CRNA GORA

Direkcija za zaštitu tajnih podataka

IZVJEŠTAJ O RADU

Direkcije za zaštitu tajnih podataka za 2024. godinu

Podgorica, januar 2025. godine

SADRŽAJ

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, 74/20 i 113/24) i Uredbom o organizaciji i načinu rada državne uprave ("Službeni list Crne Gore", br. 98/23, 102/23, 113/23, 71/24, 72/24, 90/24, 93/24, 104/24 i 117/24).

Izvještajem o radu Direkcije za zaštitu tajnih podataka obuhvaćen je pregled najvažnijih aktivnosti Direkcije u 2024. 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 saradnju, 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, inspekcijskim 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.

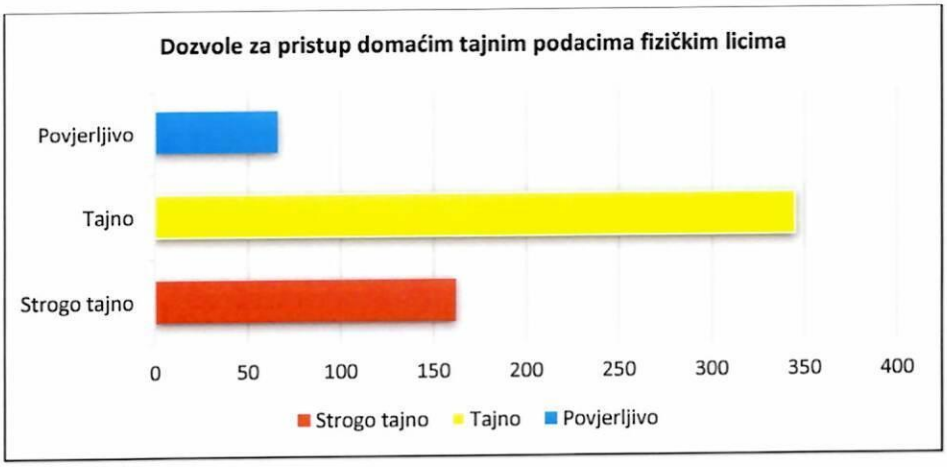
U 2024. godini, podnesena su 628 zahtjeva za izdavanje dozvola za pristup tajnim podacima, od čega je 121 zahtjeva za produženje važenja dozvole za pristup tajnim podacima, a 507 novih zahtjeva za izdavanje dozvola.

U 2024. godini, izdate su ukupno 573 dozvola za pristup tajnim podacima, od čega su 422 nove dozvole, dok je produžen rok važenja za 151 dozvolu za pristup tajnim podacima.

Za pristup tajnim podacima stepena tajnosti **STROGO TAJNO** izdato je 162 dozvole, od čega je 77 novih dozvola, a produžen je rok važenja za 85 dozvola za pristup tajnim podacima.

Za pristup tajnim podacima stepena tajnosti **TAJNO** izdato je 345 dozvola, od čega je 281 novih dozvola, a produžen je rok važenja za 64 dozvole za pristup tajnim podacima.

Za pristup tajnim podacima stepena tajnosti **POVJERLJIVO** izdato je 66 dozvole, od čega su 64 nove dozvole, a produžen je rok važenja za 2 dozvola.



U 2024. 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 2024. godini, podnijeta su dva zahtjeva za izdavanje dozvole i dva zahtjeva za produženje važenja dozvole za pristup tajnim podacima za pravno lice. Produženo je važenje jedne dozvole za pristup tajnim podacima.

Za pristup tajnim podacima za zaposlene u pravnom licu podnesen je 71 zahtjev, od čega je 59 zahtjeva za izdavanje a 12 zahtjeva za produženje važenja dozvole za pristup tajnim podacima.

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 2024. godini, nastavila saradnju sa državnim organima i pravnim licima koja u vršenju zakonom utvrđenih poslova, odnosno izvršavanju ugovorenog posla postupaju sa tajnim podacima.

Sprovođene 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 i administrativnih mjera zaštite tajnih podataka u toku 2024.godine, održani su sastanci i konsultacije sa predstavnicima Specijalnog

državnog tužilaštva, Specijalnog policijskog odjeljenja, Centralne banke, Ministarstva vanjskih poslova, Ministarstva unutrašnjih poslova.

Direkcija je sarađivala 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. Nakon popravke kripto uređaja, pokrenuta je procedura za ponovno povezivanje registra tajnih podataka u Generalnom sekretarijatu Vlade Crne Gore.

Krajem 2024. godine izvršena je nabavka informatičke opreme (serveri, storage, tape, ups) za potrebe obnavljanja i nadogradnje ovog informacionog sistema. Nadogradnja sistema planirana je za 2025.godinu.

Sprovedene su aktivnosti na planiranju zamjene kripto uređaja koji će biti u upotrebi u Direkciji do kraja 2025. godine novijim modelima koji su sertifikovani po pitanju otpornosti na kvantne prijetnje. Obavljena je komunikacija i sa drugim institucijama koje koriste uređaje istog proizvođača u cilju planiranja blagovremene zamjene ovih uređaja novijim modelima i mitigacije rizika po pitanju modernih kvantnih prijetnji na duži rok.

Odjeljenje za informatičku zaštitu tajnih podataka tokom 2024. 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.

