2025

Nacionalni plan za odgovor na sajber prijetnju, ozbiljnu sajber prijetnju, incidente i sajber krizu

MINISTARSTVO JAVNE UPRAVE

Predgovor

U svijetu koji se rapidno razvija i sve više zavisi od digitalnih tehnologija, sajber prijetnje, incidenti i krize predstavljaju ozbiljnu opasnost za političku, ekonomsku, monetarnu, odbrambenu i nacionalnu bezbjednost, kao i za svakodnevni život građana.

Nacionalni plan za odgovor na sajber prijetnju, ozbiljnu sajber prijetnju, incidente i sajber krizu osmišljen je kako bi se uspostavio sveobuhvatan okvir za prevenciju, reakciju i oporavak od sajber prijetnji i incidenata.

Svrha ovog plana je da unaprijedi kapacitete države, javnog sektora, privatnog sektora i civilnog društva u suočavanju sa sajber prijetnjama, incidentima i krizama. Ovaj Nacionalni plan usvojen je u cilju izvršavanja obaveza i nadležnosti definisanih Zakonom o informacionoj bezbjednosti ("Službeni list CG", br. 113/2024), te predstavlja strateški okvir za efikasno rješavanje sajber prijetnji, ozbiljnih sajber prijetnji i sajber krize u skladu sa odredbama tog zakona. Kroz jačanje saradnje između različitih aktera društva (javnog i privatnog sektora, akademske zajednice i svih slojeva društva), Plan će omogućiti brže i efikasnije odgovore na sajber incidente, smanjiti rizike i osigurati kontinuitet ključnih usluga.

Cilj ovog Nacionalnog plana je ne samo da zaštiti nacionalne resurse i kritičnu infrastrukturu, već i da osigura povjerenje građana u digitalne tehnologije i sisteme. Ulaganjem u zaštitu od sajber prijetnji, Crna Gora se pozicionira kao sigurna i stabilna država, spremna da se suoči sa izazovima modernog doba.

Nacionalni plan je od suštinskog značaja za održavanje bezbjednosti i prosperiteta naše zajednice, jer pruža smjernice i pristupe za efikasno upravljanje rizicima i incidentima u sajber prostoru. Sa jasno definisanim postupcima i odgovornostima, Crna Gora će biti bolje organizovana da se suoči sa budućim izazovima i osigura sigurnu digitalnu budućnost za sve svoje građane. Ovim dokumentom Crna Gora potvrđuje svoju posvećenost izgradnji sigurnog, otpornog i održivog digitalnog društva.

Ovaj dokument predstavlja javnu verziju Nacionalnog plana za odgovor na sajber prijetnje i incidente. Javna verzija daje strateški okvir, definicije uloga i mehanizama saradnje, dok operativne procedure, tehnički protokoli, tokovi eskalacije i drugi detalji od bezbjednosnog značaja čine sastavni dio interne verzije Plana, namijenjene ograničenom krugu institucija.

Sadržaj

1. Uvod

Digitalna transformacija sve snažnije oblikuje društvene, ekonomske i institucionalne procese u Crnoj Gori i šire. Njena uloga postaje presudna za razvoj modernih državnih kapaciteta, unapređenje dostupnosti usluga i povećanje efikasnosti u gotovo svim oblastima javnog i privatnog sektora. Međutim, paralelno sa povećanjem zavisnosti od digitalnih tehnologija, javlja se i rastući spektar prijetnji koje proizilaze iz kompleksnog i globalno umreženog sajber prostora. Ove prijetnje nijesu više ograničene na tehničke domene informatičkih službi – one su postale strateško pitanje od najvećeg nacionalnog značaja.

U posljednjih deset godina, svijet je svjedočio značajnom porastu sajber incidenata koji utiču na državne organe, kritičnu infrastrukturu, finansijske sisteme, zdravstvene ustanove i privredu. Napadi koji su nekada bili ograničeni na pojedince ili male kriminalne grupe danas prerastaju u sofisticirane kampanje koje uključuju organizovane kriminalne mreže, napredne uporne prijetnje (APT grupe), pa čak i države koje koriste sajber prostor kao alat za ostvarivanje geopolitičkih ciljeva. U tom smislu, sajber prijetnje predstavljaju sveobuhvatni fenomen koji nadilazi tehnički sektor i zahtijeva integrisan, koordinisan i strateški odgovor.

Za Crnu Goru, koja se nalazi u procesu intenzivne modernizacije državne uprave, digitalizacije usluga i međunarodnog povezivanja sa evropskim i regionalnim strukturama, potreba za unapređenjem nacionalne sajber bezbjednosti postaje od suštinskog značaja. Digitalna infrastruktura predstavlja osnovu za funkcionisanje mnogih državnih servisa, dok sve veća povezanost sistema stvara nove slojeve rizika koji mogu da utiču na stabilnost institucija i sigurnost građana.

Nacionalni plan za odgovor na sajber prijetnje i incidente razvijen je kao strateški instrument kojim Crna Gora unapređuje svoje kapacitete u oblasti sajber otpornosti, koordinacije i odgovora na incidente. Ovaj Plan postavlja temelje za razumijevanje, odgovaranje i oporavak od incidenata u skladu sa najboljim međunarodnim praksama. Kroz jasno definisane uloge institucija, principa saradnje i strateških ciljeva, Plan doprinosi jačanju nacionalne stabilnosti i sigurnosti, uz transparentan i koherentan pristup koji je usklađen sa evropskim standardima.

Javna verzija Plana pruža pregled strateškog okvira i predstavlja dokument dostupan široj javnosti, dok se operativne procedure, protokoli, obrasci i scenariji nalaze u internoj verziji sa ograničenom distribucijom. Ovakav model je u skladu sa praksom država članica EU i drugih međunarodnih partnera, koji odvajaju strateške i operativne elemente radi zaštite institucionalne bezbjednosti.

1.1. Metodologija izrade Nacionalnog plana

Izrada ovog Nacionalnog plana utemeljena je na robustnoj i sveobuhvatnoj metodologiji, koja garantuje njegovu relevantnost, operativnu primjenjivost i usklađenost s najvišim međunarodnim standardima (Međunarodne organizacije za standardizaciju (ISO), Evropske agencije za sajber bezbjednost (ENISA), američkog Nacionalnog instituta za standarde i tehnologiju (NIST)). Proces je obuhvatio detaljnu analizu i komparativni pregled najbolje svjetske prakse u oblasti sajber bezbjednosti, uključujući izučavanje sličnih nacionalnih planova i strategija širom svijeta, s posebnim naglaskom na modele koji su se dokazali efikasnim u suočavanju sa kompleksnim sajber izazovima.

Kao temeljni oslonac u izradi Plana, poslužili su strateški i normativni dokumenti Crne Gore, čiji su principi i odredbe integrisani u svaku fazu razvoja. Posebno su detaljno analizirani i ugrađeni elementi iz *Strategije sajber bezbjednosti 2022-2026.*, usvojene u decembru 2021. godine, koja definiše nacionalne prioritete i okvire djelovanja, kao i *Zakon o informacionoj bezbjednosti iz 2024. godine*, koji postavlja pravni temelj za sve aspekte sajber zaštite.

Nadalje, Plan je obogaćen praktičnim iskustvima i ekspertizom nacionalnog Tima za odgovor na sajber incidente (CIRT), čiji su materijali i preporuke integralni dio operativnih protokola i smjernica. Ova direktna povezanost s operativnom praksom osigurava realističnost i efikasnost predloženih rješenja.

U cilju postizanja maksimalne dubine i preciznosti, u metodologiji izrade primijenjene su kombinovane kvalitativne i kvantitativne metode. Kvantitativna analiza obuhvatila je statističke podatke o sajber incidentima i prijetnjama, omogućavajući identifikaciju trendova i ključnih ranjivosti, dok je kvalitativni pristup uključivao analizu studija slučaja, ekspertske radionice i konsultacije s relevantnim akterima iz javnog i privatnog sektora, kao i akademske zajednice.

Pored nacionalnih resursa, značajan doprinos izradi Plana dali su i materijali institucija i agencija Evropske unije, čime je osigurana usklađenost s evropskim standardima i praksama u oblasti sajber bezbjednosti. Ova sveobuhvatna metodologija garantuje da je Nacionalni plan robustan, prilagodljiv i spreman da odgovori na dinamične i sve složenije sajber prijetnje.

1.2. Trendovi vezani uz sajber prijetnje

Sajber prostor Crne Gore svjedoči eksponencijalnom rastu napada koji s godinama postaju sve kompleksniji, noseći sa sobom sve veće posljedice po nacionalnu infrastrukturu, funkcionisanje javne uprave – naročito u aktuelnoj dekadi intenzivne digitalizacije društva – te po građane kao korisnike informaciono-komunikacionih tehnologija i e-servisa. Ova ključna konstatacija istaknuta je u *Strategiji sajber bezbjednosti 2022-2026.*, usvojenoj u decembru 2021. godine, koja prepoznaje evoluirajuću prirodu i težinu sajber izazova.[1]

Potvrda navedenog zabrinjavajućeg trenda uslijedila je sredinom avgusta 2022. godine, kada je Crna Gora pretrpjela jedan od najtežih sajber napada u svojoj istoriji. Ovaj napad rezultirao je zarazom stotina administrativnih računara zlonamjernim softverom, što je dovelo do opsežnog prekida rada brojnih državnih veb-sajtova i usluga. Među pogođenim sistemima bili su vitalni segmenti javne administracije, uključujući infrastrukturu Vlade, Parlamenta, Elektroprivrede, Carine i eUprave. Napad je detektovan 19. avgusta, nakon čega je grupa uspjela da kriptuje vladinu mrežu, postavljajući zahtjev za otkupninom radi deblokade sistema.

Globalni trendovi targetiranja vitalnih servisa država na način da se privremeno ili tajno obrišu odnosno otuđe podaci i servisi, Crna Gora nije bila izuzetak. Tako je 2022. godine nacionalna kritična infrastruktura bila predmet jedne od najsofisticiranijih ransomware napada, koji je za posljedicu imao ozbiljne poremećaje u komunikaciji unutar cjelokupnog državnog sektora, a mnoge ključne usluge su bile nedostupne određeno vrijeme. Proces oporavka bio je dugotrajan i zahtijevao je angažman i ekspertizu službi prijateljskih država, naglašavajući međunarodni aspekt i kompleksnost izazova.

