Crna Gora
VLADA CRNE GORE
SEKRETARIJAT ZA RAZVOJ

- Predlog -

PROGRAM
INFORMACIONE BEZBJEDNOSTI U CRNOJ GORI

Podgorica, Maj 2008. godine

Sadržaj

UVODNE NAPOMENE

Uspostavljanje i razvoj sistema informacione bezbjednosti u svim segmentima jedne države predstavlja važnu pretpostavku za stvaranje informacionog društva. Stvaranje informacionog društva, posmatrano u širem smislu, predstavlja ne samo uslov za uključivanje određene države u međunarodne integracione procese, već i način za opstanak te države u društvu razvijenih. Osnovni subjekti informacionog društva su državna uprava, privredni subjekti i stanovništvo, dok osnovu njegovog razvoja predstavlja povjerenje tih subjekata u elektronske usluge i elektronsko poslovanje.

Kroz uspostavljanje sistema informacione bezbjednosti i upravljanje tim sistemom, državna uprava izvršava svoju ulogu u izgradnji informacionog društva. Razvojem sistema informacione bezbjednosti državna uprava uspostavlja preventivne mjere i stvara organizaciono-tehničke preduslove za sistemski razvoj zaštitnih i represivnih mjera u okviru informacionog društva. Ti procesi ne mogu se uspješno sprovoditi bez uspostavljanja konzistentnog sistema informacione bezbjednosti na nacionalnom nivou.

Na osnovu istraživanja vršenih u razvijenim državama Evropske unije (EU) i svijeta, došlo se do saznanja da za stvaranje informacionog društva nije dovoljno samo investirati u tehniku i tehnološka dostignuća, zbog čega sve razvijene države posljednjih godina intenzivno rade na programima informacione bezbjednosti u svim segmentima državnog i privrednog sektora, kao i programima razvoja bezbjednosne kulture kod najširih slojeva stanovništva.

Kroz Program informacione bezbjednosti u Crnoj Gori (Nacionalni program) obrađuju se organizacioni i upravljački aspekti uvođenja sistema informacione bezbjednosti u Crnoj Gori, polazeći od pretpostavki neophodnih za sistemski razvoj zakonskih i podzakonskih propisa, metoda, postupaka i tehničkih sistema u oblasti informacione bezbjednosti.

Donošenjem ovog nacionalnog programa započinje se sa sistemskim procesom uvođenja informacione bezbjednosti u Crnoj Gori. Taj proces podrazumijeva donošenje i nacionalne politike informacione bezbjednosti, kao i niza sprovedbenih propisa po užim bezbjednosnim oblastima (bezbjednosna provjera lica, fizička bezbjednost, bezbjednost podataka, bezbjednost informacionih sistema, bezbjednost pristupa trećih strana i vanjske saradnje). Na taj način propisuju se koordinirani postupci, odnosno sistem obaveza i odgovornosti pojedinih organa državne uprave u tom procesu. Na osnovu osnovnih dokumenata (Zakon o informacionoj bezbjednosti i nacionalna politika ili strategija informacione bezbjednosti) Vlada i nadležni organi državne uprave treba da donesu odgovarajuće uredbe, pravilnike i smjernice. Navedenim propisima treba da se obezbijede minimalni bezbjednosni kriterijumi na nivou centralne državne vlasti, što je jedan od osnovnih zahtjeva Sjevernoatlantskog saveza (NATO) u okviru Akcionog plana za članstvo (MAP).

Promjene u zakonodavstvu EU u poslednjih nekoliko godina, u značajnoj mjeri usmjerene su na razvoj bezbjednosne politike EU i zasnivaju se na iskustvu bezbjednosnog modela NATO-a, koje je stečeno u dugogodišnjem multinacionalnom okruženju. S obzirom na opredjeljenja Crne Gore da se integriše u NATO i EU, ovaj nacionalni program treba da je saglasan sa bezbjednosnim modelima koje primjenjuju te asocijacije. Proces harmonizacije zakonodavstva Crne Gore sa zakonodavstvom EU, u najskorije vrijeme će dovesti do usklađenosti svih nacionalnih propisa sa zahtjevima EU, pa i sa zahtjevima u oblasti informacione bezbjednosti.

Strateški cilj ovog nacionalnog programa je postupno širenje procesa informacione bezbjednosti na državu u cjelini, uvođenjem odgovarajućih minimalnih bezbjednosnih kriterijuma u organe javne uprave, kao i razvojem bezbjednosne kulture najširih slojeva stanovništva. Taj proces je izuzetno važan jer ljudsko društvo danas prolazi kroz transformaciju iz industrijskog u informaciono društvo. Izgradnja informacionog društva danas nije pitanje izbora, niti samo jedan od uslova međunarodnih integracija, već predstavlja uslov za opstanak u društvu razvijenih.

Prvi korak u stvaranju informacionog društva je stvaranje zajedničke arhitekture informacionih sistema državne uprave kroz projekte e-Governmenta. Elektronska državna uprava podrazumijeva interaktivne elektronske usluge organa državne uprave i javnih usluga iz oblasti zdravstva, obrazovanja i dr. Elektronska državna uprava predstavlja okosnicu razvoja informacionog društva, posebno u smislu stvaranja povjerenja stanovništva i privrednog sektora u takav način poslovanja, ali i povjerenja u državnu upravu koja sprovodi takvu modernizaciju. Iz tih razloga savremena državna uprava mora sistemski uvoditi mjere informacione bezbjednosti.

Ovaj program informacione bezbjednosti predviđa određene inicijative organa državne uprave i prema privatnom sektoru, odnosno privredi u cjelini. Te inicijative treba da se sprovode kroz različite oblike javno-privatnog partnerstva, koji su danas uobičajeni u oblasti informacione bezbjednosti u svijetu. Interes države je da postojeće bezbjednosne investicije u privredi, koje su i kod nas na relativno visokom nivou, sistemski usmjeri na dobrobit svih subjekata u državi.

Radi stvaranja konkurentnosti privrede i privlačenja stranih investitora da ulažu u domaće kompanije, uspostavljanje sistema informacione bezbjednosti na nacionalnom nivou ima neprocjenjiv značaj, tim prije što je taj proces u razvijenim zemljama i zemljama EU uveliko napredovao.

I - INFORMACIONA BEZBJEDNOST

1. Pojam informacione bezbjednosti

Pojam informacione bezbjednosti u ovom programu obrađuje se na način koji je danas prihvaćen u razvijenim zemljama svijeta i koji obezbjeđuje kompatibilnost sa konceptom informacione bezbjednosti NATO-a i EU. Pri tome treba imati u vidu da informaciona bezbjednost nije isto što i informatička bezbjednost. Naime, informaciona bezbjednost se odnosi na zaštitu informacija bez obzira na medij na kome se čuva i prenosi. Sistemom informacione bezbjednosti obuhvataju se fizička lica, procesi, organizacija i tehnologija. Taj sistem se sastoji od uravnoteženog skupa bezbjednosnih mjera, a naročito: bezbjednosne provjere lica, fizičke bezbjednosti, bezbjednosti podataka, bezbjednosti informacionih sistema, koordiniranog uvođenja formalnih procedura, kao što su procjene rizika, certifikovanje lica i uređaja i akreditacije tehničkih sistema za primjenu u određenim segmentima poslovnih procesa državne uprave. Uravnoteženost i koordinacija mjera i postupaka treba da se postiže organizacijom i upravljanjem sistemom informacione bezbjednosti.

1.1. Osnovni pojmovi

Radi pravilnog razumijevanja bezbjednosnih mjera neophodno je prethodno objasniti značenje osnovnih pojmova koji se koriste u ovom programu:

Podatak je skup razumljivih znakova koji su zapisani na određenom mediju;

Informacija je podatak sa određenim značenjem, odnosno saznanje koje se može prenijeti u bilo kojem obliku (pisanom, audio, vizuelnom, elektronskom ili nekom drugom);

Informacioni sistem je svaki sistem u okviru kojeg se prikupljaju, skladište, čuvaju, obrađuju, prikazuju i isporučuju informacije, tako da budu dostupne i upotrebljive za svako lice koje ima pravo na njihovo korišćenje;

Informatička oprema su svi fizički uređaji i sredstva koji čine informacioni sistem;

Informaciona bezbjednost podrazumijeva očuvanje:
1) povjerljivosti – da je informacija dostupna samo licima koja su ovlašćena za pristup toj informaciji;
2) integriteta – zaštita postojanja, tačnosti i kompletnosti informacije kao i procesnih metoda;
3) raspoloživosti – da autorizovani korisnici imaju mogućnost pristupa informaciji i pripadajućim sredstvima kada se usluga zahtijeva;

Zaštita je skup mjera za očuvanje bezbjednosti;

Nadzor je provjera efikasnosti sistema zaštite;

Odgovornost je ponašanje po propisanom skupu pravila;

Ovlašćenje je pravo postupanja u propisanim okvirima;

Vlasnici podataka su odgovorni za sve radnje sa podacima u njihovoj nadležnosti, tokom životnog ciklusa podataka, pri čemu radnje sa podacima podrazumijevaju nastajanje, obradu, skladištenje i arhiviranje podataka;

Informaciona infrastruktura je sva infrastruktura u određenom državnom organu ili pravnom licu, koja na bilo koji način utiče na bitna svojstva povjerljivosti, dostupnosti ili cjelovitosti podataka i u okviru koje podaci nastaju, obrađuju se ili skladište;

Vlasnici informacione infrastrukture odgovorni su za planiranje i implementaciju organizacionih i tehničkih mjera, u skladu sa važećim propisima informacione bezbjednosti;

Pravo pristupa i korišćenja informacionih resursa određuje se isključivo po načelu poslovne potrebe ("need to know"), a ne po hijerarhijskom konceptu ranga radnog mjesta;

Bezbjednosna akreditacija. Pod akreditacijom se podrazumijeva postupak u kojem nadležno nezavisno akreditaciono tijelo službeno potvrđuje pravnom ili fizičkom licu da je sposobno vršiti određene poslove. Bezbjednosna akreditacija podrazumijeva provjeru sposobnosti pravnih lica za sprovođenje procesa informacione bezbjednosti, u skladu sa relevantnim propisima o informacionoj bezbjednosti. Proces informacione bezbjednosti sastoji se od niza propisanih mjera i metoda implementiranih u vidu organizacionih i tehničkih kontrola nad poslovnim procesima određenog pravnog lica ili državnog organa;

Bezbjednosno akreditaciono tijelo. Pod akreditacionim tijelom podrazumijeva se nezavisno pravno lice ovlašćeno zakonom ili akreditovano od strane određenog centralnog akreditacionog organa, koji vrši provjeru sposobnosti pravnih lica za sprovođenje procesa informacione bezbjednosti u okviru svog poslovnog procesa;

Potvrda o bezbjednosnoj akreditaciji. Akreditaciono tijelo izdaje potvrdu o akreditaciji pravnom ili fizičkom licu za koje se utvrdi da ispunjava zahtjeve akreditacionog procesa. Potvrda o bezbjednosnoj akreditaciji označava zadovoljavanje propisanih zahtjeva procesa informacione bezbjednosti od strane određenog pravnog lica ili državnog organa. Potvrda o akreditaciji izdaje se uvijek na ograničeni vremenski period. Uobičajeni rokovi za bezbjednosne akreditacije su dvije, četiri i pet godina. Istekom akreditacionog roka sprovodi se ponovna provjera, koja pored propisanih zahtjeva procesa informacione bezbjednosti ima za cilj da utvrdi i kvalitet upravljanja životnim ciklusom podataka, informacione infrastrukture, fizičke bezbjednosti i zaposlenih lica. Potvrdom o bezbjednosnoj akreditaciji daje se ovlašćenje za vršenje određenih poslova;

Bezbjednosni certifikat. Pod certifikatom se podrazumijeva potvrda o usklađenosti određenog proizvoda, procesa ili usluge sa nacionalnim standardom ili formalnim tehničkim zahtjevima za proizvode, procese ili usluge. Bezbjednosni certifikat odnosi se na lica, proizvode ili sisteme informacione bezbjednosti. Bezbjednosnim certifikovanjem omogućava se korišćenje pojedinih tržišnih proizvoda u propisanim uslovima sa ciljem sistemske realizacije projekata informacione infrastrukture. Na primjer, proizvod kompanije X, model Y, tip Z u verziji W, može se koristiti za razmjenu podataka u državnoj upravi do stepena tajnosti "povjerljivo";

Bezbjednosno certifikaciono tijelo. Certifikaciono tijelo ili uopšte tijelo za ocjenu usklađenosti je laboratorija nezavisna od dobavljača, nadzorni ili drugi organ koji učestvuje u postupku ocjenjivanja usklađenosti. Bezbjednosno certifikovanje za potrebe organa javne uprave najčešće se organizuje u centralnim državnim organima za bezbjednost komunikacija (NCSA – National Communications SecurityAuthority). Osnovna nadležnost bezbjednosnog certifikacionog tijela je formiranje i redovno ažuriranje liste certifikovanih proizvoda za upotrebu u nacionalnom sistemu informacione bezbjednosti. Postupci sprovođenja certifikovanja sastoje se od laboratorijskih provjera ili preuzimanja određenih međunarodnih lista certifikata po utvrđenoj metodologiji. Liste certifikovanih proizvoda koriste se u procesu bezbjednosnog akreditovanja;

Organi javne uprave su državni organi, organi državne uprave, organi lokalne samouprave, i organi i organizacije koje vrše javna ovlašćenja.

1.2. Bezbjednosna provjera lica

Bezbjednosna provjera lica, pored primarnih mjera kojima se procjenjuje mogućnost dodjele ovlašćenja, podrazumijeva i aktivnu brigu oko usmjeravanja, edukacije i kontrole ispravnosti postupanja svakog pojedinca. Bezbjednosna provjera lica prvenstveno obuhvata procjenu da li se za neko lice u pogledu lojalnosti, povjerljivosti, pouzdanosti i vjerodostojnosti može dati ovlašćenje za pristup povjerljivim informacijama, a da to ne predstavlja neprihvatljiv rizik za bezbjednost informacije. Procjena treba da bude rezultat obavljene bezbjednosne provjere, odnosno provjere pouzdanosti za ona lica čije zapošljavanje ili napredovanje podrazumijeva pristup povjerljivim informacijama. Bezbjednosnu provjeru je potrebno sprovesti i za ugovorne strane, kao i za lica koja su samo privremeno u dodiru sa povjerljivim informacijama. Bezbjednosne provjere sprovode se u obimu koji je propisan za dostupni stepen povjerljivosti i uz znanje i pristanak lica koje se provjerava.

Bezbjednosna provjera lica podrazumijeva i blagovremenu bezbjednosnu informisanost, obrazovanje i obuku. Zaposleno lice mora da bude upoznato sa svojim bezbjednosnim obavezama i propisanim postupcima i redovno informisano o bezbjednosnoj politici.Takođe, mora biti upoznato i sa službenom procedurom izvještavanja za slučaj bezbjednosnih incidenata ili nepravilnosti, kao i sa sankcijama za bezbjednosne prekršaje.

Posredstvom programa bezbjednosnog obrazovanja potrebno je razvijati svijest o bezbjednosnim prijetnjama i brizi za informacijama, kao i izgrađivati sposobnost pružanja podrške bezbjednosnoj politici prilikom obavljanja svog redovnog posla.

1.3. Fizička bezbjednost

Fizička bezbjednost podrazumijeva primjenu fizičkih i tehničkih mjera zaštite na lokacijama, u zgradama i prostorijama koje zahtijevaju zaštitu od gubitaka ili kompromitacije povjerljivih informacija. Te mjere imaju za cilj da spriječe nedopušteni i nasilni pristup neovlašćenih lica, kao i odvraćanje, otkrivanje i reagovanje na djelovanje neovlašćenih lica. Mjere fizičke bezbjednosti obuhvataju i zaštitu informacija i infrastrukture od štetnog dejstva prirodnih nepogoda (požari, poplave, zemljotresi, oluje i sl.), kao i brigu oko obezbjeđivanja adekvatnih uslova (temperatura, vlaga, neprekidno napajanje, zračenje) i odabiranja pozicije prostorija.

Obim uspostavljenih fizičkih i tehničkih mjera zaštite treba da bude u skladu sa stepenom tajnosti podataka, vjerovatnoćom prijetnje i količinom informacija koje se moraju zaštititi.

1.4. Bezbjednost podataka

Bezbjednost podataka treba da se ostvaruje na osnovu zakona, primjenom propisanih bezbjednosnih i zaštitnih mjera i postupaka za dozvoljeni način prikupljanja, obradu, korišćenje, čuvanje, sprječavanje i oporavak od gubitka, ili neovlašćenog objavljivanja podataka.

Najvažniji korak u ostvarenju bezbjednosti podataka je klasifikacija ili razvrstavanje podataka s obzirom na stepen rizika i potrebne mjere zaštite bezbjednosti podataka. Klasifikacija podataka propisuje se zakonima i odgovarajućim sprovedbenim aktima, koji zajedno omogućavaju jednoznačno određivanje klase ili razreda podatka, odgovarajuće obavezne oznake i radne postupke, metode, sredstva i izvršioce, kao i sankcije za svako odstupanje od propisanog postupka unutar klase i unutar određenog pravnog okvira. Klasifikacija treba da bude najmanje onog stepena kojeg je najviši povjerljivi dio, ali treba izbjegavati kako pretjerano tako i preoskudno klasifikovanje u interesu efikasne bezbjednosti i djelotvornosti.

Klasifikacija sama po sebi ne predstavlja zaštitu, već smjernicu koja ukazuje na potrebu posebnih mjera rukovanja i zaštite. Klasifikovana informacija mora se zaštititi kroz čitav ciklus trajanja, do nivoa koji je u skladu sa njenom klasifikacijom. Sa klasifikovanom informacijom se mora postupati na način koji obezbjeđuje da je ta informacija primjereno označena, jasno određena kao klasifikovana i da ostaje klasifikovana samo u periodu za koji je to stvarno potrebno. Odgovornost za dodjelu klasifikacije i njeno periodično preispitivanje treba da ostane u nadležnosti vlasnika informacije. Po isteku potrebe za klasifikacijom potrebno je izvršiti deklasifikaciju.

