri organizacione jedinice: Odjeljenje za zaštitu tajnih podataka, Odjeljenje za informatičku zaštitu tajnih podataka, Odjeljenje za informatičku bezbjednost i odgovor na računarske incidente (CS/CIRT) i Služba za opšte poslove i finansije.



U Odeljenju za zaštitu tajnih podataka vrše se poslovi iz osnovne djelatnosti Direkcije koji se odnose na: obezbjeđenje primjene standarda i propisa iz oblasti zaštite tajnih podataka; koordiniranje aktivnosti koje obezbjeđuju zaštitu tajnih podataka povjerenih Crnoj Gori od strane drugih država i međunarodnih organizacija, izradu i ažuriranje Plana zaštite tajnih podataka, inspekcijski nadzor nad sprovođenjem Zakona o tajnosti podataka i primjenom međunarodnih ugovora, sprovođenje postupka za izdavanje dozvola za pristup tajnim podacima i izdavanje NATO i EU sertifikata za pristup NATO i EU tajnim podacima, postupka za ograničenje ili prestanak važenja dozvole, evidenciju podnijetih zahtjeva za izdavanje dozvola i evidenciju izdatih i oduzetih dozvola, NATO i EU sertifikata, obuku korisnika tajnih podataka, vođenje Centralnog registra NATO i EU tajnih podataka i saradnju sa podregistrima tajnih podataka u Stalnoj misiji Crne Gore pri NATO i Misiji Crne Gore pri EU, evidenciju NATO i EU tajnih podataka koji se prosleđuju Crnoj Gori, diseminaciju i njihovo dostavljanje korisnicima, evidenciju NATO ATOMAL tajnih podataka, evidenciju domaćih tajnih podataka, stručnu pomoć organima i organizacijama radi ispunjavanja bezbjednosno-tehničkih uslova za rad sa tajnim podacima, ustanovljavanje i vođenje registara, podregistara i kontrolnih tačaka, akreditovanje i odobravanje njihovog rada, unutrašnju kontrolu nad sprovođenjem mjera zaštite tajnih podataka, informisanje strane države odnosno međunarodne organizacije o bezbjednosti tajnih podataka koje je strana država, odnosno međunarodna organizacija predala Crnoj Gori, međunarodnu saradnju i kontinuiranu saradnju sa NATO Kancelarijom za bezbjednost (NOS) i Kancelarijom za bezbjednost Generalnog sekretarijata Savjeta EU (GSCSO) i drugi poslovi u skladu sa propisima.

U Odeljenju za informatičku zaštitu tajnih podataka podataka vrše se poslovi iz osnovne djelatnosti koji se odnose na primjenu mjera bezbjednosti za zaštitu tajnih podataka koji se primaju, obrađuju, prenose, čuvaju i arhiviraju u komunikaciono-informacionim sistemima i drugim elektronskim sistemima, od gubitka povjerljivosti, cjelovitosti ili dostupnosti, i to:

obezbjedjivanje primjene standarda i propisa iz oblasti informatičke zaštite tajnih podataka, prijem, obradu, prenos, čuvanje i arhiviranje NATO i EU tajnih podataka u elektronskoj formi, obezbjeđivanje da su kriptografski sistemi, proizvodi i mehanizmi za zaštitu tajnih podataka adekvatno i efikasno odabrani, instalirani i održavanim, nadzor nad rukovanjem kriptomaterijalima NATO i EU i nadzor nad proizvodnjom, distribucijom i čuvanjem kriptomaterijala za potrebe jedinstvenog sistema za elektronsku razmjenu domaćih tajnih podataka, proizvodnja, distribucija i čuvanje kriptomaterijala za potrebe jedinstvenog sistema za elektronsku razmjenu domaćih tajnih podataka između organa; certifikovanje komunikaciono-informacionih sistema (CIS) i procesa u kojima se obrađuju, prenose i čuvaju domaći, NATO i EU tajni podaci i certifikovanje prenosivih komunikaciono-informacionih sredstva i memorijskih medija koji se koriste u sistemu (CIS); zaštita prostorija i opreme od rizika elektromagnetnog zračenja (TEMPEST), procjena mogućeg ugrožavanja bezbjednosti tajnih podataka od upada u IS, edukacija i podizanje CIS bezbjednosne svijesti, instaliranje uređaja za čuvanje rezervnih kopija (back-up) tajnih podataka; uništavanje tajnih podataka u elektronskoj formi, memorijskih medija i uređaja za enkripciju podataka; organizovanje obuka i administracija portala za on-line obuku, ažuriranje web stranice Direkcije i dr.

U razmjeni i zaštiti tajnih podataka sa NATO i EU, vrše se poslovi koji se odnose na: bezbjednost komunikacija za izbor, upravljanje i održavanje kriptografske opreme za prenos, obradu i čuvanje tajnih podataka (NCSA - National Communication Security Authority); sprovođenje bezbjednosne akreditacije komunikaciono-informacionih sistema i procesa u kojima se koriste tajni podaci (SAA - Security Accreditation Authority), koje obuhvata rješavanje po zahtjevu za certifikovanje sistema, vršenje bezbjednosne provjere sistema, izdavanje certifikata i privremenih certifikata i vođenje evidencije u vezi s tim i upravljanje materijalima za kriptografsku zaštitu tajnih podataka i bezbjedno rukovanje, čuvanje, distribuciju i evidenciju kriptomaterijala (NDA - National Distribution Authority).

