REPUBLIKA HRVATSKA
URED VIJECA ZA NACIONALNU SIGURNOST

NACRT PRIJEDLOGA

ZAKONA O INFORMACIJSKOJ SIGURNOSTI

Zagreb, ožujak 2006.

I. USTAVNA OSNOVA ZA DONOŠENJE ZAKONA

Ustavna osnova za donošenje ovog Zakona sadržana je u odredbama clanka 36. stavka 2. i clanka 37. stavka 2. Ustava Republike Hrvatske.

II. OCJENA STANJA I OSNOVNA PITANJA KOJA SE TREBAJU UREDITI ZAKONOM TE POSLJEDICE KOJE CE DONOŠENJEM ZAKONA PROISTECI

a) Ocjena stanja

Podrucje koje se ovim zakonskim prijedlogom ima urediti djelomicno je propisano Zakonom o zaštiti tajnosti podataka (NN 108/96) i Zakonom o sigurnosnim službama (NN 32/02, 38/02). Donošenjem Zakona o zaštiti tajnosti podataka 1996. godine i njegovih podzakonskih propisa prestala je vrijediti Uredba o utvrdivanju mjerila za odredivanje tajnih podataka obrane te posebnim i opcim postupcima za njihovo cuvanje (NN 70/91). Na taj nacin se ovo važno podrucje tajnosti podataka po prvi puta u Republici Hrvatskoj uredilo Zakonom, kojim su postavljena nacela tajnosti podataka, vrste tajnosti i klasifikacija, postupci za odredivanje tajnosti, nadležnosti tijela te zaštitne mjere. U podrucju nacela tajnosti podataka ovaj Zakon propisao je niz rješenja preuzetih iz 80-tih godina prošlog stoljeca, koja danas nisu više u skladu sa suvremenim standardima tajnosti podataka zemalja Europske Unije, clanica NATO-a i drugih razvijenih demokratskih zemalja svijeta. Primjerice, to su neodgovarajuca klasifikacija po stupnjevima i vrstama tajnosti za državne podatke, nepostojanje elementarnih nacela za pristup tajnim podacima kao što su poslovna potreba (need-to-know) i sigurnosna provjera s certifikatom za osobe s pravom pristupa tajnim podacima, te neadekvatno tretiranje temeljnih demokratskih standarda kao što su zaštita osobnih podataka i pojam privatnosti opcenito. Dio ove materije koji se odnosi na sve pravne i fizicke osobe u Republici Hrvatskoj, u meduvremenu je propisan Zakonom o zaštiti osobnih podataka (NN 103/03) i Zakonom o pravu na pristup informacijama (NN 172/03). Slijedom toga, potrebno je propisati temeljne principe tajnosti podataka državne uprave koji se trebaju razraditi novim Zakonom o tajnosti podataka. Taj Zakon treba na suvremen i medunarodno prihvacen nacin tretirati pojmove klasificiranih i neklasificiranih podataka državne uprave, stupnjeve i principe klasificiranja, kao i nacela pristupa tajnim podacima.

Zakon o zaštiti tajnosti podataka (NN 108/96) nadalje propisuje nacin odredivanja zaštitnih mjera za zaštitu tajnosti podataka i to na nacin da celnicima javnih tijela i ovlaštenim dužnosnicima Republike Hrvatske daje ovlast za odredivanje posebnih zaštitnih mjera i rok od tri mjeseca za donošenje propisa o zaštitnim mjerama i drugih propisa vezanih za tajnost podataka. Ovakva odredba ima za posljedicu neodgovarajuce stanje u kojem se Republika Hrvatska nalazi danas, a to je nepostojanje nacionalnih standarda za zaštitu podataka, neadekvatan pristup tajnosti podataka u državnoj upravi i samim time lošu percepciju javnosti o pojmovima privatnosti i tajnosti. Rezultat ovakvih odredbi Zakona je to da tijela državne uprave samostalno donose vlastite mjere i standarde zaštite tajnosti podataka koje stoga na državnoj razini nisu standardizirana. U tijelima u kojima su takvi propisi doneseni i implementirani to je rezultiralo razlicitom ucinkovitošcu zaštitnih mjera i medusobno nesukladnim organizacijskim i tehnickim sigurnosnim rješenjima. Poseban problem na koji se svih ovih godina nije obratila pažnja je i to što je samo mali broj tijela državne uprave uopce osposobljen za donošenje i implementaciju mjera i standarda zaštite tajnosti podataka. Tako

