



CRNA GORA

Direkcija za zaštitu tajnih podataka

IZVJEŠTAJ O RADU
Direkcije za zaštitu tajnih podataka za 2025. godinu

Podgorica, januar 2026. godine

SADRŽAJ

UVOD	3
I NORMATIVNI POSLOVI	3
II DOZVOLE ZA PRISTUP TAJNIM PODACIMA	3
III MJERE ZAŠTITE TAJNIH PODATAKA	4
III-1 Fizičke mjere zaštite tajnih podataka	4
III-1 Informatičke mjere zaštite tajnih podataka	5
IV NATO I EU	6
IV-1. NATO	6
IV-2. EVROPSKA UNIJA	9
V MEĐUNARODNA SARADNJA	10
VI MEĐURESORSKA SARADNJA	10
VII SARADNJA SA NEVLADINIM ORGANIZACIJAMA	11
VIII OBUKE IZ OBLASTI TAJNIH PODATAKA	11
IX ORGANIZACIJA DIREKCIJE	13
X INFORMATIČKA BEZBJEDNOST I ODGOVOR NA RAČUNARSKE INCIDENTE	16
XI INSPEKCIJSKI NADZOR	21
XII BUDŽET I NABAVKE	21
XIII UPRAVLJANJE I UNUTRAŠNJA KONTROLA	22
XIV JAVNOST RADA	23

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, 117/24, 39/25, 97/25).

Izveštajem o radu Direkcije za zaštitu tajnih podataka obuhvaćen je pregled najvažnijih aktivnosti Direkcije u 2025. 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, kontinuiranim 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**.

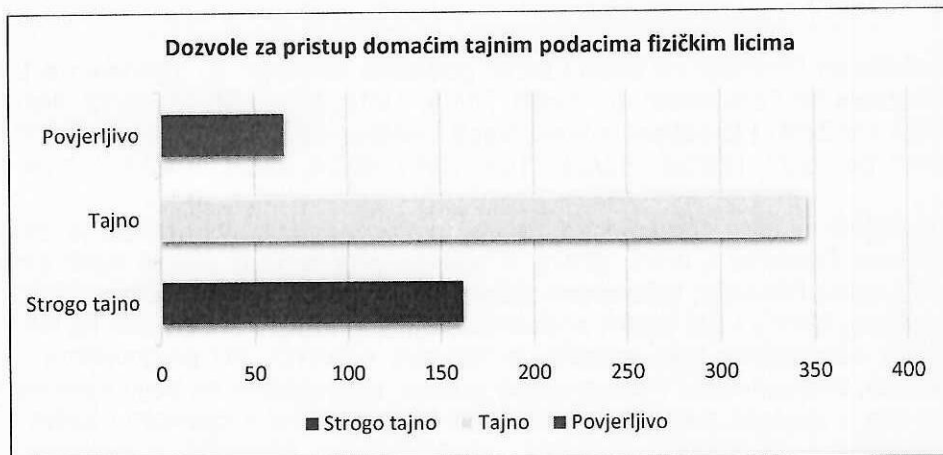
U 2025. godini, podnesena su 636 zahtjeva za izdavanje dozvola za pristup tajnim podacima, od čega je 462 zahtjeva za izdavanje novih dozvola a 174 zahtjeva za produženje važenja dozvole za pristup tajnim podacima.

U 2025. godini, izdate su ukupno 673 dozvola za pristup tajnim podacima, od čega su 507 novih dozvola, dok je produžen rok važenja za 166 dozvola za pristup tajnim podacima.

Za pristup tajnim podacima stepena tajnosti **STROGO TAJNO** izdato je 184 dozvole, od čega je 100 novih dozvola, a produžen je rok važenja za 84 dozvole za pristup tajnim podacima.

Za pristup tajnim podacima stepena tajnosti **TAJNO** izdato je 360 dozvola, od čega je 290 novih dozvola, a produžen je rok važenja za 70 dozvola za pristup tajnim podacima.

Za pristup tajnim podacima stepena tajnosti **POVJERLJIVO** izdato je 129 dozvola, od čega su 117 novih dozvola, a produžen je rok važenja za 12 dozvola.