U Odjeljenju za informatičku bezbjednost i odgovor na računarske incidente (CS/CIRT)

vrše se poslovi iz osnovne djelatnosti koji se odnose na: unaprjeđenje bezbjednosti i zaštitu vrše se poslovi iz osnovne djelatnosti koji se odnose na: unaprjeđenje bezbjednosti i zaštitu mrežne infrastrukture, monitoring mreže sa ciljem identifikacije incidenata, usklađivanje aktivnosti lokalnih CIRT timova na teritoriji Crne Gore, održavanje kontakta sa ostalim državnim organima pravnim i fizičkim licima po pitanju očuvanja i unaprijeđenja informatičke bezbjednosti, razmjenu informacija sa nacionalnim CIRT/CERT timovima drugih država putem članstva u međunarodnim organizacijama, pružanje informacija i procjenu stanja informatičke bezbjednosti, izvještavanje drugih CIRT/CERT timova, sastavljanje izvještaja i upozorenja za ostale korisnike, izradu priručnika, softverskih alata i drugih korisnih informacija vezanih za sigurnije korišćenje informacionih tehnologija, prikupljanje informacija za identifikovanje sajber prijetnji, taktika, tehnika i postupaka koje koriste akteri u sajber prostoru, istraživanje aktuelnih i potencijalnih prijetnji u sajber prostoru, analizu opsega ranjivosti u hardveru i softveru, izrada smjernica koje se odnose na rizike i mjere kontrole vezane za nove prijetnje u sajber prostoru, prevenciju, obradu i otklanjanje posljedica od računarskih incidenata na internetu i drugih rizika bezbjednosti informacionih sistema u mreži državnih organa, provjeru ranjivosti sistema, prikupljanje, evidentiranje i obradu podataka o incidentima, testiranje i primjenu novih softverskih i hardverskih sistema za zaštitu IT resursa, monitoring IS u mreži državnih organa, obradu podataka i otklanjanje posljedica u smislu utvrđivanja pojave i težine incidenta, utvrđivanje uzroka incidenta, posredovanje u kontaktiranju ostalih strana koje su uključene u incident, otklanjanje ranjivosti u sistemu, obezbjeđivanja sistema i zaštite od mogućih incidenata, definisanje liste i zaštite kritične informatičke infrastrukture, identifikovanje rizika i primjenu adekvatnih mjera zaštite kako bi se osigurao kontinuitet

poslovanja kritične informatičke infrastrukture, provjeru bezbjednosti i ranjivosti sistema i implementaciju mjera zaštite za prevenciju incidentnih situacija i ublažavanja posljedica i razvijanje plana za upravljanje sajber incidentima i obavljanje drugih poslova iz djelokruga rada Odjeljenja.

U Službi za opšte poslove i finansije vrše se poslovi koji se odnose na: izradu opštih akata, programa rada i izvještaja o radu, izradu pojedinačnih akata o ostvarivanju prava iz radnog odnosa: prijem, raspoređivanje, zarada, naknada i drugih primanja i dr., javne i povjerljive nabavke, pripremu i sačinjavanje ugovora koji sadrže tajne podatke – povjerljivi ugovori, obradu i korišćenje tajnih podataka kod povjerljivih nabavki, materijalno finansijsko poslovanje, izradu finansijskog plana, korišćenje sredstava u skladu sa budžetom i finansijskim planom, vođenje poslovnih knjiga, periodične obračune i završne račune, izradu finansijskih iskaza i dostavljanje Državnom trezoru, blagajničko i knjigovodstveno poslovanje, upoznavanje sa rezultatima unutrašnje revizije: konačnim revizorskim izvještajem i predlogom plana aktivnosti za sprovođenje preporuka za poboljšanje sistema upravljanja i unutrašnje kontrole, izradu internih pravila i procedura za uspostavljanje i sprovođenje upravljanje i razvoj unutrašnjih kontrola, aktivnosti po pitanju rodne ravnopravnosti, Plana inegriteta, saradnje sa nadležnim organima, učešće u realizaciji akcionih planova, saradnju sa nevladinim organizacijama i rješavanje zahtjeva za slobodan pristup informacijama, postupanje po prijavama zviždača, saradnju po pitanju stručnog usavršavanja zaposlenih, oglašavanje slobodnih radnih mjesta, vođenje kadrovskog informacionog sistema (KIS), evidenciju primljenih poklona, prijem, vođenje evidencije i distribuciju domaćih tajnih podataka i njihovo čuvanje, kancelarijsko poslovanje i vođenje djelovodnika i drugih knjiga, rukovanje pečatima i štambiljima i njihovo čuvanje, dostavu NATO i EU tajnih podataka i sprovođenje adekvatnih mjera zaštite prilikom dostave drugim državama i međunarodnim organizacijama, vođenje evidencije o korišćenju motornih vozila i dr.