Pored navedenih aktivnosti, Odjeljenje za informatičku zaštitu tajnih podataka u kontinuitetu sprovodi i aktivnosti u sklopu svojih nadležnosti koje se tiču upotrebe i distribucije kripto 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 informaciono 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.

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 2024. godinu (SSP 2024) direktor Direkcije za zaštitu tajnih podataka potpisao je u julu 2024. godine. NCIA je, u saradnji sa DZTP, Ministarstvom odbrane i Ministarstvom vanjskih poslova, pripremila i dostavila predlog SSP-a za 2025. godinu. Planirano je da se ovaj ugovor potpiše i da se izvrši plaćanje prema NCIA do kraja I kvartala 2025.godine.

Odjeljenje za informatičku zaštitu tajnih podataka u okviru svojih NDA (National Distribution Authority) nadležnosti u kontinuitetu se bavi rukovanjem kripto 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

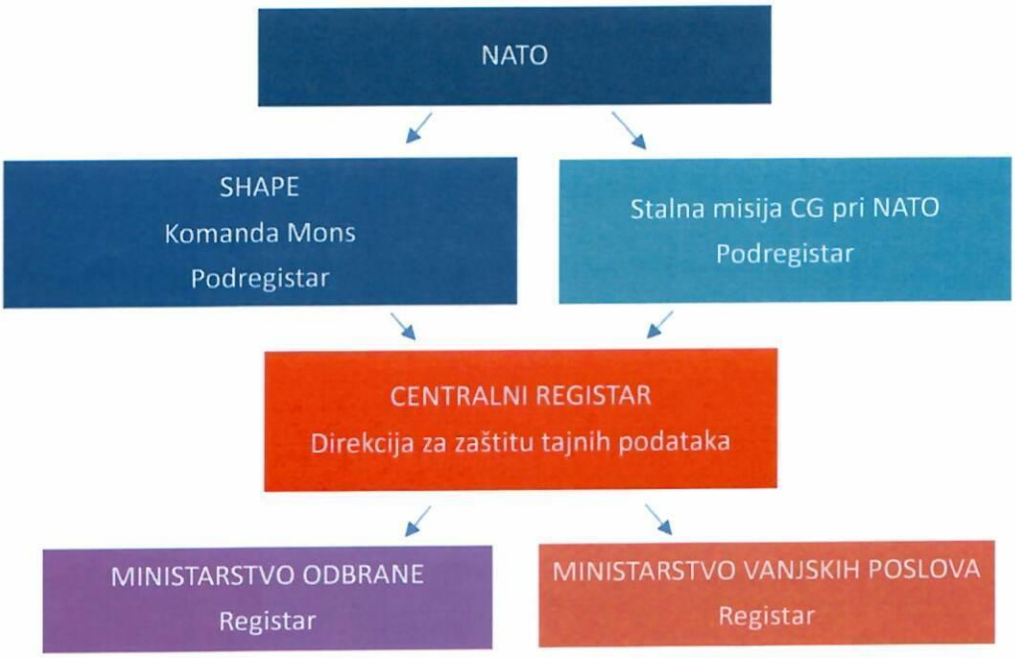
Pravni okvir za saradnju

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

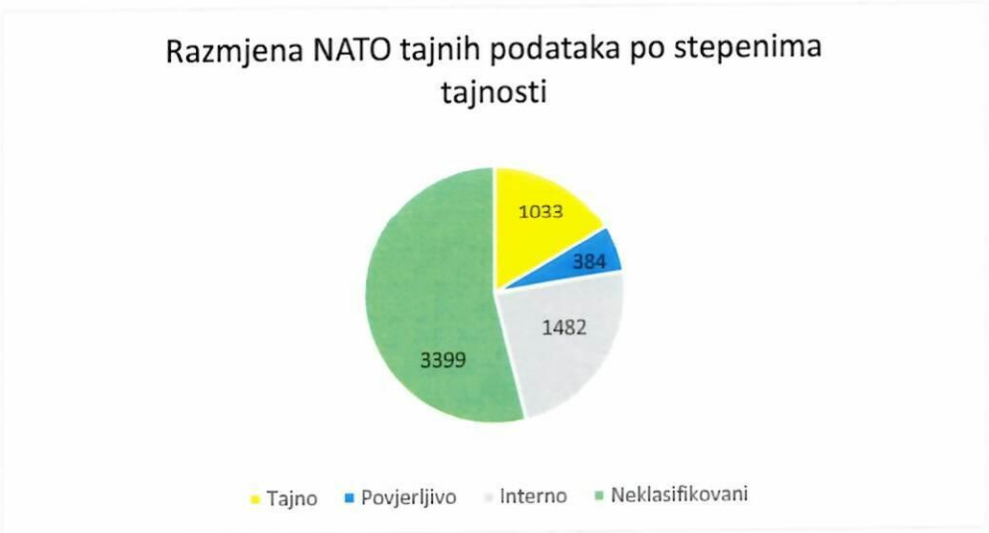
Sa NATO se u kontinuitetu odvija razmjena tajnih podataka, koja je otpočela nakon upućivanja prvog kontigenta crnogorskih vojnika u mirovnu misiju ISAF u Avganistanu, a kasnije u misiju "Resolute Support" u Avganistanu.

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).