U 2025. godini, na zahtjeve 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 2025. godini podnesen je 1 zahtjev za izdavanje dozvole za pristup tajnim podacima za pravno lice. U ovoj godini nije bilo izdatih dozvola za pristup tajnim podacima za pravno lice.

Za pristup tajnim podacima za zaposlene u pravnom licu podnesen je 41 zahtjev za izdavanje dozvole i 6 zahtjeva za produženje važenja dozvole za pristup tajnim podacima.

Prije izdavanja dozvole za pristup tajnim podacima zaposleni su u obavezi su da se edukuju o zaštiti i rukovanju tajnim podacima, odnosno bezbjednosnim pravilima i procedurama za zaštitu tajnih podataka.

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 2025. 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 bezbjednosne 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 2025.godine, održani su sastanci i konsultacije sa predstavnicima državnih organa a sve u cilju unapređenja mjera zaštite tajnih podataka.

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, Generalnom sekretarijatu Vlade Crne Gore i Stalnoj misiji Crne Gore pri NATO u Briselu.

Realizovana je nabavka nove informatičke opreme namijenjene ovom informacionom sistemu, čime su stvoreni uslovi da se u 2026. godini, nakon deset godina od njegovog uspostavljanja, izvrši potpuna tehnička obnova sistema. Krajem 2025. godine, sprovedena je nabavka kriptu uređaja koji ispunjavaju zahtjeve otpornosti na kvantne prijetnje.

Odjeljenje za informatičku zaštitu tajnih podataka je tokom 2025. godine, kontinuirano sprovodilo aktivnosti usmjerene na održavanje postojećeg sistema, kao i njegovo unapređenje u skladu sa važećim bezbjednosnim standardima.

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 kriptu 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"). Ugovor SSP za 2025. godinu potpisan je u martu 2025. Godine, od strane direktora Direkcije za zaštitu tajnih podataka.

NCIA je u saradnji sa Direkcijom, Ministarstvom odbrane i Ministarstvom vanjskih poslova, pripremila i dostavila predlog SSP ugovora za 2026. godinu, čije se potpisivanje i izmirenje obaveza prema NCIA planira u prvom kvartalu 2026. godine.

U saradnji sa NCIA realizovana je i nabavka nove opreme radi zamjene dotrajalih NS WAN radnih stanica i štampača, čija se isporuka očekuje tokom prvog kvartala 2026. godine. U toku 2025. godine obavljeno je nekoliko konsultativnih sastanaka sa predstavnicima NCIA i Ministarstva odbrane Crne Gore u vezi sa pitanjima nacionalnog preuzimanja NS WAN sistema, njegove sertifikacije i interkonekcije sa NATO CIS (Affiliate Federated Network - AFN).

U okviru NDA nadležnosti Direkcije, Odjeljenje za informatičku zaštitu tajnih podataka u kontinuitetu obavlja poslove vezane za upravljanje i distribuciju kriptomaterijala za potrebe NS WAN sistema i drugih informacionih sistema u kojima se obrađuju tajni podaci.

U periodu od 8. do 19. septembra 2025. godine, izvršena je instalacija novog DKMI sistema za upravljanje kriptomaterijalima.

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 kontingenta crnogorskih vojnika u mirovnu misiju ISAF u Avganistanu, a kasnije u misiju "Resolute Support" u Avganistanu.

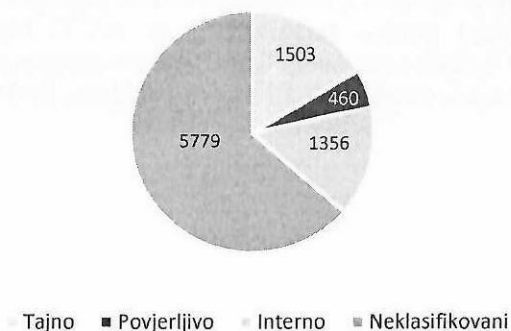
Pristupanjem Crne Gore NATO Savezu uveden je novi sistem elektronske razmjene NATO tajnih podataka NATO SECRET WAN AREA NETWORK (NS WAN) odobren od strane NATO Kancelarije za bezbjednost (NOS).