Pored navedenog, izuzetno obimnog sajber napada, Crna Gora je u posljednjih nekoliko godina izložena povećanom broju različitih sajber prijetnji. Statistički podaci ukazuju na porast broja prijetnji, pri čemu fišing napadi, usmjereni kako na pojedince tako i na državne institucije, postaju sve češći i sofisticiraniji.

[1] Izvor informacije: Strategija sajber bezbjednosti 2022-2026, str. 11

1.3. Dominantni vektori sajber napada u Crnoj Gori i poređenje sa evropskim trendovima

Pored rastućih hibridnih prijetnji, sajber špijunaže i sajber kriminala – fenomena kojima je Crna Gora izložena u savremenom globalnom kontekstu[2] – analiza nacionalnog Tima za odgovor na sajber incidente (CIRT) dosljedno identifikuje tri najčešća vektora napada u crnogorskom sajber prostoru. To su prvenstveno: fišing (phishing), malveri (malware) i DDoS napadi (Distributed Denial of Service).[3] Detaljan uvid u ove prijetnje ključan je za razumijevanje operativnog okruženja i adekvatno reagovanje:

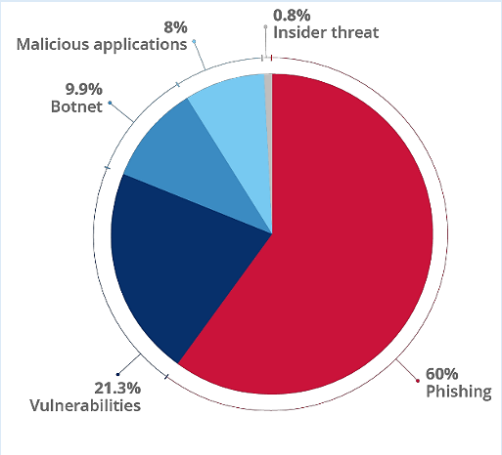
- **Fišing (eng. phishing):** Predstavlja vrstu napada koja se dominantno oslanja na metode socijalnog inženjeringa. Njegov primarni cilj je obmanom doći do osjetljivih korisničkih podataka koji služe za potvrdu identiteta, kao što su lozinke, brojevi kreditnih kartica, podaci o bankovnim računima i slično. Kroz sofisticirane prevare, napadači nastoje da navedu žrtve na dobrovoljno otkrivanje povjerljivih informacija.
- **DDoS napadi (eng. Distributed Denial of Service):** Ova vrsta sajber napada ima za cilj onesposobljavanje dostupnosti online servisa, mreže ili veb-stranice. To se postiže preopterećenjem ciljanog sistema ogromnim brojem istovremenih zahtjeva. Napadači koriste mrežu kompromitovanih računara ili uređaja (poznatu kao botnet) kako bi sinhronizovano poslali masivan broj zahtjeva ka ciljanoj mreži, preopterećujući je i čineći je nedostupnom za legitimne korisnike. Posljedice ovakvih napada kreću se od privremenog prekida usluga do značajnih finansijskih gubitaka i narušavanja reputacije.
- **Malver (eng. malware):** Obuhvata široku kategoriju zlonamjernog softvera koji je razvijen s primarnom svrhom nanošenja štete računarskim sistemima, mrežama ili podacima. Najčešće vrste malvera, koje se kontinuirano prilagođavaju novim odbrambenim mehanizmima, uključuju: viruse, crve, trojance, botove, ransomver (ransomware), bekdor (backdoor), spajver (spyware) i adver (adware). Njihova primjena može rezultirati gubitkom podataka, finansijskom štetom, kompromitacijom sistema i ugrožavanjem privatnosti.

Navedena zapažanja o dominantnim sajber prijetnjama u Crnoj Gori dosljedno se poklapaju s analizama Agencije Evropske unije za sajber bezbjednost (ENISA), što potvrđuje globalnu prirodu ovih izazova. Prema izvještaju *ENISA Threat Landscape 2024*, sedam glavnih sajber prijetnji na nivou cijele Evrope su sljedeće: ransomver, malver, socijalni inženjering, prijetnje po podatke, prijetnje po dostupnost: Uskraćivanje

[2] Izvor informacije: Strategija sajber bezbjednosti 2022-2026
[3] Izvor informacije: Cirt.me

usluga (eng. Denial of Service), manipulacija informacijama i uplitanje, napadi na lanac snabdijevanja (eng. Supply chain attacks).[4] Dok *ENISA Threat Landscape 2025* pruža statistički uvid u učestalost prijetnji.[5]

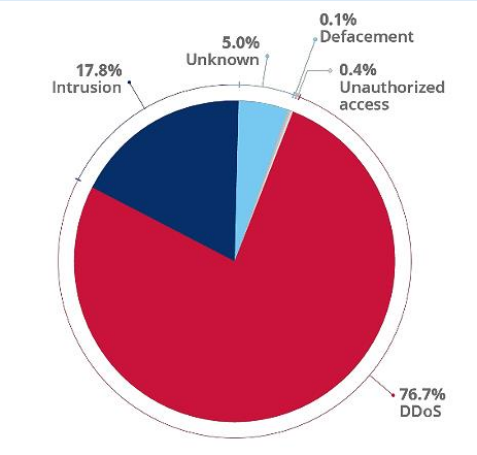
Slika 1. Najčešći identifikovani vektor početne infekcije



- **Fišing** (60%): Napadi koji se oslanjaju na manipulaciju ljudima (uključujući phishing, malspam, vishing i malvertising) čine 60% svih početnih ulaznih tačaka. Ovo je i dalje najzastupljeniji vektor.
- **Ranjivosti** (21.3%): Iskorišćavanje slabosti u softveru ili hardveru (tj. ranjivosti) predstavlja drugi najčešći način za kompromitovanje sistema.
- **Botnet** (9.9%): Upotreba botneta za inicijalni pristup čini značajan udio.
- **Zlonamjerne aplikacije** (8%): Kompromitovani softver i zlonamjerne aplikacije i dalje se koriste kao ulazni vektori.
- **Prijetnja insajdera** (0.8%): Neovlašćeni pristup koji potiče iznutra, od strane internih aktera, čini manji procenat.

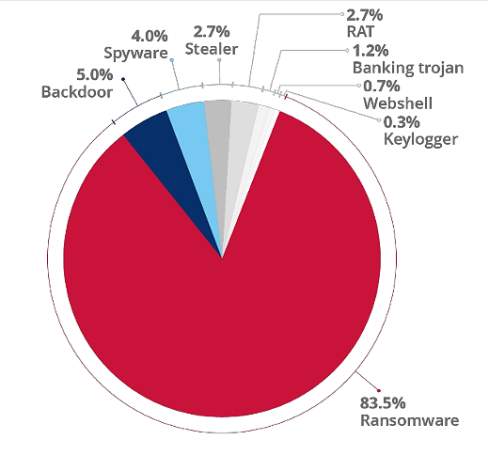
[4] Izvor informacije: ENISA Threat Landscape 2024
[5] Izvor informacije: ENISA Threat Landscape 2025

Slika 2. Distribucija tipova incidenata



- **DDoS napadi** (76.7%): Napadi uskraćivanja usluge dominiraju, čineći oko 76.7% svih registrovanih slučajeva.
- **Upadi/Provale** (17.8%): Provale ili neovlašćeni upadi u sisteme su na drugom mjestu.
- **Nepoznato** (5.0%): Incidenti čiji tip nije mogao biti precizno utvrđen ili kategorizovan.
- **Neovlašćeni pristup** (0.4%) i **Neovlaštena izmjena sadržaja** (0.1%): Ostali tipovi incidenata.

Slika 3. Distribucija identifikovanog zlonamjernog koda



- **Ransomware** (83.5%): Zlonamjerni softver za ucjenu je apsolutno dominantan, čineći 83.5% zabilježenih slučajeva, što ukazuje na primarnu finansijsku motivaciju napada.
- **Backdoor** (5.0%): Zlonamjerni kod za ponovni pristup).
- **Spyware** (4.0%): Softver za špijuniranje.
- **RAT** (2.7%): Alat za daljinsko administriranje (Remote Access Trojan).
- Ostali

Ove tri slike zajedno pružaju jasnu sliku o tome kako napadi počinju (slika 1.), koje su njihove primarne manifestacije (slika 2.) i koji je krajnji cilj (slika 3.), gdje pet najčešće ciljanih sektora napada uključuju javnu upravu (38.2%), transport (7.5%), digitalnu infrastrukturu i usluge (4.8%), finansije (4.5%) i proizvodnju (2.9%).

Ova podudarnost u identifikaciji prijetnji naglašava neophodnost međunarodne saradnje i usklađivanja nacionalnih strategija sajber bezbjednosti sa najboljim evropskim i globalnim praksama.

2. Svrha i ciljevi Plana

Svrha Nacionalnog plana za odgovor na sajber prijetnje i incidente jeste da uspostavi jedinstven, usklađen i održiv okvir za upravljanje sajber rizicima na nacionalnom nivou. Plan definiše temeljne principe, uloge i mehanizme saradnje između institucija, pružalaca digitalnih usluga, subjekata od posebnog značaja i drugih aktera čije aktivnosti utiču na bezbjednost informacionih sistema u Crnoj Gori. Ovim dokumentom se obezbjeđuje strateški pristup u prevenciji, otkrivanju, prijavljivanju i ublažavanju posljedica sajber incidenata, uz jačanje ukupne digitalne otpornosti države.

Nacionalni plan ima za cilj da doprinese izgradnji pouzdanog i bezbjednog digitalnog prostora kroz unapređivanje institucionalnih kapaciteta, jačanje koordinacije, povećanje otpornosti kritične infrastrukture i promovisanje kulture sajber bezbjednosti na svim nivoima. Plan naglašava značaj pravovremene razmjene informacija, saradnje između državnih organa i privatnog sektora, kao i aktivnog učešća Crne Gore u regionalnim i međunarodnim inicijativama koje doprinose unapređenju bezbjednosnih standarda.