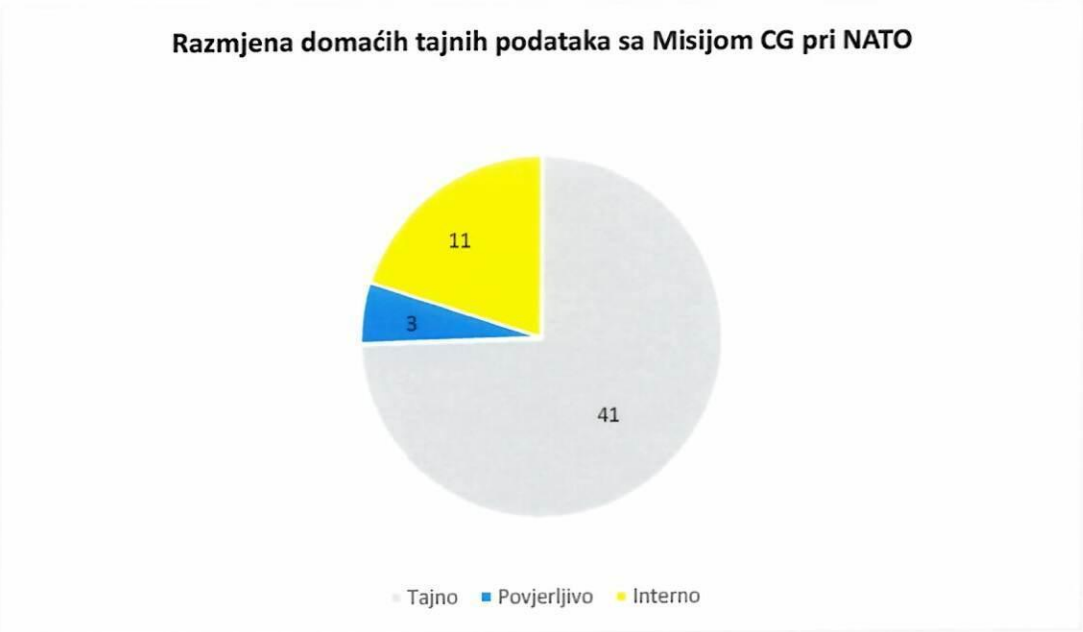
*šematski prikaz razmjene tajnih podataka sa NATO

U 2024. godini razmijenjeno je ukupno 6298 NATO tajnih podatka različitih stepena tajnosti, od čega 1033 stepena tajnosti TAJNO, 384 stepena tajnosti POVJERLJIVO, 1482 stepena tajnosti INTERNO i 3399 neklasifikovanih podataka.



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

Sa Stalnom misijom Crne Gore pri NATO u Briselu u 2024. godini, razmijenjeno je ukupno 55 tajnih podatka različitih stepena tajnosti, od čega 41 stepena tajnosti TAJNO, 3 stepena tajnosti POVJERLJIVO i 11 stepena tajnosti INTERNO.



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 2024. godini izdala je 207 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 inspekcijska kontrola

NATO tajni podaci proslijeđeni 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 2024.godine, kontinuirana praćena realizacija preporuka i korektivnih mjera iz Izvještaja o izvršenom inspekcijskom 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 inspekcijskoj 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

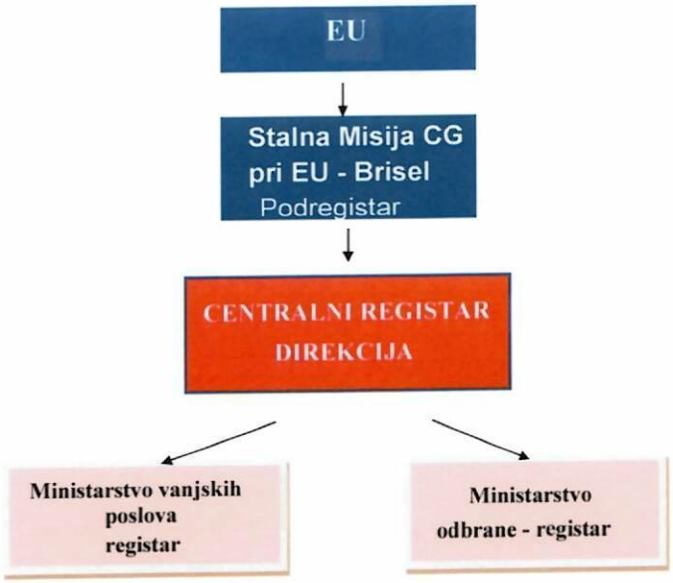
Poglavlje 10 – Informatičko društvo i mediji

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 2024. godini izdala je 3 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.

U periodu od 18. do 20. novembra tekuće godine, predstavnici Direkcije za zaštitu tajnih podataka, prisustvovali su u Ljubljani na 6S - Konferenciji regionalnih nacionalnih bezbjednosnih organa (NSA). Centralna tema ove 6S Konferencije, bila je korišćenje tajnih podataka u sudskim postupcima, kao i pozicija regionalnih NSA u sistemu državne uprave. Takođe, prezentovani su i Instrumenti za tehničku pomoć u sprovođenju zakonodavstva Evropske unije, te smjernice koje se odnose na način apliciranja država u TAIEX i Twinning projektima. Pored predstavnika iz Crne Gore, učesnici ove Konferencije bili su i predstavnici ostalih 5 država- Makedonije, Srbije, Bosne i Hercegovine, Hrvatske, i Slovenije koja je bila domaćin ove Konferencije.