*šematski prikaz razmjene tajnih podataka sa NATO

U 2025. godini razmijenjeno je ukupno 3319 NATO tajnih podataka različitih stepena tajnosti, od čega 1503 stepena tajnosti TAJNO, 460 stepena tajnosti POVJERLJIVO, 1356 stepena tajnosti INTERNO i 5779 neklasifikovanih podataka.

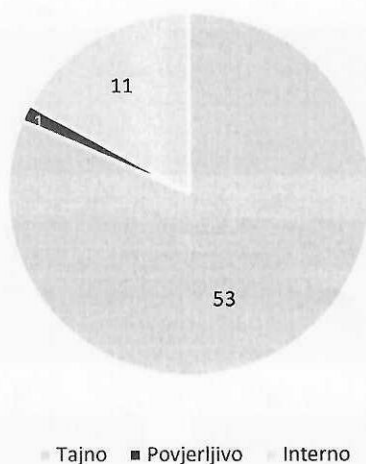
Razmjena NATO tajnih podataka po stepenima tajnosti



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

Sa Stalnom misijom Crne Gore pri NATO u Briselu u 2025. godini, razmijenjeno je ukupno 65 tajnih podataka različitih stepena tajnosti, od čega 53 stepena tajnosti TAJNO, 1 stepena tajnosti POVJERLJIVO i 11 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, kursovima, 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 2025. godini izdala je 213 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 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 oktobra mjeseca 2025.godine, realizovana posjeta i 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

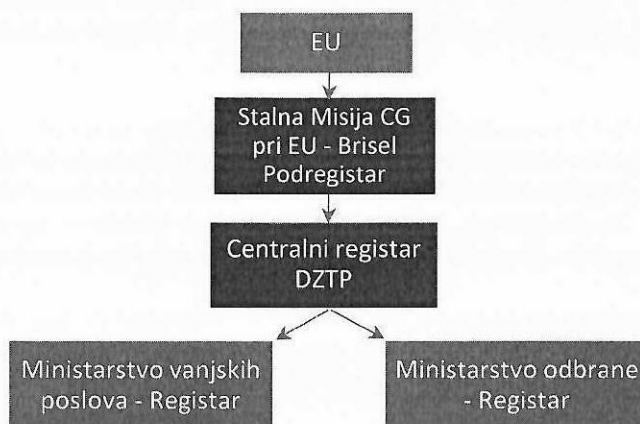
Poglavlje 10 – Informatičko društvo i mediji

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 2025. godini izdala je 4 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 okviru međunarodne saradnje nastavljena je saradnja sa te su realizovane posjete od strane kolega iz Republike Sjeverne Makedonije, Slovenije i a sve u cilju razmjene iskustava, dobrih praksi i planiranih aktivnosti po pitanju ove vrste saradnje.

U periodu od 22.- 25.09.2025. godine službenici Direkcije učestvovali na godišnjoj MISWG međunarodnoj konferenciji o industrijskoj bezbjednosti koja je održana u Vilniusu, Litvanija. Zemlje članice kao i međunarodne organizacije koje se nalaze u sastavu MISWG predstavile su novine u svojim propisima koji se odnose na tajnost podataka sa akcentom na industrijsku bezbjednost i razgovarale o dobrim praksama i izazovima sa kojima se suočavamo.

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.

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 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, sarađivalo se sa Ministarstvom unutrašnjih poslova, Ministarstvom vanjskih poslova, Upravom Carina, Poreskom upravom, te kontinuiranim sastancima sa Ministarstvom prostronog planiranja, urbanizma i državne imovine, i Ministarstvom ekonomskog razvoja kroz rad na propisu iz nadležnosti tog organa, 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 TAIXE instrumenata tehničke podrške, uspostavljena elektronska aplikacija za E-trening, koja pruža mogućnost državnim službenicima za lakšim i savremenijim edukovanjem u ovoj oblasti.

Stručno osposobljavanje i usavršavanje službenika Direkcije

U okviru Programa stručnog osposobljavanja Uprave za ljudske resurse u 2025. 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.