Pravilnikom o unutrašnjoj organizaciji i sistematizaciji Direkcije za zaštitu tajnih podataka od 25.06.2021.godine, sistematizovano je 28 službeničkih radnih mjesta za 28 izvršilaca, uključujući i direktora. Ukupan broj zaposlenih izvršilaca je 23 od čega je jedno profesionalno vojno lice koje je upućeno iz Vojske Crne Gore na rad u Direkciju.

U izvještajnom periodu pripremljen je Predlog Pravilnika o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji i sistematizaciji Direkcije za zaštitu tajnih podataka, i upućen na mišljenje nadležnim organima.

U skladu sa Sporazumom zaključenim između Ministarstva vanjskih poslova i Direkcije za zaštitu tajnih podataka, jedan službenik Direkcije upućen je na period od dvije godine u Stalnu misiju Crne Gore pri NATO u Briselu. Ovaj službenik je prva "kontakt tačka" u Podregistru tajnih podataka u Misiji, za prijem NATO tajnih podataka i njihovu distribuciju Centralnom registru Direkcije.

Pripremljen je i usvojen Kadrovski plan Direkcije za zaštitu tajnih podataka za 2023. godinu., i uz saglasnost Ministarstva finansija, dostavljen je Upravi za ljudske resurse.

Kadrovskim planom Direkcije za zaštitu tajnih podataka za 2023. godinu, planirano je zapošljavanje za 2 radna mjesta u okviru Odjeljenja za informatičku bezbjednost i odgovor na računarske incidente (CS/CIRT), što će zbog nedostatka novčanih sredstava biti realizovano do kraja drugog kvartala 2024.godine.

U ovom izvještajnom periodu, izvršeno je redovno ažuriranje podataka o zaposlenima u aplikaciju Kadrovskog informacionog sistema (KIS). Takođe, sprovedena je Analiza potreba za obukama Direkcije za zaštitu tajnih podataka, i u skladu sa tim dostavljen je Izvještaj Upravi za ljudske resurse.

X INFORMATIČKA BEZBJEDNOST I ODGOVOR NA RAČUNARSKE INCIDENTE

Odjeljenje za informatičku bezbjednost i odgovor na računarske incidente – CIRT, osnovano je u skladu sa Zakonom o informacionoj bezbjednosti („Službeni list CG”, br. 14/2010, 40/2016, 74/2020, i 67/2021.), 2012. Godine, kao dio zajedničkog projekta Vlade Crne Gore i Međunarodne telekomunikacione unije (ITU). Odjeljenje je zaduženo za prevenciju i zaštitu od računarskih incidenata s ciljem očuvanja sajber bezbjednosti u Crnoj Gori. U skladu sa Zakonom o tajnosti podataka i Zakonom o informacionoj bezbjednosti vrši funkciju zaštite od računarskih bezbjednosnih incidenata na Internetu i drugih rizika u vezi sa informacionom bezbjednošću.

Krovni dokument predstavlja Strategija sajber bezbjednosti Crne Gore 2022-2026 (u daljem tekstu Strategija), kojom je prepoznato sedam operativnih ciljeva, čija je realizacija detaljnije definisana kroz pojedinačne zadatke Akcionog plana (AP) za 2022-2023. godinu, i to: unapređenje ljudskih i finansijskih resursa, efikasan mehanizam za odgovor na sajber incidente, unapređenje mjera prevencije i edukacije o sajber bezbjednosti, poboljšanje odgovora na sajber kriminal, osnažen i harmonizovan sistem zaštite podataka, razvoj i unapređenje saradnje s nacionalnim i međunarodnim partnerima i uspostavljen sistem zaštite kritične infrastrukture. U izvještajnom periodu, shodno AP za implementaciju Strategije, Odjeljenje za informatičku bezbjednost i odgovor na računarske incidente, je realizovalo aktivnosti za koje su bila odobrena finansijska sredstva.

U izvještajnom periodu, shodno AP za implementaciju Strategije, Odjeljenje za informatičku bezbjednost i odgovor na računarske incidente (u daljem tekstu: CIRT) je realizovalo aktivnosti za koje su bila odobrena finansijska sredstva. Za realizaciju aktivnosti iz AP za 2023 godinu, neophodno je bilo obezbijediti sredstva u iznosu od **1.035.000€**, ali je CIRT-u odobreno samo 70.700€. Iako je Strategijom prepoznato godišnje povećanje budžetskih izdvajanja za razvoj sajber kapaciteta za 10%, CIRT-u je za 2024. godinu odobreno **70.700€**, što predstavlja iznosi samo 6,8% od neophodnih sredstava za period 2022-2023 godine.

U svom djelovanju CIRT sprovodi proaktivne i reaktivne mjere. Proaktivnim mjerama djeluje prije incidenata i drugih događaja koji mogu ugroziti bezbjednost informacionih sistema, a u cilju sprečavanja ili ublažavanja rizika od incidenata. Reaktivnim mjerama odgovara na incidente i ublažava posledice koje mogu ugroziti bezbjednost sistema.