U oktobru tekuće godine u Sofiji je održana i 14. SEENSA Konferencije s obzirom da je predsjedavajuća ove konferencija bila Bugarska. 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.

Takođe u mjestu Bankya u Bugarskoj, održana je Konferencija regionalne inicijative SEENSA (Nacionalni bezbjednosni organi jugoistočne Evrope), u periodu od 28. do 31. maja 2024.godine, na nivou eksperata za bezbjednost lica (Personnel Security) na teme bezbjednosti lica i obuka za korisnike tajnih podataka a u cilju daljeg jačanja saradnje i razmjeni iskustava između zemalja jugoistočne Evrope.

U okviru saradnje sa NATO, Direktor Direkcije za zaštitu tajnih podataka u oktobru 2024. godine, učestvovao je na redovnom godišnjem sastanku NATO bezbjednosnog komiteta koji je održan u Briselu, NATO HQ, na nivou direktora Nacionalnih bezbjednosnih organa.

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

U okviru međunarodne saradnje realizovane su posjete od strane kolega iz Republike Sjeverne Makedonije, Slovenije i Bosne i Hercegovine a sve u cilju razmjene iskustava, dobrih praksi i planiranih aktivnosti po pitanju ove vrste saradnje.

U periodu 15. do 19. septembra 2024. u Tirani (Albanija), održana je godišnja konferencija MISWG (Multinational Industrial Security Working Group), čija je članica i Crna Gora od 2023.godine. Na konferenciji je učestvovalo 114 delegata iz 37 zemalja članica, 5

međunarodnih organizacija, i jedna zemlja koja je učestvovala kao gost. Konferencija je bila prilika da se podijele najbolje prakse na polju međunarodne industrijske bezbjednosti kako bi se zaštitili tajni podaci u vremenu sve većeg suočavanja sa bezbjednosnim prijetnjama i izazovima, razviju i usvoje standardizovane procedure koje su garant zajedničkim interesima zemalja članica, ojača saradnja i razviju kontakti na polju industrijske bezbjednosti.

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

U cilju jačanja saradnje u oblasti sajber bezbjednosti CIRT kontinuirano sarađuje 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 sprovođenje 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. Takođe, sa Ministarstvom odbrane saradnja se realizovala i kroz izradu Predloga uredbe o izmjenama i dopunama Uredbe o bližim uslovima i načinu sprovođenja administrativnih i fizičkih mjera zaštite tajnih podataka.

Saradnja sa Agencijom za nacionalnu bezbjednost, takođe se u kontinuitetu realizuje 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 Predloga budžeta Direkcije za zaštitu tajnih podataka za 2025. 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 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 sarađivalo sa Ministarstvom pravde, Ministarstvom unutrašnjih poslova, Ministarstvom vanjskih poslova, Upravom Carina, Specijalnim državnim tužilaštvom, kao i drugim državnim institucijama i pravnim licima, koji su obveznici primjene Zakona o tajnosti podataka.

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 sarađivala 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

Službenici Odjeljenja za informatičku zaštitu tajnih podataka u periodu od 04. do 16. februara 2024. Godine, pohađali su u USA (Columbia) obuku za korištenje DACAN kriptografskog informacionog sistema DKMI.

Predstavnik Odjeljenja za informatičku zaštitu tajnih podataka je u periodu od 10. do 12. aprila 2024. Godine, boravio u studijskoj posjeti u Ljubljani, u cilju razmjene iskustva iz domena informacione bezbjednosti tajnih podataka i industrijske bezbjednosti sa kolegama iz National Security Authority Slovenia.

Službenici Odjeljenja za informatičku zaštitu tajnih podataka učestovali su na NDA konferenciji na kojoj učestvuju predstavnici NDA iz država članica NATO u Parizu od 16. do 18. aprila 2024. godine.

Dva službenika Direkcije u maju 2024. godine, pohađala su kurs i sertifikovali se za ISO/IEC 27001:2022 eksternog revizora.

U periodu od 15. do 19. jula 2024. godine u NCIA centru za obuku u Portugalu, dva službenika Direkcije pohađala su obuku za upravljanje kripto materijalima (004 Crypto administration course).

Predstavnici Odjeljenja za informatičku zaštitu tajnih podataka učestvovali su od 8. do 10. oktobra 2024. godine na VTC 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 sastancima međunarodnog BICES akreditacionog tijela (BICES Accreditation Board, BSAB).

U okviru Programa stručnog osposobljavanja Uprave za ljudske resurse u 2024. godini, sa predavačima iz Direkcije, organizovano je više obuka na temu tajnosti podataka i informatičke zaštite tajnih podataka. Pored obuka koje su održane u saradnji sa Upravom za ljudske resurse, Direkcija je organizovala i posebne obuke za potrebe državnih organa.

Obavljeno je više konsultacija sa predstavnicima državnih institucija i privatnih kompanija po pitanju mjera informatičke i TEMPEST zaštite i procesa akreditacije informacionih sistema u kojima se obrađuju tajni podaci.