Službenici Odjeljenja za informatičku zaštitu tajnih podataka učestvovali su na godišnjoj NDA konferenciji predstavnika država članica NATO, koja je održana u Atini u periodu od 1. do 3. aprila 2025. godine. U periodu od 22. do 26. septembra 2025. godine u NCIA centru za obuku u Portugalu dva službenika Direkcije pohađala su obuku NATO CIS Security Officer.

Zaposleni u Odjeljenju učestvovali su u međunarodnoj sajber vježbi „Immediate Response 25 – Cyber Soko 25“(TTX, Train the Trainers), koja je realizovana u periodu od 26. maja do 6. juna 2025. godine.

U okviru implementacije DKMI sistema u Podgorici, u periodu od 8. do 19. septembra 2025. godine, organizovana je obuka zaposlenih za rukovanje kriptomaterijalima u ovom

informacionom sistemu. U sastavu sedmočlane multiresorske crnogorske delegacije predstavnik Direkcije, uzeo je učešće na Regionalnoj konferenciji o hibridnim prijetnjama, uz vježbu simulacije hibridnog napada na Zapadnom Balkanu održanoj u Tirani (Albania) od 17-20. 11. 2025. godine. Konferencija je realizovana u organizaciji Evropskog centra izvrsnosti za suprotstavljanje hibridnim prijetnjama (Hybrid CoE), Vlade Republike Albanije i Odjeljenja za globalne poslove Kanade (GAC). Održavanje konferencije je jedna od aktivnosti koju Hybrid CoE sprovodi u cilju fokusiranja na region Zapadnog Balkana i prijetnjama sa kojima se suočava.

Predstavnici Direkcije, učestvovali su na regionalnoj 6S konferenciji na temu prekomjerne klasifikacije tajnih podataka („Overclassified“), održanoj u Skoplju u periodu od 26. do 28. novembra 2025. godine. U periodu od jula do septembra 2025. godine, državni službenici zaposleni u u državnim organima, koji posjeduju bezbjednosne dozvole za pristup NATO tajnim podacima, realizovali su online testiranje putem portala Direkcije za online obuke. Tokom godine obavljene su konsultacije sa predstavnicima državnih institucija i privatnog sektora u vezi sa mjerama informatičke i TEMPEST zaštite, kao i postupcima akreditacije informacionih sistema u kojima se obrađuju tajni podaci.

U okviru redovne inspekcijske posjete NATO Office of Security (NOS), održane u Podgorici od 30. septembra do 2. oktobra 2025. godine, predstavnici Odjeljenja prezentovali su postojeće mjere zaštite informacionih sistema za razmjenu nacionalnih i NATO tajnih podataka, kao i planirane aktivnosti na njihovom daljem unapređenju.

Direkcija za zaštitu tajnih podataka je u okviru SAA nadležnosti (Security Accreditation Authority) učestvovala u aktivnostima međunarodnog BICES akreditacionog tijela (BICES Accreditation Board, BSAB).

Predstavnik Odjeljenja za informatičku zaštitu tajnih podataka tokom 2025. godine, učestvovao je u radu Interresorne komisije za suprotstavljanje hibridnim prijetnjama.