Oznaka neklasifikovano ili nepostojanje klasifikacione oznake ne podrazumijeva tretiranje tog podatka kao javnog i ne predstavlja odobrenje za njegovo objavljivanje. Objavljivanje neklasifikovanih podataka mora se vršiti u skladu sa posebno propisanim formalnim procedurama.

U poslovnom procesu, posebno u segmentu kancelarijskog poslovanja, bezbjednost podataka podrazumijeva postojanje bezbjednosnih procedura za prijem, rukovanje, skladištenje, arhiviranje, uništavanje, distribuciju, umnožavanje, prepisivanje, prevođenje, izdavanje, uvid i objavljivanje podataka. Bezbjednosne procedure uključuju i postojanje sistema evidencije o kontroli pristupa i izvršenim radnjama, kao i kretanju i mjestu podataka.

1.5. Bezbjednost informacionih sistema – INFOSEC

Bezbjednost informacionih sistema (INFOSEC) podrazumijeva bezbjednost podataka na elektronskim medijima i računarima (COMPUSEC), bezbjednost podataka u sistemima za prenos podataka (COMSEC), kao i bezbjednost informacione infrastrukture u posebnim kategorijama prostora od različitih vrsta pasivnog ili aktivnog prisluškivanja (TECSEC).

Bezbjednost informacionih sistema obuhvata primjenu mjera za zaštitu podataka koji su u fazi obrade, skladištenja, ili prenosa, od gubitka tajnosti, cjelovitosti i raspoloživosti, kao i radi sprečavanja gubitka cjelovitosti ili raspoloživosti samih sistema. Bezbjednosne mjere uključuju mehanizme i procedure koje treba da budu implementirane u svrhu odvraćanja, prevencije, detektovanja i oporavka od uticaja incidenata koji djeluju na tajnost, cjelovitost i raspoloživost podataka i pratećih sistemskih servisa i resursa, uključujući i izvještavanje o bezbjednosnim incidentima.

Bezbjednost informacionih sistema je dinamičan proces tokom cijelog životnog ciklusa sistema, zbog čega se on mora posmatrati od faze njegovog planiranja, razvoja, sprovođenja, operativnosti i rasta do rashodovanja i uništavanja prema potrebi. To je, ustvari, proces upravljanja rizikom koji se koristi za procjenu, nadgledanje, ukidanje, izbjegavanje, prenos ili prihvatanje rizika. Upravljanje rizikom je vještina koja stavlja u ravnotežu troškove primjene dodatnih bezbjednosnih mjera sa koristi koja od toga proizlazi. Svrha procesa upravljanja rizikom je obezbjeđivanje permanentne funkcionalnosti bezbjednosnih ciljeva, tajnosti, cjelovitosti i raspoloživosti podataka.

Životni ciklus informacionog sistema mora da prati i dokumentacija koja se odnosi na bezbjednost. Ona podrazumijeva uzajamno djelovanje između svih strana uključenih u rad informacionog sistema, od korisnika preko organa odgovornih za planiranje,implementaciju i operativnost, do tijela nadležnog za davanje bezbjednosne akreditacije za rad.

Dokumentacija koja se odnosi na bezbjednost obuhvata elaborat o bezbjednosti, bezbjednosnu procjenu, uputstva za operativnu upotrebu sistema i saglasnost za upotrebu sistema.

Bezbjednosna akreditacija sistema podrazumijeva da je dostignut zadovoljavajući nivo zaštite informacionog sistema i da se taj nivo treba održavati.

U načelu, bezbjednost informacionog sistema obuhvata sve što i informaciona bezbjednost u širem smislu, samo primijenjeno u užim tehnološkim okvirima.

1.6. Bezbjednost poslovne saradnje

Poslovna saradnja obuhvata uobičajene postupke nabavke, razvoja i održavanja opreme, u okviru čega postoji razmjena određenih podataka o organizaciji i/ili tehnologiji između ugovornih strana. Pri tome, odgovornost za obradu podataka ostaje u nadležnosti organa javne uprave (npr. razvoj ili kupovina programa za praćenje poslovanja za potrebe državnog organa).

Vanjska saradnja je dublji oblik saradnje u kojoj vanjski poslovni subjekat ima odgovornost za obradu podataka određenog organa javne uprave.

U okviru svakog pristupa trećih strana, a naročito u okviru vanjske saradnje, potrebno je procijeniti rizik. Procjena rizika obuhvata elemente kao što su način pregovaranja i dodjele povjerljivih ugovora, način pristupa eksternih lica opremi i prostoru, utvrđivanje razloga i potrebe za pristupom, potreba sprovođenja bezbjednosne provjere kompanije i u njoj zaposlenih lica, izbor oblika ugovora, utvrđivanje bezbjednosnih zahtjeva u ugovorima, razrada procedure razmjene povjerljivih podataka i sl.

Kada se radi o bezbjednosti poslovne saradnje, u okviru NATO programa koristi se termin industrijska bezbjednost, koji između ostalog podrazumijeva i bezbjednosnu provjeru kompanija i u njima zaposlenih lica (FSC – Facility Secure Clearance i PSC - Personnel Security Clerance) koje na nacionalnom nivou sarađuju na NATO programima, uz potpisivanje prethodnih ugovora o prihvatanju obaveza, prema sporazumu o bezbjednosti informacija.

U okviru ove oblasti bezbjednosti pojavljuju se i neke savremene kategorije, čiji je smisao i dalje bezbjednost saradnje sa trećim stranama. To su različite inicijative za prevencijom monopola u pojedinim oblastima javnih nabavki, s obzirom da monopoli mogu uzrokovati ozbiljne bezbjednosne posljedice. Kao najznačajnija takva inicijativa danas se pojavljuje inicijativa za ravnopravnim tretmanom programske podrške otvorenog izvornog koda od strane organa javne uprave (Open Source Software – OSS, različite verzije operativnih sistema zasnovanih na Linuxu i pratećih programskih aplikacija). U ovoj oblasti postoji formalna inicijativa EU, kao i formalno ocjenjivanje uspješnosti OSS inicijative potencijalnih država pristupnica EU. U oblasti izgradnje informaciono-komunikacionih sistema, usljed liberalizacije tržišta telekomunikacija, ali i uopšte zbog kvaliteta razvoja projekata, neophodno je u državnu upravu uvesti praksu ugovora o nivou usluge (SLA – Service Level Agreement). Takvi ugovori obuhvataju sporazum sa davaocem usluge o kvalitetu, prioritetima, rokovima, odgovornostima i sl., a posljedica su složenog poslovnog odnosa u kojem se radi o kompleksnim uslugama ili uslugama koje realizuje više kompanija, od kojih posljednja u nizu zaključuje ugovor sa krajnjim korisnikom.

2. Upravljanje sistemom informacione bezbjednosti

Uspješna primjena sistema informacione bezbjednosti u organima javne uprave, ili uopšte u okviru bilo koje poslovne organizacije, zahtijeva sistemsko upravljanje različitim aspektima informacione bezbjednosti, u skladu sa odgovarajućim zakonskim i podzakonskim propisima.
Baš zbog važnosti i nužnosti ujednačavanja postupaka i procedura informacione bezbjednosti u svim organima javne uprave, upravljanje informacionom bezbjednošću mora biti usklađeno sa

organizacionom hijerarhijom same državne uprave. Svi propisi o informacionoj bezbjednosti treba da se donose na najvišem izvršnom nivou, bilo da se radi o državi ili poslovnom subjektu. Na taj način se obezbjeđuje obavezna primjena tih akata po svim hijerarhijskim organizacionim nivoima, što omogućava postizanje minimalnih bezbjednosnih kriterijuma cijelog sistema (države ili kompanije). Iz tog razloga, u slučaju informacione bezbjednosti jedne države, donošenje akata i upravljanje sistemom informacione bezbjednosti mora se sprovoditi na nacionalnom nivou. Najčešće to je na nivou Vlade, odnosno stručnih organa nacionalnog bezbjednosnog sistema i Vlade. To važi i za informacionu bezbjednost privrednih subjekata, koja takođe počinje na najvišem nivou same uprave kompanije.

Kroz proces upravljanja informacionom bezbjednošću treba da se obezbijedi trajno usavršavanje zakonskog okvira, počevši od bezbjednosne politike, preko sprovedbenih uredbi, pravilnika i uputstava, do detaljnih procedura postupanja pojedinih organa javne uprave. Upravljanje informacionom bezbjednošću obuhvata postupke kao što su identifikacija resursa, klasifikacija podataka, upravljanje rizikom, planiranje i implementacija mjera, postupci certifikovanja lica i uređaja, postupci akreditacije sistema za rad, nadzor implementacije i efikasnosti mjera i postupaka, praćenje informacionih sistema u toku životnog ciklusa, sistemska edukacija i sl.

Aktivne mjere informacione bezbjednosti su mjere koje se primjenjuju "prije događanja bezbjednosnih incidenata" i imaju za cilj da spriječe događanje incidenata. Taj dio mjera predstavlja suštinu sistema informacione bezbjednosti i sastoji se od bezbjednosne politike i sprovedbenih akata, organizacionih i tehničkih normi i standarda, procjene i upravljanja rizikom, periodičnog preispitivanja procesa i sl.

Reaktivne mjere informacione bezbjednosti su mjere koje se primjenjuju "nakon događanja bezbjednosnih incidenata" i imaju za cilj da izvrše procjenu i oporavak od šteta prouzrokovanih bezbjednosnim incidentima, preispitaju organizacione i tehničke djelove sistema u svrhu budućeg sprečavanja sličnih incidenata, kao i da sprovedu prikupljanje dokaznog materijala za otkrivanje i zakonsko procesuiranje počinioca određenog bezbjednosnog incidenta. Dobro organizovan sistem upravljanja informacionom bezbjednošću jedne države ima neposredno preventivni uticaj na ukupno stanje bezbjednosti države i čini osnovu za razvoj efikasnih represivnih postupaka savremenog informacionog društva.

3. Organizacija sistema informacione bezbjednosti

Za efikasno sprovođenje kompleksnog procesa upravljanja informacionom bezbjednošću, uspostavljanje usklađenog sistema odgovornosti državnih organa predstavlja nezamjenjiv uslov. U cilju međusobne usklađenosti i očekivane efikasnosti takve organizacije u raznim državama, danas se koristi generički model organizacionih tijela, u okviru kojih su grupisani pojedini funkcionalni zahtjevi koji proizilaze iz opšteg procesa informacione bezbjednosti.

Pojam informacione bezbjednosti može se odnositi na međunarodne asocijacije (npr.NATO), pojedinačne države ili državne saveze kao što je EU, pri čemu postoje značajne razlike u organizacionoj strukturi vlasti pojedinih država. Iz tog razloga, organizacija informacione bezbjednosti najčešće se definiše korišćenjem generičkog modela organizacionog tijela. Analizom funkcionalnih zahtjeva organizacionih tijela u generičkom modelu i primjenom određenih načela, tzv. generičke nadležnosti dodjeljuju se konkretnim nacionalnim tijelima. Na taj način se obezbjeđuje međusobna usklađenost sistema informacione bezbjednosti različitih država ili asocijacija, uz uvažavanje različitosti u organizacionoj strukturi javne vlasti pojedinih država. Kod raspodjele funkcionalnih zahtjeva primjenjuju se načela delegiranja odgovornosti na najveći nivo organizacije, razdvajanja razvojnih i operativnih funkcionalnosti u cilju međusobnog

podsticanja kvalitetnijih rješenja, usklađenosti rada bezbjednosnog i civilnog sektora državne uprave, primarne odgovornosti samih državnih organa za sopstvene implementacije i sl.

Osnovni skup generičkih organizacionih tijela, kojima se obezbjeđuje međusobna usklađenost različitih nacionalnih modela organizacije sistema informacione bezbjednosti i koji je primjeren zahtjevima NATO-a i EU, sadrži sljedeća generička organizaciona tijela:

Centralno državno bezbjednosno tijelo odgovorno za usklađenost opštih bezbjednosnih mjera u državi (**NSA** – National Security Authority);

Centralno državno komunikaciono bezbjednosno tijelo, odgovorno za usklađenost tehničkih bezbjednosnih mjera (**NCSA** – National Communications Security Authority);

Centralno državno tijelo za bezbjednosne akreditacije komunikaciono-informacionih sistema ili više povezanih državnih tijela u nacionalnu hijerarhiju (**SAA** – Security Accreditation Authority);

Državna tijela ili organizacione jedinice u državnim tijelima odgovorne za nadzor operativnosti mjera INFOSEC-a u komunikaciono-informacionim sistemima (**CIS OA** – Communications and Information System Operating Authority);

Državna tijela ili organizacione jedinice u državnim tijelima odgovorne za planiranje i implementaciju mjera INFOSEC-a u komunikaciono-informacionim sistemima (**CIS PIA** – Communications and Information System Planning and Implementation Authority);

Centralno državno tijelo i nacionalna hijerarhija državnih i privatnih tijela ili organizacionih jedinica tijela, odgovornih za bezbjednosne incidente na Internetu i drugim mrežama koje su zasnovane na javnoj komunikacionoj infrastrukturi (**CERT** – Computer Emergency Response Team).

II - ZAHTJEVI INFORMACIONE BEZBJEDNOSTI I MEĐUNARODNI ODNOSI

1. Opšta razmatranja

U okviru integracionih procesa najčešće se postavljaju eksplicitni i implicitni zahtjevi prema državama pristupnicama. Eksplicitni zahtjevi se navode u dokumentima koje potpisuju države pristupnice i izražavaju se u obliku određene vrste partnerskih ciljeva. Implicitni zahtjevi sadržani su u nizu formalno-pravnih procedura i propisa određene zajednice i treba ih sagledavati i harmonizovati uporedo sa dogovorenim integracionim ciljevima. Taj posao obavljaju stručni timovi država pristupnica, a rezultati takvog posla, iako često nijesu istaknuti kao eksplicitni ciljevi integracionog procesa, preduslov su ostvarenja tih ciljeva.

U oblasti informacione bezbjednosti takođe susrijećemo obje vrste zahtjeva integracionih procesa. Implicitni zahtjevi informacione bezbjednosti vrlo su kompleksni i proizilaze iz niza propisa. U prvom redu, to su propisi poznati kao bezbjednosna politika i sprovedbeni akti, ali i različiti zakoni, uredbe, rezolucije i akcioni programi u oblasti projekata elektronske državne uprave i informacionog društva.

U okviru integracionih procesa Crne Gore u EU i NATO, zahtjevi informacione bezbjednosti sadržani su u programima NATO-a Partnerstvo za mir (PfP) i Akcioni plan za članstvo (MAP), Sporazumu o stabilizaciji i pridruživanju u EU (SSP), kao i u bezbjednosnoj politici NATO-a i EU i pratećim sprovedbenim dokumentima bezbjednosne politike. Takođe, ti zahtjevi su posebno izraženi u programu eEurope 2005, kroz odluke, rezolucije i druge programske dokumente Savjeta Evropske unije i Evropske komisije u oblasti informacionog društva. Proces harmonizacije nacionalnog i EU zakonodavstva u mnogim oblastima doticaće se pitanja koja spadaju u okvire ili se dotiču okvira informacione bezbjednosti (reforma državne uprave, kancelarijsko poslovanje, osavremenjavanje kaznenog zakonodavstva i sl.).

Saglasno stavovima Evropske komisije, bezbjednost je preduslov punog razvoja informacionog društva, ključna komponenta vizije Interneta sljedeće generacije i jedan od šest prioriteta programa eEurope 2005. Bezbjednost nije samo tehnološki izazov već u velikoj mjeri obuhvata ljude i poslovne procese, zbog čega se smatra sastavnim dijelom savremenog društva.

Oblast informacione bezbjednosti, osim u okviru pomenutih integracionih procesa, tretira se i u okviru međunarodnih bilateralnih Sporazuma o uzajamnoj zaštiti tajnih podataka. Tim sporazumima države se usaglašavaju oko istovjetnosti stepena tajnosti, označavanju tajnih podataka, prosljeđivanju tajnih podataka, preduzimanju mjera za zaštitu tajnih podataka, povredi propisa o uzajamnoj zaštiti, nadležnim organima i sl. Sporazumima se uređuje da prosljeđivanje tajnih podataka preko zaštićenih informaciono-komunikacionih sistema podrazumijeva postojanje akreditacije za te sisteme. Takođe, sporazumom se uređuje da jedna strana od druge može zatražiti uvjerenje za neku stranku na njenoj državnoj teritoriji u smislu postojanja ovlašćenja za pristup tajnim podacima sa određenim stepenom tajnosti.Nadležni organi za sprovođenje tih sporazuma su organi određeni unutrašnjim zakonodavstvom država koje zaključuju sporazum. Sporazume o uzajamnoj zaštiti tajnih podataka potpisuju Vlade.

2. Harmonizacija pravnog sistema Crne Gore sa zahtjevima NATO i EU

Informaciona bezbjednost predstavlja jednu od strateških odrednica EU, ali je prepoznata i kao međunarodni problem. Savjet Evrope je usvojio konvencije, evropske sporazume i pripadajuće protokole, kao i preporuke kojima se nastoji, između ostalog, urediti i pitanje informacione

bezbjednosti. Strategija EU prema bezbjednosnoj problematici određena je Odlukom Savjeta Evropske unije o prihvatanju bezbjednosne politike i Odlukom Evropske komisije o sprovođenju bezbjednosne politike.