da je u praksi slucaj da su ovi podzakonski propisi doneseni, i barem u odredenoj mjeri provedeni, uglavnom samo u tijelima sigurnosnog sustava u širem smislu (sigurnosno-obavještajne službe, Ministarstva Obrane, Unutarnjih i Vanjskih poslova). Najveci broj tijela državne uprave u Republici Hrvatskoj nema kadrovske resurse i potrebna znanja za donošenju i implementaciju ovakvih mjera i standarda te propise nije niti donio, ili je mjere zaštite pokušao implementirati kroz vanjsku komercijalnu uslugu, kupljenu na tržištu bez jasnih kriterija i tehnickih zahtjeva, upitne primjerenosti državnim potrebama. Zakljucno se može reci da problem postoji na dva nivoa. Prvi nivo su nedovoljni kadrovski resursi i potrebna znanja za koncipiranje sigurnosnih mjera za zaštitu podataka u vecini tijela, a drugi nivo je da i pri definiranim standardima zaštite podataka veliki broj tijela nema strucno-kadrovske potencijale za implementaciju, održavanje i unapredivanje zaštitnih mjera.

Ovakvo stanje predstavlja sigurnosni problem za Republiku Hrvatsku, ali i vrlo skup pristup, u kojem se na nekoordiniran i nesustavan nacin realiziraju i financiraju razlicita organizacijska i tehnicka sigurnosna rješenja u tijelima državne uprave. U takvom stanju Republika Hrvatska ne može uspostaviti i garantirati minimalne zahtjeve informacijske sigurnosti na nacionalnoj razini, što je temeljni zahtjev NATO-a i EU u aktualnim integracijskim procesima. U tom smislu može se jasno reci da postojeci zakonski okvir u podrucju informacijske sigurnosti nije uskladen sa zahtjevima NATO-a i EU, a medunarodno standardiziran i zahtijevan institucionalni okvir u podrucju informacijske sigurnosti u Republici Hrvatskoj prakticno ne postoji, što predstavlja zapreku koju treba nužno otkloniti na putu daljnjeg približavanja euro-atlantskim integracijama.

Zakonom o sigurnosnim službama (NN 32/02, 38/02), na temelju iskustava u NATO programu Partnerstva za mir, kojemu je Republika Hrvatska pristupila u svibnju 2000. godine, propisani su prvi temelji organizacije informacijske sigurnosti na nacionalnoj razini, koji su bili uvjet pristupa Republike Hrvatske Akcijskom planu za clanstvo u NATO-u (MAP) 2002. godine. Ovim Zakonom je osnovan Ured Vijeca za nacionalnu sigurnost, nadležan izmedu ostalog za provedbu sigurnosnih mjera potrebnih za zaštitu povjerljivih informacija i dokumenata u razmjeni izmedu Republike Hrvatske i stranih obrambenih organizacija te Središnji registar za prijem i pohranu dokumenata. Pored toga, Ured je postao nadležan za tehnicke poslove u podrucju informacijske sigurnosti do osnivanja posebnog tehnickog tijela, Zavoda za informacijsku sigurnost i kripto-zaštitnu tehnologiju, koje Uredu u tim poslovima treba pružati tehnicku potporu. Ovakvim propisom Republika Hrvatska je zapocela izgradnju zajednicke organizacije na nacionalnoj razini za potrebe suradnje s NATO-om, sukladno zahtjevima NATO-a. Ovim Zakonom uvedeni su u Republici Hrvatskoj medunarodno prihvaceni standardi za postojanje središnjeg državnog tijela za informacijsku sigurnost (National Security Authority – NSA) i središnjeg državnog tijela za tehnicka podrucja informacijske sigurnosti (National Communication Security Authority – NCSA ili Infosec Authority – IA). U periodu od donošenja ovog Zakona 2002. godine do danas, Ured je preuzeo i proveo vecinu svojih nadležnosti u ovom podrucju, dok je formiranje Zavoda samo zapoceto. Zbog pravnih nedorecenosti u odredbama Zakona, Zavod nikada nije formiran, inicijalna proracunska sredstva nisu korištena, a poslove Zavoda u okviru suradnje s NATO-om obavljali su privremeni ravnatelj i Ured Vijeca za nacionalnu sigurnost. Najveci problem spomenutih odredbi ovog Zakona je pokušaj parcijalnog rješavanja pojma informacijske sigurnosti, u okvirima suradnje s NATO-om i u okvirima sigurnosnog sustava Republike Hrvatske. Vremenom se, kroz provedbu Akcijskog plana za clanstvo u NATO-u, pokazalo da se zahtjevi informacijske sigurnosti postavljaju za državnu upravu u cjelini te da je nužno uskladiti pristup na nacionalnoj razini u podrucju informacijske sigurnosti sa zahtjevima ne samo NATO-a, vec i EU.