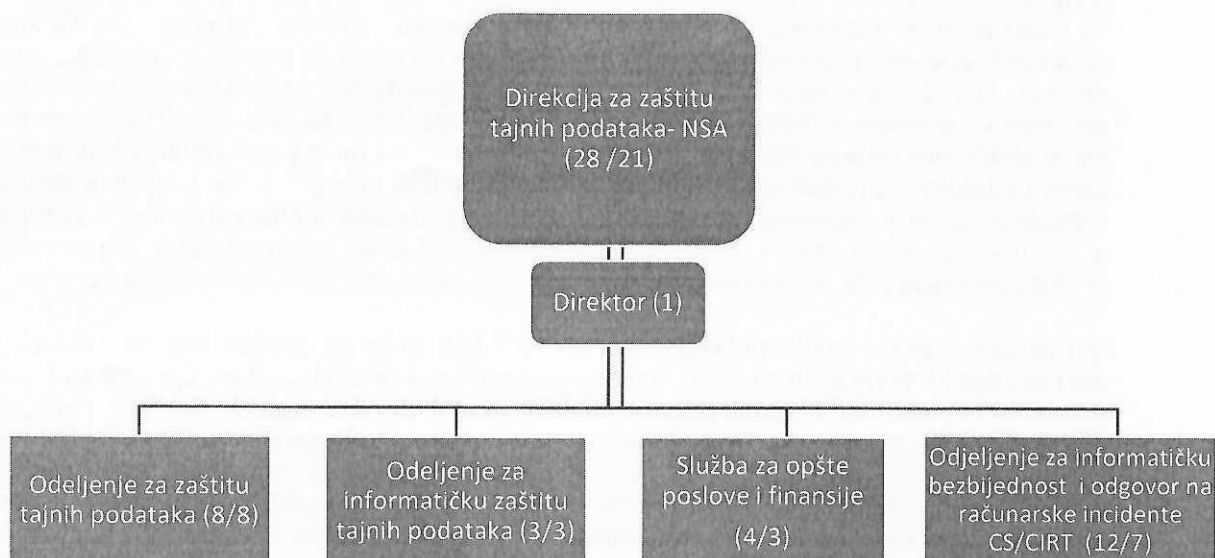
Službenici Direkcije u okviru Programa stručnog osposobljavanja Uprave za kadrove u 2025. godini, pohađali su sljedeće obuke: Postupak ocjenjivanja državnih službenika i namještenika, Prekršajni postupak, Zaštita ličnih podataka, Inspekcijski nadzor, Mobing, Postupak pred komisijom za žalbe, Bezbjednosna kultura, Zaštita i zdravlje na radu, Državni protokol, Ready4EU (obuka za sticanje znanja i vještina za rad u institucijama, tijelima i agencijama EU)., Sastanci mreže za upravljanje ljudskim resursima, Uloga i odgovornost ovlašćenih lica kod poslodavca.

IX ORGANIZACIJA DIREKCIJE

Direkcija vrši poslove iz svoje nadležnosti u okviru Odjeljenja 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.

Pripremljen je Nacrt novog Pravilnika o unutrašnjoj organizaciji i sistematizaciji Direkcije za zaštitu tajnih podataka, čije usvajanje se očekuje u I kvartalu 2026.god.

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.



U Odjeljenju 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 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 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 sistematizovano je 28 službeničkih radnih mjesta, uključujući i direktora. Ukupan broj zaposlenih izvršilaca je 24 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.

U skladu sa Kadrovskim planom za 2025. godinu, imenovan je vršilac dužnosti direktora Direkcije.

U Direkciji za zaštitu tajnih podataka miruju prava i obaveze iz rada i po osnovu rada:

- službeniku koji je u skladu sa Sporazumom zaključenim između Ministarstva vanjskih poslova i Direkcije za zaštitu tajnih podataka, raspoređen u Misiju Crne Gore pri NATO u Briselu, do 2027 godine.

- službenici koja je obavljala poslove samostalne savjetnice I za međunarodnu saradnju u Odjeljenju za zaštitu tajnih podataka, u Direkciji za zaštitu tajnih podataka, zbog upućivanja bračnog druga u Misiju Crne Gore pri NATO u Briselu, Kraljevina Belgija.

- službeniku koji je obavljao poslove samostalnog savjetnika I za CS/NCIRT u Odjeljenju za informatičku bezbjednost i odgovor na računarske incidente (CS/CIRT), u Direkciji za zaštitu tajnih podataka zbog izbora, odnosno imenovanja na državnu funkciju čije vršenje zahtijeva privremeni prestanak rada kod poslodavca, do isteka jednog mandata.

Donijet je Plan integriteta Direkcije za zaštitu tajnih podataka i Upitnik za procjenu efektivnosti i efikasnosti Plana integriteta za 2025. 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 2025.godinu, i dostavljen Izvještaj o sprovedenoj analizi Upravi za ljudske resurse. Pripremljena je i dostavljena Ministarstvu javne uprave Funkcionalna analiza ljudskih resursa Direkcije za zaštitu tajnih podataka.