EU je izvršila i detaljnu razradu bezbjednosnog pristupa u području mrežne bezbjednosti informacionih sistema, kao i pristupa razvoju informacionog društva. Jasna bezbjednosna strategija daje osnovu za izgradnju informacione infrastrukture na kojoj će se zasnivati savremeno informaciono društvo i omogućava razvoj bezbjednosne kulture javne uprave i privatnog sektora, ali i najširih slojeva stanovništva. Takav pristup rezultirao je glavnim ciljevima i pratećim aktivnostima koje su unesene u same temelje Akcionog Plana eEurope 2005. Jedan od osnovnih vanjskopolitičkih ciljeva Crne Gore je ulazak u punopravno članstvo EU. Potpisivanjem Sporazuma o stabilizaciji i pridruživanju (SSP) između Crne Gore, s jedne strane, i Evropskih zajednica i njihovih država članica, s druge strane, Crna Gora je i službeno preuzela obvezu usklađivanja nacionalnog zakonodavstva sa pravnom tekovinom EU (Acquis Communautaire), uporedo sa obvezama uspostavljanja političkog dijaloga, unapređivanja ekonomskih odnosa, razvoja zone slobodne trgovine, obezbjeđivanja regionalne saradnje, kao i podsticanja saradnje u nizu drugih područja. Iz toga proizlazi da će se i zakonodavstvo Crne Gore, takođe, morati usklađivati sa potrebama i zahtjevima u oblasti informacione bezbjednosti. Potpisivanjem SSP-a Crna Gora se, između ostalog, obvezala da će "osnažiti saradnju na daljem razvijanju informacionog društva, pripremu društva za digitalno doba, međusobno funkcionisanje mreža i usluga, izraditi plan usvajanja zakonodavstva EU na području informacionog društva".

Neke od obaveza informacione bezbjednosti za države članice EU, odnosno za buduće države pristupnice, proizilaze iz sljedećih dokumenata:

Rezolucijom Savjeta Evropske unije 2002/C 43/02 od 28/01/2002 definišu se specifične aktivnosti u oblasti mrežne i informacione bezbjednosdti za države članice EU. To su npr:

- povećanje svijesti o mrežnoj i informacionoj bezbjednosti putem odgovarajuće edukacije;
- promovisanje korišćenja standarda ISO – 15408 (Common Criteria) sa ciljem međusobnog priznavanja povezanih područja certifikovanja;
- primjena efikasnih interoperabilnih bezbjednosnih rješenja zasnovanih na prepoznatljivim normama, što uključuje i primjenu programske podrške otvorenog koda (Open Source Software – OSS), u projektima elektronske Vlade i elektronskih javnih nabavki, kao i primjenu elektronskih potpisa i pouzdane autentikacije za sve javne interaktivne usluge;
- efikasan odgovor na bezbjednosne incidente (CERT – Computer Emergency Response Team) i međusobna razmjena podataka i saradnja na području mrežne i informacione bezbjednosti.

Akcionim Planom eEurope 2005 predložene se sljedeće aktivnosti:

- osnivanje Cyber security task force (CSTF) sa punom funkcionalnošću;
- postizanje "kulture bezbjednosti" u dizajnu i implementaciji informacionih i komunikacionih proizvoda;
- ostvarenje bezbjedne komunikacije za razmjenu klasifikovanih vladinih informacija.

S obzirom da je područje informacione bezbjednosti od strateškog interesa za EU, postavljeni su i formalni programi kao što je MODINIS, kojim se područje primjene mjera informacione bezbjednosti širi na Evropsko ekonomsko područje (države EEA) i države pristupnice EU. Program MODINIS se sastoji u praćenju mjera poboljšanja mrežne i informacione bezbjednosti u okviru Akcionog Plana eEurope 2005 i njegovih nacionalnih verzija, ali i opšteg utvrđivanja

stanja bezbjednosne kulture i mjera za podsticanje bezbjednosne kulture i primjene dobre bezbjednosne prakse u nacionalnim okvirima.

U okviru Akcionog plana za članstvo u NATO-u (MAP), koji je takođe strateški interes Crne Gore, važno je ukazati na formalni partnerski cilj PG G 0360 I – "Nacionalni program za bezbjednosnu kooperaciju sa NATO-om", koji podrazumijeva uspostavljanje minimalnih bezbjednosnih kriterijuma na nacionalnom nivou, i to u četiri osnovna bezbjednosna područja: fizička bezbjednost, bezbjednosna provjera lica, bezbjednost podataka i INFOSEC. Sadržaj tog zahtjeva definisan je bezbjednosnom politikom i sprovedbenim dokumentima bezbjednosne politike NATO-a, i svodi se na donošenje nacionalne bezbjednosne politike usklađene sa NATO-vom u osnovnim bezbjednosnim pitanjima i principima upravljanja bezbjednošću.

Da bi se navedeni bezbjednosni zahtjevi EU i NATO-a mogli sprovesti na nacionalnom nivou u Crnoj Gori, potrebno je uspostaviti usklađen sistem odgovornosti državnih organa, koji će sprovoditi kompleksan proces upravljanja informacionom bezbjednošću. Organizacija informacione bezbjednosti Crne Gore, u cilju međusobne usklađenosti sa EU i NATO organizacijom, treba da zadovoljava generički model organizacionih tijela, u okviru kojih su grupisani pojedini funkcionalni zahtjevi koji proizilaze iz bezbjednosne politike i sprovedbenih dokumenata EU i NATO-a, odnosno iz njihovog sistema informacione bezbjednosti.

3. Organizacioni zahtjevi NATO-a

Međusobne političke konsultacije, saradnja i planiranje odbrane podrazumijevaju razmjenu klasifikovanih informacija između potpisnica NATO saveza i budućih članica tog saveza. Ta se saradnja ne odnosi samo na vojne organe, već i na javnu upravu i privatni sektor. Saglasno odredbama o međusobnoj zaštiti i čuvanju NATO klasifikovanih dokumenata donesen je Sporazum o bezbjednosti informacija koji definiše okvir i sadržaj bezbjednosnih standarda, a obuhvata dokumente bezbjednosne politike, smjernice i implementacione direktive kao podršku tim dokumentima.

Potpisnice navedenog sporazuma dužne su obezbijediti:

1. Prilagođavanje nacionalnih zakonskih propisa, kako bi se NATO informacije štitile u skladu sa NATO pravilima, što se prvenstveno odnosi na propise iz oblasti:

- **Bezbjednosna provjera lica**. Za sva lica koja imaju ovlašćenje za pristup NATO klasifikovanim informacijama treba izvršiti odgovarajuću bezbjednosnu provjeru i dodijeliti adekvatno bezbjednosno ovlašćenje (PSC – Personal Security Clearance);
- **Fizička bezbjednost**. Obezbijediti primjenu tehničkih mjera zaštite za mjesta, prostorije i zgrade u kojima se rukuje NATO klasifikovanim informacijama (NATO registri i podregistri u organima javne uprave);
- **Bezbjednost informacija**. Obezbijediti pravilno klasifikovanje i označavanje povjerljivih NATO informacija i materijala, kao i obezbijediti evidencioni sistem za primanje, evidentiranje, rukovanje, distribuciju i uništavanje informacija;
- **Bezbjednost informacionih sistema** (INFOSEC). Svi sistemi u kojima se rukuje NATO klasifikovanim informacijama treba da podliježu procesu bezbjednosnog odobrenja, koji se zasniva na bezbjednosnim ciljevima povjerljivosti, cjelovitosti i dostupnosti;
- **Industrijska bezbjednost**. Treba vršiti provjeru za subjekte (FSC – Facility Secure Clearance) koje na nacionalnom nivou sarađuju na NATO programima, kao i potpisivanje prethodnih ugovora o prihvatanju obaveza prema sporazumu o bezbjednosti informacija.

2. Osnivanje organa uprave za nacionalnu bezbjednost nadležnog za NATO aktivnosti, koji će sprovoditi zaštitne bezbjednosne mjere. Ovdje treba naglasiti da dokumenti NATO bezbjednosne politike ne zahtijevaju da se osnivaju novi organi koji obavljaju funkcije generičkih organizacionih tijela, već samo dodjelu funkcionalnosti tih tijela nekom od postojećih organa uprave.

Dokumenti NATO politike definišu sljedeća nacionalna tijela povezana sa bezbjednošću:

NSA – National Security Authority. Centralno državno bezbjednosno tijelo koje predstavlja najviši nivo bezbjednosne vlasti i ima ulogu centralnog tijela za kontakt sa NATO kancelarijom za bezbjednost (NOS). NSA je odgovorno za koordinaciju svih pitanja koja se odnose na NATO bezbjednosnu politiku unutar države i za praćenje njihove primjene kako bi se obezbijedio zajednički nivo zaštite klasifikovanih informacija. Odgovornosti NSA uključuju i brigu o održavanju bezbjednosti NATO klasifikovanih informacija u državnim, vojnim i civilnim organima, brigu oko sprovođenja periodičnih inspekcija, kao i brigu o sprovođenju bezbjednosne provjere za sve njene državljane koji imaju pristup informacijama klasifikovanim sa NATO POVJERLJIVO i iznad toga.

NCSA – National Comunications Security Authority. Centralno državno tijelo za bezbjednost komunikacija, koje treba da potvrdi da su kriptografski sistemi, proizvodi i mehanizmi za zaštitu NATO informacija, adekvatno i efikasno odabrani, vođeni i održavani. Uz to, NCSA treba da kontroliše kriptografske tehničke podatke koji se odnose na zaštitu NATO informacija unutar države, kao i da izvještava o NATO komunikacionoj bezbjednosti i sa njom povezanim INFOSEC pitanjima. NCSA treba da sarađuje sa NSA.

NDA – National Distribution Authority. Centralno državno tijelo (ili više državnih tijela povezanih u nacionalnu hijerarhiju), odgovorno za rukovanje NATO kriptomaterijalima unutar svoje države. To tijelo treba da obezbijedi primjerene procedure za bezbjedno rukovanje, čuvanje, distribuciju i evidentiranje cjelokupnog kriptomaterijala. NDA treba da djeluje u koordinaciji sa NSA.

SAA – Security Accreditation (Approval) Authority. Centralno državno tijelo (ili više državnih tijela povezanih u nacionalnu hijerarhiju) odgovorno za izdavanje bezbjednosnog odobrenja za sisteme u kojima se skladište, procesuiraju i distribuiraju NATO klasifikovane informacije.

CIS Operating Authority. Državna tijela ili organizacione jedinice u državnim tijelima odgovorne za nadzor operativnosti mjera INFOSEC-a u komunikaciono-informacionim sistemima u kojima se skladište, procesuiraju i distribuiraju NATO klasifikovane informacije.

CIS Planning and Implementation Authority. Državna tijela ili organizacione jedinice u državnim tijelima odgovorne za planiranje i implementaciju mjera INFOSEC-a u komunikaciono-informacionim sistemima u kojima se skladište, procesuiraju i distribuiraju NATO klasifikovane informacije.

4. Organizacioni zahtjevi EU

Organizacioni zahtjevi EU u oblasti informacione bezbjednosti izraženi su prvenstveno u okviru bezbjednosne politike EU i sprovedbenih propisa, a dodatno su razrađeni i predstavljaju preduslove realizacije niza drugih EU dokumenata i programa navedenih u poglavlju II-2.

Osnovni skup generičkih organizacionih tijela, koji proizilazi iz EU bezbjednosne politike i strategije pristupa informacionoj bezbjednosti, čine:

NSA – National Security Authority. Centralno državno bezbjednosno tijelo koje predstavlja najviši nivo bezbjednosne vlasti i ima ulogu centralnog tijela za kontakt sa Glavnim sekretarijatom Savjeta Evropske unije (GSC – General Secretariat of the Council) i daje predstavnika u Odbor za bezbjednost (SC – Security Committee). NSA je odgovoran za koordinaciju svih pitanja koja se odnose na EU bezbjednosne politike unutar svoje države i za nadzor nad primjenom bezbjednosnih mjera, kako bi se obezbijedio zajednički stepen zaštite klasifikovanih informacija. Odgovornosti NSA uključuju i brigu o održavanju bezbjednosti EU klasifikovanih podataka u organima javne uprave, brigu oko sprovođenja periodičnih inspekcija, kao i brigu o sprovođenju odgovarajućeg certifikovanja za sve državljane koji imaju pristup EU klasifikovanim podacima.

SAA – Security Accreditation (Approval) Authority. Centralno državno tijelo (ili više državnih tijela povezanih u nacionalnu hijerarhiju) za bezbjednosne akreditacije komunikaciono-informacionih sistema odgovorno za izdavanje bezbjednosnih odobrenja za sisteme u kojima se skladište, procesuiraju i distribuiraju EU klasifikovane informacije. Potrebnu tehničku pomoć obezbjeđuje u koordinaciji sa pripadajućim IA. SAA djeluju u koordinaciji sa nadležnim NSA.

IA – INFOSEC Authority. Centralno državno tijelo za bezbjednost komunikacija. To tijelo je nadležno za: predlaganje i usklađivanje tehničkih dokumenata koji se odnose na politiku informacione bezbjednosti, davanje tehničkih savjeta i podršku nacionalnom procesu bezbjednosne akreditacije (SAA), učestvovanje u izradi i preispitivanju sistemskih bezbjednosnih zahtjeva (SSRS), sprovođenje obuke i edukacije na nacionalnom nivou, davanje tehničkih savjeta u okviru istraga INFOSEC incidenata, donošenje tehničkih smjernica i propisivanje autorizovane programske podrške. Sarađuje sa relevantnim tijelima EU i država članica po pitanjima mrežne i komunikacione bezbjednosti. Rad IA odvija se u koordinaciji sa nadležnim NSA.

ITSOA – IT System Operational Authority. Državna tijela ili organizacione jedinice u državnim tijelima koje imaju odgovornost za implementaciju mjera INFOSEC-a u svojim informaciono-komunikacionim sistemima tokom njihovog životnog ciklusa. Ta tijela su odgovorna nacionalnom IA. U tijelima je moguće odgovornost ITSOA delegirati na IT odjeljenja ili posebni tehnički organ. U okviru EU prakse odgovornost ITSOA uobičajeno se dodjeljuje vlasniku tehničkog sistema (TSO – Technical Systems Owner). U oblasti vlasništva podataka, vlasnik podataka (IO – Information Owner) razlikuje se od TSO, koji je odgovoran za postavljanje zahtjeva za pristup podacima, pri čemu se ta odgovornost može delegirati na određenog rukovaoca podacima (Information Manager) ili rukovaoca bazama podataka (Database Manager) unutar njihove nadležnosti.

CISO i LISO koordinatori informacione bezbjednosti. Na nivou nacionalnih sistema se određuju CISO (Central Information Security Officer) koordinatori informacione bezbjednosti, a pojedina tijela prema potrebi određuju LISO koordinatore informacione bezbjednosti (Local Information Security Officer). Ti koordinatori su odgovorni za operativnost mjera informacione bezbjednosti u informacionim sistemima za koje su nadležni. U tijelima se odgovornost za operativnost mjera informacione bezbjednosti može dodijeliti nadležnom koordinatoru informacione bezbjednosti (officers/site officers), uz uslov samostalnosti koordinatora informacione bezbjednosti, odnosno nezavisnosti od nadležne ITSOA organizacione jedinice. Svi CISO i LISO koordinatori odgovorni su nacionalnom IA, koji treba da se brine za uspostavljanje nacionalne mreže koordinatora informacione bezbjednosti.

CERT – Computer Emergency Response Team. Centralno državno tijelo i nacionalna hijerarhija državnih tijela ili organizacionih jedinica tijela, odgovornih za bezbjednosne incidente na Internetu i drugim mrežama zasnovanim na javnoj komunikacionoj infrastrukturi. Hijerarhija se najčešće sastoji od vrhovnog nacionalnog CERT-a, zatim hijerarhije unutar državnih tijela (vrhovni CERT državne uprave i CERT-ovi specifičnih ministarstva, kao što su MO i MUPJU) i različitih privrednih subjekata (TK operatori, finansijske institucije i sl.). Svrha hijerarhije je međusobno izvještavanje o incidentima po vertikali, horizontalna komunikacija sa svojim funkcionalnim parom u inostranstvu, kao i podrška istragama incidenata na najvišem nacionalnom nivou.

5. Evropska agencija za mrežnu i informacionu bezbjednost – ENISA

Evropski Parlament, Savjet Evropske unije i Evropska komisija su na stanovištu da je potrebna što jača evropska koordinacija u oblasti informacione bezbjednosti. Da bi se postigao taj cilj uspostavljena je agencija sa pravnim ovlašćenjima na području EU. U skladu sa Uredbom Evropskog Parlamenta i Savjeta Evropske unije osnovana je Evropska agencija za mrežnu i informacionu bezbjednost (EuropeanNetwork and Information Security Agency – ENISA). Ta Agencija treba da uživa povjerenje organa javne uprave, kao i privatnog sektora u državama članicama. Osnovni cilj Agencije je da kreira zajedničko razumijevanje u Evropi o pitanjima koja se odnose na informacionu bezbjednost, što je neophodno da bi se obezbijedila raspoloživost i bezbjednost mreža i informacionih sistema u EU. Agencija treba da pruža pomoć nadležnim nacionalnim tijelima u primjeni mjera EU koje se odnose na mrežnu i informacionu bezbjednost. Agencija ima savjetodavne i koordinacione funkcije i otvorena je za učešće trećih država koje imaju sporazume sa EU. U njoj se prikupljaju i analiziraju podaci koji se odnose na informacionu bezbjednost.

U procesu uspostavljanja sistema informacione bezbjednosti u Crnoj Gori, nadležne nacionalne institucije u oblasti mrežne i informacione bezbjednosti, treba da ostvare neophodnu saradnju s ENISA-om. U okviru te saradnje, biće moguće podsticati proces harmonizacije zakonodavstva u oblasti informacione bezbjednosti i ubrzati uspostavljanje sistema informacione bezbjednosti u Crnoj Gori.

III - STANJE INFORMACIONE BEZBJEDNOSTI U CRNOJ GORI

1. Opšta razmatranja

U Crnoj Gori ne postoji praksa sistemskog sprovođenja informacione bezbjednosti u državnoj upravi i društvu u cjelini, mada je u nekim službama (vojne i bezbjednosne strukture) ostvarivan visok nivo bezbjednosti. U pojedinim privrednim sektorima, kao što je npr. finansijski sektor, izvršena su značajna ulaganja u oblasti informacione bezbjednosti, ali ne postoje inicijative, mjere i standardi koji bi takva ulaganja usmjeravali i obezbijedili primjenu relevantnih bezbjednosnih standarda, već to zavisi isključivo od poslovne politike svake pojedine kompanije ili vlasnika. Trenutno stanje sistema zaštite informacionog sistema organa javne uprave nije u skladu sa standardima EU i razvijenih zemalja.