Ciljevi Nacionalnog plana obuhvataju:

1. **Unapređenje nacionalnog okvira sajber bezbjednosti** kroz jasno definisane nadležnosti institucija, mehanizme koordinacije i strateško planiranje.
2. **Razvoj i jačanje kapaciteta institucija** za prevenciju, detekciju i odgovor na sajber prijetnje i incidente.
3. **Osiguranje kontinuiteta funkcionisanja digitalnih servisa**, posebno onih od javnog i posebnog značaja.
4. **Podizanje nivoa svijesti i znanja** o sajber rizicima među institucijama, privrednim subjektima i građanima.
5. **Usklađivanje sa međunarodnim standardima i najboljim praksama**, uključujući obaveze proistekle iz procesa evropskih integracija.
6. **Promovisanje kulture bezbjednosti i odgovornog ponašanja** u digitalnom prostoru, kao zajedničke obaveze ukupnog društva.

Ovaj Plan predstavlja strateški okvir koji povezuje različite aktere i resurse radi efikasnog upravljanja prijetnjama i jačanja digitalne otpornosti Crne Gore. U kombinaciji sa internom verzijom Nacionalnog plana, koja sadrži operativne procedure i tehničke smjernice, obezbjeđuje se cjelovit sistem za prepoznavanje, rješavanje i ublažavanje posljedica sajber incidenata.

3. Pravne osnove i međunarodne obveze

Nacionalni plan za odgovor na sajber prijetnje i incidente zasniva se na važećem normativnom okviru Crne Gore u oblasti informacione bezbjednosti, kao i na međunarodnim standardima, obavezama i principima koji oblikuju savremene politike zaštite digitalnog prostora.

Temeljni domaći propis u ovoj oblasti je Zakon o informacionoj bezbjednosti ("Službeni list CG", br. 113/2024), koji uvodi savremeniji i sveobuhvatniji sistem upravljanja sajber bezbjednošću, usklađen sa evropskim regulativama i standardima. Novi Zakon jača nadležnosti institucija, unapređuje obaveze subjekata od posebnog značaja, definiše jasnije mehanizme prijavljivanja incidenata i uvodi naprednije institucionalne i tehničke mjere u skladu sa praksom država članica Evropske unije. Na ovaj način stvaraju se pretpostavke za usklađivanje sa zahtjevima evropskog zakonodavstva koje proizilazi iz NIS2 direktive, kao i za dalji razvoj nacionalnog sistema sajber otpornosti.

U okviru međunarodnih obaveza, Crna Gora slijedi standarde, preporuke i smjernice međunarodnih organizacija i partnera sa kojima ostvaruje saradnju. To uključuje principe Evropske unije u oblasti bezbjednosti mreža i informacija, aktivnosti NATO-a u oblasti sajber odbrane, kao i praksu relevantnih međunarodnih tijela koja se bave unapređenjem bezbjednosnih politika i razmjenom stručnih znanja. Posebno su značajne inicijative koje se odnose na razvoj kapaciteta, učešće u zajedničkim projektima i unapređenje mehanizama za razmjenu informacija o sajber rizicima.

Shodno zakonskim nadležnostima, Ministarstvo javne uprave odgovorno je za izradu, održavanje i ažuriranje Nacionalnog plana, kao i za obezbjeđivanje njegove usklađenosti sa međunarodnim obavezama i standardima. Time se obezbjeđuje da politika sajber bezbjednosti u Crnoj Gori bude utemeljena na savremenim praksama i kontinuirano prilagođena razvoju evropskog i globalnog bezbjednosnog okruženja.

Nacionalni plan, kao strateški dokument, povezuje domaći pravni okvir sa međunarodnim standardima koji utiču na oblikovanje sigurnog i otpornog digitalnog prostora Crne Gore. Usklađenost sa evropskim i regionalnim praksama omogućava Crnoj Gori da se aktivno uključi u društvene, ekonomske i političke procese savremene digitalne transformacije i da obezbijedi visok nivo zaštite svojih informacionih sistema.

4. Pojmovi i koncepti sajber bezbjednosti

Razumijevanje ključnih pojmova od suštinskog je značaja za izgradnju dosljednog i efikasnog sistema upravljanja sajber rizicima.

U ovoj javnoj verziji Nacionalnog plana koriste se sljedeći osnovni pojmovi u strateškom smislu:

Sajber prijetnja je svaki potencijalni događaj, radnja ili okolnost koja može dovesti do narušavanja bezbjednosti digitalnih sistema.

Sajber incident je događaj koji je doveo do narušavanja povjerljivosti, integriteta ili dostupnosti mrežnih i informacionih sistema.

Ozbiljan sajber incident je incident koji može izazvati veće posljedice po rad institucija, privredu ili kritičnu infrastrukturu i zahtijeva koordinisano reagovanje.

Sajber kriza označava stanje u kome posljedice jednog ili više incidenata prevazilaze mogućnosti pojedinačne institucije i zahtijevaju djelovanje na nacionalnom nivou.

Sajber otpornost je sposobnost sistema da spriječi, izdrži, apsorbuje i se oporavi od sajber incidenata, uz minimalne poremećaje u funkcionisanju.

Povjerljivost, integritet i dostupnost predstavljaju osnovne principe zaštite informacionih sistema i podataka.

Pojmovi koji nijesu definisani ovom javnom verzijom Plana imaju značenje utvrđeno Zakonom o informacionoj bezbjednosti.

Definisani pojmovi služe kao osnov za razumijevanje ključnih koncepata i procesa u oblasti sajber bezbjednosti. Njihovo precizno korišćenje omogućava efikasniju komunikaciju, pravilnu primjenu propisa i razvoj koordinisanih mjera zaštite mrežnih i informacionih sistema u skladu sa savremenim bezbjednosnim izazovima.

5. Pregled prijetnji, incidenata i sajber kriza

Digitalni ekosistem Crne Gore postaje sve značajniji za funkcionisanje javnih institucija, privrede i društva u cjelini. Razvoj e-uprave, digitalnih servisa i međusobno povezanih informacionih sistema donosi brojne prednosti, ali istovremeno stvara prostor za nove i sve složenije bezbjednosne rizike. Sajber prijetnje više nijesu izolovani tehnički problemi, već strateški izazovi koji mogu uticati na stabilnost države, kontinuitet javnih usluga, ekonomiju i svakodnevni život građana.

U savremenom okruženju uočava se stalna evolucija prijetnji. One nastaju u kontekstu globalno dostupnih tehnologija, sve naprednijih alata za digitalne napade, kao i sve većeg prisustva organizovanih kriminalnih grupa i drugih aktera sa raznovrsnim motivima. Napadi mogu biti vođeni finansijskim interesom, kao dio šire kriminalne infrastrukture, ali i kao sredstvo političkog ili geopolitičkog pritiska. Zbog toga se sajber bezbjednost više ne može posmatrati isključivo kao tehničko pitanje već kao integralni dio nacionalne bezbjednosti.

U posljednjim godinama Crna Gora je, slično brojnim evropskim državama, zabilježila porast složenijih i koordinisanih incidenata. Posebno je značajan napad iz **avgusta 2022. godine**, kada je više državnih organa bilo izloženo organizovanom napadu visokog intenziteta, koji je privremeno poremetio funkcionisanje pojedinih informacionih sistema. Iako je odgovor institucija omogućio stabilizaciju stanja i kontinuitet ključnih usluga, ovaj događaj jasno je ukazao na ranjivost digitalnog prostora i potrebu za dodatnim jačanjem institucionalnih kapaciteta, otpornosti i koordinacije. Napad iz 2022. godine predstavlja važnu referencu u nacionalnom kontekstu, jer je pokazao da sofisticirane prijetnje mogu imati šire posljedice i zahtijevati sinhronizovano djelovanje više organa istovremeno.

Sajber prijetnje sa kojima se Crna Gora suočava obuhvataju širok spektar metoda i tehnika. Najčešće uključuju pokušaje neovlašćenog pristupa sistemima, kompromitovanje korisničkih naloga, distribuciju malvera, fišing kampanje, iznudu putem ransomware-a, narušavanje integriteta podataka, kao i pokušaje prekida rada servisa. Pored ovih tradicionalnih oblika napada, sve prisutnije su i kombinovane prijetnje, koje uključuju i elemente socijalnog inženjeringa, manipulaciju informacijama ili iskorišćavanje ranjivosti u procesima i ljudskim faktorima. Ovakvi napadi posebno su opasni jer se teško detektuju i mogu dovesti do značajnih posljedica prije nego što institucije shvate da je incident u toku.

Važan element u razumijevanju nacionalnog okvira prijetnji jeste i to što incidenti često prelaze granice pojedinačnih institucija. Zbog povezanosti informacionih sistema, napad koji započne u jednoj organizaciji

može imati posljedice i na druge subjekte koji koriste povezane servise, infrastrukturne resurse ili zajedničke standarde. Na ovaj način, lokalizovani incidenti mogu prerasti u događaje koji zahtijevaju koordinaciju na višem nivou ili uključivanje nacionalnih mehanizama upravljanja krizama. To dodatno naglašava potrebu za sistematskim pristupom i unapređenjem saradnje između državnih organa, regulatora, subjekata od posebnog značaja i provajdera digitalnih servisa.

Iako se prijetnje stalno mijenjaju, postoje određene karakteristike koje se mogu prepoznati u globalnim trendovima. Napadi su sve automatizovaniji, prilagođeniji ciljevima i često raspodijeljeni kroz više faza. Mnoge kriminalne grupe funkcionišu na tržišnim principima, nudeći usluge napada kao komercijalne proizvode. U takvom okruženju čak i tehnički slabiji akteri mogu sprovoditi sofisticirane napade koristeći dostupne alate, što dodatno komplikuje procjenu rizika. Istovremeno, napredne uporne prijetnje (APT) postaju sve prisutnije i predstavljaju izazov i za najrazvijenije zemlje, čime se naglašava potreba za međunarodnom saradnjom i praćenjem globalnih trendova.

Ovaj Plan prepoznaje da se nacionalni okvir prijetnji mora sagledavati strateški, a ne incidentno. To znači da prijetnje nijesu samo pojedinačni događaji, već dio šireg konteksta koji zahtijeva kontinuirano praćenje, analizu i planiranje. U tom smislu, razumijevanje prijetnji podrazumijeva i procjenu njihovog mogućeg uticaja na funkcionisanje institucija, privrede, kritične infrastrukture i društva u cjelini. Takva procjena rizika predstavlja osnov za donošenje odluka o prioritetima, mjerama unapređenja zaštite i investicijama u kapacitete.