Jednom službeniku je prestao radni odnos zbog sticanja prava na starosnu penziju.

U 2025. godini, obrazovana je Komisija koja je izvršila redovni godišnji popis pokretnih i nepokretnih stvari i obaveza sa stanjem na dan 31.12.2024. godine. Izrađen je tabelarni prikaz osnovnih sredstava za 2024. godinu i dostavljen je Izvještaj o popisu pokretne imovine i PS-obraci 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 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.

Predstavnici CIRT-a su učestvovali radnim grupama za izradu zakona, strategija, akcionih planova kao i Radnoj grupi za pregovaračko poglavlje 10 – Informatičko društvo i mediji.

Pripremljen kratki prilog o realizovanim aktivnostima u CIRT-u za prethodni period, koji sadrži informacije o aktivnostima i dostignućima u okviru poglavlja 10 – Informatičko društvo i mediji, za predstojeći II sastanak Odbora za stabilizaciju i pridruživanje.

Proaktivne mjere

Tokom 2025. godine, putem društvenih mreža i zvanične internet stranice www.gov.me/cirt kontinuirano smo informisali javnost o aktuelnim sajber prijetnjama, sa posebnim fokusom na fišing kampanje i različite oblike internet prevara. Redovno smo dijelili praktične savjete za prepoznavanje fišing pokušaja i pružali smjernice za bezbjedno korišćenje interneta, čime smo doprinijeli jačanju svijesti o sajber bezbjednosti. Posebna pažnja posvećena je edukaciji roditelja o adekvatnom praćenju on-line aktivnosti djece.

Putem društvenih mreža obilježavali smo ključne datume i preporuke iz oblasti sajber bezbjednosti, istovremeno promovišući dobre prakse i bezbjednosne standarde. Na svim kanalima komunikacije redovno su objavljivana upozorenja na aktuelne prijetnje, preporuke za prevenciju incidenata i informativni sadržaji namijenjeni različitim kategorijama korisnika.

Zvanična internet stranica (www.gov.me/cirt) bila je centralna platforma za informisanje, edukaciju i podizanje svijesti o sajber prijetnjama. Tokom godine, najčitaniji crnogorski on-line mediji (CDM, Aktuelno, Dan, Montenegro Magazine, Bankar, Gradski, Volim Podgoricu) kontinuirano su prenosili naše objave, preporuke i upozorenja, čime je dodatno proširen domet naših informacija prema široj javnosti. Tokom godine ostvarili smo i intenzivnu komunikaciju sa medijima. Posebno se izdvaja saradnja sa BIRN-om („Balkan Investigative Reporting Network“), regionalnom mrežom specijalizovanom za istraživačko novinarstvo i analitičko izvještavanje. Kao jedan od najuticajnijih istraživačkih medija na Balkanu, BIRN se bavi temama od javnog interesa, uključujući digitalnu bezbjednost, transparentnost i zaštitu privatnosti građana. BIRN je učestalo upućivao upite u vezi fišing napada i opšte situacije u oblasti sajber bezbjednosti u Crnoj Gori, čime je dodatno podignuta vidljivost našeg rada i važnost pravovremenog informisanja javnosti.

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 saradnji sa eksternim konsultantom, identifikovali smo ključne institucije u kojima je neophodno uraditi skeniranje na ranjivosti. Ove aktivnosti će nam pomoći da identifikujemo ranjivosti i predložimo mjere za unapređenje bezbjednosti sistema u ovim institucijama

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.

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 2025. 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 2025. godine nastavljen trend rasta broja prijavljenih incidenata u odnosu na prethodne godine. Tokom 2024. godine CIRT-u je prijavljeno ukupno 788 incidenata, dok je u 2025. godini CIRT registrovao 859 prijave. Ovaj trend se ogleda i u činjenici da je CIRT-u, tokom 2025. 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.

Po prijavi napada na informacioni sistem, na temelju uzetih imidža servera, računara i mrežnih uređaja, sprovedena je temeljna istraga koja je omogućila identifikaciju izvora napada i njegovog opsega. Nakon analize, pripremljen je sveobuhvatan izvještaj koji je dostavljen Upravi policije, specijalizovanom Odsjeku za visoko-tehnološki kriminalitet, za dalju istragu i preduzimanje odgovarajućih mjera kao i Zavodu za hidrologiju i seizmologiju.