Suštinu informacione bezbjednosti predstavlja postizanje minimalnih, a zatim i adekvatnih bezbjednosnih kriterijuma na nivou organa javne uprave. Da bi se to moglo postići potrebno je utvrditi nacionalnu politiku informacione bezbjednosti i sprovedbene akte i smjernice za javnu upravu. U skladu sa tim biće neophodno podsticati tehničku standardizaciju i javno-privatno partnerstvo u izgradnji informacionog društva u cjelini. Kroz proces uvođenja informacione bezbjednosti mora se, između ostalog, osavremeniti sistem bezbjednosne klasifikacije dokumenata i ujednačiti načini postupanja sa podacima, kao i razgraničiti podatke u vlasništvu javne uprave od javnih podataka, odnosno uvesti jasne i transparentne procedure objavljivanja podataka u organima javne uprave.

Uređivanje informacione bezbjednosti samo jednim nacionalnim zakonom nije dovoljno za sistemsko regulisanje tog kompleksnog multidisciplinarnog područja. Zbog toga, Crnoj Gori u ovoj oblasti predstoji ozbiljna sistemska razrada zakonodavstva i odgovarajuća reorganizacija javne uprave, sa ciljem da se ova oblast uredi po standardima EU i NATO.

Razvoj informacione tehnologije i infrastrukture u državi treba da bude uslovljen razvojem bezbjednosno-zaštitnih mjera upotrebe tih tehnologija i infrastrukture, ali i razvojem bezbjednosne kulture najširih slojeva stanovništva. Takav pristup doprinijeće sticanju povjerenja svih subjekata informacionog društva u razvoj novih e-usluga. Upravo nedostatak povjerenja najširih slojeva stanovništva, uz nerazvijenost infrastrukture, jedan je od značajnih razloga sporog razvoja novih e-usluga.

2. Zakonodavni okvir

U ovom dijelu programa prikazuju se propisi koji imaju značajnu ulogu u procesu stvaranja savremenog koncepta informacione bezbjednosti u Crnoj Gori. Navode se predlozi konkretnih potreba za izmjenama i dopunama postojećih propisa, odnosno za donošenjem novih koji su neophodni za uspostavljanje sistema informacione bezbjednosti, kao i nosioci i rokovi usklađeni sa potrebama ovog programa.

2.1. Zakon o tajnosti podataka

Zakon o tajnosti podataka ("Sl.list CG", br.14/08) propisuje vrste i stepene tajnosti, kao i mjere i postupke za utvrđivanje, upotrebu i zaštitu tajnosti podataka. Prema tom zakonu, tajni podaci su podaci čijim bi otkrivanjem nepozvanom licu nastupile ili bi mogle nastupiti štetne posljedice za bezbjednost Crne Gore ili za njene političke ili ekonomske interese, a odnose se na (1) odbranu, (2) javnu bezbjednost, (3) inostrane poslove, (4) obavještajnu i bezbjednosnu djelatnost državnih organa, (5) naučne, istraživačke, tehnološke, ekonomske i finansijske interese države u oblastima

odbrane, javne bezbjednosti, inostranih poslova i obavještajne i bezbjednosne djelatnosti državnih organa, (6) sisteme, uređaje, projekte i planove u oblastima odbrane, javne bezbjednosti, inostranih poslova i obavještajne i bezbjednosne djelatnosti državnih organa Crne Gore. Tajnom podatku određuje se jedan od stepena tajnosti: (1) strogo tajno, (2) tajno, (3) povjerljivo, (4) interno.Način i postupak označavanja tajnosti podatka propisuje Vlada Crne Gore.

Pristup tajnim podacima stepena tajnosti "strogo tajno", "tajno" i "povjerljivo" može ostvariti samo lice kome je, na osnovu sprovedene bezbjednosne provjere, izdata dozvola za pristup tajnim podacima. Izuzetno, pristup tajnim podacima bez dozvole za pristup tajnim podacima ima određen broj lica utvrđen ovim zakonom, ali samo tajnim podacima potrebnim za vršenje njihovih ovlašćenja. Pristup tajnim podacima stepena tajnosti "interno" imaju svi zaposleni u organu i organizaciji. Tajni podaci stranih država ili međunarodnih asocijacija zadržavaju oznake stepena tajnosti koji su u upotrebi u tim državama ili asocijacijama.

Dozvolu za pristup tajnim podacima izdaje Direkcija za zaštitu tajnih podataka, na osnovu bezbjednosne provjere koju sprovodi Agencija za nacionalnu bezbjednost, u skladu sa zakonom. Ta direkcija ima status organa uprave sa svojstvom pravnog lica.

Po Zakonu o tajnosti podataka dužni su postupati organi javne uprave, kao i pravna i fizička lica kada u vršenju zakonom utvrđenih poslova, odnosno izvršavanju ugovorenog posla saznaju za tajne podatke.

2.2. Zakon o slobodnom pristupu informacijama

Zakonom o slobodnom pristupu informacijama ("Sl.list RCG",br.68/05) utvrđeni su uslovi pod kojima je moguće ostvarivati pravo na pristup informacijama koje se nalaze u posjedu organa vlasti. To pravo ima svako domaće i strano pravno i fizičko lice, u skladu sa zakonom. Međutim, pravo na pristup informacijama ne isključuje potrebu zaštite tih informacija i brigu o njihovoj bezbjednosti. U tom smislu, u slučajevima utvrđenim ovim zakonom, organi vlasti mogu uskratiti pravo na pristup informaciji.

Pravo na pristup informacijama ostvaruje se neposrednim uvidom u dokumente koji sadrže traženu informaciju, prepisivanjem informacije od strane podnosioca zahtjeva u prostorijama organa vlasti ili dostavljanjem fotokopije tražene informacije. Zahtjev za ostvarivanje prava na pristup informaciji podnosi se u pisanoj formi, neposredno, putem pošte ili elektronskim putem.

2.3. Krivično zakonodavstvo

Krivični zakonik ("Sl.list RCG", br. 70/03, 13/04 i 47/06) usklađen je sa odredbama Konvencije o sajber kriminalu i u isti su uključena nova krivična djela protiv bezbjednosti računarskih podataka i to: (1) oštećenje računarskih podataka i programa, (2) računarska sabotaža, (3) pravljenje i unošenje računarskih virusa, (4) računarska prevara, (5) neovlašćeno korišćenje računara ili računarske mreže, (6) ometanje funkcionisanja elektronske obrade i prenosa podataka i računarske mreže, (7) neovlašćeni pristup zaštićenom računaru i računarskoj mreži i (8) sprječavanje i ograničavanje pristupa javnoj računarskoj mreži. Ovaj zakonik je u primjeni od 2.04.2004. godine.

Odredbama važećeg Zakonika o krivičnom postupku ("Sl.list RCG", br.71/03 i 47/06), donekle su riješena pitanja koja se odnose na sprovođenje kriminalističkih obrada, prvenstveno presretanje i nadzor komunikacija na Internetu, prekogranični pristup podacima, kao i način obavljanja provjera korisnika Interneta u hitnim slučajevima. U članu 237 stav 1 predviđa se tajni nadzor i tehničko snimanje telefonskih razgovora, odnosno sredstava za tehničku komunikaciju na daljinu. Međutim od stupanja na snagu ovog zakona u 2004. godini ništa značajnije nije urađeno kako bi

se mogla nadzirati i presrijetati komunikacija učinilaca krivičnih djela na Internetu, kako putem e-maila tako i putem svih drugih oblika komunikacije na Internetu. Zbog toga, uz stvaranje organizaciono-tehničkog sistema koji će obavljati opisane zadatke neophodno je izmijeniti odgovarajuće odredbe Zakonika o krivičnom postupku, kako bi se saglasno odredbama Konvencije o sajber kriminalu, mogućnost korišćenja ovakvih mjera, u slučajevima izdavanja naredbe od strane istražnog sudije, proširilo i na krivična djela koja su navedena u Konvenciji. U konkretnom slučaju to se odnosi na naprijed opisana nova krivična djela, kao i na sva krivična djela koja se odnose na povrede autorskih prava, koja su takođe eksplicitno navedena u Konvenciji i inkorporirana u Krivični zakonik (Glava dvadeset prva-krivična djela protiv intelektualne svojine, čl.233 do 238).

U toku je izrada novog Zakonika o krivičnom postupku u kojem se mjere tajnog nadzora, kao posebne dokazne radnje iz poglavlja o pretkrivičnom postupku važećeg zakonika, premještaju u opšte odredbe, pa će se ubuduće moći primjenjivati ne samo u izviđaju (pretkrivičnom postupku) već i u istrazi. Izmjene se vrše i u odnosu na katalog krivičnih djela za koja se mogu narediti mjere tajnog nadzora, jer dosadašnjim katalogom nijesu bila obuhvaćena neka djela među kojima i određena korumptivna krivična djela, odnosno djela koja bi bez primjene ovih mjera bilo teže dokazati.

Na taj način implementiraće se veći dio formalnih zahtjeva koje Crna Gora treba da uskladi u okviru borbe protiv računarskog kriminala. Važno je naglasiti da će u postupku primjene navedenih propisa biti potrebno obraditi kompleksno područje računarske forenzike. U tom dijelu je preostao veliki dio posla i neophodno ga je riješiti u koordinaciji Ministarstva pravde i Ministarstva unutarnjih poslova i javne uprave sa nosiocima ključnih dijelova Nacionalnog programa informacione bezbjednosti u Crnoj Gori (NSA, NCSA,CERT).

Takođe, biće neophodno implementirati nova rješenja i dodatno poboljšati postojeće propise koji se odnose na zaštitu nacionalne privrede u okviru savremenih trendova informacionog društva. Kao primjer, ukazuje se na dvije ključne oblasti povezane sa programom informacione bezbjednosti. Prva oblast je sve češće primjenjivano kriptovanje podataka od strane krajnjih korisnika – pravnih lica (virtuelne private mreže i sl.). Danas se u svijetu zakonski uređuju postupci kao što su evidentiranje, certifikovanje i akreditovanje kriptografske opreme. Druga značajna oblast odnosi se na savremeni pristup reviziji poslovanja kompanija. Taj proces se, s obzirom na informatizaciju skoro svih poslovnih subjekata, neizbježno premješta u elektronsku oblast (propisi o čuvanju e-pošte, e-transakcijama, skladištenju kripto ključeva i sl.). Iz tih razloga u narednom period treba planirati donošenje propisa koji se odnose na zaštitu nacionalne privrede i povezani su sa informacionom bezbjednošću.

Plan aktivnosti usklađivanja sa Nacionalnim programom informacione bezbjednosti:

- donošenje novog Zakonika o krivičnom postupku u skladu sa promjenama Krivičnog zakonika, prema planu Ministarstva pravde;
- razvoj i implementacija organizaciono-tehničkog sistema za tajni nadzor usluga i trgovine putem Interneta, saglasno važećem zakonodavstvu, od strane nadležnih državnih organa i davaoca Internet usluga u Crnoj Gori, prema planu bezbjednosnog sistema;
- planiranje poboljšanja propisa koji se odnose na zaštitu nacionalne privrede u okviru savremenih trendova informacionog društva, analiza potreba i mogućnosti u 2009. godini, u koordinaciji Ministarstva pravde, Ministarstva za ekonomski razvoj i Ministarstva unutarnjih poslova i javne uprave, uz saradnju organa uprave nadležnog za nacionalnu politiku informacione bezbjednosti.

2.4. Arhive, registri i kancelarijsko poslovanje

Ako se neka informacija nalazi na određenom fizičkom mediju, neovlašćeni pristup najčešće rezultira krađom tog medija ili nekom vrstom kopiranja informacija koje se na njemu nalaze. Pristup neovlašćenog lica određenom fizičkom mediju sprečava se metodama tehničke i fizičke zaštite. Međutim, kad su u pitanju informacije u elektronskom obliku, krađa je "nevidljiva" i mora se sprečavati novim, drukčijim sredstvima.

Danas skoro sve informacije nastaju u elektronskom obliku. Ukoliko su odštampane na papiru, one su već u sekundarnom obliku koji je izgubio mnoge atribute koje ima izvornik. Zbog toga nije prihvatljiva situacija u kojoj se dnevno uništavaju ogromne količine izvornih oblika informacija u elektronskom obliku, jer se uglavnom čuvaju u sekundarnoj formi na papiru. S obzirom na to, jedan od važnijih zadataka sistema informacione bezbjednosti je da obezbijedi čuvanje informacija u njihovom izvornom elektronskom obliku.

Zakonom o arhivskoj djelatnosti ("Sl.list RCG", br.25/92 i 6/94) uređeno je čuvanje informacija, odnosno arhivske građe. Međutim, tim zakonom nijesu uređena pitanja koja se odnose na čuvanje arhivske građe u elektronskom obliku. Zbog toga je neophodno izvršiti inoviranje ovog i drugih propisa, kako bi se obezbijedili sistemski uslovi za čuvanje arhivske građe u elektronskom obliku, pri čemu bi se obaveza čuvanja elektronskog oblika trebala odnositi i na arhivsku građu kojoj je original u štampanom obliku, a postoji kopija u elektronskom obliku. Pri tome je neophodno tehničkim metodama (kriptovanjem, elektronskim potpisom i sl.) obezbijediti zaštitu nepromjenjivosti izvorne informacije.

Publikacije čine značajan dio nacionalnog informacionog prostora. Zakonom o izdavaštvu ("Sl.list RCG", br. 20/95) utvrđena je obaveza dostavljanja tzv. "obaveznog primjerka" Centralnoj narodnoj biblioteci "Đurđe Crnojević" na Cetinju, koja ga je dužna čuvati. Međutim, iako i publikacije nastaju u elektronskom obliku pa se tek onda umnožavaju u štampanom obliku, ne postoji obaveza niti čuvanja niti dostavljanja Centralnoj narodnoj biblioteci elektronskog oblika publikacije. Zbog toga je neophodno inovirati Zakon o izdavaštvu tako da, uz dostavljanje štampanog primjerka, izdavača obavezuje i na dostavljanje propisanog elektronskog oblika publikacije.

Da bi se mogle iskoristiti prednosti postojanja informacija u elektronskom obliku neophodno je te informacije računarski povezati. I pored toga što se sa takvim poduhvatima započelo još prije više decenija (JMBG, matične knjige) i pojedinačnih nastojanja da se objedine pojedini registri i evidencije, Crna Gora još uvijek nema tri osnovna centralna državna registra: prostornih jedinica, poslovnih subjekata i stanovništva. Podaci koji bi trebali da se nađu u tim registrima distribuirani su u nekoliko registara i evidencija, ili čak i ne postoje (npr. registar organa javne uprave). Zbog toga je neophodno stvoriti uslove za jednoznačnu i računarsku identifikaciju i povezivanje podataka o pravnim licima, stanovništvu i prostornim jedinicama. Objedinjavanje podataka u osnovne centralne registre ne podrazumijeva njihovo fizičko skladištenje u jednu bazu podataka ili na isti fizički medijum. Takođe, ne podrazumijeva ni nadležnost jednog organa nad njihovim prikupljanjem, obradom i čuvanjem. Objedinjavanje prije svega podrazumijeva centralizovano staranje o organizaciji i strukturiranju podataka, definisanju pristupa i nadzoru nad sprovođenjem. Tako npr, za registre privrednih društava, udruženja građana, političkih stranaka, vjerskih zajednica, poljoprivrednika, slobodnih zanimanja i drugih, pojedinačno mogu biti nadležni različiti organi, ali sistem identifikacije i pristupa tim podacima mora biti planiran i objedinjen.

Registar prostornih jedinica koji obuhvata opštine, naselja, ulice, katastarske parcele i objekte nužno mora imati jedinstveni identifikator i biti dostupan u elektronskom obliku, na jednom

mjestu. Pored tehničkih mjera, potrebno je uskladiti zakonske i druge propise na način da subjekti koji imaju pravo i obavezu da stvaraju i ukidaju prostorne jedinice, kao i da donose i mijenjaju njihove nazive i oznake, moraju o tome obavijestiti administratora registra prostornih jedinica.

Registar poslovnih subjekata ili registar pravnih lica treba da bude integralan, a njihova identifikacija mora biti jedinstvena i pristup podacima obezbijeđen kroz jedinstveni interfejs, bez obzira što su nad različitim pravnim licima nadležni različiti organi državne uprave i lokalne samouprave.

Centralni registar stanovništva treba da obuhvati sva lica koja dolaze u kontakt i razmjenjuju lične informacije sa Crnom Gorom. Danas se ti podaci nalaze u matičnim knjigama rođenih, umrlih, vjenčanih i državljana, kao i drugim evidencijama za koje su nadležni različiti organi uprave. Pojedina lica nalaze se u jednom, nekoliko ili svim navedenim registrima i evidencijama.

Uredba o kancelarijskom poslovanju organa državne uprave ("Sl.list RCG", br.61/92) nije primjerena današnjem vremenu kada svi dokumenti u državnoj upravi nastaju u elektronskom obliku. Ta uredba je zasnovana na modelu koji ne poznaje pojam informacione bezbjednosti, kao ni minimalne bezbjednosne standarde na nacionalnom nivou. Sve to predstavlja ograničavajući faktor za aktuelnu informatizaciju javne uprave.

Kancelarijsko poslovanje predstavlja segment informacione bezbjednosti na nacionalnom nivou i mora biti usklađeno sa Nacionalnim programom informacione bezbjednosti. Zbog toga je neophodno donijeti novu Uredbu o kancelarijskom poslovanju, kojom bi se utvrdila obaveza čuvanja svih dokumenata i informacija u elektronskom obliku, kao i njihovo povezivanje elektronskim putem sa svim ostalim podacima u organima javne uprave, u skladu sa otvorenim standardima zapisa (npr. "Open Archive Initiative").