Proaktivne mjere

S obzirom na to da je najbolji način za borbu protiv sajber prijetnji proaktivno djelovanje, CIRT je tokom 2023. godine sprovodio proaktivne mjere s ciljem smanjenja rizika od incidenata. U sklopu proaktivnih mjera CIRT je sproveo niz aktivnosti na podizanju svijesti o sajber bezbjednosti, kroz objavljivanje edukativnih članaka, informacija o bezbjednosnim propustima i ranjivostima, preporukama za zaštitu u sajber prostoru i informisanjem javnosti putem portala www.gov.me/cirt i naloga na društvenim mrežama (facebook, Instagram, twitter) s ciljem pružanja pristupačnih i jednostavnih savjeta krajnjim korisnicima. Takođe, u sklopu proaktivnih mjera, predstavnici CIRT-a su djelovali putem javnih medija – gostovanja na televizijama i u radio emisijama.

I ove godine je CIRT obilježio dan sigurnog interneta, u februaru, gdje je kroz kanale na društvenim mrežama i sajtu distribuirao materijale i smjernice u cilju podizanja svijesti o značaju informacione bezbjednosti. Takođe CIRT je posebnu pažnju posvetio i oktobru mjesecu koji je poznat kao međunarodni mjesec informacione bezbjednosti gdje je poseban osvrt stavljen na temu socijalnog inženjeringa koji je prepoznat kao najveća sajber prijetnja u toku prethodne godine. Aktivnosti su sprovedene u skladu sa ENISA planom za podizanje svijesti o socijalnom inženjeringu. Po dogovoru sa predstavnicima ENISE, distribuiran je materijal koji su pripremili za obilježavanje mjeseca sajber bezbjednosti. Takođe, povodom mjeseca sajber bezbjednosti, u organizaciji CIRT-a i Odsjeka za informaciono komunikacione tehnologije Skupštine Crne Gore održana je radionica posvećena podizanju svijesti o sajber bezbjednosti. Radionica je imala za cilj upoznavanje učesnika sa sve učestalijim prijetnjama, sa fokusom na zaštitu djece na internetu.

Shodno Zakonu o informacionoj bezbednosti, a u skladu sa aktivnostima predviđenih Strategijom ažurirana je lista lokalnih CIRT-ova tj. kontakt osoba zaduženih za uspostavljanje sistema zaštite od računarskih i bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti tih sistema, koji će neposredno saradivati sa CIRT-om radi usklađivanja postupanja organa i pravnih lica u primjeni mjera informacione bezbjednosti.

U sklopu provjere ranjivosti izvršene su aktivnosti na skeniranju mreže i servera u par institucija raspoloživim alatima. Analiza serverske i mrežne infrastrukture je obuhvatila identifikaciju, prikupljanje i analizu izvještaja radi otkrivanja malicioznih aktivnosti.

U sklopu svojih redovnih aktivnosti CIRT objavljuje ranjivosti, najnovije informacije u oblasti sajber bezbjednosti, upozorenja i preporuke za građane i korisnike i šalje obavještenja o zaraženim IP adresama operaterima.

Po dogovoru sa Agencijom za elektronske komunikacije i poštansku djelatnost i internet servis provajderima(ISP) na sedmičnom nivou ISP-ovima se dostavljaju informacije o kompromitovanim adresama iz njihovog adresnog opsega.

S obzirom na veliki broj prijavljenih incidenata koji se odnose na fišing sa Udruženjem banaka Crne Gore pokrenuta je kampanja o podizanju svijesti o korišćenju bankovnih usluga.

Reaktivne mjere

U sklopu reaktivnih mjera CIRT obavlja poslove koordinacije i odgovora na incidentne situacije u sajber prostoru Crne Gore. Incidenti se prijavljuju putem web portala www.gov.me/cirt i putem email-a na kontakt@cirt.me.

Kroz analizu incidenata u sajber prostoru Crne Gore za period od 2014. do 2023. godine evidentno je da su globalne sajber prijetnje prisutne u Crnoj Gori i da se statistika ne razlikuje u velikoj mjeri u odnosu na sajber prostor Crne Gore. Analiza trenutnog stanja, pokazala je da je i tokom 2023. godine nastavljen trend rasta broja prijavljenih incidenata u odnosu na prethodne godine. Tokom 2022. godine CIRT-u je prijavljeno ukupno 672 incidenta, dok je u 2023. godini CIRT registrovao 751 prijavu. Ovaj trend se ogleda i u činjenici da je CIRT-u, tokom 2023. godine, prijavljen najveći broj incidenata koji su se odnosili na malver, uključujući maliciozne programe za ucjenu, tj. ransomvere. Zabilježen je veliki broj prevara na internetu poput finansijskih prevara i phishing napada kao i povećan broj incidenata koji su se odnosili na zloupotrebu profila na društvenim mrežama. Primjetan je i značajan porast broja napada na informacione sisteme državnih organa i pravnih lica.