Po prijavi napada na informacioni sistem, na temelju uzetih imidža servera, računara i mrežnih uređaja, sprovedena je temeljna istraga koja je omogućila identifikaciju izvora napada i njegovog opsega. Nakon analize, pripremljen je sveobuhvatan izvještaj koji je dostavljen Upravi policije, specijalizovanom Odsjeku za visoko-tehnološki kriminalitet, za dalju istragu i preduzimanje odgovarajućih mjera kao i FK Budućnost.

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
2024	49	126	93	11	472	37	788
2025	57	132	115	15	497	43	859

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 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

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 regionalnoj naprednoj tehničkoj vježbi u okviru projekta CyberSEE gdje je glavni cilj aktivnosti bio da učesnicima pruži praktične vještine zajedničkih istraga, dijeljenja informacija i međunarodne/međuinstitucionalne saradnje, kroz rješavanje praktičnih problema sajber kriminala i sajber bezbjednosti. Učešće na "Strengthening cooperation and real-time information exchange between LEA's and CERT's"
- Učešće na godišnjim konferencijama ISS World Euro and Underground Economy Conference.

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 drugoj peer razmjeni između EU CERT timova (Kipar CERT) i CERT timova Zapadnog Balkana
- CERT of Croatia and Western Balkan CERTs – peer exchange
- 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 trećeg izdanja „Balkan Cybersecurity Days“
- Učešće na „Western Balkans Cyber Camp“

EGA je ključni partner u okviru EU-finansiranih projekata koji se sprovode u Crnoj Gori i drugim zemljama Zapadnog Balkana (Albanija i Sjeverna Makedonija). Ovaj projekat ima cilj da ojača

otpornost i kapacitete državnih institucija za odgovor na velike sajber krize i napade, unaprijedi tehničke i operativne kapacitete kroz zajedničke obuke i koordinaciju i poboljša sprečavanje, odgovor i koordinaciju u slučaju velikih sajber incidenata. Projekat „Cybersecurity Rapid Response 2.0“ je nastavak ranijih aktivnosti koje su počele 2022. godine, fokusirane na povećanje spremnosti na sajber napade i usklađivanje sa EU standardima.

- Učešće na FIRST tehničkom kolokvijumu.
- Učešće na 37th Annual FIRST Conference i sastanku Nacionalnih CERT-ova
- Učešće na Cybersecurity Conference - CyberChess 2025

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 vježbovni aktivnosti Crne Gore u oblasti kriznih situacija u okviru NATO
- 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
- Radionica Unapređenje sajber bezbjednosti na Balkanu - Učešće i pomoć pri organizaciji dvodnevne radionica Unapređenje sajber bezbjednosti na Balkanu, u organizaciji CRDF Global uz podršku Stejt departmenta SAD-a
- Učešće na Cyber Threat Intelligence konferenciji
- Učešće na obuci “SIM3 Auditor Certification Training”
- Učešće na 17. Međunarodnoj konferenciji o sajber sukobima – CyCon 2025
- Učešće na „Study Visit and Hands-On Training at AKSK Cyber Lab and Range”
- Učešće na Donor Coordination Meetingu, koji je održan u okviru High-Level Cybersecurity Conference – Western Balkans CyberPulse 2025, koju je organizovao Regionalni savjet za saradnju (RCC) uz podršku Evropske komisije, u saradnji sa Western Balkans Cyber Capacity Center (WB3C). Učešće je pružilo priliku za koordinaciju aktivnosti donatora, razmjenu informacija i iskustava, te jačanje regionalnih kapaciteta u oblasti sajber-bezbjednosti
- Učešće na „Regional Cybercrime Cooperation Exercise“
- Studijska posjeta i učešće na praktičnoj vježbi koju je organizovala Agencija za sajber bezbjednost republike Albanije u organizaciji e-Governance akademije.

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
- sa CRDF o implementaciji projekta unapredja sajber bezbednosti na Zapadnom Balkanu.