Godine 2004. strucna skupina sastavljena od relevantnih strucnjaka državnog i akademskog sektora, u organizaciji Središnjeg državnog ureda za e-Hrvatsku, zapocela je izradu sveobuhvatnog Nacionalnog programa informacijske sigurnosti u Republici Hrvatskoj. Cilj je bio sustavno razraditi potrebne izmjene zakonodavnog i institucionalnog okvira u Republici Hrvatskoj, kako bi se sustav državne uprave u Republici Hrvatskoj kompletno uskladio sa standardima razvijenih demokratskih zemalja, a napose sa zemljama Europske Unije i clanicama NATO-a. Nacionalni program informacijske sigurnosti u Republici Hrvatskoj, nakon javne rasprave, 31. ožujka 2005., prihvatila je Vlada Republike Hrvatske. Strateški, dugorocni cilj Programa, je izgraditi cvrste temelje za razvoj informacijskog društva u Republici Hrvatskoj (programi EU: e-Europe 2005 i 2010, program RH e-Hrvatska 2007), bez cega ce biti upitan bilo kakav gospodarski prosperitet Republike Hrvatske u iducem desetljecu. Takticki, kratkorocno, programom je isplaniran niz mjera kojima ce se postupno, u roku od nekoliko godina, uz najmanje moguce izmjene zakonodavnog i institucionalnog okvira, dovesti Republiku Hrvatsku do suvremenog, medunarodno prihvacenog koncepta informacijske sigurnosti, kao temelja vlastitog sustava nacionalne sigurnosti, ali i razvoja društva u cjelini. Sukladnost zahtjevima medunarodnih integracijskih procesa u NATO i EU postavljena je kao uvjet u Nacionalnom programu te njegova provedba osigurava Republici Hrvatskoj uredenje nacionalnih pitanja iz podrucja informacijske sigurnosti na nacin sukladan najvišim NATO i EU zahtjevima.

Nacionalni program donio je niz preporuka vezanih za potrebne izmjene zakonodavstva, reorganizaciju institucija i potrebu potpune promjene dosadašnje prakse koja potjece iz Zakona o zaštiti tajnosti podataka iz 1996. godine i podzakonskih propisa donesenih temeljem ovog Zakona. Sustavni pristup informacijskoj sigurnosti odnosi se, ne samo na državnu upravu u cjelini, vec i na gradanstvo i privatni sektor. U tom smislu Nacionalni program je obuhvatio planiranje mjera informacijske sigurnosti za stupove vlasti (izvršnu, zakonodavnu i sudbenu), nivoe vlasti (državna, lokalna), javne institucije, gradanstvo i privatni sektor. Pri tome je nacin propisivanja, sadržaj i opseg mjera bitno razlicit i primjeren potrebama svakog od ovih segmenata društva. Predvidene su i mjere koje se odnose na sustavan pristup edukaciji i razvoju sigurnosne svijesti u najširim društvenim slojevima, u okviru kojih ce u buducnosti biti potrebno uvesti odgovarajuce edukacijske programe za državne dužnosnike, službenike i namještenike, interdisciplinarne visokoškolske programe informacijske sigurnosti te provoditi postupne izmjene i prilagodbu školskih programa osnovnog i srednjeg obrazovanja potrebama suvremenog društva.