Plan aktivnosti usklađivanja sa Nacionalnim programom informacione bezbjednosti:

- Donošenje novih propisa o kancelarijskom poslovanju potrebno je uskladiti sa ovim programom u toku 2009. godine;
- Planiranje, odnosno preispitivanje koncepta državnih registara potrebno je sprovesti tokom 2008. godine (posebni ekspertski tim);
- Kroz harmonizaciju propisa sa EU potrebno je uskladiti Zakon o arhivskom poslovanju i Zakon o izdavačkoj djelatnosti tokom 2008. i 2009. godine (Ministarstvo kulture, sporta i medija, Državni arhiv).

3. Standardizacija u oblasti računarske i komunikacione tehnologije i informacione bezbjednosti

Razvoj informacionog društva pretpostavlja tehnološku podršku, u okviru koje se razlikuju aplikativna i infrastrukturna podrška. Tehnološki nivo potreban za iskorišćavanje potencijala informacionog društva ne može se postići ako se ne obezbijedi odgovarajuća interoperabilnost aplikativne i infrastrukturne podrške. Interoperabilnost je sposobnost informacionih i komunikacionih sistema i poslovnih procesa da podrže protok podataka i omoguće razmjenu informacija i znanja. Okvir interoperabilnosti čini skup normi, standarda i preporuka koji opisuju postignuti ili željeni dogovor zainteresovanih strana o načinu međupovezivanja. Taj okvir mora pratiti tehnološke, normativne i poslovne promjene.

Norme i standardi su dogovor zainteresovanih strana u okviru određene tehnološke oblasti. Predmet dogovora može biti različit, od opisa procesa do fizičkih svojstava nekog dijela opreme. S obzirom na tehnološki razvoj, norme i standardi se mijenjaju prateći i prilagođavajući se

razvoju tehnologije i potrebama korisnika. Međunarodne i nacionalne norme su dogovori koji su doneseni i potvrđeni u okviru ovlašćenog tijela za standardizaciju. Uz norme postoje obavezni, vlasnički i otvoreni standardi. Obavezni standardi su oni koji su zbog postojanja posebnog javnog interesa utvrđeni zakonom (npr.standardi u oblasti bezbjednosti proizvoda). Vlasnički standardi nastaju kada privatne kompanije stave na tržište raznorodne proizvode i kroz tržišnu utakmicu jedan ili više takvih proizvoda dostignu dominantnu poziciju, čime se uspostavi de fakto standard bez potvrde ovlašćenog tijela za standardizaciju. Vlasnici takvih standarda mogu postavljati ograničenja na primjenu standarda tako što zahtijevaju plaćanje naknade za njihovu primjenu ili ne omogućavaju pristup tehničkoj dokumentaciji standarda. Otvoreni standardi su oni koji su dostupni svima pod jednakim uslovima i bez plaćanja naknade, na način da su svi detalji tehničke dokumentacije standarda otvoreno dostupni i da je obezbijeđena trajna dostupnost svim verzijama standarda. Svaki subjekat može za potrebe svojih poslovnih procesa definisati sopstvene interne standarde.

Tradicionalni pristup standardizaciji kroz proces usklađivanja u tehničkim odborima i preuzimanja međunarodnih standarda (ISO, ITU, IEEE i druge) u oblasti informatičke i komunikacione tehnologije (ICT-a), pokazao se kao neadekvatan. Razlog je prvenstveno u izuzetnoj dinamici, ali i kompleksnosti ICT oblasti. Zbog toga se u oblasti ICT-a često javljaju određene nekonzistentnosti na nacionalnom nivou, u smislu nepokrivenosti pojedinih oblasti ili pak ograničenja i kolizije pojedinih standarda usljed brzog razvoja tehnologije.

Alternativni pristupi standardizaciji ICT-a u svijetu zasnivaju se na vlasničkim i otvorenim standardima. U modelu vlasničkih standarda određena interesna grupacija kompanija usaglašava nove ili preuzima privatne standarde pojedine kompanije. Takav pristup može dovesti do tržišne polarizacije, selektivnosti i netransparentnosti, ali i ograničenja tržišnog nadmetanja. Upravo iz navedenih razloga danas se u razvijenim zemljama, koje su u procesu stvaranja informacionog društva, naglašava važnost otvorenih standarda koji se razvijaju u okviru nekomercijalnih strukovnih organizacija i omogućavaju ravnopravan pristup tehničkoj dokumentaciji svim zainteresovanim stranama. Država u ovakvim procesima ima zadatak da stvara okvir i pretpostavke za efikasan proces nacionalne standardizacije, kao i podsticanje usvajanja otvorenih standarda i međunarodnih normi. Glavni subjekti u procesu standardizacije moraju biti privredni subjekti i državni stručni organi. Zbog toga i EU u okviru stvaranja informacionog društva kroz program eEurope 2005, ima poseban prateći program standardizacije. Cilj tog programa je koordinacija evropskih organizacija za standardizaciju (CEN, CENELEC, ETSI), podsticanje primjene otvorenih standarda i sistemska analiza postojećih standarda na području EU, sa ciljem preispitivanja i dopune standarda s aspekta potreba u oblasti ICT-a i informacione bezbjednosti, odnosno programa eEurope 2005.

Krajem 2003. godine u SAD-u je formiran široki program nacionalne standardizacije sa aspekta bezbjednosti u cjelini (ne samo za ICT oblast), tzv. ANSI-HSSP (American National Standards Institute – Homeland Security Standards Panel). Tu inicijativu prati i EU sa proširenim programom standardizacije zaštite i bezbjednosti stanovništva. Oba navedena programa standardizacije, u približno jednakom odnosu, obuhvataju oblast informacione bezbjednosti i tradicionalnu bezbjednosnu oblast civilne zaštite.

Osim na navedenom primjeru, značaj standardizacije informacione bezbjednosti ogleda se i kroz javne službe kao što je zdravstvo, odnosno kroz informatizacione procese zdravstva u razvijenim državama, koji se zasnivaju upravo na normama ICT-a i informacione bezbjednosti (programi SAD-a u okviru HIPAA zasnivaju se na standardizaciji ICT-a, podataka i informacionoj bezbjednosti). Navedeni procesi utiču i na tradicionalni proces međunarodne standardizacije, tako da je ISO (međunarodna organizacija za standardizaciju) pokrenula dugoročni program

Bezbjednosne tehnike u informacionoj tehnologiji (ISO/IEC JTC 1/SC27), koji ima za cilj da uspješnu strategiju standardizacije razvijenih zemalja usmjeri prema međunarodnoj standardizaciji.

Proces informacione bezbjednosti podrazumijeva dva povezana segmenta standardizacije. Prvi segment čini standardizacija samih informaciono-komunikacionih tehnologija (ICT), a drugi standardizacija bezbjednosnih tehnika ICT-a. Do sada formalna aktivnost u ovim područjima standardizacije u Crnoj Gori gotovo i nije postojala, ali su za 2008. godinu, u okviru nadležnosti novoosnovanog Instituta za standardizaciju, planirane značajne aktivnosti.

Proces standardizacije u Crnoj Gori sprovodi Institut za standardizaciju. Do kraja aprila 2007. godine posao standardizacionog tijela u Crnoj Gori obavljao je Centar za standardizaciju Crne Gore, od kada je sa radom započeo Institut za standardizaciju Crne Gore, saglasno Odluci Vlade RCG o osnivanju instituta za standardizaciju Crne Gore ("Sl.list RCG", br. 21/07).

Plan aktivnosti usklađivanja sa Nacionalnim programom informacione bezbjednosti:
Nakon osnivanja, tokom prve polovine 2009. godine, organ nadležan za bezbjednost informacionih sistema, posredstvom Instituta za standardizaciju Crne Gore, treba da se uključi u rad ISO/IEC pododbora za bezbjednosne tehnike u IT-u ISO/IEC JTC 1/SC27 u kojem djeluje niz susjednih država i država pristupnica u EU.

4. Interoperabilnost

Uspostavljanje interoperabilnosti na tehničkom, semantičkom i organizacionom nivou predstavlja bitan preduslov za efikasnu primjenu informacione i komunikacione tehnologije u složenim sistemima kakav je i državna uprava. Nezavisan i nekoordiniran razvoj, bez usvajanja tehničkih normi koje bi informacioni sistemi morali zadovoljavati, doveo je do toga da je tehnička interoperabilnost informacionih sistema različitih organa, a često i unutar jednog istog organa, u državnoj upravi problematična. Semantička interoperabilnost praktično ne postoji, jer još uvijek nijesu uvedeni standardi zapisa i značenja pojedinih podataka u informacionim sistemima. Radi uspostavljanja tehničke i semantičke interoperabilnosti aplikativnih rješenja u državnoj upravi biće neophodno definisati i sopstvene standarde za zapis i razmjenu podataka između organa državne uprave, kao i između privatnog sektora, odnosno stanovništva i državne uprave. Proces definisanja takvih standarda mora biti otvoren i uključivati sve zainteresovane strane iz javnog i privatnog sektora (dobavljače aplikacija i opreme, službenike i namještenike u državnoj upravi, interesna udruženja, akademsku zajednicu i dr.). Standardi državne uprave trebaju da budu otvoreni standardi, tj. javno dostupni svima bez naplate. Referentna lista normi i standarda mora biti dio tehničke dokumentacije za svaku nabavku robe, radova i usluga u oblasti primjene informacione i komunikacione tehnologije. U oblasti informacione bezbjednosti postavljaju se zahtjevi i na najvišem nivou interoperabilnosti-organizaciona interoperabilnost (koncepcija bezbjednosne politike i minimalnih bezbjedenosnih kriterijuma), naravno uz pretpostavku da su zadovoljena prva dva nivoa.

Za potrebe uspostavljanja interoperabilnosti koja je neophodna za razmjenu podataka unutar EU Evropska komisija je pokrenula program IDAbc u okviru kojeg se postavlja Evropski okvir za interoperabilnost i pokreću pilot projekti aplikacija za razmjenu podataka između organa uprave država članica EU. Posebna pažnja se poklanja uspostavljanju elektronskog identiteta i interoperabilnih sistema za identifikaciju i autorizaciju pristupa zajedničkim resursima.

5. Pregled ostalog zakonodavstva koje je u vezi sa informacionom bezbjednošću

Imajući u vidu karakteristike informacione bezbjednosti, koja kao i savremena informaciona i komunikaciona tehnologija zadire u sve pore društvenog života, razumljivo je da veliki broj oblasti ima dodirne tačke sa informacionom bezbjednošću. Cilj ovog programa je da identifikuje bitne segmente postojećeg zakonodavstva u Crnoj Gori koji su značajni za uspostavljanje nacionalnog sistema informacione bezbjednosti. To, s jedne strane, uključuje postojeće propise koji su koncepcijski neusklađeni sa savremenim društvenim procesima, a s druge strane, neke savremene elemente zakonodavstva Crne Gore koji nijesu do sada u praksi u potpunosti sprovedeni.

Prioritet ovog programa je da se po hitnom postupku inovira samo onaj dio propisa koji su smetnja uvođenju savremenog organizacionog modela informacione bezbjednosti u Crnoj Gori, saglasno međunarodnim, prvenstveno EU i NATO, standardima. Ostali propisi i praksa postupanja u nekim oblastima, koje su sa aspekta uvođenja informacione bezbjednosti manje važne, inoviraće se i usklađivati u okviru sveobuhvatnog procesa harmonizacije crnogorskog zakonodavstva sa zakonodavstvom EU, saglasno Nacionalnom programu za pridruživanje EU. Jedan od takvih primjera je Zakon o elektronskom potpisu ("Sl.list RCG", br. 55/03), čija će potpuna primjena biti moguća tek kada se obezbijede pretpostavke kojima se bavi ovaj program. Takođe, tu je i Zakon o telekomunikacijama ("Sl.list RCG", br. 59/00) koji je djelimično usklađen sa propisima EU u oblasti liberalizacije telekomunikacionog tržišta, zbog čega je taj postupak potrebno nastaviti donošenjem novog Zakona o elektronskim komunikacijama.

6. Institucionalni okvir

6.1. Savjet za odbranu i bezbjednost

Saglasno članu 131 Ustava Crne Gore ("Sl.list CG", br. 1/07), Savjet za odbranu i bezbjednost Crne Gore čine: predsjednik Crne Gore, predsjednik Skupštine i predsjednik Vlade. Predsjednik Crne Gore je predsjednik ovog savjeta.

Savjet za odbranu i bezbjednost je nadležan da:

- donosi odluke o komandovanju Vojskom Crne Gore;
- analizira i ocjenjuje bezbjednosnu situaciju u Crnoj Gori i donosi odluke za reduzimanje odgovarajućih mjera;
- postavlja,unapređuje i razrješava oficire Vojske;
- predlaže Skupštini proglašenje ratnog i vanrednog stanja;
- predlaže upotrebu Vojske u međunarodnim snagama;
- vrši i druge poslove utvrđene Ustavom ili zakonom.

6.2. Sekretarijat za razvoj

Sekretarijat za razvoj je organ uprave osnovan Uredbom o organizaciji i načinu rada državne uprave ("Sl.list RCG", br 54/04,...,32/07 i "Sl.list CG", br.6/07, 16/07 i 26/08). Saglasno članu 31 te uredbe Sekretarijat za razvoj, između ostalog, vrši poslove uprave koji se odnose na:

- pripremu i implementaciju nacionalne strategije razvoja informacionog društva;
- unapređenje, razvoj i funkcionisanje informacionog sistema organa državne uprave;
- uspostavljanje tehnološke i sigurnosne informatičke infrastrukture u državnim organima;
- racionalizaciju upotrebe informatičkih resursa u organima državne uprave;
- povezivanje informacionih sistema organa državne uprave;
- utvrđivanje tehničkih i drugih pravila upotrebe informatičke opreme u državnim organima;

- utvrđivanje stručnih i normativnih podloga za pridruživanje Crne Gore Evropskoj uniji u područjima razvoja i primjene informaciono-komunikacione tehnologije (e-Europe);
- obavljanje objedinjene nabavke informatičkih resursa i Internet servisa za organe državne uprave;
- vođenje Centralnog biračkog spiska;
- primjenu i sprovođenje propisa koji se odnose na elektronski potpis i vršenje nadzora nad primjenom tih propisa;
- druge poslove koji su mu određeni u nadležnost.

6.3. Direkcija za zaštitu tajnih podataka

U skladu sa članom 62 Uredbe o organizaciji i načinu rada državne uprave, Direkcija za zaštitu tajnih podataka počeće sa radom Inajkasnije 26.05.2008. godine. Saglasno članu 74 Zakona o tajnosti podataka i članu 44a navedene Uredbe, ta direkcija vrši poslove koji se odnose na:

- obezbjeđenje primjene standarda i propisa iz oblasti zaštite tajnih podataka;
- usvajanje plana zaštite tajnih podataka za vanredne i hitne slučajeve;
- organizovanje vršenja poslova organa u vezi sa razmjenom tajnih podataka sa stranim državama i međunarodnim organizacijama;
- organizovanje vršenja poslova koji se odnose na obezbjeđenje zaštite tajnih podataka koji su povjereni Crnoj Gori od strane drugih država i međunarodnih organizacija;
- informisanje strane države odnosno međunarodne organizacije o bezbjednosti stranih tajnih podataka koje je Crnoj Gori predala strana država, odnosno međunarodna organizacija;
- učestvovanje u izradi planova i programa Crne Gore za članstvo u međunarodnim organizacijama iz oblasti obezbjeđenja zaštite tajnih podataka;
- planiranje i ostvarivanje međunarodne saradnje u zaštiti tajnih podataka;
- predlaganje mjera za unaprjeđenje zaštite tajnih podataka;
- pokretanje inicijative za zaključivanje međunarodnih ugovora sa stranim državama i međunarodnim organizacijama iz oblasti tajnih podataka;
- sprovođenje postupka po zahtjevima za izdavanje dozvola za pristup tajnim podacima;
- izdavanje dozvola za pristup tajnim podacima i bezbjednosne dozvole za pristup tajnim podacima;
- organizovanje prijema i dostavljanja tajnih podataka korisnicima;
- razmjenu tajnih podataka sa stranim državama i međunarodnim organizacijama;
- preduzimanje mjera radi obukekorisnika tajnih podataka i organa za postupanje sa tajnim podacima u skladu sa standardima i propisima;
- vođenje evidencije o izdatim dozvolama za pristup tajnim podacima;
- izradu i vođenje Centralnog registra tajnih podataka i tajnih podataka strane države ili međunarodne organizacije;
- druge poslove koji su joj određeni u nadležnost.

6.4. Centar informacionog sistema Univerziteta Crne Gore

Centar informacionog sistema Univerziteta Crne Gore (CIS) bavi se razvojem, izgradnjom i održavanjem računarsko-komunikacione infrastrukture koja povezuje akademske i naučno-istraživačke ustanove u Crnoj Gori u jedinstveni informatički sistem. CIS je komunikaciono čvorište akademske mreže Univerziteta Crne Gore (UCG), akademski Internet provajder i razvojni centar kompletnog aplikativnog softvera informacionog sistema UCG. Takođe, CIS je operativno tijelo MRENA-a (Montenegro Research and Education Network), član evropske asocijacije akademskih mreža TERENE (Trans-European Research and Education Networking Association) i koordinator dva međunarodna projekta koje finansira EC u okviru FP6 (SEEREN2 i SEE-GRID2). Jednom riječju, CIS je od strane crnogorske i evropske javnosti prepoznat kao ICT institucija koja održava i unapređuje akademsku mrežu i servise na nacionalnom nivou.

Sa proglašenjem nezavisnosti Crna Gora je stekla pravo na korišćenje resursa međunarodnih kodova koje dodjeljuju određene međunarodne organizacije. Radi upravljanja internet domenom prema pravilima koja propisuje svjetska internet zajednica bilo je neophodno obrazovati tijela koja će pratiti i realizovati sve aktivnosti vezane za implementaciju domena. U tom smislu, Vlada Republike Crne Gore, zaključkom sa sjednice od 30.11.2006. godine, odredila je CIS za administratora nacionalnog internet domena ".ME".