Predstavnik Odjeljenja za informatičku zaštitu tajnih podataka od oktobra 2024. godine učestvuje u radu Interresorne komisije za suprotstavljanje hibridnim prijetnjama. Jedan od glavnih zadataka ove komisije je finalizacija Nacrta Strategije za suprotstavljanje hibridnim prijetnjama sa pratećim Akcionim planom, čije usvajanje je predviđeno Srednjoročnim programom rada Vlade Crne Gore 2024-2027, kao i Programom pristupanja Crne Gore EU za 2024-2027.

Službenici Direkcije u okviru Programa stručnog osposobljavanja Uprave za kadrove u 2024.godini, pohađali su sljedeće obuke: Upravljanja projektima finansiranim iz EU fondova, Poslovni sastanci, Pregovaranje i pregovaračke vještine, Pisanje izvještaja, Upravni postupak, Pravno-tehnička pravila za izradu propisa sa smjernicama za usklađivanje propisa Crne Gore sa pravnim poretkom Evropske unije i Izrada zakona i drugih propisa u skladu sa pravno-tehničkim pravilima za izradu propisa i smjernicama za usklađivanje propisa Crne Gore sa pravnim poretkom Evropske unije su teme iz oblasti Izrada i evaluacija javnih politika, Vještine komunikacija sa strankama, Vještine prezentacije - javni nastup su teme iz oblasti Razvoj vještina,A1 program obrazovanja za sticanje ključnih vještina komunikacija s javnošću u javn om sektoru, Izvještavanje u javnom sektoru, Otkrivanje i postupanje po obavještenjima i sumnjama na nepravilnosti i prevare, Otvorenost javne uprave.

Takođe, u okviru Programa stručnog osposobljavanja Uprave za kadrove, sa predavačima iz Direkcije, kontinuirano su se organizovale obuke na temu tajnosti podataka i informatičke zaštite tajnih podataka, za potrebe zaposlenih u Ministarstvu odbrane i Vojsci Crne Gore, kao i za potrebe službenika lokalnih samouprava i ostalih državnih organa.

IX ORGANIZACIJA DIREKCIJE

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.

Vlada Crne Gore utvrdila je Pravilnik o izmjenama i dopunama Pravilnika o unutrašnjoj organizaciji i sistematizaciji Direkcije za zaštitu tajnih podataka, broj: 05-197/24-2, koji je stupio na snagu 22.03.2024. godine.

U skladu sa članom 78 Zakona o informacionoj bezbjednosti, koji je stupio na snagu 05. decembra 2024.godine, precizirano je da će danom donošenja akta o unutrašnjoj organizaciji i sistematizaciji Agencije za sajber bezbjednost, Agencija od Direkcije za zaštitu tajnih podataka, preuzeti državne službenike koji su vršili poslove u okviru organizacione jedinice CIRT, opremu i službenu dokumentaciju.

Donošenjem navedenog zakona, prestale su da važe odredbe čl. 74 stav 1 tačka 8b i člana 74a Zakona o tajnosti podataka, a kojima su bili definisani poslovi i nadležnost CIRT-a.

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 prestank 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 Odjeljenju 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: obezbjeđivanje 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 zaštitu 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, rasdpoređivanje, 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 sistematizovano je 28 službeničkih radnih mjesta za 28 izvršilaca, uključujući i direktora. Ukupan broj zaposlenih izvršilaca je 25 od čega je jedno profesionalno vojno lice koje je upućeno iz Vojske Crne Gore na rad u Direkciju.

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 2024. godinu i uz saglasnost Ministarstva finansija, dostavljen je Upravi za ljudske resurse.

U skladu sa Kadrovskim planom za 2024. godinu, imenovan je vršilac dužnosti direktora Direkcije, a radni odnos na neodređeno su zasnovala 2 izvršioca u organizacionoj jedinici Odjeljenje za informatičku bezbjednost i odgovor na računarske incidente (CS/CIRT), i to radno mjesto broj 14 - Samostalni savjetnik II za (CS/CIRT) i radno mjesto 21-viši savjetnik III za (CS/CIRT).

Donijet je Plan integriteta Direkcije za zaštitu tajnih podataka i Upitnik za procjenu efektivnosti i efikasnosti Plana integriteta za 2024. godinu.

U izvještajnom periodu, izvršeno je redovno ažuriranje podataka o zaposlenima u aplikaciji Kadrovski informacioni sistem-Centralna kadrovska evidencija. Takođe, sprovedena je Analiza potreba za obukama Direkcije za zaštitu tajnih podataka za 2024.godinu, i dostavljen Izvještaj o sprovedenoj analizi Upravi za ljudske resurse.

U Direkciji je tokom 2024.godine, obrazovana Komisija koja je izvršila redovni godišnji popis pokretnih i nepokretnih stvari i obaveza sa stanjem na dan 31.12.2023. godine. Izrađen je tabelarni prikaz osnovnih sredstava za 2023. godinu, i dostavljen je Izvještaj o popisu pokretne imovine i PS-obrasci Upravi za državnu imovinu.

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 2024. godine sprovodio proaktivne mjere s ciljem smanjenja rizika od incidenata. U sklopu proaktivnih mjera CIRT je sproveo niz aktivnosti na podizanju svijesti o sajber bezbjednost. Naša misija bila je osnaživanje građana, organizacija i zajednica kroz edukaciju, informisanje i promociju dobrih praksi. Kroz društvene mreže (facebook, Instagram, twitter) i zvaničnu internet stranicu www.gov.me/cirt, kontinuirano smo informisali javnost o aktuelnim sajber prijetnjama, sa posebnim fokusom na fišing i razne vrste internet prevara.