Godina	Napad na web sajtove i IS	Prevare putem Interneta	Zloupotreba profila na društvenim mrežama	Neprikladan sadržaj na Internetu	Malver	Ostali (Uznemiravanje, Ucjene...)	Ukupno
2011	1	-	-	-	-	-	1
2012	3	2	-	1		-	6
2013	5	3	10	-	1	3	22
2014	5	6	20	5		6	42
2015	6	17	37	19	17	36	132
2016	18	20	36	14	50	25	163
2017	91	18	34	9	368	12	532
2018	13	68	50	6	363	37	537
2019	19	70	79	11	387	38	604
2020	25	84	90	15	383	44	641
2021	21	75	86	9	430	51	672
2022	30	81	77	6	459	31	684
2023	42	117	84	8	466	34	751

Regionalna i međunarodna saradnja

U cilju jačanja saradnje u oblasti sajber bezbjednosti pored institucija EU-a i NATO-a, CIRT kontinuirano saraduje i član je međunarodnih organizacija kao što su:

- FIRST (Forum of Incident Response and Security Teams) - međunarodna konfederacija CSIRT-ova koji saraduju i zajedno rješavaju računarsko-bezbjednosne incidente te promovišu programe prevencije. CIRT je član FIRST od 2013 godine.

- TF-CSIRT Trusted Introducer–(Task Force CSIRT) - radna grupa koja unapređuje saradnju i koordinaciju između CSIRT-a u Evropi i susjednim zemljama, istovremeno uspostavljajući veze s relevantnim organizacijama na globalnom nivou i u drugim regijama. CIRT je akreditovani član od 2013. godine.
- ITU (International Telecommunication Union) - međunarodna unija za telekomunikacije
- OSCE/OEBS (Organization for Security and Co-operation in Europe) - organizacija za evropsku bezbjednost i saradnju.
- RCC (Regional Cooperation Council) – savjet za regionalnu saradnju.
- COE (Council of Europe) - Savjet Evrope.

PROJEKTI

CIRT je i u 2023. godini nastavio sa implementacijom projekta iPROCEEDS2 (projekat Evropske unije i Savjeta Evrope). Cilj projekta je jačanje kapaciteta u borbi protiv sajber kriminala i taretiranje procedura na internetu i obezbjeđivanju elektronskih dokaza u Jugoistočnoj Evropi i Turskoj. U okviru projekta realizovane su sledeće aktivnosti koje su organizovane shodno projektnom planu:

- Predstavnik CIRT-a je učestvovao u panelu „Krivičnopravna saradnja: iskustvo i izazovi onlajn ksenofobije i rasizma“ na Međunarodnoj konferenciji o ksenofobiji i rasizmu izvršenih putem računarskih sistema“ u kojem je prezentovao studije slučaja i pravnog okvira za suzbijanje govora mržnje u Crnoj Gori
- CIRT je organizovao događaj i učestvovao u trodnevnoj radionici/simulaciji sajber napada na temu jačanje saradnje između pravosuđa u kojoj je učestvovalo 20 predstavnika iz Crne Gore iz Uprave policije, CIRT-a, EKIP-a, sudstva i tužilaštva.
- Predstavnik CIRT-a je učestvovao na „Konferenciji o podzemnoj ekonomiji“ gdje je imao priliku da čuje iskustva razvijenih zemalja i njihove odgovore na globalne sajber prijetnje i da učestvuje na radionicama o prikupljanju dokaza web digitalne forenzike i onlajn prevare.
- Predstavnik CIRT-a je učestvovao u tehničkoj vježbi/simulaciji sajber napada, a fokusirana je na saradnju između zajednice sajber bezbjednosti (prvenstveno CSIRT) i organa za sprovođenje zakona (LEA) kako bi se poboljšala spremnost zemalja da odgovore sajber izazovima.
- Predstavnici CIRT-a su učestvovali na tehničkoj vježbi/simulaciji sajber napada, a fokusirana je na jačanje saradnje i zajedničko rješavanje incidenta istraživanje napada i odgovor na sajber incidente/sajber kriminal.
- Predstavnik CIRT-a je učestvovao sastanku na temu „Uticaj vještačke inteligencije u sajber bezbjednosti“ koju su vodili predstavnici nacionalnog organa za sajber bezbjednost, sa ciljem da se pronađu najbolji ciljevi za sledeću iteraciju Praške konferencije o sajber bezbjednosti.
- Predstavnik CIRT-a je učestvovao na konferenciji i obuci "Balkan Cybersecurity Day" u organizaciji Forum of Incident Response and Security Teams (FIRST) u saradnji sa DCAF-om i iPROCEEDS-2

- Predstavnik CIRT-a je učestvovao na regionalnom događaju "Moldova Cyber Week" koji je dio evropskog mjeseca sajber bezbjednosti (ECSM) koji se bavi zaštitom kritične informatičke infrastrukture i podizanjem svijesti o sajber bezbjednosti u regionu.
- Predstavnici CIRT-a su učestvovali na sastancima povodom evaluacije i napretka ostvarenog projekta iPROCEEDS-2, kao i završnom sastanku projektnog tima iPROCEEDS2 i prisustvo Octopus konferenciji.