7. Infrastrukturni okvir

Nacionalna politika informacione bezbjednosti i njeni sprovedbeni akti, trebaju da obezbijede sistemski pristup svim segmentima vitalne državne infrastrukture, pa i onim segmentima koji se iznajmljuju od telekomunikacionih (TK) operatora ili davaoca Internetskih usluga. Liberalizacija telekomunikacija u Crnoj Gori, iako postepeno, vodi ciljevima kao što su tržišno nadmetanje i deregulacija, ali donosi i niz pratećih bezbjednosnih problema. Jedan od značajnijih je intencija inostranih vlasnika TK operatora za udaljenim, prekograničnim upravljanjem TK mrežama, čime se za vlasnika smanjuju troškovi, ali se ugrožava nacionalna bezbjednost. Značajan problem predstavlja i ekstrateritorijalni Internet saobraćaj koji se događa i unutar nacionalne komunikacije.

Posljedica takvog stanja je mogućnost da poruka poslata e-poštom na odredište unutar istog grada, prije konačnog odredišta, pređe jednu ili više državnih granica. To iz razloga što je moguće da TK operator ili davalac internet usluga, koji ima podružnice u više susjednih država, ima privatne vodove koji povezuju te podružnice i u određenom trenutku može mu se isplatiti da centralizuje sistem u samo jednoj od tih država. Sa daljom liberalizacijom tržišta u međunarodnom javnom govornom prometu, slična situacija može se očekivati i u telefoniji, prvenstveno mobilnoj. Cilj bezbjednosne procjene informaciono-komunikacionih projekata javne uprave je da prepozna i izbjegne takve rizike, dok je zadatak nacionalne politike informacione bezbjednosti da postavi ciljeve koji će omogućiti razvoj mehanizama zaštite i prevencije (regulativnih, organizacionih i/ili tehničkih) od rizika, na dobrobit svih subjekata informacionog društva – stanovništva, privrede i države u cjelini. Jedan od značajnih problema koji treba strateški riješiti kroz nacionalnu politiku informacione bezbjednosti je i pristup telekomunikacionoj infrastrukturi u Crnoj Gori. To pretpostavlja jasno definisanje vlasništva nad postojećim telekomunikacionim kanalima i vodovima u Crnoj Gori, postojanje strategije korišćenja takvih vodova od strane organa javne uprave, kao i poštovanje određenih bezbjednosnih pravila za sve privatne vlasnike infrastrukture. Uz TK kanale i vodove, koji su u vlasništvu bivšeg državnog TK operatora, postoji i kablovska infrastruktura u vlasništvu privatnih kompanija, koju je potencijalno moguće koristiti za projekte kao što je Računarsko-komunikaciona mreža organa javne uprave.

Vlada Republike Crne Gore sa TK operatorom (Crnogorski telekom) ima zaključena dva ugovora o korišćenju TK infrastrukture, od kojih jedan o ustupanju kapaciteta u optičkom kablu za period od 20 godina i drugi o korišćenju VPN servisa za period od četiri godine.

Donošenje nacionalne politike informacione bezbjednosti jedan je od najboljih načina kako savremena država može postepeno i sistemski riješiti navedene probleme. Primjena informacione i komunikacione tehnologije danas predstavlja jedan od osnovnih preduslova za povećanje efikasnosti u poslovanju, kako u privatnom sektoru, tako i u organima javne uprave. Međutim, tehnologija nije i ne može biti sama sebi svrha. Informaciona tehnologija treba, prije svega, da bude osnova i stimulans za restrukturiranje poslovnih procesa u organima javne uprave i međusobnu koordinaciju tih organa.

Svaki informacioni sistem treba da se postepeno i sistemski nadograđuje i kvalitetno održava kroz cijeli životni ciklus, u svakoj svojoj fazi od inicijalizacije i idejnog projekta, preko razvoja, implementacije, korišćenja pa sve do rashodovanja. Bezbjednosna procjena mora biti dio svih tih faza životnog ciklusa. Izgradnja Računarsko-komunikacione mreže organa javne uprave neophodna je za ostvarivanje elektronskih usluga za stanovništvo i poslovne subjekte, kao i za međusobno povezivanje organa javne uprave.

Bezbjednosna procjena projekta Računarsko-komunikacione mreže organa javne uprave nije moguća sve do potpunog uspostavljanja sistema informacione bezbjednosti u Crnoj Gori, što predstavlja dodatni razlog za ubrzano uspostavljanje tog sistema.

IV - PODJELA NADLEŽNOSTI U ODNOSU NA PODATKE I INFORMACIONU INFRASTRUKTURU U CRNOJ GORI

1. Opšta razmatranja

Savremeni sistem informacione bezbjednosti pretpostavlja jasno određivanje nadležnosti pojedinih organa koji upravljaju tom kompleksnom organizacijom. Pri tome je neophodno izvršiti razdvajanje nadležnosti između ključnih funkcionalnosti u sistemu informacione bezbjednosti, postići organizacionu i tehničku kompetentnost svih organa u upravljačkom lancu informacione bezbjednosti, kao i uskladiti odgovarajuće propise na nacionalnom nivou. Ovaj program daje načelne kriterijume i preporuke za organizacioni model sistema informacione bezbjednosti, ali tek sa donošenjem neophodnih dokumenata i početkom rada ključnih organa, u Crnoj Gori stvoriće se uslovi za postupanje i stvarne promjene u ovoj oblasti.

Sistem informacione bezbjednosti posmatran s aspekta savremene javne uprave, pretpostavlja podjelu najmanje na dvije grupe organa javne uprave i pravnih lica. U principu, to bi mogli biti organi javne uprave i privatni sektor. Razlog za obrazovanje više grupa nalazi se prvenstveno u bitno različitom tretmanu informacione bezbjednosti u svakoj pojedinoj grupi (ciljevi, potrebe, zahtjevi), ali i bitno različitom konceptu pravnog regulisanja oblasti informacione bezbjednosti unutar tih grupa.

U Crnoj Gori sistem informacione bezbjednosti je najracionalnije primijeniti sprovođenjem različitih aktivnosti i mjera u okviru dvije grupe - organima javne uprave i pravnim licima. Grupa pravnih lica sastoji se od privatnog sektora u širem smislu, odnosno tu se svrstavaju ostala pravna lica i sva privredna društva, bez obzira na tip vlasništva (privatno, državno ili mješovito) ili osnivača.

Pored propisivanja minimalnih kriterijuma, država dodatno može obrazovati posebne grupe pravnih lica, prvenstveno s aspekta nacionalne bezbjednosti. Takve posebne grupe država određuje na osnovu procjene kritične nacionalne infrastrukture u smislu opasnosti od terorizma, rata i svih potencijalnih rizika za nacionalnu bezbjednost. Proces određivanja kritične nacionalne infrastrukture odvija se u okviru sistema nacionalne bezbjednosti, a spisak kritične nacionalne infrastrukture redovno se objavljuje u okviru strategije nacionalne bezbjednosti i treba da bude dostupan javnosti. Savjet za odbranu i bezbjednost može, na predlog nadležne bezbjednosne službe usklađen sa nadležnim ministarstvom, odrediti posebnu grupu organa i kompanija iz bilo koje od navedenih grupa, čija je djelatnost od vitalnog značaja za određenu kritičnu nacionalnu infrastrukturu (npr. elektroenergetski sistem). Za takvu posebnu grupu najčešće se uz niz drugih mjera, utvrđuje i poseban skup minimalnih kriterijuma informacione bezbjednosti, u saradnji nadležnih organa bezbjednosnog sistema, nadležnog ministarstva i predstavnika pravnih lica koja spadaju u određenu posebnu grupu. Razlika u odnosu na grupu pravnih lica je u tome što se tu minimalni bezbjednosni kriterijumi postavljaju nezavisno od saglasnosti samih pravnih lica na koje će se oni odnositi, ali se svima na koje se takvi kriterijumi odnose pruža mogućnost aktivnog učestvovanja u definisanju takve posebne politike i sprovedbenih akata informacione bezbjednosti.

Da bi se definisao sistem upravljanja informacionom bezbjednošću na nacionalnom nivou, neophodno je za svaku od navedenih grupa utvrditi nekoliko osnovnih kategorija kao što su: vlasnici podataka, vlasnici informacione infrastrukture, posebni propisi informacione bezbjednosti koji uređuju tu grupu, kao i nadležne organe u upravljanju informacionom bezbjednošću u svakoj od tih grupa.

Vlasnici podataka odgovorni su za sve radnje sa podacima u njihovoj nadležnosti, tokom životnog ciklusa podataka, kao i za planiranje i implementaciju organizacionih i tehničkih mjera, u skladu sa važećim propisima informacione bezbjednosti i svojom nadležnošću. Pri tome, radnje sa podacima podrazumijevaju nastajanje, obrađivanje, skladištenje i arhiviranje podataka.

Informaciona infrastruktura obuhvata svu infrastrukturu u određenom organu javne uprave ili pravnom licu koja na bilo koji način utiče na osnovna svojstva povjerljivosti, dostupnosti ili cjelovitosti podataka i u okviru koje podaci nastaju, obrađuju se ili skladište. Vlasnici informacione infrastrukture su odgovorni za tu infrastrukturu tokom njenog životnog ciklusa, kao i za planiranje i implementaciju organizacionih i tehničkih mjera, u skladu sa važećim propisima informacione bezbjednosti i svojom nadležnošću.

S obzirom na stanje informacione bezbjednosti u Crnoj Gori i potrebe prikazane u ovom programu, neophodno je na početku ovog procesa donijeti Zakon o informacionoj bezbjednosti, koji će predstavljati krovni dokument za uspostavljanje organizacione strukture informacione bezbjednosti u obje grupe. U skladu sa tim zakonom, u okviru razrade pravnog okvira nižim podzakonskim aktima informacione bezbjednosti treba uvažiti specifičnosti, potrebe i zahtjeve organa javne uprave i pravnih lica.

Zakonom o informacionoj bezbjednosti treba da se utvrde nadležnosti i djelokrug upravljačkih organa u sistemu informacione bezbjednosti, kako bi se moglo pristupiti izradi cjelovitog sistema propisa o informacionoj bezbjednosti. Pri tome, biće neophodno donijeti niz novih i inovirati neke postojeće propise u Crnoj Gori. Uz Zakon o informacionoj bezbjednosti biće neophodno donijeti nacionalnu strategiju ili politiku informacione bezbjednosti, kao osnovni krovni dokument u kojem se definišu osnovna bezbjednosna načela, oblasti i obim primjene, kao i mjere nadležnih organa u sprovođenju informacione bezbjednosti. Svi ostali dokumenti informacione bezbjednosti (uredbe, pravilnici, uputstva, smjernice i sl.), bez obzira na koju grupu organa javne uprave i pravnih lica se primjenjuju, moraju biti potpuno usklađeni sa Zakonom o informacionoj bezbjednosti i nacionalnom strategijom ili politikom informacione bezbjednosti. Na taj način obezbjeđuje se konzistentnost cjelokupnog sistema informacione bezbjednosti u Crnoj Gori.

Sistem informacione bezbjednosti neposredno zavisi od poslovnih procesa u pojedinim organima javne uprave i pravnim licima. S obzirom na česte promjene i prilagođavanja poslovnih procesa, koje su uslovljene brzim razvojem tehnologije i globalizacijom, sistem informacione bezbjednosti mora upravljati promjenama statusa i pripadnosti pojedinih organa i pravnih lica određenim grupama u smislu informacione bezbjednosti. Odluku o tome najčešće donosi Centralno državno bezbjednosno tijelo (NSA), a to važi i za slučaj uključivanja novih organa u sistem informacione bezbjednosti.

2. Organi javne uprave

Odgovornost vlasnika podataka u organima javne uprave mora biti jasno utvrđena i stavljena u nadležnost starješine svakog pojedinog organa javne uprave. Pri tome ta odgovornost podrazumijeva rukovodnu odgovornost za uspostavljanje potrebnih procedura i organizacionu kontrolu funkcionisanja i usklađenosti tih procedura informacione bezbjednosti. Pored starješine, koji predstavlja najodgovornije lice za organizaciju informacione bezbjednosti, takva organizacija mora unutar organa utvrditi izvršnu odgovornost rukovodne hijerarhije i svakog službenika i namještenika posebno.

Vlasnici informacione infrastrukture u organima javne uprave vode brigu o informaciono-komunikacionoj opremi tokom cjelokupnog životnog ciklusa opreme (planiranje, projektovanje, nabavka, opremanje, upravljanje, održavanje, rashodovanje, uništavanje). Vlasnici informacione infrastrukture su najčešće sami organi javne uprave, ali ta odgovornost može biti prenesena na određene unutrašnje organizacione jedinice tehničkog profila. Za organe javne uprave koji nemaju adekvatne organizacione jedinice moguće je da Sekretarijat za razvoj, kao organ uprave nadležan za proces informatizacije državne uprave, bude nosilac organizacione i nadzorne odgovornosti vlasnika informacione infrastrukture u takvim organima.

Zahtjevi koji se odnose na upravljačke organe za organe javne uprave postavljeni su kroz bezbjednosnu politiku EU i NATO-a, i danas su na ovakav način organizovani sistemi informacione bezbjednosti u skoro svim razvijenim državama svijeta. Poštovanjem takvih zahtjeva postiže se organizaciona interoperabilnost, koja za svaku državu ima veoma veliku važnost u međunarodnoj saradnji i integracionim procesima. Zbog toga je neophodno organizaciju informacione bezbjednosti u Crnoj Gori prilagoditi međunarodnim standardima, ali istovremeno i zadržati dio nadležnosti uspostavljenih u nacionalnom zakonodavstvu, koji je usklađen sa konceptom informacione bezbjednosti.

2.1. NSA (National Security Authority)

NSA (National Security Authority) ili centralno državno bezbjednosno tijelo je uobičajeno krovno ili koordinaciono tijelo bezbjednosnog sistema. U Crnoj Gori to treba da bude Direkcija za zaštitu tajnih podataka . Saglasno Zakonu o tajnosti podataka ta direkcija obavlja i funkciju NDA (National Distribution Authority) ili Centralnog distribucionog tijela za povjerljive materijale NATO-a.

Konačno određivanje organa koji bi preuzeo funkcionalnost zajedničkog NSA unutar Crne Gore i početak rada tog organa od presudne je važnosti za Crnu Goru. NSA je inicijator aktivnosti u cjelokupnom sistemu informacione bezbjednosti i nosilac izrade nacionalne politike informacione bezbjednosti, kao strateškog dokumenta koji inicira sve naredne regulacione procese iz oblasti informacione bezbjednosti jedne države.

NCSA (National Comunications Security Authority) ili Centralno tijelo za bezbjednost komunikacija, kao i SAA (Security Acreditation Authority) ili Centralno državno tijelo za bezbjednosne akreditacije, uobičajeno predstavljaju tehničko tijelo bezbjednosnog sistema. Funkcije NCSA i SAA u slučaju Crne Gore treba da obavlja Direkcija za zaštitu tajnih podataka. Zbog značajnog obima poslova i povećanja efikasnosti u procesu bezbjednosnih akreditacija, uobičajeno je da se od strane centralnog SAA akredituju lokalni SAA za pojedine specifične nacionalne programe.

Da bi Direkcija za zaštitu tajnih podataka mogla imati nadležnosti u okvirima informacione bezbjednosti i ispuniti očekivanja ovog programa neophodno je, nakon donošenja Zakona o informacionoj bezbjednosti, kroz inoviranje Uredbe o organizaciji i načinu rada državne uprave, proširiti njen djelokrug kojim bi bile obuhvaćene funkcionalnosti informacione bezbjednosti saglasno zahtjevima integracionih procesa EU i NATO, i to:

- funkcionalnost Direkcije kao centralnog državnog tijela za bezbjednost komunikacija (NCSA);
- funkcionalnost Direkcije kao centralnog državnog tijela odgovornog za rukovođenje kriptomaterijalima (NDA);
- funkcionalnost Direkcije kao centralnog državnog tijela za bezbjednosne akreditacije informaciono- komunikacionih sistema (SAA).

Akreditacioni proces podrazumijeva akreditovanje informaciono-komunikacionih procesa na određeni vremenski period (najčešće 2 do 4 godine) i kasnije redovno obnavljanje akreditacionog procesa. Uz proces bezbjednosnih akreditacija, izuzetno je važan operativni nadzor mjera informacione bezbjednosti (CIS Operating), koji sprovode bezbjednosne službe, u skladu sa nadležnostima utvrđenim zakonom. Operativni nadzor se sprovodi nad organima javne uprave koji su akreditovani za rad. Kroz taj nadzor se prati poštovanje propisanih procedura, kao i planiranje i upravljanje promjenama u sistemu, koje se neminovno događaju u toku redovnog rada sistema, bilo zbog tehnoloških ili organizacionih promjena. U organima javne uprave veoma je važno poštovati načelo razdvajanja nadležnosti, pa je potrebno operativni nadzor u potpunosti razdvojiti od procesa planiranja i implementacije. Proces planiranja i implementacije metoda i mjera informacione bezbjednosti (CIS Planning & Implementation) redovno obavlja vlasnik informacione infrastrukture.

2.2. CERT arhitektura

Radi preventivnog djelovanja i efikasne koordinacije prilikom rješavanja računarskih bezbjednosnih incidenata na Internetu, neophodno je uspostaviti hijerarhijski organizovanu infrastrukturu CERT timova sa centralnim državnim CERT-om kao vrhovnim koordinacionim organom.

Organi javne uprave najčešće imaju posebni koordinacioni CERT, čiju funkciju u Crnoj Gori treba da obavlja Sekretarijat za razvoj. Uz to mogu se radi efikasnosti organizovati CERT-ovi u okviru specifičnih ministarstava kao što su Ministarstvo odbrane i Ministarstvo unutrašnjih poslova i javne uprave.

Članovi ove hijerarhijske infrastrukture su i CERT-ovi ili slična organizaciona tijela koja uspostavljaju davaoci Internetskih usluga, TK operatori, finansijske institucije i druge kompanije koje imaju interes ili značajan uticaj na funkcionisanje nacionalne informacione infrastrukture.