U skladu sa prethodno navedenim u Osnovnoj školi „Pavle Rovinski" organizovana je radionica o bezbjednosti na internetu za učenike petog razreda. Radionica je osmišljena kako bi se učenicima pružile neophodne informacije i vještine koje će im pomoći da prepoznaju potencijalne opasnosti na internetu i adekvatno se zaštite. Radionica je obuhvatila ključne teme za razumijevanje i primjenu principa sajber bezbjednosti. Kroz interaktivne aktivnosti, diskusije i praktične primjere učenici su imali priliku da diskutuju o prednostima i manama korišćenja interneta, nauče kako da prepoznaju sigurne internet stranice, zaštite svoje lične podatke, te pravilno koriste društvene mreže i video igre. Posebna pažnja posvećena je pravilima lijepog ponašanja na internetu, koja uključuju poštovanje drugih korisnika, izbjegavanje uvredljivih komentara i sajber nasilja (cyberbullying), kao i važnosti korišćenja kompleksnih lozinki kako bi se bolje zaštitili od neovlašćenog pristupa i sačuvali privatnost naloga na internetu. Takođe, održana je radionica u Omladinskom centru Podgorica na temu „Razumijevanje sajber nasilja i on-line sigurnosti u Crnoj Gori ".

Na društvenim mrežama su obilježavani svjetski dani koji se tiču sajber bezbjednosti, a istovremeno su iskorišćeni za promovisanje dobrih praksi. Neki od dana koji su obilježeni su: Dan sigurnog interneta, Svjetski dan rezervnih kopija, Međunarodni dan lozinki, Svjetski dan društvenih mreža, itd... Osim svjetskih dana, na društvenim mrežama kao i na sajtu postavljena su upozorenja i preporuke za bezbjedno korišćenje interneta. Tokom 2024. godine kreirano je i postavljeno na sajtu šest biltena, koji su obuhvatali globalne vijesti, analize i zanimljivosti iz oblasti sajber bezbjednosti. Ovi bilteni su pružili korisnicima vrijedne informacije o aktuelnim prijetnjama, inovacijama u oblasti zaštite podataka, te praktične savjete za unapređenje digitalne sigurnosti. Cilj biltena bio je ne samo informisanje, već i podsticanje šire zajednice na usvajanje dobrih praksi u sajber prostoru.

Shodno Zakonu o informacionoj bezbednosti, a u skladu sa aktivnostima predviđenih Strategijom ažurirana je lista lokalnih CIRT-ova tj. kontakt osoba zaduženaih za uspostavljanje sistema zaštite od računarskih i bezbjednosnih incidenata na internetu i drugih rizika bezbjednosti tih sistema, koji će neposredno sarađivati 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.
U skladu sa nadležnostima na sedmičnom nivou ISP-ovima se dostavljaju informacije o kompromitovanim adresama iz njihovog adresnog opsega.

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 elektronske pošte na kontakt@cirt.me. Kroz analizu incidenata u sajber prostoru Crne Gore za period od 2014. do 2024. 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 2024. godine nastavljen trend rasta broja prijavljenih incidenata u odnosu na prethodne godine. Tokom 2023. godine CIRT-u je prijavljen ukupno 751 incident, dok je u 2024. godini CIRT registrovao 788 prijava. Ovaj trend se ogleda i u činjenici da je CIRT-u, tokom 2024. 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	Nepriklad an 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
2024	49	126	93	11	472	37	788

Regionalna i međunarodna saradnja

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

- FIRST (Forum of Incident Response and Security Teams) - Međunarodna konfederacija CSIRT-ova koji sarađuju 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 zemjama, 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

Projekat CyberSEE za jugoistočnu Evropu i Tursku je počeo sa implementacijom 01. januara 2024. godine. Ovo je zajednički projekat Evropske unije i Savjeta Evrope, finansiran preko Evropske unije pod instrumentom IPA III i Savjeta Evrope, a izvršava se preko C-PROC-a. Projekat je nastavak prethodnih projekata iPROCEEDS i iPROCEEDS2 koji imaju za cilj jačanje zakonskog okvira i kapaciteta organa za sprovođenje prava u borbi protiv sajber kriminala. U okviru projekta realizovane su sledeće aktivnosti koje su organizovane shodno projektnom planu:

- Učešće na „ISS World Europe 2024"
- Učešće na "Strengthening cooperation and real- time information exchange between LEA's and CERT's"
- Učešće na Regionalnoj vježba iz oblasti sajber kriminala „Saradnja CIRT (CERT) - ova i organa za sprovođenje zakona"

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:

- Učešće na Online obuci o Artemisu, skeneru bezbjednosnih ranjivosti otvorenog koda koji je razvio CERT.PL
- Učešće na konferenciji i ransomver obuci vezano za pripremu i odgovore na ransomver kako bi se ojačala sajber otpornost. Događaj je organizovao DCAF i FIRST u sklopu drugog izdanja „Balkan Cybersecurity Days".