Nacionalnim programom preporucene su pripremne radnje kao minimalan skup mjera koje je potrebno provesti kako bi Republika Hrvatska uopce mogla zapoceti prilagodbu medunarodnim zahtjevima, standardima i praksi postupanja u podrucju informacijske sigurnosti. Pripremnim radnjama oznaceni su medunarodno prihvaceni standardi koji sve zemlje obvezuju na propisivanje zakonodavnog okvira koji se odnosi na pristup na nacionalnoj razini i državnu upravu u cjelini te na odredivanje tijela s ovlastima za propisivanje i usmjeravanje sigurnosnih standarda na nacionalnoj razini. U tom smislu pripremne radnje odnose se na odgovarajuce zakonske promjene kojima treba potpuno izmijeniti Zakon o zaštititi tajnosti podataka iz 1996. godine, doraditi Zakon o sigurnosnim službama iz 2002. godine u podrucju informacijske sigurnosti te medusobno uskladiti nove prijedloge zakona koji ce ciniti buduci zakonski sustav informacijske sigurnosti u Republici Hrvatskoj. Predvideno je da se ovaj novi zakonski sustav sastoji od tri nova zakona: Zakona o tajnosti podataka, Zakona o informacijskoj sigurnosti i Zakona o sigurnosno-obavještajnom sustavu Republike Hrvatske.

Tako novi Zakon o tajnosti podataka treba propisati temeljne principe tajnosti podataka državne uprave te na suvremen i medunarodno prihvacen nacin mora tretirati pojmove klasificiranih i neklasificiranih podataka državne uprave, stupnjeve tajnosti i nacela klasificiranja, kao i nacin i uvjete pristupa tajnim podacima.
Novi Zakon o informacijskoj sigurnosti treba definirati pet sigurnosnih podrucja za razvoj mjera i standarda informacijske sigurnosti (sigurnosnu provjeru osoblja, fizicku sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost vanjske suradnje – industrijska sigurnost). Isto tako treba definirati sustav kompleksne hijerarhije podzakonske regulative: nacionalnu politiku informacijske sigurnosti, uredbe, pravilnike, interne akte i njihove medusobne odnose i rokove u kojima ih nadležna tijela trebaju donijeti. Potrebno je i na medunarodno prihvatljiv nacin odrediti nadležnosti potrebnih tijela na nacionalnoj razini i to za razvoj i usmjeravanje sigurnosnih standarda, te za nadzor i implementaciju. Ovakav Zakon treba biti okvir informacijske sigurnosti, koji ce se kroz definiran sustav podzakonske hijerarhije i tijekom dvogodišnjeg procesa popunjavati sadržajima, od opcih nacela prema posebnim i od organizacijskih detalja prema tehnickim.
Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske potrebno je u skladu s prethodna dva zakona harmonizirati pristup podrucju informacijske sigurnosti unutar sigurnosnog sustava Republike Hrvatske sa onim na nacionalnoj razini te prilagoditi ustroj i ovlasti pojedinih tijela sigurnosnog sustava koja u podrucju informacijske sigurnosti imaju nadležnosti na nacionalnoj razini u Republici Hrvatskoj. To su prvenstveno Ured Vijeca za nacionalnu sigurnost kao središnje državno tijelo za informacijsku sigurnost, odgovorno za donošenje i usmjeravanje mjera i standarda informacijske sigurnosti, i Zavod za sigurnost informacijskih sustava kao središnje državno tijelo za tehnicka podrucja informacijske sigurnosti, te sigurnosne službe, koje ce imati odgovarajucu ulogu nadzora propisanih mjera i standarda informacijske sigurnosti. Predradnje moraju rezultirati potpuno funkcionalnim središnjim državnim tijelima za opca i tehnicka podrucja informacijske sigurnosti (NSA, NCSA) sa svim potrebnim ovlastima, kadrovskom i ostalom infrastrukturom za rad, jer ce ta tijela biti pokretac razvitka sustava informacijske sigurnosti, propisan Zakonom o informacijskoj sigurnosti.