Tako uspostavljena hijerarhija treba da omogući razmjenu informacija o računarskim bezbjednosnim problemima, blagovremena upozorenja o računarsko-bezbjednosnim rizicima i efikasnu komunikaciju u istragama i rješavanju računarsko-bezbjednosnih incidenata, kako u Crnoj Gori, tako i sa odgovarajućim inostranim organima. Isto tako, potrebno je usaglasiti zajedničke promotivne i edukativne djelatnosti, kako za pojedine grupe korisnika, tako i za najširu grupu korisnika koji imaju pristup računarskim mrežama.

Centralni državni CERT treba uspostaviti posebnim aktom, obezbijediti mu potrebne resurse i dati ovlašćenja, kako bi mogao vršiti sljedeće poslove:

Uspostavljanje nacionalne CERT infrastrukture. Veoma je značajno uspostaviti nacionalnu strukturu CERT-ova unutar relevantnih ustanova i privatnih pravnih lica i obezbijediti njihovo koordinirano djelovanje. Centralni državni CERT treba da utvrdi pravila i način rada nacionalne CERT infrastrukture, kao i da radi na podsticanju uspostavljanja te infrastrukture:

- podsticanje i pomoć prilikom uspostavljanja ostalih CERT-ova u nacionalnoj CERT infrastrukturi, kroz saradnju sa upravom, savjetovanje i edukaciju zaposlenih – članova CERT-ova;
- pomoć pri uključivanju ostalih CERT-ova u međunarodne organizacije i udruženja CERT-ova;
- definisanje osnovnih potrebnih funkcionalnosti CERT-ova, njihove međusobne komunikacije, kao i odnosa prema Centralnom državnom CERT-u (izvještavanje, razmjena informacija između CERT-ova i sa drugim relevantnim tijelima van Crne Gore);

- koordinacija zajedničke saradnje sa ostalim relevantnim organima javne uprave.

Reagovanje na ozbiljne bezbjednosne incidente. U slučaju događanja značajnih incidenata ili incidenata koji prelaze okvire djelovanja pojedinih CERT-ova:

- koordiniranje rješavanja bezbjednosnih incidenata koji svojim obimom ili tipom ugrožavaju funkcionisanje Interneta ili moguće za život opasne aktivnosti;
- koordiniranje rješavanja incidenata koji ne spadaju u nadležnost ni jednog od ostalih CERT-ova, a bar jedna od uključenih strana je iz Crne Gore.

Prevencija računarsko-bezbjednosnih incidenata. Podrška podizanju opšteg nivoa računarske bezbjednosti u organima javne uprave, pravnim licima i najširem krugu korisnika:

- informisanje javnosti o značaju i unapređenju računarske bezbjednosti kroz izdavanje edukativnih materijala i javno djelovanje;
- informisanje stručne javnosti i ostalih CERT-ova kroz savjetovanje, izdavanje stručnih materijala i blagovremenih upozorenja o ranjivostima računarskih sistema;
- organizacija i sprovođenje akcija i postupaka koje će upozoriti na postojeće propuste u računarsko-komunikacionoj infrastrukturi, a koji mogu biti iskorišćeni za ugrožavanje njenog funkcionisanja i davanje preporuka o načinu uklanjanja tih propusta.

Polazeći od dosadašnjeg djelovanja, stečenih znanja i iskustva, funkciju Centralnog državnog CERT-a treba staviti u nadležnost CIS-u. Na taj način se može obezbijediti njegovo brzo uspostavljanje, uz optimalno ulaganje resursa. Za uspostavljanje i funkcionisanje Centralnog državnog CERT-a potrebno je obezbijediti finansijske i druge resurse, koji će omogućiti njegovo efikasno djelovanje.

3. Pravna lica

Odgovornost vlasnika podataka u grupi pravnih lica mora biti uvijek jasno utvrđena i stavljena u nadležnost uprave kompanije. Takvo postavljanje odgovornosti u osnovi je svih savremenih zakona iz oblasti korporativnog upravljanja, kao i normi i preporuka za informacionu bezbjednost poslovanja kompanija. Pri tome, ta odgovornost podrazumijeva rukovodnu odgovornost za uspostavljanje potrebnih procedura informacione bezbjednosti i organizacionu kontrolu rada i usklađenosti tih procedura. Uz upravu kompanije, koja predstavlja nosioca odgovornosti za organizaciju informacione bezbjednosti, takva organizacija mora unutar kompanije definisati izvršnu odgovornost rukovodne hijerarhije i svakog zaposlenog.

Vlasnici informacione infrastrukture u grupi pravnih lica dužni su da se staraju o informaciono-komunikacionoj opremi tokom cjelokupnog životnog ciklusa opreme (planiranje, projektovanje, nabavka, opremanje, upravljanje, održavanje, rashodovanje, uništavanje). Pri tome će primjenjivati aktuelne propise koje donose nadležni organi javne uprave i pravilnike o poslovanju same kompanije.

S obzirom da u grupu pravnih lica spadaju kompanije sa različitom kombinacijom osnivača i vlasništva (privatno, državno ili mješovito), kao i neke infrastrukturne kompanije (elektroprivreda, komunalna preduzeća, željeznica, itd.), koje su u procesu privatizacije ili to mogu biti u budućnosti, najčešće se primjenjuje sličan tretman i kod takvih pravnih lica. U tom smislu Elektroprivreda, kao još neprivatizovana kompanija, sa svojom TK infrastrukturom može biti osnova za razvoj mreže organa javne uprave. To znači da organi državne uprave, nakon ulaska u proces informacione bezbjednosti organa javne uprave, trebaju da predlože idejni koncept javno-privatnog partnerstva u informacionoj bezbjednosti. Takvo javno-privatno partnerstvo ima za cilj da u procesu informacione bezbjednosti aktivira i sve ostale nedržavne

resurse, na dobrobit svih subjekata informacionog društva, ali i u cilju prosperiteta države u cjelini (konkurentnost i imidž države u svijetu).

Cilj javno-privatnog partnerstva je da usaglasi pristup bezbjednosnoj politici u grupi pravnih lica, odnosno između državnog, javnog i privatnog sektora. Rezultat javno-privatnog partnerstva može biti niz formalnih mjera (zakoni, standardi, sporazumi i sl.), ali i neformalnih koordiniranih postupaka u različitim sektorima čitavog društva (popularizacija, edukacija, programi, akcije i sl.). Inicijativu javno-privatnog partnerstva treba zasnivati na iskustvima u organizaciji informacione bezbjednosti u grupi organa javne uprave, kao i predloga nadležnih organa iz te grupe.

V - BEZBJEDNOSNA POLITIKA

1. Opšta razmatranja

Pod bezbjednosnom politikom podrazumijeva se hijerarhijski uređen skup dokumenta informacione bezbjednosti, koji predstavlja osnovu za implementaciju sistema informacione bezbjednosti. Uopšte, dokumenti bezbjednosne politike mogu se podijeliti na krovne, sprovedbene i izvršne, kao i na standarde i preporuke.

Bezbjednosnom politikom obezbjeđuje se uvođenje prije svega minimalnih, a zatim i neophodnih bezbjednosnih kriterijuma. Za organe javne uprave, to je i jedan od osnovnih zahtjeva integracionih procesa NATO-a i EU. U okviru bezbjednosne politike ostalih subjekata, koristi se samo manji dio nacionalnog zakonodavnog okvira propisanog za organe javne uprave, a u većoj mjeri se oslanja na svjetski priznate organizacione i bezbjednosne standarde (npr. ISO 27001), kao i iskustva u javno-privatnom partnerstvu u oblasti informacione bezbjednosti.

1.1. Krovni dokumenti

U ovu vrstu dokumenata svrstavaju se zakoni, strategije ili politike kojima se informaciona bezbjednost razmatra na opštem nivou, ne ulazeći u detalje njene implementacije. Krovni dokumenti sadrže definiciju informacione bezbjednosti, njene ošte ciljeve i razmjere i nemaju cilj opisivanje stanja, već donošenje odluka o podršci ciljevima informacione bezbjednosti. Ti dokumenti treba da budu precizni, jasni i uravnoteženi između funkcionalnosti i bezbjednosti. Sa njima trebaju da se upoznatju svi subjekti na koje se ti dokumenti odnose. Krovni dokumenti, između ostalog, podrazumijevaju i definisanje odgovornosti za upravljanje i sprovođenje informacione bezbjednosti. Najčešće se zajednički krovni dokument informacione bezbjednosti uređuje zakonom. Prateći krovni dokument Zakona o informacionoj bezbjednosti treba da bude nacionalna strategija ili politika informacione bezbjednosti, koja definiše osnovne bezbjednosne principe, oblasti i obuhvat. Pored navedenih krovnih dokumenata u kompanijama treba da postoje i krovni dokumenti bezbjednosne politike koje donosi uprava kompanije.

1.2. Sprovedbeni dokumenti

Sprovedbenim dokumentima vrši se razrada krovnih dokumenata na pojedine bezbjednosne oblasti, kao što su bezbjednosna provjera lica, fizička bezbjednost, bezbjednost podataka i INFOSEC-a, kao i dalja razrada tih bezbjednosnih oblasti na organizaciono tehničke specifikacije kojima se uređuju metode upravljanja bezbjednošću u pojedinim oblastima i razrađuju formalni postupci procjene rizika, certifikovanja lica i opreme i akreditacije.

Sprovedbeni propisi se najčešće donose kao uredbe i pravilnici. Pravilnicima se vrši razrada pojedinih elementa sistema i daju opšte organizaciono tehničke smjernice. Organi javne uprave koji imaju specifične bezbjednosne potrebe (MUPJU, MO i sl.) mogu umjesto sprovođenja nacionalnih pravilnika koji definišu minimalne bezbjednosne kriterijume donijeti vlastite pravilnike. U tom slučaju saglasnost na primjenu takvih pravilnika daju NSA i NCSA. Saglasnost se daje nakon utvrđivanja da predloženi pravilnik zadovoljava minimalne bezbjednosne kriterijume postavljene na nacionalnom nivou. Uputstva za sprovođenje Pravilnika izrađuje svaki organ javne uprave za sebe, kako u slučaju primjene nacionalnog pravilnika, tako i u slučaju primjene vlastitog pravilnika.

U sprovedbene dokumente kompanija spadaju opšte organizacione politike kao analogija uredbama, odnosno funkcionalne politike kao analogija pravilnicima. Te dokumente donosi uprava kompanije, na predlog menadžmenta kompanije nadležnog za bezbjednost.

1.3. Izvršni dokumenti

Izvršni dokumenti predstavljaju razradu sprovedbenih dokumenata i to u vidu uputstava koja kao posljednja u lancu egzaktno opisuju način na koji je potrebno implementirati postojeće pravilnike i funkcionalne politike. Najčešće, izrada uputstava koja se odnose na tehnologiju spada u nadležnost IT struktura, izrada uputstava vezanih za procese i organizaciju u nadležnost upravljačkih struktura, a izrada uputstava vezanih za zaposlene u nadležnost struktura za upravljanje ljudskim resursima. Prilikom izrade tih uputstava treba da se koriste utvrđeni elementi bezbjednosne politike i sprovedbenih akata, raspoložive preporuke i tzv. metode najbolje prakse u pojedinom organizacionom ili tehničkom procesu.

1.4. Standardi

Standard je dokument odobren od nadležnog tijela koji za opštu i višekratnu upotrebu daje pravila, uputstva ili karakteristike za aktivnosti i njihove rezultate i garantuje najbolji stepen uređenosti u datim uslovima. U oblasti informacione bezbjednosti, standardi predstavljaju rješenje zajedničkih potreba za jedinstvenim sistemom upravljanja bezbjednošću informacija. Poslovanje u skladu sa standardima omogućava pouzdano upravljanje informacionom bezbjednošću i stvara povjerenje u međusobnom poslovanju. Takvi poslovni standardi mogu postati i nacionalne standardi. U tom smislu organi državne uprave u koordinaciji sa privatnim sektorom treba da pokreću inicijative za usvajanje i primjenu međunarodnih organizaciono-tehničkih standarda informacione bezbjednosti kroz nacionalne standardizacione procese. Da bi opšti tehnički i bezbjednosni standardi, koji su prihvaćeni u okviru nacionalnih standardizacionih procesa, postali dio bezbjednosne politike, moraju biti utvrđeni odgovarajućim propisima unutar grupe organa javne uprave ili grupe pravnih lica na koju se odnose.

1.5. Preporuke

Preporuke definišu preporučene načine zaštite sistema. Implementacija mjera definisanih preporukama poželjna je ali ne i obavezna, što preporuke čini fleksibilnim elementom u primjeni bezbjednosne politike. Preporuke se najčešće koriste na onim mjestima gdje bezbjednost nije moguće, potrebno ili poželjno strogo definisati.

2. Bezbjednosna politika u organima javne uprave

Bezbjednosna politika koja se odnosi na organe javne uprave sastoji se od Zakona o informacionoj bezbjednosti, nacionalne strategije ili politike informacione bezbjednosti i sprovedbenih uredbi, koje se dalje razrađuju pravilnicima i detaljnim procedurama.

Nacionalnu politiku informacione bezbjednosti, kao krovni dokument, treba da donosi Skupština Crne Gore i njime se izražava odlučnost u podršci ciljevima informacione bezbjednosti. Donošenje takvog dokument je neophodno, jer se njime obezbjeđuje ujednačeno bezbjednosno postupanje od strane različitih organa javne uprave sa ciljem uvođenja minimalnih bezbjednosnih kriterijuma jedne države. Na osnovu tog dokumenta pokreće se proces izrade sprovedbenih akata (uredbi) koje donosi Vlada Crne Gore i koji obavezuju sve organe javne uprave. Ti sprovedbeni akti predstavljaju osnovu kasnijih inicijativa koje se odnose na grupu pravnih lica, odnosno državu u cjelini.

Razrada uredbi vrši se kroz organizaciono tehničke smjernice u formi obavezujućih pravilnika koje donose nadležni organi bezbjednosnog sistema, saglasno ovlašćenjima utvrđenim zakonom (nacionalni pravilnici) ili pravilnika koje donose sami organi (vlastiti pravilnici), kao i detaljnih uputstava usklađenih sa propisima, koja donose sami organi.

3. Bezbjednosna politika u pravnim licima

Na grupu pravnih lica se najčešće utiče kroz norme i otvorene standarde prihvaćene u okviru nacionalnih, ali i međunarodnih standardizacionih procesa. Takođe, uobičajeno je da država vrši uticaj na organizaciju i sprovođenje informacione bezbjednosti kroz određene oblike javno-privatnog partnerstva i traženja zajedničkih ciljeva države i privatnih kompanija, čime se postiže ujednačavanje nivoa informacione bezbjednosti između organa javne uprave i pravnih lica, odnosno društva u cjelini. Na obaveze i nadležnosti u pogledu informacione bezbjednosti unutar pravnih lica država može uticati i kroz Zakon o informacionoj bezbjednosti, kao i kroz nacionalnu strategiju ili politiku informacione bezbjednosti.

Dokumenti bezbjednosne politike koji se odnose na pravna lica , odnosno privatni sektor su: krovni dokumenti bezbjednosne politike (zakon i nacionalna strategija, bezbjednosna politika uprave kompanije), detaljne bezbjednosne politike (opšte organizacione i funkcionalne politike) i procedure. Osnovni element politike je odluka koju donosi uprava, a kojom se izražava odlučnost uprave u podršci ciljevima informacione bezbjednosti.

VI - EDUKACIJA I RAZVOJ BEZBJEDNOSNE KULTURE

Povoljna društvena klima zasnovana na transparentnom protoku informacija ključna je za razvoj bezbjednosne kulture u društvu. Bezbjednosni standardi nijesu tajna već osnovni zahtjev svakog radnog mjesta u kompaniji odnosno javnoj upravi. Bez bezbjednosne kulture nemoguće je obezbijediti razvoj informacionog društva. Neophodno je uvesti i stalno razvijati formalne informacione obrazovne programe, od osnovnog, preko srednjeg pa do visokog školstva i obrazovnih programa prilagođenih za javnu upravu. Takvi informacioni programi moraju obuhvatiti elemente bezbjednosne kulture savremenog informacionog društva. Uz to, potrebno je stalno djelovati prema širokim društvenim grupama, kroz različite oblike publikacija, javnih tribina i sl. Pristup problemima informacione bezbjednosti mora biti integralni dio pristupa popularizaciji informatizacije i Interneta, odnosno informacionog društva u cjelini.

1. Razvoj bezbjednosne kulture

S obzirom da je za zaštitu informacija bitno svako lice koje sa njima dolazi u kontakt, svijest o mogućnosti zloupotrebe informacija i informisanost o postupcima i sredstvima zaštite od velike je važnosti za informacionu bezbjednost. Iz tog razloga razvoj svijesti i informisanosti su podjednako važni kao i uvođenje samih mjera ili sredstava zaštite.

Svijest o informacionoj bezbjednosti treba da bude prisutna kod svakog građanina. Ali, nivo potrebne svjesnosti se razlikuje, zavisno od njihove uloge u korišćenju, stvaranju i rukovanju informacijama, kao i od vrste informacija. Zbog toga je neophodno identifikovati osnovne ciljne grupe na koje treba djelovati.

Svi građani treba da znaju kako informacija koju oni mogu koristiti nastaje, mijenja se, obrađuje, razmjenjuje i skladišti. Takođe, treba da su informisani sa kojim sopstvenim postupcima mogu ugroziti bezbjednost informacija i koji su osnovni izvori rizika za bezbjednost informacija.

Rukovaoci informacijama u okviru svoje nadležnosti moraju dodatno biti svjesni i svoje lične odgovornosti za tuđe informacije, potencijalnih grešaka koje mogu prouzrokovati rukovanjem informacijama, kao i načina na koji mogu svojim djelovanjem ugroziti njihovu bezbjednost.