Javna verzija Plana namjerno ne sadrži detaljne tehničke informacije, statističke podatke, liste ranjivosti, kategorizacije incidenata niti druge operativne elemente koji su dio interne verzije dokumenta. Time se obezbjeđuje da strateški okvir bude transparentan i razumljiv, dok se povjerljive procedure i podaci štite u skladu sa najboljom međunarodnom praksom. Fokus javnog poglavlja jeste da pruži razumijevanje šireg bezbjednosnog okvira i potrebu za daljim jačanjem nacionalnih kapaciteta.

U tom kontekstu, Nacionalni plan naglašava važnost izgradnje sistema koji može otvoreno prepoznati rizike, pravovremeno reagovati na incidente i obezbijediti oporavak digitalnih servisa. Ovaj pristup uključuje kontinuirano unapređenje tehničke infrastrukture, jačanje institucionalne saradnje, razvoj specijalizovanih znanja i promociju kulture bezbjednosti na svim nivoima.

Konačno, nacionalni okvir prijetnji ne posmatra se kao statična kategorija, već kao dinamičan koncept koji će se mijenjati u skladu sa razvojem tehnologije, promjenama u međunarodnom okruženju i praksama

koje se odnose na sajber bezbjednost. Zato će se i ovaj Plan redovno ažurirati kako bi ostao usklađen sa stvarnim izazovima i mogućnostima Crne Gore u digitalnom prostoru.

6. Upravljanje sajber bezbjednošću, vrste prijetnji, incidenata i kriza

Ovaj dio opisuje upravljanje sajber bezbjednošću te vrste sajber prijentji, incidenata i kriza u skladu sa *Zakonom o informacionoj bezbjednosti* i objašnjava nadležnosti svakog od organa i subjekta u Crnoj Gori. Hronološkim redom objašnjena su sljedeća područja:

- **Upravljanje sajber bezbjednošću** – predstavlja polaznu osnovu koju su dužni primijeniti svi organi i subjekti u Crnoj Gori;
- **Vrste prijetnji, incidenata i kriza** – prijetnje, incidenti i krize stalno se mijenjaju i postaju sve sofisticiraniji stoga je potrebno konstantno pratiti trendove i educirati se o navedenom;
- **Procjena uticaja sajber prijetnje, ozbiljne prijetnje i incidenta** - svi organi i subjekti u Crnoj Gori dužni su samostalno stalno vršiti procjenu uticaja svih izazova s kojima se susreću;
- **Nivoi negativnog uticaja sajber prijetnje, ozbiljne sajber prijetnje i incidenta** – određivanje nivoa provode Agencija za sajber bezbjednost i CIRT državne uprave;
- **Sajber kriza** – sajber kriza predstavlja ozbiljan izazov koji zahtijeva koordinisanu reakciju svih ključnih aktera u oblasti sajber bezbjednosti i njome se upravlja na nivou države.

6.1. Upravljanje sajber bezbjednošću

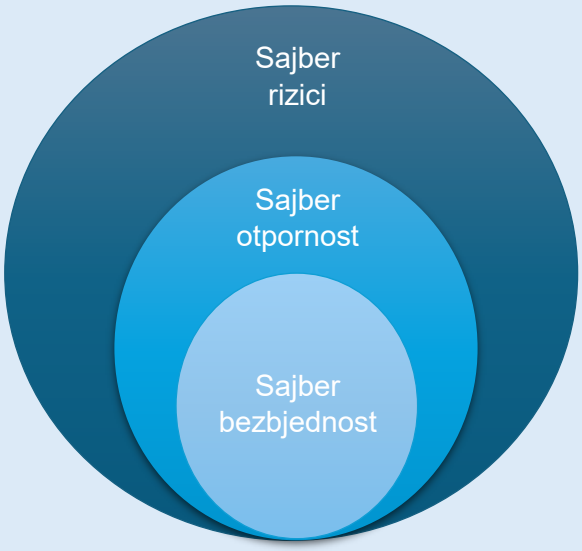
Upravljanje sajber bezbjednošću predstavlja strateški i nacionalni imperativ za Crnu Goru u digitalnom dobu. Ono nije samo tehnički zadatak, već sveobuhvatan okvir za upravljanje sajber rizikom na najvišem nivou, i to od strane svih subjekata koji su obveznici postupanja po *Zakonu o informacionoj bezbjednosti*. Upravljanje sajber bezbjednošću osigurava kontinuirano smanjenje sajber rizika, izgradnju sajber otpornosti, održavanje kontinuiteta kritičnih usluga i zaštitu nacionalne bezbjednosti i ekonomskog prosperiteta. Sistematičan pristup ključan je za očuvanje povjerenja građana i jačanje ukupne stabilnosti u suočavanju sa neizbježnim sajber prijetnjama, incidentima i potencijalnim krizama.

Sajber rizik je neizbježna polazna tačka u modernom digitalnom svijetu. Sajber rizik je prisutan i u porastu zbog proliferacije digitalizacije i uvođenja novih tehnologija. Svi subjekti moraju ga tretirati kao neminovnost i integrisati ga u sveukupnu poslovnu strategiju. Prihvatanje postojanja sajber rizika direktno diktira prelazak na viši strateški cilj – sajber otpornost.

Sajber otpornost je strateški cilj i nova paradigma upravljanja koja proizlazi iz prihvatanja neizbježnosti postojanja sajber rizika. Sajber otpornost je sposobnost subjekta da predvidi, izdrži, oporavi se od i prilagodi se opterećenjima i rizicima, istovremeno održavajući kontinuitet poslovanja i pružanje usluga. Da bi se postigao ovaj strateški cilj (otpornost), moraju se implementirati adekvatni i integrisani setovi mjera, što je domena sajber bezbjednosti.

Sajber bezbjednost je skup tehničkih i organizacionih mjera informacione bezbjednosti koje se koriste za implementaciju i postizanje sajber otpornosti. Vrste mjera informacione bezbjednosti propisane su *Zakonom o informacionoj bezbjednosti*. Sajber bezbjednost predstavlja temeljne kontrole i defanzivne mjere koje služe za smanjenje sajber rizika, kojima se postiže sajber otpornost. Bezbjednost je dakle operativno sredstvo kojim se gradi i održava otpornost sistema. Njihov međusoban odnos prikazan je na slici broj 4.

Slika 4. Sajber rizik → Sajber otpornost → Sajber bezbjednost



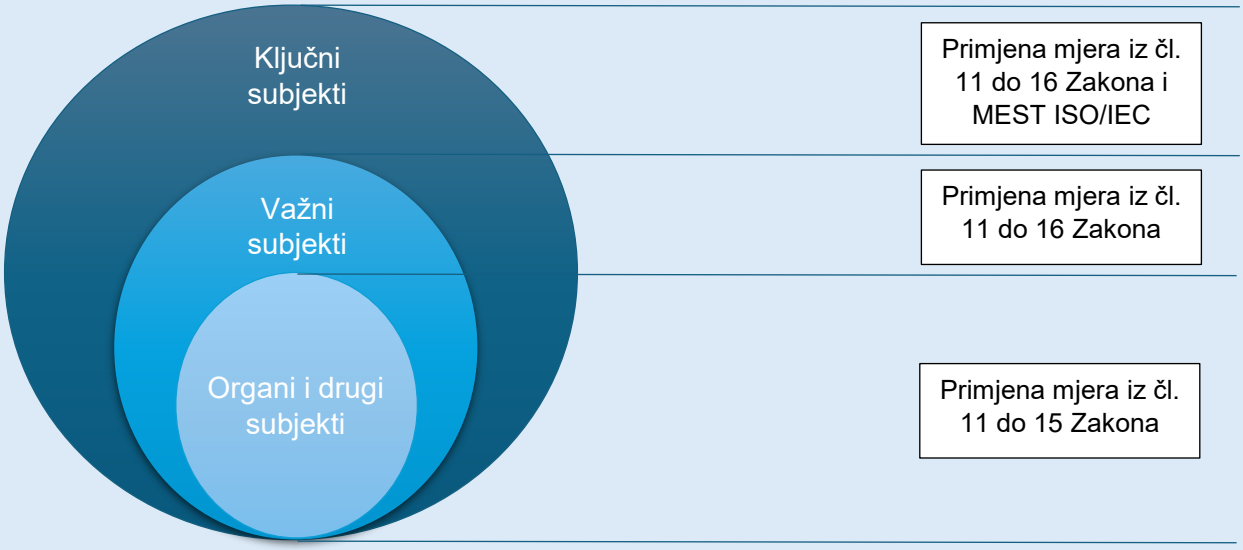
Upravljanje sajber bezbjednošću počinje prihvatanjem sajber rizika; to prihvatanje vodi postavljanju strateškog cilja sajber otpornosti (sposobnost nastavka rada); a taj cilj se postiže kroz primjenu i kontinuirano unapređenje mjera sajber bezbjednosti. Za uspostavu okvira upravljanja sajber bezbjednošću vidi aneks 1.

Savremeni digitalni prostor karakteriše stalna pojava novih oblika sajber rizika, prijetnji i bezbjednosnih incidenata, što iziskuje kontinuirano prilagođavanje pristupa i primjenu mjera zaštite. U skladu sa *Zakonom o informacionoj bezbjednosti*, obavezu preduzimanja mjera imaju:

- **Državni organi**, ministarstva i drugi organi uprave;
- **Organi jedinica lokalne samouprave**, organi lokalne uprave i službe formirane po zakonu o lokalnoj samoupravi;
- **Pravna lica sa javnim ovlašćenjima**;
- **Privredna društva i druga pravna i fizička lica** koja pristupaju podacima, postupaju s njima ili upravljaju mrežnim i informacionim sistemima.

Svi ovi subjekti dužni su da primjenjuju odgovarajuće **mjere informacione bezbjednosti**, koje obuhvataju kako zaštitu podataka, tako i zaštitu od sajber prijetnji i incidenata.

Slika 5. Obaveza primjene mjera informacione bezbjednosti



Obaveza primjene mjera informacione bezbjednosti objašnjena je u čl. 18 Zakona o informacionoj bezbjednosti.