b) <u>Osnovna pitanja koja se predlažu urediti Zakonom</u>

Zakon o informacijskoj sigurnosti kao novota u hrvatskom pravnom poretku ureduje cjelovit sustav informacijske sigurnosti Republike Hrvatske kao suštinski dio sustava nacionalne sigurnosti, ali i suvremenog informacijskog društva u cjelini. Zakon u cijelosti definira sve elemente sustava, njihove medusobne odnose, nacin i smjer pojedinacnog i zajednickog funkcioniranja te nadležnosti nadzora. Informacijsku sigurnost tijela javne vlasti u smislu ovog Zakona predstavlja skup mjera i standarda koji služi ocuvanju temeljnih svojstava povjerljivosti, cjelovitosti i raspoloživosti klasificiranih i neklasificiranih podataka u radu državne uprave. Cjelovitost i raspoloživost informacijskih sustava u kojima se podaci obraduju, prenose ili pohranjuju, takoder mora biti adekvatno zašticena. Pri tome je važno uociti kako i podaci koji nisu klasificirani mogu imati veliku važnost pa se i za njih primjenjuje odgovarajuci skup mjera i standarda koji služi ocuvanju svojstava cjelovitosti i raspoloživosti podataka koji nisu povjerljivi. Sustav informacijske sigurnosti razraduje se promatrajuci sve mjere, standarde i nadležnosti tijela kroz podjelu na pet medunarodno prihvacenih sigurnosnih podrucja informacijske sigurnosti: sigurnosne provjere, fizicka sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost vanjske suradnje ili

industrijska sigurnost. Zakon predstavlja okvir sustava informacijske sigurnosti, koji ce se popunjavati sadržajima (mjere i standardi) kroz razvoj kompleksne hijerarhije podzakonske regulative za koji je odreden ukupan rok od 18 mjeseci (ukljucuje i prethodnu unutarnju organizaciju središnjih državnih tijela za informacijsku sigurnost). Daljnjih tri mjeseca predvideno je za donošenje internih provedbenih akata, te još šest mjeseci za njihovu provedbu u tijelima javne vlasti.

Zakonski prijedlog veliku pažnju posvecuje podzakonskom okviru, odnosno propisima informacijske sigurnosti. Stoga se detaljno razraduje vrsta i hijerarhija propisa, nadležnost i rokovi njihova donošenja, kako uslijed kompleksnosti i višeslojnosti propisa ne bi došlo do medusobne kolizije ili nedostatka pojedinih propisa. Ovakav pristup je medunarodnopravno prihvacen i osigurava sustavno uvodenje informacijske sigurnosti od opcih propisa prema posebnim, od funkcionalnih prema provedbenim te od organizacijskih prema tehnickim. Na taj nacin se izmedu ostalog osigurava i trajnije prihvacanje pojedinih opcih nacela informacijske sigurnosti i njihova što manja ovisnost o tehnološkim i organizacijskim promjenama pojedinih poslovnih procesa koje su ceste i neizbježne. Složena hijerarhija propisa zapocinje Nacionalnom politikom informacijske sigurnosti koju donosi Hrvatski sabor na prijedlog Vlade Republike Hrvatske i uz suglasnost Predsjednika Republike. Nacionalna politika informacijske sigurnosti ima za cilj izbalansirati pristup informacijskoj sigurnosti u razlicitim segmentima tijela javne vlasti, ovisno o stupu (izvršna, zakonodavna, sudbena) i nivou vlasti (državna, lokalna) kojem pojedino tijelo pripada. Na taj nacin, na najvišoj razini vlasti, uskladuju se ciljevi i dosezi informacijske sigurnosti u svim tijelima javne vlasti. Nacionalna politika informacijske sigurnosti daje smjernice za sadržaj mjera informacijske sigurnosti koje ce se provoditi u pojedinim segmentima tijela javne vlasti, a koje treba propisati Vlada svojim uredbama.