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

- Učešće u radu Operativnog tima za sprovođenje NATO vježbe CMX, 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.
- Učešće u radu Operativnog tima za koordinaciju vježbovnih aktivnosti Crne Gore u oblasti kriznih situacija u okviru NATO
- Učešće na konferenciji i obukama za prikupljanje i analizu sajber prijetnji, analizu malvera i korišćenje platforme MISP. Događaj je organizovan od strane „First" i „Carnegie Mellon University" – „First Cyber Threat Intelligence"
- Učešće na konferenciji i sajber vježbi „Global CyberDrill" - Na sajber vježbama su simulirani različiti scenariji napada, uključujući phishing, DDoS napade i ransomware. Učesnici su se takmičili u rješavanju izazova i brzom odgovoru na sajber prijetnje. Međunarodna unija za telekomunikacije (ITU) i Savjet za sajber bezbjednost (UAE CSC) organizovali su konferenciju i globalnu sajber vježbu

- Učešće na konferenciji „Unlocking digital success“ i seminaru „Digital government services and cyber security“ - Organizator konferencije je estonska eGovernance akademija (EGA), a CRDF Global zajedno sa Ministarstvom spoljnih poslova SAD (US state department) podržao je učešće zemalja institucija na Zapadnom Balkanu koji unapređuju digitalne ekosisteme svojih zemalja i usluge e-uprave pomažući u izgradnji njihovih mreža i zaštite kritične infrastrukture. Na seminaru su eksperti iz EGA prezentovali njihova iskustva i rješenja iz oblasti sajber bezbijednosti dok je CRDF predstavio produžetak projekta za jačanje ajber bezbjednosti u regionu.
- U okviru EU projekta „Cyber Balkans“ organizovan je prvi regionalni sastanak CSIRT/CERT/CIRT timova zapadnog Balkana. Cilj ovih sastanka je jačanje saradnje i razmjena informacija između CERTova u regionu. Prvi domaćin je bila albanska uprava za elektronske sertifikate i sajber bezbjednost (AKCESK) na temu obrađivanja veoma sofisticiranog napada „wiper“.
- Učešće na radionici posvećenoj planu za odgovor na sajber incidente pri čemu je posebna pažnja posvećena prevenciji phishing napada i analizi malvera. Radionica je organizovana od strane sajber stručnjaka iz Kancelarije za odbrambenu saradnju (ODC) Ambasade SAD u Crnoj Gori.
- Učešće na WB3C konferenciji „Building regional cyber resilience” - Konferencija je okupila stručnjake iz regiona radi razmjene iskustava i jačanja sajber otpornosti kroz diskusije o ključnim izazovima i rješenjima.
- Učešće na panelu na konferenciji „Izazovi i mogućnosti sajber bezbjednosti na Zapadnom Balkanu“ - Konferencija je obuhvatila diskusije o kritičnoj infrastrukturi gdje sam kao panelista istakla praktična rešenja iz perspektive privatnog i javnog sektora, istražujući kako nove tehnologije mogu poboljšati bezbjednost kritične infrastrukture.
- Učešće na obuci o sajber higijeni, gdje su prezentovane sigurnosne prakse i mjere za zaštitu od sajber prijetnji koju je organizovao CRDF GLOBAL.
- Učešće i pomoć pri organizaciji dvodnevne radionica „Multi-Sector Cybersecurity TTX: Unapređenje sajber bezbjednosti na Balkanu“, u organizaciji CRDF Global uz podršku Stejt departmenta SAD-a.
- Učešće na takmičenju Capture The Flag i prisustvo Klasteru sajber bezbijednosti koji se održao uz podršku CRDF globala.
- Učešće na International TTX „Cyber Resilience Strategies“
- Učešće na Connect 2024: Regional CERTs Cybersecurity Excellence Conference
- Učešće na regionalnom „Western Balkan Cyber Camp “ u organizaciji Uprave za elektronsku sertifikaciju i sajber bezbjednost iz Albanije (AKCESK) na kojem je učestvovalo 48 studenata iz zemalja regiona (8 studenata iz Univerziteta Crne Gore) koji su učestvovali na Cyber drill-u
- Učešće na konferenciji „Underground Economy Conference“
- Učestvovao na regionalnoj vježbi „Cybersecurity Reporting Training“ u organizaciji e-Governance Academy EGA
- Učešće na nacionalnoj radionici za pripremu integrisanog plana održivosti nuklearne bezbjednosti (INSSP) u organizaciji Ministarstva ekologije, održivog razvoja i razvoja sjevera
- Učešće na Trećoj regionalnoj sesiji tehničke razmjene kolega u organizaciji SRB CERT-a
- Učešće na ITU forumu za cyber bezbjednost i CiberDrill za Evropu i Mediteran. Učešće na panelu “Strengthening Europe - Mediterranean Cybersecurity Partnerships:

Lessons from the Past, Strategies for the Future". Učešće na Cyber drill vježbi. Cilj je da se unaprijedi sposobnost komunikacije i reagovanja na incidente timova učesnika iz evropskih zemalja. Takođe nastoji da podstakne kolektivne i zajedničke napore za ublažavanje sajber prijetnji među timovima za reagovanje na incidente računarske bezbjednosti (CSIRT) iz Evrope i arapskih regiona Mediterana.