Za uspješnu i efikasnu primjenu ovih mjera, ključno je da svaki organ i subjekt **uspostavi sopstveni okvir za upravljanje sajber bezbjednošću**, koji uključuje funkcije i kategorije usklađene sa važećim propisima i standardima.

6.2. Vrste prijetnji, incidenata i kriza

Na osnovu *Zakona o informacionoj bezbjednosti*, Crna Gora se formalno susreće sa sljedećim **vrstama incidenata i kriza** u domenu sajber bezbjednosti:

Tabela 1. Vrste prijetnji, incidenata i prijetnji

Vrsta	Opis	Posljedice / Uslovi
Sajber prijetnja	Svaka moguća okolnost, događaj ili djelovanje koje može negativno uticati na sistem ili podatke	- Mogućnost neovlaštenog pristupa mrežnim ili informacionim sistemima - Prikupljanje informacija - Identifikovane ranjivosti bez njihove zloupotrebe - Priprema napada bez još uvijek aktivne štete
Ozbiljna sajber prijetnja	Sajber prijetnja sa tehničkim karakteristikama koje ukazuju na značajan uticaj	- Mogućnost ozbiljne povrede povjerljivosti, integriteta i dostupnosti podataka - Potencijalna izmjena ili brisanje kritičnih podataka - Moguće ugrožavanje funkcionalnosti ključnih servisa - Visok nivo tehničke složenosti napada (npr. APT, ransomware u fazi širenja)
Incident	Događaj koji kompromituje povjerljivost, cjelovitost ili dostupnost podataka ili usluga	- Realizovana šteta, uključujući: Neovlašten pristup; Neovlaštena izmjena podataka; Djelimično ili trajno uništenje podataka; Povreda integriteta sistema - Gubitak pristupa uslugama (DoS/DDoS) - Finansijska i reputacijska šteta organizacije
Sajber kriza	Stanje koje ugrožava nacionalnu bezbjednost, zdravlje, ekonomiju ili životnu sredinu	- Masovno narušavanje kontinuiteta usluga - Paraliza ključnih nacionalnih funkcija (Vlada, zdravstvo, energija) - Kompromitacija velikih količina osjetljivih podataka (npr. podaci građana, zdravstvo) - Potreba za višesektorskim angažmanom i vanrednim mjerama - Značajna politička, ekonomska ili sigurnosna destabilizacija

Vrste prijetnji, incidenata i sajber kriza predstavljaju različite nivoe ozbiljnosti i uticaja na informacionu bezbjednost, ali su međusobno povezane i često se prepliću u praksi. Sajber prijetnje su početni oblik rizika, koje same po sebi ne moraju uzrokovati štetu, ali ukazuju na potencijalne ranjivosti i mogućnosti za buduće napade. Ozbiljne sajber prijetnje nose veću tehničku složenost i veći potencijal za narušavanje bezbjednosti, što zahtijeva pojačane mjere prevencije i nadzora. Incidenti su konkretni događaji u kojima dolazi do kompromitacije podataka ili sistema, sa stvarnim posljedicama po funkcionalnost i integritet. Najteži oblik su sajber krize, koje prelaze granice pojedinačnih organizacija i ugrožavaju nacionalnu bezbjednost, ekonomiju i društvo u cjelini, zahtijevajući koordinisani odgovor na višesektorskom nivou. Upravo zbog ove hijerarhije i složenosti, svaki nivo zahtijeva specifične pristupe i mjere, od preventivnih do kriznih, kako bi se efikasno zaštitili digitalni sistemi i podaci.

6.3. Procjena uticaja sajber prijetnje, ozbiljne prijetnje i incidenta

Organi i drugi subjekti obavezni su da sami **vrše procjenu uticaja** sajber prijetnje ili incidenta na kontinuitet i kvalitet pružanja usluga kao i na povjerljivost i integritet informacija i sistema.

Procjena uticaja vrši se na osnovu sljedećih kriterijuma:

- **Povjerljivost**: neovlašćen pristup, iznošenje (eksfiltracija) ili objava podataka;
- **Integritet**: neovlašćena izmjena podataka, sistema ili procesa;
- **Dostupnosti usluge**: broj korisnika koji nijesu mogli da ostvare pristup ili su imali značajne teškoće u ostvarivanju pristupa usluzi;
- **Vrijeme trajanja** sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta;
- **Uticaj na reputaciju i geografska zastupljenost** sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta (ako je moguće utvrditi).

Procjena se vrši na osnovu značaja uticaja sajber prijetnje ili incidenta na kontinuitet pružanja usluga.

Nakon izvršene procjene svaki organ i subjekt dužan je da kategorizuje svaki događaj kao:

- Sajber prijetnja, ozbiljna sajber prijetnja i incident **koji nemaju uticaj** na kontinuitet pružanja usluga, ili
- Sajber prijetnja, ozbiljna sajber prijetnja i incident **koji negativno utiču** na kontinuitet pružanja usluga.

Ovisno o kategorizaciji događaja predviđene su i radnje koje je potrebno izvršiti. Navedeno će biti detaljno objašnjeno u narednom poglavlju pod nazivom Operativna koordinacija rješavanja sajber prijetnje, ozbiljne sajber prijetnje, incidente i sajber krize.

6.3.1 Model bodovanja procjene uticaja

Procjena uticaja se sprovodi kroz standardizovani model bodovanja radi smanjenja subjektivnosti i obezbjeđivanja uporedivosti između institucija i sektora. Za svaki kriterijum dodjeljuje se ocjena od 1 do 5, gdje 1 označava nizak uticaj, a 5 kritičan uticaj. Ukupni skor predstavlja zbir ocjena po kriterijumima, na osnovu kojeg se određuje nivo negativnog uticaja u skladu sa tačkom 6.4.

Kriterijumi bodovanja (1–5):

1. **Povjerljivost:** neovlašćen pristup, iznošenje (eksfiltracija) ili objava podataka.
   1.1. **1 bod:** Neovlašćen pristup bez pristupa stvarnom sadržaju podataka; Pokušaj pristupa ili izlaganje metapodataka bez osjetljivog sadržaja; Nema potvrđene eksfiltracije niti čitanja podataka;
   1.2. **2 boda:** Neovlašćen pristup ograničenom skupu nekritičnih, internih podataka; Podaci niske osjetljivosti;
   1.3. **3 boda:** Ako su kompromitovani lični podaci (identifikacioni/finansijski/kontakt);
   1.4. **4 boda:** Ako su kompromitovani posebne kategorije ličnih podataka ili podaci visoke osjetljivosti (npr. zdravlje, bezbjednosni podaci, tajni/klasifikovani podaci stepena tajnosti/klasifikacije interno i povjerljivo, pristupni podaci kredencijalni);
   1.5. **5 bodova:** Ako su kompromitovani **kredencijali administrativnih naloga**, ključevi za enkripciju, sistemske tajne ili tajni/klasifikovani podaci sa nacionalnim implikacijama odnosno stepena tajnosti/klasifikacije tajno i strogo tajno.

2. **Integritet:** neovlašćena izmjena podataka, sistema ili procesa.
   2.1. **1 bod:** Izmjene bez operativnog značaja; Privremene ili testne izmjene koje su brzo uočene i reverzibilne; Nema uticaja na odlučivanje, prava ili obaveze;
   2.2. **2 boda:** Izmjene u operativnim, nekritičnim podacima;
   2.3. **3 boda:** Izmjene u **službenim evidencijama, registrima, finansijskim podacima, evidencijama prava/obaveza** ili podacima koji utiču na odlučivanje;

2.4. **4 boda:** Izmjene u **kritičnim državnim registrima, sistemima za menadžent identitetima (IAM/AD), konfiguracijama bezbjednosti, logovima/audit tragovima**, ili podacima sa bezbjednosnim implikacijama;

2.5. **5 bodova:** Izmjene koje mogu uzrokovati **pogrešne odluke velikih razmjera**, finansijsku štetu velikog obima, ugrožavanje bezbjednosti ili destabilizaciju ključnih funkcija države.

3. **Dostupnost:** prekid ili degradacija usluga i kritičnih funkcija. Ocjena se određuje prema *najvišem relevantnom* efektu: (a) trajanju prekida i/ili (b) procentu pogođenih korisnika usluge.

3.1. **1 bod:** Uticaj na ≤ **1%** korisnika usluge ili lokalni uticaj bez prekida ključne funkcionalnosti;

3.2. **2 boda:** Uticaj na >1% do **5%** korisnika usluge ili kratkotrajna degradacija usluge;

3.3. **3 boda:** Uticaj na >5% do **20%** korisnika usluge ili djelimičan prekid usluge;

3.4. **4 boda:** Uticaj na >20% do **50%** korisnika usluge ili značajan prekid ključne funkcionalnosti;

3.5. **5 bodova:** Uticaj na **50% i više** korisnika usluge ili potpuni prekid kritične usluge.

4. **Vrijeme trajanja** sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta: vrijeme od T0 (inicijalna detekcija/validacija događaja) do T_kraj (stabilizacija i prestanak aktivnog negativnog uticaja).

4.1. **1 bod:** Vrijeme trajanja ≤ 30 minuta (brzo stabilizovan događaj, bez dužeg negativnog uticaja);

4.2. **2 boda:** Vrijeme trajanja > 30 minuta do 2 sata;

4.3. **3 boda:** Vrijeme trajanja > 2 sata do 6 sati;

4.4. **4 boda:** Vrijeme trajanja > 6 sati do 10 sati;

4.5. **5 bodova:** Vrijeme trajanja > 10 sati (dugotrajan događaj sa produženim negativnim uticajem).

5. **Uticaj na reputaciju i geografska zastupljenost** sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta (ako je moguće utvrditi).

5.1. **1 bod:** Lokalni uticaj (jedna lokacija/organ ili ograničen broj korisnika) bez medijskog interesovanja; reputacioni efekat zanemarljiv ili interno ograničen;

5.2. **2 boda:** Uticaj na više lokacija unutar jedne institucije ili jedne opštine; ograničeno interesovanje javnosti; reputacioni efekat nizak;

5.3. **3 boda:** Regionalni uticaj (više opština ili više organa u jednom regionu); primjetno interesovanje javnosti i/ili medija; reputacioni efekat srednji;

5.4. **4 boda:** Nacionalni uticaj (više sektora/organa na nivou države) ili incident od visokog javnog interesa; značajno medijsko izvještavanje; reputacioni efekat visok;

5.5. **5 bodova:** Široko nacionalni ili prekogranični uticaj (uključujući međunarodni odjek); dugotrajan ili intenzivan medijski pritisak; ozbiljno narušeno povjerenje javnosti i/ili međunarodnih partnera.