U sklopu projekta su kontinuirano realizovane aktivnosti shodno projektnom planu koji ima za cilj unapređenje saradnje i jačanje kapaciteta za sajber bezbjednost i sajber kriminal.

Takođe CIRT je nastavio i sa implementacijom projekta "Dobro upravljanje sajber bezbjednosti na Zapadnom Balkanu", koji finansira Ministarstvo vanjskih poslova i međunarodnog razvoja (FCDO) Ujedinjenog Kraljevstva i sprovodi DCAF (Ženevski centar za upravljanje sektorom bezbjednosti). U okviru projekta realizovane su sledeće aktivnosti:

- Predstavnik CIRT-a je učestvovao na webinaru „Razvoj CERT timova u regionu“ koji je organizovao DCAF – Ženevski centar za upravljanje bezbednosnim sektorom, u saradnji sa CERT-ovima Zapadnog Balkana
- Predstavnici CIRT-a su učestvovali u obuci za medijski trening krizne komunikacije koju je organizovao DCAF u saradnji sa CIRT.ME za državne službenike zadužene za oblast sajber bezbjednosti.
- Predstavnici CIRT-a su učestvovali na webinaru „Timovi za reagovanje na incidente u oblasti računarske bezbjednosti: strukture i funkcije ” koji je organizovao DCAF u saradnji sa CERT-ovima Zapadnog Balkana.
- Predstavnici CIRT-a su učestvovali u studijskoj posjeti u kojoj su imali priliku da razmjene iskustva sa hrvatskim Nacionalnim CERT- u koje je u okviru projekta DCAF organizovano a zajedno sa njemačkom razvojnom agencijom GIZ-a (Njemačko društvo za međunarodnu saradnju) i Ministarstva vanjskih poslova Njemačke.
- Predstavnik CIRT-a je učestvovao u studijskoj posjeti u kojoj su razmijenjena iskustva sa predstavnicima Ministarstva vanjskih poslova, Ministarstva unutrašnjih poslova, Ministarstva odbrane i agencije za informacionu bezbjednost Njemačke.

Pored aktivnosti predviđene prethodnim projektima a u cilju jačanja međunarodne saradnje realizovane su i sledeće aktivnosti:

- Predstavnik CIRT-a je učestvovao u radu Operativnog tima za sprovođenje NATO vježbe CMX23, osnova vježbe upravljanja krizama (CMX) je testiranje elemenata NATO sistema za odgovor na krize u cilju održavanja i unapređenja sposobnosti NATO-a za čitav spektar izvedenih operacija.
- Predstavnik CIRT-a je učestvovao u radu Operativnog tima za koordinaciju vježbovnihi aktivnosti Crne Gore u oblasti kriznih situacija u okviru NATO
- U sklopu jačanja regionalne saradnje predstavnici CSEC-a (Cyber Security Excellence Centre) iz Bosne i Hercegovine su posjetili CIRT.ME tim, gdje im je prezentovana uloga CIRT-a sa osvrtom na dosadašnje i buduće aktivnosti CIRT.ME.
- Predstavnici CIRT-a su učestvovali u u obuci vezano za simulaciju sajber krize od strane EU u saradnji sa "E-Governance Academy" iz Estonije i MJU

- Predstavnik CIRT-a je učestvovao na Konferenciji i zvaničnom predavljanju osnivanja bosanskohercegovačke organizacije-Women4Cyber BiH koje je omogućilo lakše umrežavanje Crne Gore u članstvo s obzirom da je Crna Gora podnijela inicijativu i aplikaciju za osnivanje Women4Cyber poglavlja.
- Predstavnik CIRT-a je učestvovao u operativnoj simulacionoj vježbi sajber bezbjednosti u sklopu EU projekta podrške: "Projekat brzog reagovanja u oblasti sajber bezbjednosti za Albaniju, Crnu Goru i Sjevernu Makedoniju".
- Predstavnik CIRT-a je učestvovao na panelu „Iskustvo država o sajber napadima na mrežu državnih organa“ na Međunarodnoj konferenciji o borbi protiv sajber kriminala u organizaciji Ministarstva pravosuđa i uprave Hrvatske, Ministarstva pravosuđa SAD-a i State Department-a gdje su prezentovana iskustva Crne Gore iz perspektive CIRT-a.
- Predstavnici CIRT-a su učestvovali u panelu „Saradnja ključnih državnih i nedržavnih institucija i državnih izbornih komisija u zaštiti integriteta i kredibiliteta izbora“ na Konferenciji „Digitalizacija izbornih procesa: perspektive sajber bezbjednosti i međuinstitucionalne koordinacije“ u organizaciji Međunarodnog instituta za demokratiju i izbornu pomoć: Na panelu je prezentovano iskustvo i izazovi digitalizacije u izbornim procesima u Crnoj Gori.
- Učešće na radionici “Jačanje saradnje u borbi protiv sajber kriminala na Zapadnom Balkanu”, (Ova radionica je imala za cilj jačanje saradnje i razmjenu informacija u realnom vremenu između LEA i CERT-ova kao i identifikaciju i razmjenu najboljih praksi između država članica EU i zemalja Zapadnog Balkana. U okviru radionice, predstavnici CIRT-a su prezentovali stanje sajber bezbjednosti u Crnoj Gori kao i ulogu CIRT-a u ovoj oblasti)
- Predstavnik CIRT-a je učestvovao na panelu Regionalna diskusija: Zvanični mehanizmi za regionalnu reakciju na nasilje i prijetnje u online prostoru koja je organizovana u sklopu projekta SMART Balkans – Civilno društvo za povezani Zapadni Balkan.
- Predstavnici CIRT-a su učestvovali na regionalnoj vježbi u organizaciji Instituta za softversko inženjerstvo (SEI) i Biroa za sajber i digitalnu politiku (CDP) Stejt departmenta, za odabrane nacionalne cert timove iz centralne i istočne evrope. Cilj ovog događaja bio je da okupi odabrane regionalne timove za upravljanje računarskim bezbjedonosnim incidentima.
- Predstavnik CIRT-a je učestvovao na High-Level Cybersecurity Conference – Towards a resilient cyberspace in the Western Balkans, u organizaciji Regional Cooperation Council (RCC)
- Predstavnik CIRT-a na „7th Meeting of the Project Steering Committee“ u organizaciji Savjeta Evrope
- Predstavnici CIRT-a su učestvovali na obuci Evropskog centra izvrsnosti za suprotstavljanje hibridnim prijetnjama (COE Hybrid) - vježbi za zaštitu demokratskih procesa tokom izbora, odnosno za sprečavanje miješanja u izbore
- Predstavnik CIRT-a je prisustvovao CTF i Live-Fire regionalnoj vježbi za simulaciju kibernetičkog napada uživo (Blue Team) u organizaciji e-Governance Academy i CybExer Technologies u saradnji sa Ministarstvom javne uprave.