U svrhu pripremanja spomenutih propisa informacijske sigurnosti koje donose Hrvatski sabor (Nacionalna politika informacijske sigurnosti) i Vlada (uredbe o mjerama informacijske sigurnosti), te u svrhu donošenja pravilnika s nacionalnim standardima informacijske sigurnosti koji ce se primjenjivati u realizaciji propisanih mjera, prijedlogom Zakona se definiraju tijela koja ce imati ovlasti središnjih državnih tijela za informacijsku sigurnost, odgovornih za koordinaciju i usmjeravanje aktivnosti, predlaganje i donošenje propisa. Zakonskim Prijedlogom se propisuje da Ured Vijeca za nacionalnu sigurnost (UVNS) postaje središnje državno tijelo za informacijsku sigurnost koje u medunarodnopravnoj nomenklaturi zemalja clanica NATO-a predstavlja: National Security Authority – NSA, tijelo odgovorno za koordinaciju svih aktivnosti oko primjene mjera i donošenja standarda informacijske sigurnosti u tijelima javne vlasti te za koordinaciju svih drugih tijela koja imaju nadležnosti ili sudjeluju u izradi ili provedbi propisa informacijske sigurnosti. Zakonskim Prijedlogom se propisuje da Zavod za sigurnost informacijskih sustava (ZSIS) postaje središnje državno tijelo za tehnicka podrucja informacijske sigurnosti (National Communication Security Authority – NCSA ili Infosec Authority - IA). Zavod djeluje u uskoj koordinaciji s Uredom, a osim opcih poslova na sigurnosti informacijskih sustava i mreža tijela javne vlasti, nadležan je za sigurnosne akreditacije informacijskih sustava i mreža tijela javne vlasti (Security Accreditation Authority - SAA), za upravljanje kriptomaterijalima (National Distribution Authority – NDA) te za poslove tijela za odgovore na racunalne ugroze (CERT-a - Computer Emergency Response Team) u tijelima javne vlasti.

Kako bi se potrebna pažnja posvetila prevenciji i otklanjanju sigurnosnih problema vezanih uz sigurnost javnih racunalnih mreža u Republici Hrvatskoj, koje se nužno koriste i u realizaciji državnih komunikacijskih mreža, te omogucila ucinkovita medunarodna suradnja Republike

Hrvatske u ovom podrucju, zakonskim Prijedlogom osniva se CERT[1]. Pored ukljucenja u EU, NATO i medunarodnu mrežu CERT-ova, CERT bi djelovao u uskoj koordinaciji sa dva središnja državna tijela za informacijsku sigurnost na problematici i koordinaciji postupanja vezanih za sigurnosne racunalne incidente u RH, a napose na državnim racunalnim mrežama. Kao javna ustanova, organizirana na temeljima postojeceg, medunarodno afirmiranog akademskog CERT-a u okviru Hrvatske akademske i istraživacke mreže – CARNet, CERT ce biti kljucna institucija za promoviranje informacijske sigurnosti u najširim društvenim slojevima Republike Hrvatske, ali i medunarodno.

Jedan od najvažnijih zadataka informacijske sigurnosti je osigurati sustavnu primjenu mjera u okviru informatizacije državne uprave i javnog sektora u širem smislu. Za razliku od privatnog sektora gdje se te mjere trebaju promovirati i poticati u svrhu preventive i zaštite gradanstva i gospodarstva, ovdje se radi o propisivanju i provedbi obvezujucih propisa u tijelima javne vlasti. Stoga je nužno zakonom propisati koncept provedbe mjera informacijske sigurnosti koji ce osigurati sustavnu informatizaciju državne uprave, u okviru koje ce mjere informacijske sigurnosti biti planirane i primijenjene na propisan nacin. Zakonskim Prijedlogom je propisan medunarodno prihvacen nacin, kojim se definiraju nadležna centralna tijela za potporu u poslovima planiranja i implementacije (CIS[2] Planning and Implementation), koja ove poslove obavljaju u tijelima javne vlasti koja nemaju adekvatne vlastite strucne resurse za planiranje i implementaciju. Centralno tijelo za ove poslove u Republici Hrvatskoj bio bi Središnji državni ured za e-Hrvatsku (SDUeH), nadležan za razvitak informacijskog sustava državne uprave, dok bi u okviru obrazovnog i akademskog sektora ove poslove provodilo Ministarstvo znanosti, obrazovanja i športa. Nedavnim osnivanjem Agencije za potporu informacijskih sustava i tehnologije, Vlada Republike Hrvatske i Grad Zagreb kao osnivaci, omogucavaju SDUeH izvršnu potporu za ove poslove, kakva se za potrebe Ministarstva znanosti, obrazovanja i športa planira kroz Hrvatsku akademsku i istraživacku mrežu (CARNet) te Sveucilišni racunski centar (SRCE).