6.4. Nivoi negativnog uticaja sajber prijetnje, ozbiljne sajber prijetnje i incidenta

Nivoi negativnog uticaja sajber prijetnji, ozbiljnih sajber prijetnji i incidenata predstavljaju važnu dimenziju u procjeni rizika i planiranju odgovora na ove izazove. Ovi nivoi mogu varirati od manjih poremećaja u poslovnim operacijama, koji se mogu brzo otkloniti, do ozbiljnih posljedica koje ugrožavaju osnovne funkcije, povjerljivost i integritet podataka. Na najvišem nivou, negativni uticaj može rezultirati prekidom rada kritične infrastrukture, masovnim curenjem osjetljivih podataka, značajnim finansijskim gubicima i trajnim narušavanjem ugleda organa / subjekta. Razumijevanje različitih nivoa uticaja omogućava svima da jasno definišu prioritete i resurse koji su potrebni za rješavanje ovih prijetnji. Upravo kroz ovu analizu nivoa uticaja, moguće je postaviti pragove tolerancije na rizik i osigurati pravovremenu reakciju koja će minimizirati štetu i ubrzati proces oporavka, čime se unapređuje ukupna sajber otpornost i zaštita digitalne bezbjednosti.

Određivanje nivoa negativnog uticaja sajber prijetnje, ozbiljne sajber prijetnje i incidenta na kontinuitet pružanja usluga je **direktna nadležnost Agencije za sajber bezbjednosti i CIRT-a državne uprave**.

Po prijemu početnog obavještenja Agencija, odnosno CIRT državne uprave sprovodi analizu uticaja sajber prijetnje, ozbiljne sajber prijetnje, odnosno incidenta na kontinuitet pružanja usluga i mogućih načina reagovanja na te sajber prijetnje, odnosno incident i utvrđuje nivo incidenta koji može biti:

- **niski**
- **srednji**
- **visoki**.

Primjeri procjene nivoa sajber incidenta povezano s kriterijumima uticaja, primjerima incidenata, obvezama organa i subjekta te ulogom Agencije i CIRT-a državne uprave predstavljeno je u tabeli 2. Dok će operativno postupanje biti objašnjeno u narednom poglavlju.

Tabela 2. Procjene nivoa sajber incidenta

Nivo incidenta	Bodovi	Kriterijumi uticaja	Primjeri incidenata	Obaveze organa/subjekta	Uloga Agencije / CIRT-a
NISKI	5-11	- Ograničen broj korisnika - Kratko trajanje (<2h) - Lokalan domet - Nema gubitka osjetljivih podataka	- Privremeni pad interne aplikacije - Neuspjela phishing poruka - Blokiran pristup dijelu mreže	- Samostalno otklanjanje - Interna registracija incidenta - Jednom mjesečno obavještava Agenciju, odnosno CIRT državne uprave	- Po potrebi daju smjernice
SREDNJI	12-18	- Veći broj korisnika - Trajanje 2–10h - Regionalni domet - Potencijalni uticaj na podatke	- DDoS napad - Uspješan malver na serveru - Curenje podataka zaposlenih	- - Početno obavještenje najkasnije u roku od 24 sata od trenutka saznanja - Periodični izvještaji (svaka 72 sata) - Završni izvještaj (30 dana)	- Aktivno učestvuju u rješavanju - Smjernice i nadzor
● VISOKI	19-25	- Širok broj korisnika - Trajanje >10h - Nacionalni / prekogranični domet - Kompromitovani ključni podaci	- Ransomware na ključnim sistemima - Napad na bazu građana - Curenje osjetljivih podataka	- - Početno obavještenje najkasnije u roku od 24 sata od trenutka saznanja - Prvi izvještaj (72 sata) - Periodični izvještaji (svaka 24 sata) - Završni izvještaj (30 dana)	- Preuzimaju vođstvo - Koordinacija s bezbjednosnim organima i Vladom - Moguć prijedlog sajber krize

6.5. Sajber kriza

Sajber kriza u kontekstu Crne Gore predstavlja ozbiljan izazov koji zahtijeva koordinisanu reakciju svih ključnih aktera u oblasti sajber bezbjednosti. U sve digitalizovanijem društvu, gdje javna uprava, privreda i građani u velikoj mjeri zavise od mrežnih i informacionih sistema, sajber kriza može ugroziti funkcionisanje državnih institucija, kritične infrastrukture i povjerenje građana u digitalne sisteme. Crna Gora se, kao i druge države, suočava sa rastućim brojem sofisticiranih sajber napada koji zahtijevaju ne samo tehničku spremnost, već i strateški pristup u prevenciji, upravljanju i oporavku od krize. Kroz primjenu *Zakona o informacionoj bezbjednosti* i jačanje kapaciteta specijalizovanih timova, kao što su CIRT-ovi, Crna Gora razvija mehanizme za odgovor na sajber prijetnje. Međutim, sajber kriza nije samo tehnološki problem, već i društveni i ekonomski izazov, koji zahtijeva kontinuiranu edukaciju, saradnju između javnog i privatnog sektora, kao i međunarodnu podršku kako bi se unaprijedila otpornost države na ovakve prijetnje.

Operativno postupanje u rješavanju sajber krize biti će objašnjeno u narednom poglavlju.

Pomoć u rješavanju incidenta i sajber krize

U rješavanju incidenta srednjeg, odnosno visokog nivoa i sajber krize Agencija i CIRT državne uprave mogu koristiti ekspertsku pomoć domaćih i međunarodnih institucija i organizacija, kao i razmjenjivati informacije sa tim instutucijama i organizacijama.

Saradnje s privatnim sektorom (JPP model)

Svrha i strateško opredjeljenje – Djelotvorno rješavanje sajber incidenata i kriza na nacionalnom nivou zahtijeva integraciju svih raspoloživih resursa. S obzirom na to da privatni sektor upravlja dijelom kritične informacione infrastrukture i posjeduje velik fond specijalizovanih eksperata i alata, ključno je formalizovati saradnju kroz model javno-privatnog partnerstva (JPP). Ova saradnja se uspostavlja s ciljem da se državnim kapacitetima, tako i kapacitetima različitih organa i subjekata osigura brz pristup naprednoj tehničkoj ekspertizi, alatima za forenziku, kao i aktuelnim obavještajnim podacima o prijetnjama (threat intelligence), čime se umanjuje teret odgovora na krizu i smanjuje vrijeme oporavka.

Modeli angažovanja i ugovorne obaveze – Saradnja s privatnim sektorom mora biti regulisana unaprijed definisanim ugovorima i protokolima, a ne zavisiti o *ad-hoc* pozivima. Najvažniji model je sklapanje Ugovora o brzom angažovanju (Retainer Agreement) sa specijalizovanim kompanijama za incident

response i sajber forenziku. Ovim ugovorima se osigurava da privatni eksperti budu na raspolaganju Agenciji za sajber bezbjednost i CIRT-u državne uprave unutar strogo definisanog roka. Ti ugovori moraju jasno definisati opseg podrške, uključujući sprovođenje forenzičke analize, zaustavljanje širenja napada i radnje za oporavak sistema.

Etički i pravni okvir kriznog angažmana – Svi oblici saradnje s privatnim sektorom moraju biti zasnovani na principu da operativno vođstvo i donošenje konačnih odluka u rješavanju krize ostaje isključivo u domenu CIRT-a državne uprave i Agencije za sajber bezbjednost. Privatni partneri djeluju isključivo kao podrška i savjetodavna snaga. Ugovori o JPP-u moraju eksplicitno regulisati pitanja povjerljivosti i sigurnosti podataka, posebno onih državnih, kojima privatni eksperti pristupaju tokom sanacije. Neophodno je uvođenje i obaveznih zajedničkih vježbi (u skladu sa poglavljem 5. Nacionalnog plana) s privatnim partnerima, kako bi se protokoli angažovanja i timska saradnja testirali i potvrdili prije nego što nastupi stvarna sajber kriza. Implementacijom ovih mjera, Plan osigurava da se stručnost privatnog sektora koristi kao ključni element nacionalne odbrambene arhitekture u fazi odgovora i oporavka od sajber krize.

7. Sistem upravljanja sajber bezbjednošću i uloga institucija

Uloga institucija u nacionalnom sistemu sajber bezbjednosti zasniva se na zakonski definisanim nadležnostima i međusobnoj saradnji. Tabela koja slijedi daje pregled ključnih aktera i njihovih strateških odgovornosti u procesu upravljanja sajber prijetnjama i incidentima.

Tabela 3. Politički, strateški, operativni i tehnički nivoi sprovođenja plana

	Akteri	Odgovornosti
Politički nivo	• Vlada Crne Gore	• Politička odluka o proglašenju sajber krize
Strateški nivo	• Ministarstvo javne uprave • Agencija za sajber bezbjednost	• Strateška i operativna koordinacija upravljanja sajber i nesajber aspektima sajber krize i incidentima visokog nivoa uticaja
Operativni nivo	• Druga ministarstva i nadležni organi • Regulatorna tela	• Obezbeđuje pojačanu (ili: unapređenu) saradnju i koordinaciju • Povezuje strateški i tehnički nivo • Koordinacija kriznog sajber menadžmenta, procene situacije i akcionih mera za ublažavanje posledica
Tehnički nivo	• CIRT državne uprave • Nacionalni CIRT • Sektorski CIRT-ovi	• Praćenje i nadzor incidenata, uključujući kontinuiranu analizu pretnji i rizika • Upravljanje incidentima i njihovo rešavanje

Nacionalni sistem upravljanja sajber bezbjednošću zasniva se na podjeli odgovornosti i koordinaciji između ključnih institucija na nacionalnom nivou. Uloge se definišu na strateškom nivou, dok su operativne procedure dio interne verzije Plana.