U cilju unapređenja regionalne i međunarodne saradnje održani su sastanci sa:

- norveškim predstavnikom Centra za integritet u sektoru odbrane Kraljevine Norveške (CIDS) sa predlogom za buduću saradnju.
- načelnikom makedonskog CIRT-a (MKD-CIRT) u vezi platforme za obuku i evaluaciju znanja u oblasti sajber bezbjednosti
- predstavnicima Globalne sajber alijanse koja ima cilj da minimizuje sajber rizik a vezano za temu članstva u toj alijansi koja se ostvaruje prema propisanoj proceduri i popunjavanjem aplikacije.
- britanskim ekspertima na temu evaluacije DCAF projekta i prezentacije konkretnih rezultata o uspješnosti projekta i mogućoj daljoj saradnji.

XI INSPEKCIJSKI NADZOR

U skladu sa članom 80 Zakona o tajnosti podataka, Direkcija za zaštitu tajnih podataka vrši inspeksijski nadzor u pogledu primjene mjera zaštite tajnih podataka i nad primjenom međunarodnih ugovora koji se odnose na tajne podatke, u skladu s ovlaštenjima propisanim članom 81 Zakona.

Inspektor Direkcije za zaštitu tajnih podataka u toku 2023. godine, vršio je inspeksijski nadzor u skladu sa godišnjim Planom inspeksijskog nadzora.

Inspeksijski nadzor vršen je u odnosu na primjenu Zakona o tajnosti podataka i podzakonskih akata za njegovo sprovođenje.

Po osnovu **Plana inspeksijskog nadzora**, izvršen je inspeksijski nadzor u Ministarstvu odbrane, Ministarstvu vanjskih poslova, Upravi za izvršenje krivičnih sankcija, Vrhovnom državnom tužilaštvu, kao i nadzor u u pravnim licima.

Direkcija kontinuirano upućuje zahtjeve organima državne uprave za dostavljanje podataka o obrazovanju Komisije za periodično preispitivanje tajnih podataka i o licima koja su imenovana za članove tih komisija.

Inspektor za kontrolu primjene mjera zaštite tajnih podataka Direkcije za zaštitu tajnih podataka, u okviru svojih nadležnosti, nalaže mjere za unapređivanje zaštite tajnih podataka i saraduje sa licima određenim za vršenje unutrašnje kontrole u organima i organizacijama u kojima nastaju tajni podaci ili koji koriste tajne podatke. U cilju unapređenja mjera zaštite tajnih podataka inspektor je održao sastanke i konsultacije, sa licima određenim za vršenje unutrašnje kontrole, odgovornim za sprovođenje mjera zaštite tajnih podataka u organima i organizacijama u kojima rade.

Unutrašnja kontrola

Zakonom o tajnosti podataka propisano je da su organi i drugi subjekti dužni da obezbjeđuju vršenje redovne unutrašnje kontrole nad sprovođenjem mjera zaštite tajnih podataka utvrđenih Zakonom o tajnosti podataka i da su dužni da odrede lice za vršenje unutrašnje kontrole.

U skladu sa navedenim, Direkcija je i tokom 2023. godine, zatražila od organa podatke o licima određenim za vršenje unutrašnje kontrole, a u cilju kontinuirane saradnje inspektora Direkcije sa tim licima, radi unapređenja mjera zaštite tajnih podataka.