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 2025. godine, vršio je inspekcijski nadzor u odnosu na primjenu Zakona o tajnosti podataka i podzakonskih akata za njegovo sprovođenje u skladu sa godišnjim Planom inspekcijskog nadzora.

U skladu sa Planom inspekcijskog nadzora, izvršen je inspekcijski nadzor Ministarstvu odbrane, Agenciji za Nacionalnu bezbjednost, Upravnom sudu, Ministarstvu vanjskih poslova, Upravi za izvršenje krivičnih sankcija i Vrhovnom državnom tužilaštvu.

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 u kontinuitetu i tokom 2025. godine, zahtijevala 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 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. Takođe, u kontinuitetu se insistira da organi u čijem radu nastaju tajni podaci, odrede lice za vršenje redovne unutrašnje kontrole.

XII BUDŽET I NABAVKE

Budžet

Zakonom o budžetu za 2025. godinu odobrena su sredstva za finansiranje Direkcije za zaštitu tajnih podataka u iznosu od 775.695,79€.

U izvještajnom periodu od raspoloživih sredstava isplaćeno je 641.623,63€.

U skladu sa zaključcima Vlade Crne Gore, Direkcija je krajnje racionalno trošila sredstva opredijeljena Budžetom za 2025.godinu, te je utrošila 82,71% odobrenih sredstva.

Nabavke

Direkcija je u skladu sa članom 84 Zakona o javnim nabavkama 30.01.2025. godine, donijela Plan javnih nabavki za 2025. godinu.

U izvještajnom periodu, u skladu sa Pravilnikom o načinu sprovođenja jednostavnih nabavki, roba i usluga realizovano je jednostavnih nabavki u iznosu od 21.755,22 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 2025.godinu.

Upravi za državnu imovinu za 2025.godine, kao nadležnom organu za sprovođenje postupaka centralizovanih javnih nabavki odobren je iznos od 9.442,00€ za potrebe Direkcije. Sredstva se odnose na administrativni materijal, rashode za gorivo i osiguranje zaposlenih i vozila.

Planom posebnih javnih nabavki u oblasti odbrane i bezbjednosti planirane su dvije nabavke i to: nabavka licenci za sistem za zaštitu od sajber napada, nabavka softvera za forenzičku analizu i skeniranje sistema na ranjivost i nabavke sertifikovanih NATO/EU kriptografskih uređaja potrebnih za elektronsku razmjenu nacionalnih tajnih podataka stepena tajnosti TAJNO.

Nadležnom organu blagovremeno je podnijet polugodišnji i godišnji Izvještaj o jednostavnim nabavkama, kao i Izvještaj o izuzećima od primjene u postupcima javnih nabavki za 2025. godinu.

U 2025. godini, izvršen je redovni godišnji popis pokretnih i nepokretnih stvari i obaveza sa stanjem na dan 31.12.2024. 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 2025. godini pripremljeni su i dostavljeni Ministarstvu finansija:

- godišnji izvještaj o aktivnostima na sprovođenju i unapređenju upravljanja i kontrola za 2025. godinu,
- godišnji izvještaj o obavještenjima o sumnjama na nepravilnosti i prevare za 2025. godinu.

U Direkciji za zaštitu tajnih podataka tokom 2025.godine, donijeto je 6 internih pravila i procedura, i to:

1. Interna procedura o angažovanju lica po ugovoru o djelu u Direkciji za zaštitu tajnih podataka,
2. Interna procedura o dodatnom radu;
3. Interno pravilo o bližim uslovima za obavljanje privremenih i povremenih poslova;
4. Interno uputstvo o postupanju po prijavama na prevaru, odnosno nepravilnostima u direkciji za zaštitu tajnih podataka;

5. Instrukcije za prepoznavanje i način postupanja u slučaju pojave sukoba interesa;
6. Uputstvo o postupanju po prijavi zviždača o ugrožavanju javnog interesa koje upućuje na postojanje korupcije, zaštita zviždača i vođenje evidencije.

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.02-010/26-230-2
Podgorica, 06.4.2026.godine

v.d. DIREKTORA



Savo Vučinić