S obzirom da, po pravilu, svi državni službenici i namještenici rukuju određenim informacijama koje su od posebnog značaja za građane, njihova odgovornost je tim veća, pa i razvoj svijesti treba da bude usklađen sa takvom odgovornošću i značajem informacija.

Uz starješine i rukovodeća lica u organima javne uprave najčešće se povezuje i pojam vlasnika podataka, zbog čega su ta lica i najodgovornija za određeni skup podataka. Prilikom strateškog planiranja, predlaganja zakonskih i drugih propisa, ulaganja u infrastrukturu i razvoj, starješine i rukovodeća lica treba da imaju posebnu odgovornost za planiranje i sprovođenje informacione bezbjednosti.

2. Organi nadležni za razvoj bezbjednosne kulture

U principu, svaki građanin treba da je odgovoran za razvoj svijesti o informacionoj bezbjednosti u svojoj životnoj i radnoj sredini. Uz to, pojedini organi treba da imaju i specifične nadležnosti i obveze. Nosioci planiranja programa razvoja bezbjednosne kulture za sve ciljne grupe treba da bude Direkcija za zaštitu tajnih podataka (u svojstvu NSA), u saradnji sa Sekretarijatom za razvoj i Centralnim državnim CERT-om.

Za sprovođenje programa razvoja bezbjednosne kulture za stanovništvo i rukovaoce informacijama nosilac treba da bude Centralni državni CERT, a za državne službenike i namještenike, starješine i rukovodeća lica u državnim organima nosioci mogu biti Direkcija za zaštitu tajnih podataka i Sekretarijat za razvoj, u saradnji sa Upravom za kadrove.

3. Programi edukacije

U Crnoj Gori još uvijek ne postoje specijalizovane škole ili smjerovi za obuku stručnjaka za informacionu bezbjednost. Nedostaje i sistematsko organizovanje seminara ili drugih oblika doživotnog obrazovanja. Iz tih razloga neophodno je podsticati osnivanje stručnih udruženja na nacionalnom nivou, uvođenje sistemskog obrazovanja stručnjaka i uključivanje tema iz oblasti informacione bezbjednosti u redovne školske programe.

3.1. Informatičko obrazovanje i bezbjednosna kultura

Za uspješan razvoj Informacionog društva neophodno je informatičko obrazovanje cjelokupnog stanovništva. Prije svega, neophodno je u obrazovni sistem uključiti potrebne sadržaje, ali i obezbijediti obrazovanje za stanovništvo koje je završilo svoj formalni obrazovni ciklus.

Za sve nivoe obrazovanja potrebno je propisati adekvatno informatičko obrazovanje ujednačeno na nacionalnom nivou, sa odgovarajućim sadržajima iz oblasti informacione bezbjednosti. Neophodno je podsticajnim mjerama pokrenuti poslijediplomske studije u oblasti informacione bezbjednosti.

3.2. e-Obrazovanje

Za građane koji su završili tradicionalno obrazovanje treba obezbijediti uslove za sticanje informatičkog obrazovanja i ovladavanje informacionom bezbjednošću. S obzirom da je u pitanju potencijalno veliki broj građana, sa vrlo širokim spektrom znanja i sposobnosti, taj cilj se može ostvariti jedino korišćenjem novih obrazovnih tehnologija koje zainteresovanom licu omogućavaju izbor mjesta, termina, način i obima obrazovanja. Te tehnologije danas se nazivaju e-Obrazovanje.

3.3. Stručni ispit za rad u državnim organima

Program stručnog ispita, koji polažu državni službenici i namještenici, treba da sadrži i teme iz informatičkog obrazovanja, sa posebnim sadržajima iz oblasti informacione bezbjednosti. Uz provjeru znanja, neophodno je obezbijediti i kvalitetno obrazovanje iz tih oblasti. Obavezne seminare iz oblasti informacione bezbjednosti treba organizovati i za starješine državnih organa.

3.4. Obrazovanje informatičara u organima javne uprave

Informatičarima zaposlenim u organima javne uprave treba obezbijediti trajno informatičko obrazovanje sa naglaskom na oblast informacione bezbjednosti

4. Nosioci planiranja informatičkog obrazovanja i bezbjednosne kulture

Do kraja 2010. godine, za sve nivoe formalnog obrazovanja, od osnovnog do visokoškolskog, nosilac aktivnosti putem predavanja i radionica, treba da bude Ministarstvo prosvjete i nauke. Takođe, to ministarstvo treba da bude nosilac buduće revizije obrazovnih programa. Formalne programe trebalo bi donijeti do kraja 2011. godine.

Direkcija za zaštitu tajnih podataka, u saradnji sa Sekretarijatom za razvoj i Upravom za kadrove treba da bude nosilac planiranja informatičkog obrazovanja i bezbjednosne kulture za starješine, službenike i namještenike, vojna lica i informatičare u organima javne uprave, do kraja 2009. godine, kao i planiranja adekvatnog e-Obrazovanja do kraja 2010. godine.

5. Nadležnost za sprovođenje plana informatičkog obrazovanja i bezbjednosne kulture

Na svim nivoima formalnog obrazovanja, neformalne aktivnosti bi trebalo da sprovode upravljački organi u sistemu informacione bezbjednosti (Ministarstvo prosvjete i nauke u saradnji sa Direkcijom za zaštitu tajnih podataka, Sekretarijatom za razvoj i CIS-om).

Formalne visokoškolske dodiplomske i poslijediplomske aktivnosti treba sprovoditi posredstvom Ministarstva prosvjete i nauke, kroz postojeća i buduća iskustva ostvarena preko Elektrotehničkog fakulteta i ostalih visokoškolskih ustanova. Ostale formalne obrazovne aktivnosti u osnovnim, srednjim i visokim školama, ostvarivale bi se kroz redovne izmjene programa i sprovođenje novih programa u tim ustanovama.

VII - SPROVOĐENJE PROGRAMA

Radi efikasnog sprovođenja ovog programa neophodno je razraditi faze realizacije i predvidjeti odgovarajuće metode praćenja njegovog sprovođenja. U tom smislu, praćenje će biti povjereno posebnoj stručnoj radnoj grupi, koja će kvartalno procjenjivati sprovođenje programa, dok će organi javne uprave, koji saglasno ovom programu preuzimaju centralnu državnu ulogu u informacionoj bezbjednosti, dnevno procjenjivati njegovo sprovođenje.

1. Faze sprovođenja

Da bi se ovaj program mogao sprovoditi potrebno je izvršiti određene predradnje, koje se posebno prikazuju u okviru prve faze, jer predstavljaju preduslov za izvođenje narednih faza.

1.1. Prva faza

Sa aktivnostima se može započeti nakon što Vlada Crne Gore donese ovaj program, a čine ih sljedeći poslovi:

- obrazovanje nove stručne radne grupe za praćenje sprovođenja ovog programa. Nosilac posla je Sekretarijat za razvoj. Rok za obrazovanje je jun 2008. godine;
- donošenje Zakona o informacionoj bezbjednosti. Nosilac posla je Sekretarijat za razvoj, u saradnji sa organima uprave iz domena odbrane i bezbjednosti. Rok je četvrti kvartal 2008. godine;
- inoviranje Zakona o tajnosti podataka u dijelu koji uređuje nadležnosti Direkcije za zaštitu tajnih podataka u oblasti informacione bezbjednosti. Nosilac je Ministarstvo odbrane, u saradnji sa Direkcijom za zaštitu tajnih podataka, Sekretarijatom za razvoj i Ministarstvom unutrašnjih poslova i javne uprave. Rok je prvi kvartal 2009. godine;
- uspostavljanje Centralnog državnog tijela za računarske incidente (Centralni državni CERT). Nosilac je CIS, u saradnji sa Sekretarijatom za razvoj. Rok je prvi kvartal 2009. godine;
- inoviranje Uredbe o organizaciji i načinu rada državne uprave u dijelu koji se odnosi na nadležnosti Direkcije za zaštitu tajnih podataka. Nosilac je Ministarstvo unutrašnjih poslova i javne uprave. Rok je drugi kvartal 2009. godine;
- usklađivanje propisa o kancelarijskom poslovanju sa propisima o informacionoj bezbjednosti. Nosilac je Ministarstvo unutrašnjih poslova i javne uprave. Rok je drugi kvartal 2009. godine;
- izrada plana za razvoj kapaciteta i procedura fizičke bezbjednosti i bezbjednosti podataka unutar odbrambenih i bezbjednosnih struktura, saglasno NATO standardima datim u C-M (2002)49. Nosilac posla je Direkcija za zaštitu tajnih podataka, u saradnji sa Ministarstvom inostranih poslova i organima uprave iz domena odbrane i bezbjednosti. Rok je drugi kvartal 2009. godine;
- inoviranje Projekta Računarsko-komunikaciona mreža organa državne uprave sa bezbjednosnog aspekta. Nosilac je Sekretarijat za razvoj. Rok je prvi kvartal 2010. godine.

1.2. Druga faza

Sa drugom fazom može da se započne u drugom kvartalu 2009. godine. Ova faza podrazumijeva sljedeće poslove:

- donošenje Nacionalne strategije ili politike informacione bezbjednosti. Nosilac je Direkcija za zaštitu tajnih podataka u saradnji sa Sekretarijatom za razvoj i organima uprave iz domena odbrane i bezbjednosti. Rok je četvrti kvartal 2009. godine;
- uspostavljanje Referentne liste normi i standarda i uključivanje potrebnih normi i otvorenih standarda iz oblasti informacione bezbjednosti. Nosilac je Direkcija za zaštitu

tajnih podataka u saradnji sa Institutom za standardizaciju. Rok je četvrti kvartal 2009. godine;
- uspostavljanje mreže INFOSEC koordinatora za organe javne uprave. Nosilac je Direkcija za zaštitu tajnih podataka u saradnji sa Sekretarijatom za razvoj, Ministarstvom inostranih poslova, organima uprave iz domena odbrane i bezbjednosti i CIS-om. Rok je prvi kvartal 2010. godine;
- uspostavljanje osnovnih funkcionalnosti od strane centralnih upravljačkih organa u sistemu informacione bezbjednosti. Nosilac je Direkcija za zaštitu tajnih podataka (NSA), u saradnji sa Sekretarijatom za razvoj i CIS-om. Rok je drugi kvartal 2010. godine;
- donošenje Uredbe sa ciljem sprovođenja Nacionalne politike informacione bezbjednosti. Nosilac je Direkcija za zaštitu tajnih podataka u saradnji sa Ministarstvom odbrane, Ministarstvom unutrašnjih poslova i javne uprave i Sekretarijatom za razvoj. Rok je drugi kvartal 2010. godine;
- donošenje Pravilnika i Smjernica za pojedine bezbjednosne oblasti. Nosioci su Direkcija za zaštitu tajnih podataka, Sekretarijat za razvoj i CIS, u skladu sa svojim nadležnostima. Rok je treći kvartal 2010. godine;
- bezbjednosna akreditacija Projekta Računarsko-komunikaciona mreža organa državne uprave. Nosilac je Direkcija za zaštitu tajnih podataka. Rok je treći kvartal 2010. godine;
- izrada programa razvoja bezbjednosne kulture. Nosilac je Direkcija za zaštitu tajnih podataka, u saradnji sa Sekretarijatom za razvoj, Upravom za kadrove i CIS-om. Rok je četvrti kvartal 2010.godine;
- planiranje pravne regulative za zaštitu stanovništva i privrednih subjekata u okviru savremenog informacionog društva. Nosilac je Ministarstvo unutrašnjih poslova i javne uprave, u saradnji sa Ministarstvom pravde, Direkcijom za zaštitu tajnih podataka, Sekretarijatom za razvoj i CIS-om. Rok je četvrti kvartal 2010. godine.

Završetak Druge faze planira se do kraja četvrtog kvartala 2010. godine, čime bi Crna Gora ispunila zahtjeve NATO-a u vezi sa informacionom bezbjednošću.

1.3. Treća faza

Treća faza se može djelimično preklapati sa drugom fazom i započeti u trećem kvartalu 2010. godine, nakon donošenja najvažnijih propisa predviđenih za Drugu fazu (Nacionalna politika informacione bezbjednosti i sprovedbene uredbe). Ova faza podrazumijeva sljedeće poslove:

- usaglašavanje pristupa politici informacione bezbjednosti u organima javne uprave. Nosilac je Direkcija za zaštitu tajnih podataka, u saradnji sa Ministarstvom odbrane, Ministarstvom unutrašnjih poslova i javne uprave i Sekretarijatom za razvoj. Rok je četvrti kvartal 2010. godine;
- inoviranje programa edukacije za neformalne edukacijske aktivnosti u obrazovanju. Nosilac je Ministarstvo prosvjete i nauke, u saradnji sa Direkcijom za zaštitu tajnih podataka, Sekretarijatom za razvoj i CIS-om. Rok je četvrti kvartal 2010. godine;
- izrada programa edukacije i kataloga znanja iz domena informacione bezbjednosti za obrazovanje državnih službenika i namještenika u organima javne uprave. Nosilac je Ministarstvo unutrašnjih poslova i javne uprave, u saradnji sa Sekretarijatom za razvoj, Ministarstvom odbrane i Upravom za kadrove. Rok je četvrti kvartal 2010. godine;
- donošenje Smjernica i Preporuka informacione bezbjednosti za organe javne uprave. Nosilac je Direkcija za zaštitu tajnih podataka, u saradnji sa Sekretarijatom za razvoj, Ministarstvom inostranih poslova i organima uprave iz domena odbrane i bezbjednosti. Rok je prvi kvartal 2011. godine;
- koordinacija SAA procesa za organe javne uprave. Nosilac je Direkcija za zaštitu tajnih podataka, u saradnji sa Sekretarijatom za razvoj. Rok je drugi kvartal 2011. godine.

Završetkom Treće faze ispunili bi se osnovni zahtjevi Programa eEurope 2005 i uopšte zahtjevi EU u vezi sa informacionom bezbjednošću.

1.4. Četvrta faza

Četvrta faza može se djelimično preklapati sa trećom fazom i započeti u drugom kvartalu 2011. godine. Ta faza podrazumijeva sljedeće poslove:

- usklađivanje pristupa javno-privatnom partnerstvu u informacionoj bezbjednosti. Nosilac je Vlada Crne Gore, a učesnici državni i privatni subjekti predviđeni ovim programom. Rok je treći kvartal 2011. godine;
- implementiranje inicijativa u okviru javno-privatnog partnerstva. Nosilac je Vlada Crne Gore, a učesnici državni i privatni subjekti predviđeni ovim programom. Rok je četvrti kvartal 2011. godine;
- izrada programa edukacije i kataloga znanja za osnovno i srednje obrazovanje u Crnoj Gori. Nosioci su Zavod za školstvo i Centar za stručno obrazovanje, u saradnji sa Ministarstvom prosvjete i nauke. Rok je četvrti kvartal 2011. godine;
- izrada programa edukacije i kataloga znanja za visoko obrazovanje u Crnoj Gori (dodiplomsko i poslijediplomsko). Nosilac je Ministarstvo prosvjete i nauke u saradnji sa univerzitetima i fakultetima u Crnoj Gori. Rok je četvrti kvartal 2011. godine.

Završetak Četvrte faze planira se do kraja 2011. godine, čime bi Crna Gora ispunila sve zahtjeve za stvaranje savremenog informacionog društva, obuhvatajući na taj način sve bitne subjekte, tj. organe javne uprave, stanovništvo i privredu.

2. Mehanizmi za praćenje sprovođenja programa

Radi praćenja procesa uspostavljanja sistema informacione bezbjednosti u Crnoj Gori, u početnoj fazi, do preuzimanja obaveza od strane nadležnih organa, bila bi nadležna novoformirana stručna radna grupa. Da bi taj proces praćenja bio usklađen sa informatizacijom u Crnoj Gori, rad ove radne grupe bi preko Sekretarijata za razvoj trebao biti usklađen sa izvršenjem ostalih važnih infrastrukturnih projekata, kao što su Računarsko-komunikaciona mreža organa državne uprave i sl. Iz tog razloga Sekretarijat za razvoj, kao organ uprave nadležan za poslove informatizacije, treba da formira stručnu radnu grupu koja će pratiti sprovođenje ovog programa. Na taj način bi se mogla obezbijediti neophodna koordinacija aktuelnih i budućih projekata informatizacije sa procesom postepenog uspostavljanja organizacije informacione bezbjednosti.

Novoformirana stručna radna grupa, radi kontinuiteta, treba da bude sastavljena od predstavnika organa uprave koji su učestvovali u izradi ovog programa, kao i od predstavnika organa koji će neposredno raditi na pripremi za preuzimanje predviđenih poslova u okviru sistema informacione bezbjednosti u Crnoj Gori, i to:

- Sekretarijata za razvoj;
- Ministarstva odbrane;
- Ministarstva unutrašnjih posliova i javne uprave;
- Ministarstva inostranih poslova;
- Ministarstva pravde;
- Sekretarijata za evropske integracije;
- Uprave policije;
- Agencije za nacionalnu bezbjednost;
- Ministarstva finansija;
- Ministarstva prosvjete i nauke;
- Direkcije za zaštitu tajnih podataka (NSA);

- CIS-a;
- organa nadležnog za zaštitu podataka o ličnosti.

Novoformirana stručna radna grupa bi imala zadatak da tokom 2008 i 2009. godine kvartalno prati uspostavljanje funkcionalnosti u pojedinim organima. Preuzimanje upravljačkih funkcija informacione bezbjednosti treba da bude obavljeno do kraja drugog kvartala 2010. godine. Od početka trećeg kvartala 2010. godine upravljačke funkcije u informacionoj bezbjednosti moraju se sprovoditi autonomno od strane nadležnih organa, u skladu sa ovim programom i Nacionalnom politikom informacione bezbjednosti u Crnoj Gori. Stručna radna grupa bi se tokom 2010 i 2011. godine sastajala u posljednjem kvartalu godine, kako bi pripremila godišnje izvještaje za Vladu Crne Gore. U prvom kvartalu 2012. godine pripremio bi se završni četvorogodišnji izvještaj, nakon čega bi prestala potreba za radom stručne radne grupe.