Direkcija za zaštitu tajnih podataka će u narednom periodu insistirati da organi u čijem radu nastaju tajni podaci odrede lice za vršenje redovne unutrašnje kontrole, u protivnom biće prinuđena da pokrene postupak odgovornosti.

XII BUDŽET I NABAVKE

Budžet

Zakonom o budžetu za 2023. godinu odobrena su sredstva za finansiranje Direkcije za zaštitu tajnih podataka u iznosu od 537.390,24€.

U izvještajnom period od raspoloživih sredstava isplaćeno je 495.924,18€.

U skladu sa zaključcima Vlade Crne Gore, Direkcija je krajnje racionalno trošila sredstva opredijeljena Budžetom za 2023.godinu, te utrošila 92,28% odobrenih sredstva.

Nabavke

Direkcija je u skladu sa članom 84 Zakona o javnim nabavkama 31.01.2023. godine donijela Plan javnih nabavki za 2023. godinu.

U izvještajnom periodu, u skladu sa Pravilnikom o načinu sprovođenja jednostavnih nabavki, roba i usluga realizovano je jednostavnih nabavki u iznosu od 22.138,82 eura.

Shodno Uredbi o načinu planiranja i sprovođenja centralizovanih javnih nabavki, koje sprovodi Uprava za katastar i državnu imovinu kao nadležni organ za sprovođenje postupaka centralizovanih javnih nabavki, dostavljen Plan potreba za predmetima centralizovanih javnih nabavki za 2023.godinu.

Uprava za katastar i državnu imovinu za 2023.godine, kao nadležni organ za sprovođenje postupaka centralizovanih javnih nabavki odobren je iznos od 8.000,00€. Sredstva se odnose na administrativni materijal, rashode za gorivo, komunikacione usluge, osiguranje.

Planom posebnih javnih nabavki u oblasti bezbjednosti i odbrane planirane su dvije nabavke i to: nabavka kripto uređaja za elektronsku razmjenu nacionalnih podataka stepena tajnosti TAJNO kao i nabavka sistema za virtuelizaciju. Postupak predmetne nabavke označen je stepenom tajnosti „INTERNO“.

Nadležnom organu blagovremeno je podniet Izveštaj o sprovedenim postupcima javnih nabavki i zaključenim ugovorima o javnim nabavkama, kao i Izveštaj o izuzećima od primjene u postupcima javnih nabavki za 2023. godinu.

U 2023. godini, izvršen je redovni godišnji popis pokretnih i nepokretnih stvari i obaveza sa stanjem na dan 31.12.2022. godine u Direkciji za zaštitu tajnih podataka, i izvršeno upoređivanje stanja dobijenog popisom sa stanjem iz knjigovodstva.

XIII UPRAVLJANJE I UNUTRAŠNJE KONTROLE

Upravljanje i unutrašnje kontrole obuhvataju postupke upravljanja sredstvima subjekta, finansijske i druge kontrole i unutrašnju reviziju radi uspješnog upravljanja i ostvarivanja poslovnih ciljeva subjekta, na transparentan, pravilan, ekonomičan, efikasan i efektivan način.

U skladu sa obavezama koje proističu iz Zakona o upravljanju i unutrašnjim kontrolama u javnom sektoru, u 2023. godini pripremljeni su i dostavljeni Ministarstvu finansija:

- Godišnji izvještaj o aktivnostima na sprovođenju i unapređenju upravljanja i kontrola za 2023. godinu,
- Godišnji izvještaj o obavještenjima o sumnjama na nepravilnosti i prevare za 2023. godinu.
- Registar rizika Direkcije za zaštitu tajnih podataka za 2023. godinu, i
- Upitnik za samoprocjenu upravljanja i kontrola za 2023. godinu.

Interna pravila i procedure sadrže opis procedure, ovlašćena lica i kontrolne mehanizme i sastavni su dio Knjige procedura Direkcije za zaštitu tajnih podataka za upravljanje i unutrašnju kontrolu.

U skladu sa Sporazumom zaključenim sa Ministarstvom odbrane, poslovi unutrašnje revizije u Direkciji za zaštitu tajnih podataka povjereni su Odjeljenju za unutrašnju reviziju Ministarstva odbrane. Ministarstvo odbrane podnijelo je Ministarstvu finansija i socijalnog staranja Godišnji izvještaj o unutrašnjoj reviziji izvršenoj u Direkciji za zaštitu tajnih podataka za 2023. godinu.

XIV JAVNOST RADA

Direktor Direkcije redovno je izvještavao javnost o najznačajnijim pitanjima iz nadležnosti Direkcije za zaštitu tajnih podataka.

Direkcija je ažurno odgovarala na upućena pitanja medija.

Za potrebe javnosti rada, Direkcija je ažurirala svoju internet stranicu www.nsa.gov.me na kojoj su objavljeni podaci o značajnim aktivnostima, kao i informacije koje je organ dužan da objavi na svojoj internet stranici u skladu sa članom 12 Zakona o slobodnom pristupu informacijama.

Podgorica, 09. april 2024. godine

01-267/24-2