- Učešće na Hack.lu konferenciji - Hack.lu je godišnja konferencija fokusirana na teme vezane za računarsku bezbjednost, kriptografiju, privatnost i hakovanje
- Učešće na TAIEX Regionalnoj radionici o sajber bezbjednosti i ENISA studijska posjeta
- Učešće na OSCE radionici na temu „Nacionalna klasifikacija sajber incidenata" Klasifikacija sajber incidenata: Izvještaj o novonastalim praksama u regionu OEBS-a Svrha nacionalnog sistema klasifikacije sajber incidenata. Uspostavljanje i operacionalizacija sistema klasifikacije sajber incidenata – proces i institucionalni aranžmani; ljudi i resursi. Sistemi klasifikacije sajber incidenata – međunarodna saradnja. Izazovi u razvoju i primjeni nacionalnih sistema klasifikacije sajber incidenata
- Učešće na tehničkom kolokvijumu „Technical course on assessment nad mitigation on cyber vulnerabilities" u organizaciji e-Governance akademije
- Učešće na tehničkom kolokvijumu „Technical training for CSIRT/SOC stuff on managing threath intelligence information"
- Učešće na obuci „Ključni elementi strategije komunikacije i odnosa s medijima za CIRT timove" u organizaciji e-GA
- Učešće u programu pod nazivom Digital Guardians „Empowering Youth for Online Safety and Digital Citizenship". Cilj programa je bio bezbjedno snalaženje na internetu i promosivanje odgovornog digitalnog ponašanja kao i sticanje digitalne pismenosti sajber bezbjednost i koje vrste sajber napada postoje.

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

- sa Savjetom za regionalnu saradnju (RCC) gdje je predstavljena platforma za jačanje saradnje u oblasti sajber bezbjednosti koja predstavlja centralizovani izvor informacija o EU projektima usmjerenih na sajber bezbjednost.
- o sajber bezbednosti na Zapadnom Balkanu u organizaciji RCC-a i AKCESK-a.

XI INSPEKCIJSKI NADZOR

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

Inspektor Direkcije za zaštitu tajnih podataka u toku 2024. godine, vršio je inspekcijski nadzor u skladu sa godišnjim Planom inspekcijskog nadzora.

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

U skladu sa Planom inspekcijskog nadzora, izvršen je inspekcijski nadzor u Ministarstvu odbrane, Upravi za izvršenje krivičnih sankcija i Vrhovnom državnom tužilaštvu, kao i nadzor u pravnim licima. Vanredni inspekcijski nadzor izvršen je u Centralnoj banci Crne Gore.

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 sarađuje 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 2024. 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 2024. godinu odobrena su sredstva za finansiranje Direkcije za zaštitu tajnih podataka u iznosu od 695.644,90€.

U izvještajnom periodu od raspoloživih sredstava isplaćeno je 651.228.79€.

U skladu sa zaključcima Vlade Crne Gore, Direkcija je krajnje racionalno trošila sredstva opredijeljena Budžetom za 2024. godinu, te je utrošila 93.61% odobrenih sredstva.

Nabavke

Direkcija je u skladu sa članom 84 Zakona o javnim nabavkama 25.01.2024. godine, donijela Plan javnih nabavki za 2024. godinu.

U izvještajnom periodu, u skladu sa Pravilnikom o načinu sprovođenja jednostavnih nabavki, roba i usluga realizovano je jednostavnih nabavki u iznosu od 30.292.68 eura.

Shodno Uredbi o načinu planiranja i sprovođenja centralizovanih javnih nabavki, koje sprovodi Uprava za državnu imovinu kao nadležni organ za sprovođenje postupaka centralizovanih javnih nabavki, dostavljen je Plan potreba za predmetima centralizovanih javnih nabavki za 2024. godinu.

Uprava za državnu imovinu za 2024. godine, kao nadležni organ za sprovođenje postupaka centralizovanih javnih nabavki odobren je iznos od 9.050,00€. Sredstva se odnose na administrativni materijal, rashode za gorivo i osiguranje zaposlenih i vozila.

Planom posebnih javnih nabavki u oblasti odbrane i bezbjednosti realizovane su tri nabavke i to: nabavka licenci za sistem za zaštitu od sajber napada, nabavka softvera za forenzičku analizu i skeniranje sistema na ranjivost i nabava opreme za sisitem za elektronsku razmjenu nacionalnih podataka stepena tajnosti „TAJNO".

Nadležnom organu blagovremeno je podnijet godišnji i polugodišnji Izvještaj o jednostavnim nabavkama, kao i Izvještaj o izuzećima od primjene u postupcima javnih nabavki za 2024. godinu.

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 2024. godini pripremljeni su i dostavljeni Ministarstvu finansija:
- Godišnji izvještaj o aktivnostima na sprovođenju i unapređenju upravljanja i kontrola za 2024. godinu,
- Godišnji izvještaj o obavještenjima o sumnjama na nepravilnosti i prevare za 2024. godinu.
- Upitnik za samoprocjenu upravljanja i kontrola za 2024.godinu.

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. Odjeljenje za unutrašnju reviziju u toku 2024.godine., u Direkciji izvršilo je Reviziju popisa imovine koju koristi Direkcija, kao i Reviziju službenih putovanja, putnih troškova i službenih dnevnica u Direkciji. Nakon toga, podnešeni su Izvještaji o sprovedenim revizijama, sa preporukama koje Direkcija za zaštitu tajnih podataka treba da otkloni u toku 2025.godine.

XIV JAVNOST RADA

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

Direkcija je ažurno odgovarala na 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.

Broj. 05-344/25-2
Podgorica, 22.4.2025.godine

v.d. DIREKTORA

Savo Vučinić