Ministarstvo javne uprave (MJU)

Ministarstvo javne uprave ima centralnu stratešku ulogu u oblasti sajber bezbjednosti. Ono kreira politike, donosi regulatorne okvire, koordinira rad institucija na nacionalnom nivou i odgovorno je za izradu i ažuriranje Nacionalnog plana za odgovor na sajber prijetnje i incidente, u skladu sa članom 38 Zakona o informacionoj bezbjednosti. Ministarstvo obezbjeđuje konzistentan razvoj digitalne bezbjednosti u zemlji, prati međunarodne trendove i sarađuje sa relevantnim organizacijama na regionalnom i globalnom nivou.

Agencija za sajber bezbjednost

Agencija djeluje kao stručno i regulatorno tijelo koje nadgleda i razvija mehanizme zaštite mrežnih i informacionih sistema subjekata van državne uprave. Njena uloga obuhvata tehničku analizu ranjivosti, proaktivno skeniranje sistema uz saglasnost subjekata, izradu tehničkih pravila, kao i promociju standarda kao što je MEST ISO/IEC 27001. Agencija takođe ima ključnu ulogu u edukaciji, podizanju svijesti i obuci relevantnog kadra.

Organi državne uprave

Svaki organ je odgovoran za bezbjednost svojih informacionih sistema, kao i za blagovremeno otkrivanje, prijavljivanje i upravljanje incidentima koji utiču na njihov rad. Institucije sprovode propisane mjere zaštite i sarađuju sa Agencijom i CIRT državne uprave u cilju jačanja ukupne otpornosti.

Subjekti od posebnog značaja i kritična infrastruktura

Subjekti koji upravljaju kritičnim digitalnim infrastrukturama ili pružaju usluge od posebnog značaja imaju povećanu obavezu u oblasti sajber bezbjednosti. Oni su dužni da primjenjuju napredne mjere zaštite, vrše procjene rizika, preduzimaju aktivnosti radi ublažavanja ranjivosti i obezbjeđuju kontinuitet pružanja usluga. Njihova uloga je posebno važna jer incidenti u ovim sektorima mogu imati značajne posljedice po funkcionisanje društva, ekonomiju i javnu bezbjednost.

Privatni sektor i provajderi digitalnih usluga

Privatni sektor ima važnu ulogu u jačanju nacionalne sajber otpornosti, posebno u oblastima gdje se pružaju digitalne usluge od javnog interesa. Saradnja sa državnim organima, razmjena informacija i implementacija dobrih praksi ključni su elementi njihovog doprinosa.

Akademska zajednica i stručna javnost

Institucije nauke i obrazovanja doprinose razvoju znanja, istraživanju i edukaciji u oblasti sajber bezbjednosti. Njihova uloga je važna u podizanju svijesti, obuci kadrova i dugoročnoj modernizaciji sektora.

Efikasan sistem upravljanja sajber bezbjednošću zasniva se na saradnji između svih aktera. Ministarstvo javne uprave i Agencija za sajber bezbjednost čine jezgro koordinacionog mehanizma, dok ostale institucije i subjekti sarađuju u skladu sa svojim nadležnostima. Razmjena informacija, koordinisano planiranje i pravovremena komunikacija ključni su za uspješno upravljanje prijetnjama i incidentima.

8. Nacionalni okvir vježbi

Vježbe iz oblasti sajber bezbjednosti predstavljaju ključni instrument za provjeru spremnosti institucija, unapređenje njihovih kapaciteta i jačanje ukupne otpornosti digitalnog ekosistema Crne Gore. One omogućavaju da se u kontrolisanim uslovima provjere procedure, komunikacioni tokovi i mehanizmi saradnje, kao i da se identifikuju potencijalne slabosti koje je potrebno otkloniti prije nego što dođe do stvarnih incidenata.

Sajber vježbe imaju višestruke ciljeve: one doprinose boljem razumijevanju prijetnji, poboljšavaju koordinaciju između institucija, podižu nivo znanja zaposlenih i omogućavaju procjenu primijenjenih mjera bezbjednosti u praksi. Kroz sistematsko izvođenje vježbi, institucije jačaju svoje sposobnosti da pravovremeno prepoznaju i efikasno odgovore na incidente, posebno one koji mogu imati šire posljedice po funkcionisanje informacionih sistema i javnih usluga.

Na nacionalnom nivou, vježbe se sprovode u okviru institucionalnog okvira koji uključuje organe državne uprave, subjekte od posebnog značaja, nadležne tehničke timove i druge aktere u digitalnom prostoru. Učešće svih relevantnih institucija omogućava provjeru međusektorske saradnje, što je od posebne važnosti u situacijama kada incidenti prevazilaze kapacitete pojedinačnih organizacija i zahtijevaju koordinisan odgovor.

Crna Gora aktivno učestvuje i u regionalnim i međunarodnim sajber vježbama, uključujući aktivnosti koje organizuju ENISA, NATO, FIRST i partnerske države. Učešće u takvim vježbama omogućava sticanje praktičnog iskustva, praćenje međunarodnih trendova, usvajanje najboljih praksi i unapređenje sposobnosti za odgovor na sajber prijetnje koje mogu imati prekogranični karakter.

Rezultati vježbi predstavljaju važan izvor informacija za unapređenje politika, procedura i institucionalnih kapaciteta. Na osnovu naučenih lekcija razvijaju se preporuke i predlozi koji doprinose kontinuiranom jačanju nacionalne sajber otpornosti. Time vježbe postaju integralni dio ciklusa planiranja, unapređenja i provjere sistema sajber bezbjednosti Crne Gore.

Operativni planovi vježbi, scenariji, metodologije i tehničke procedure sastavni su dio interne verzije Nacionalnog plana i nijesu dostupni u ovom javnom dokumentu.

9. Međunarodna saradnja

Međunarodna saradnja predstavlja jedan od ključnih elemenata nacionalnog sistema sajber bezbjednosti. Zbog prirode digitalnog prostora, u kojem prijetnje lako prevazilaze državne granice, nijedna zemlja ne može samostalno obezbijediti dovoljan nivo otpornosti. Zato je Crna Gora posvećena razvoju partnerstava, razmjeni informacija i aktivnom učešću u regionalnim i međunarodnim inicijativama iz oblasti sajber bezbjednosti.

Crna Gora ostvaruje kontinuiranu saradnju sa institucijama i organizacijama Evropske unije, kao i sa državama članicama EU kroz različite mehanizme razmjene informacija, zajedničke analize prijetnji, pripremu preporuka i učešće u međunarodnim projektima. Učešće u evropskim programima omogućava Crnoj Gori pristup savremenim znanjima, standardima i iskustvima, što je od posebnog značaja u kontekstu evropskih integracija i usklađivanja sa najboljim praksama.

Važan segment međunarodne saradnje Crne Gore predstavlja partnerstvo sa NATO-om u oblasti sajber odbrane. Kroz programe i aktivnosti koje Alijansa sprovodi u dijelu izgradnje kapaciteta, razmjene informacija, zajedničkih obuka i tehničke podrške, institucije Crne Gore dodatno jačaju svoje sposobnosti za preventivno djelovanje i odgovor na kompleksne digitalne prijetnje. Saradnja sa NATO-om omogućava pristup ekspertizi država saveznica i predstavlja važan oslonac u unapređenju nacionalne sajber otpornosti.

Crna Gora sarađuje i sa međunarodnim organizacijama kao što su ENISA i FIRST, kroz učešće u mrežama stručnjaka, treninzima, razmjenu tehničkih saznanja i programe procjene spremnosti. Ovakvi oblici saradnje doprinose usvajanju međunarodnih standarda i praksi, kao i jačanju sposobnosti institucija da odgovore na savremene prijetnje. Dodatno, Crna Gora razvija saradnju sa DCAF-om (Ženevskim centrom za upravljanje sektorom bezbjednosti), posebno u oblasti jačanja institucionalnih kapaciteta, obuka, razvoja politika i unapređenja dobrog upravljanja u sektoru bezbjednosti. DCAF pruža stručnu podršku i savjetodavne programe koji doprinose profesionalizaciji i jačanju otpornosti crnogorskih institucija u oblasti sajber bezbjednosti.

Pored institucionalnih mehanizama, Crna Gora jača bilateralnu saradnju sa partnerskim državama i organizacijama koje posjeduju napredne kapacitete u oblasti sajber bezbjednosti. Takva saradnja obuhvata razmjenu podataka o prijetnjama, stručne konsultacije, zajedničke obuke i mogućnosti za učešće u međunarodnim vježbama. Bilateralni odnosi posebno su značajni u situacijama kada je potrebno brzo i

efikasno reagovati na prijetnje koje imaju transnacionalni karakter ili zahtijevaju specijalizovanu ekspertizu.

Međunarodna saradnja predstavlja trajni proces i važan element održavanja stabilnosti digitalnog prostora Crne Gore. Kroz aktivno učešće u međunarodnim okvirima, razmjenu informacija i jačanje kapaciteta institucija, Crna Gora doprinosi zajedničkoj bezbjednosnoj arhitekturi i unapređuje sopstvenu otpornost na savremene sajber prijetnje.

10. Sajber krizna komunikacija

Sajber krizna komunikacija predstavlja ključni element u odgovoru na bezbjednosne incidente u digitalnom prostoru. U kontekstu sve učestalijih i sofisticiranijih sajber prijetnji, blagovremena, tačna i koordinisana komunikacija između nadležnih institucija, sektora i javnosti predstavlja osnovu za efikasno upravljanje rizicima, prijetnjama, incidentima i krizama, te minimizaciju štete i očuvanje povjerenja javnosti. **Krizna komunikacija je interna i eksterna**.

Svrha i ciljevi komunikacije

Sajber krizna komunikacija nije samo informisanje javnosti, već je to strateška funkcija koja ima za cilj:

- **Minimizaciju štete**: Pravovremenim informisanjem o incidentu sprječava se njegovo dalje širenje i umanjuje panika.
- **Očuvanje povjerenja**: Održavanje povjerenja javnosti i partnera u digitalne sisteme i sposobnost institucija da upravljaju krizom.
- **Podršku odlučivanju**: Osiguravanje da sve relevantne strane (operativni timovi, Vlada, međunarodni partneri) dobiju tačne informacije za donošenje odluka.

Akteri i koordinaciona uloga

Sistem krizne komunikacije obuhvata niz mjera, procedura i protokola za razmjenu informacija između različitih aktera. Uloga navedenih aktera prikazana je u tabeli ispod.

Tabela 4. Akteri i koordinaciona uloga

Kategorija aktera	Primjeri i uloga u komunikaciji
Ključni koordinatori	Ključna koordinaciona uloga pripada **Ministarstvu javne uprave** i **Agenciji za sajber bezbjednost**. Oni su zaduženi za uspostavljanje i nadzor komunikacionih protokola.
Interni operativni akteri	**CIRT državne uprave** i **sektorski CIRT-ovi** zaduženi su za tehničku razmjenu informacija o prijetnjama i statusu incidenta.
Nadležne institucije	**Nadležna ministarstva** i **ključni i važni subjekti** aktivno razmjenjuju informacije unutar sistema.
Organi bezbjednosti	**Organi bezbjednosti** imaju svoju ulogu, posebno u aspektima borbe protiv dezinformacija.
Međunarodni partneri	Komunikacija uključuje i **međunarodne partnere**, što je ključno za globalno koordinisani odgovor na prekogranične prijetnje.

Borba protiv dezinformacija i lažnih narativa

U toku različitih prijetnji, incidenata i kriza, posebna pažnja posvećuje se borbi protiv lažnih narativa i manipulacije informacijama.

Za ovaj kritični aspekt krizne komunikacije, posebno su zaduženi:

- Agencija za nacionalnu bezbjednost (ANB).
- Ministarstvo unutrašnjih poslova (MUP).
- Ministarstvo odbrane.

Ovi organi djeluju u koordinaciji sa Vladom Crne Gore i Vijećem za nacionalnu bezbjednost Crne Gore.

Post-incidentna analiza i unapređenje

Nakon završetka incidenta / krize, obavezno se izrađuje komunikaciona analiza.

Svrha ove analize je osigurati stalno unapređenje kapaciteta za kriznu komunikaciju i povećati otpornost sistema.

Komunikaciona analiza mora da sadrži:

- Pregled sprovedenih komunikacionih aktivnosti.
- Procjenu efikasnosti korišćenih kanala.
- Preporuke za poboljšanje budućih komunikacionih protokola.

Vlada Crne Gore određuje nositelja izrade analize.

10.1. Interna sajber krizna komunikacija

Interna sajber krizna komunikacija provodi se između svih aktera uključenih u rješavanje prijetnji, incidenata i kriza u skladu sa koracima određenim u poglavlju 4. Operativna koordinacija rješavanja sajber prijetnje, ozbiljne sajber prijetnje, incidente i sajber krize.

10.2. Eksterna sajber krizna komunikacija

Eksterna sajber krizna komunikacija provodi se prema različitim vrstama javnosti (mediji, stručna javnost, građani) ovisno o procjeni nivoa sajber incidenta (tabela 2.) i koracima u operativnoj koordinaciji rješavanja sajber prijetnje, ozbiljne sajber prijetnje, incidente i sajber krize (poglavlje 6.) u skladu sa sljedećim komunikacijskim protokolima:

Komunikacijski protokol I		
Nivo incidenta	**Kriterijumi uticaja**	**Koordinator komunikacije**
□ NISKI	- Ograničen broj korisnika - Kratko trajanje (<2h) - Lokalan domet	Agencija za sajber bezbjednosti odnosno Ministarstvo javne uprave daju kratko saopštenje za javnost na službenom webu.

Komunikacijski protokol II		
Nivo incidenta	**Kriterijumi uticaja**	**Koordinator komunikacije**
SREDNJI	- Veći broj korisnika - Trajanje 2–10h - Regionalni domet	Ministarstvo javne uprave daje kratko saopštenje putem javnih servisa po određivanju nivoa incidenta te detaljno saopštenje po njegovom završetku.

Komunikacijski protokol III		
Nivo incidenta	**Kriterijumi uticaja**	**Koordinator komunikacije**
● VISOKI	- Širok broj korisnika - Trajanje >10h - Nacionalni / prekogranični domet	Ministarstvo javne uprave daje kratko saopštenje putem javnih servisa po određivanju nivoa incidenta. Ministarstvo javne uprave najmanje jednom dnevno daje detaljno saopštenje, sve do završetka incidenta. Ministarstvo javne uprave daje detaljno saopštenje po završetku incidenta. Sva saopštenja se daju putem javnih servisa.

Komunikacijski protokol IV		
Nivo incidenta	**Kriterijumi uticaja**	**Koordinator komunikacije**
SAJBER KRIZA	- Nacionalni / prekogranični domet	Vlada Crne Gore formira Krizni komunikacioni tim. Krizni komunikacioni tim komunicira sa različitim vrstama javnosti (mediji, stručna javnost, građani) ovisno o procjeni, no ne manje od dvaputa dnevno. Sva saopštenja se daju putem javnih servisa.

11. Završna razmatranja

Nacionalni plan za odgovor na sajber prijetnje i incidente predstavlja ključni strateški dokument kojim Crna Gora jača svoj institucionalni, tehnološki i društveni okvir za zaštitu digitalnog prostora. U okruženju obilježenom intenzivnim tehnološkim promjenama i sve sofisticiranijim prijetnjama, Plan postavlja osnov za izgradnju stabilnog, otpornog i koordinisanog sistema koji je sposoban da prepozna, spriječi i ublaži posljedice sajber incidenata.

Ovaj dokument utvrđuje zajedničku viziju i smjer djelovanja organa državne uprave, subjekata od posebnog značaja, tehničkih timova i drugih aktera čiji rad utiče na funkcionalnost i bezbjednost informacionih sistema. Jasno definisani principi, uloge i mehanizmi saradnje omogućavaju da digitalna infrastruktura bude zaštićena, da javne usluge ostanu dostupne, a povjerenje građana i privrede u elektronske servise bude očuvano i unaprijeđeno.

Kao strateški dokument, Nacionalni plan doprinosi modernizaciji ukupnog bezbjednosnog sistema države, jačanju kapaciteta institucija i unapređivanju međuinstitucionalne saradnje. On služi i kao okvir za izgradnju partnerstava na regionalnom i međunarodnom nivou, čime Crna Gora postaje aktivan učesnik u zajedničkim naporima za očuvanje bezbjednosti i stabilnosti digitalnog prostora.

Posebno je značajno to što Plan podstiče razvoj kulture sajber bezbjednosti u cijelom društvu. Digitalna bezbjednost nije odgovornost samo institucija — ona zahtijeva angažovanje pojedinaca, privrede, akademske zajednice i civilnog sektora. Jačanjem svijesti, unapređenjem znanja i promocijom odgovornog ponašanja u digitalnom prostoru, Crna Gora stvara uslove za dugoročnu otpornost na sajber rizike.

Nacionalni plan ne predstavlja samo odgovor na savremene izazove, već i platformu za napredak. On se oslanja na postojeće kapacitete, ali i otvara prostor za dalji razvoj, inovacije i profesionalizaciju sistema sajber bezbjednosti. Time ovaj dokument daje strateški doprinos modernizaciji javne uprave, povećanju efikasnosti institucija i unapređenju sigurnosti građana i privrede u digitalnom okruženju.

12. Praćenje primjene i ažuriranje Nacionalnog plana

Sprovođenje Nacionalnog plana zasniva se na kontinuiranom praćenju stanja u oblasti sajber bezbjednosti, unapređenju institucionalnih kapaciteta i evaluaciji učinka mjera koje sprovode nadležni organi. Ministarstvo javne uprave, u saradnji sa Agencijom za sajber bezbjednost i drugim relevantnim institucijama, obezbjeđuje strateški nadzor nad sprovođenjem Plana i prati njegovu primjenu na nacionalnom nivou. Ovo uključuje praćenje trendova u oblasti sajber prijetnji, sprovođenje aktivnosti definisanih u Planu i identifikovanje potreba za dodatnim mjerama unapređenja.

U skladu sa članom 38 Zakona o informacionoj bezbjednosti, Ministarstvo javne uprave nadležno je za izradu, održavanje i ažuriranje Nacionalnog plana. Revizija Plana vrši se najmanje jednom u dvije godine ili ranije ukoliko to zahtijevaju nove prijetnje, tehnološke promjene, međunarodne obaveze ili nalazi analiza i izvještaja relevantnih institucija. Proces ažuriranja zasniva se na preporukama svih organa koji učestvuju u identifikovanju rizika, sprovođenju vježbi i rukovanju incidentima. Na osnovu njihovih nalaza i preporuka, Ministarstvo javne uprave priprema izmjene i dopune Plana, čime se obezbjeđuje njegova trajna aktuelnost, relevantnost i usklađenost sa standardima i najboljim praksama.

Nacionalni plan je živi dokument koji se razvija u skladu sa razvojem digitalnih tehnologija, međunarodnim trendovima i iskustvima stečenim kroz upravljanje incidentima, sprovođenje vježbi i međunarodnu saradnju. Institucije Crne Gore nastaviće da unapređuju svoje kapacitete, podižu nivo obuke, jačaju mehanizme saradnje i primjenjuju najbolje prakse u oblasti sajber bezbjednosti.

Ovaj dokument, u kombinaciji sa internom verzijom Plana, obezbjeđuje sveobuhvatan institucionalni okvir za zaštitu digitalnih sistema, odgovor na prijetnje i kontinuirani razvoj nacionalne sajber otpornosti.

Aneks

Aneks 1. Uspostava okvira upravljanja sajber bezbjednošću

Funkcije	Kategorije
Upravljanje	Organizacioni kontekst
	Pristup upravljanja rizikom
	Uloge, odgovornosti i ovlašćenja
	Politika
	Nadzor
	Upravljanje rizikom lanca snabdijevanja sajber bezbjednošću
Identifikacija	Upravljanje imovinom
	Procjena rizika
	Poboljšanje
Zaštita	Upravljanje identitetom, autentifikacija i kontrola pristupa
	Svjesnost i obuka
	Bezbjednost podataka
	Bezbjednost platformi i aplikacija
	Otpornost tehnološke infrastrukture
Otkrivanje	Kontinuirani nadzor
	Analiza štetnih događaja
Odgovor	Upravljanje incidentima
	Analiza incidenta
	Izvještavanje i komunikacija o odgovoru na incidente
	Ublažavanje incidenta
Oporavak	Izvršenje plana oporavka od incidenta
	Komunikacija o oporavku od incidenta

M I N I S T A R

mr Marash Dukaj