Kako bi se osiguralo stalni ciklus planiranja, provodenja, provjere i dorade (PDCA[3]), sustav mora ukljuciti element nadzora informacijske sigurnosti. Nadzor je predviden na dva koncepcijski razlicita nacina zbog razlicitih zahtjeva informacijske sigurnosti i karakteristika segmenata tijela javne vlasti na koje se odnose. Prvi nacin odnosi se na središnja tijela izvršne vlasti i sukladan je konceptu koji koristi NATO, pri cemu se definiraju institucije nadležne za ovaj proces nadzora (CIS Operating). Prijedlogom Zakona za ovaj posao odredene su sigurnosno-obavještajne agencije, koje sukladno svojoj nadležnosti (civilna i vojna), osiguravaju propisanu primjenu mjera i standarda informacijske sigurnosti u središnjim tijelima državne uprave. U svim ostalim tijelima javne vlasti koristi se drugi, nešto manje zahtjevan nacin, sukladan EU zahtjevima. U tim tijelima propisuje se obveza postavljanja odgovarajucih koordinatora informacijske sigurnosti koji mogu biti centralni za više tijela ili lokalni. Ovi koordinatori su imenovani od strane tih tijela i njihovi su zaposlenici, ali prema uvjetima koja se odreduju na nacionalnoj razini, u središnjem državnom tijelu za informacijsku sigurnost, koje je nadležno i za strucno usmjeravanje i pracenje rada ovih koordinatora, putem uredbe Vlade Republike Hrvatske . Poslovi koje obavljaju sigurnosno-

[1] Naziv CERT, iako izvorno potjece od kratice engleskog jezika Computer Emergency Response Team, danas je medunarodno priznat kao naziv ove vrste poslova i upotrebljava se u nacionalnim nazivima tijela koja imaju ovlasti ove vrste u nacionalnim okvirima (EU, Austrija, Grcka, Malta, Italija, Švicarska, Portugal, Njemacka, Švedska, …). Ovaj naziv je uvriježen i u RH jer je vec niz godina u upotrebi kao CARNet CERT, koji bi ovim zakonskim Prijedlogom trebao iz akademskog prerasti u nacionalni CERT.

[2] Communication and Information Systems – CIS, komunikacijski i informacijski sustavi

[3] Plan, Do, Check, Act – PDCA, stalni ciklus planiranja, provodenja, provjere i dorade odredenih standarda

obavještajne agencije i koordinatori, su poslovi redovitog nadzora organizacije i implementacije propisanih mjera svih pet sigurnosnih podrucja informacijske sigurnosti u tijelima javne vlasti, te izvještavanja celnika tijela javne vlasti i nadležnih središnjih državnih tijela za informacijsku sigurnost, o stanju i ucinkovitosti propisanih standarda u tijelima javne vlasti te o mogucim poboljšanjima istih. Smisao nadzora informacijske sigurnosti prvenstveno je u stalnom usmjeravanju propisanih mjera i standarda informacijske sigurnosti te ispomoci strucnog i sigurnosnog osoblja u samim tijelima javne vlasti, zaduženog za održavanje i administriranje organizacijskih i tehnickih mjera i sustava iz svih sigurnosnih podrucja informacijske sigurnosti, realiziranih u tijelima javne vlasti. U tom smislu, nadzor se obavlja u unaprijed planiranim terminima, a o rezultatima nadzora donosi se izvješce koje se dostavlja celniku tijela javne vlasti te središnjem državnom tijelu za informacijsku sigurnost. Središnje državno tijelo za informacijsku sigurnost, uz pomoc tijela za tehnicka podrucja informacijske sigurnosti, nadzornih tijela/koordinatora, te tijela za planiranje i implementaciju, zaduženo je za koordinaciju postupka otklanjanja nepravilnosti u provedbi mjera ili nedostatnosti propisa. Celnici tijela javne vlasti odgovorni su za otklonjanje utvrdenih nedostataka u svojoj nadležnosti. U slucaju utvrdenih nepravilnosti na informacijskom sustavu za koji je provedena periodicna sigurnosna akreditacija, u suradnji sa središnjim državnim tijelom za tehnicka podrucja informacijske sigurnosti, ovisno o vrsti nepravilnosti, utvrduje se daljnja valjanost akreditacije.

Drugim rijecima zakonskim Prijedlogom namjerava se propisati:

- sve sastavnice sustava informacijske sigurnosti, njihov djelokrug i medusobne odnose (središnja državna tijela za informacijsku sigurnost, nacionalni CERT, tijela za planiranje i implementaciju, tijela za nadzor, koordinatori informacijske sigurnosti u tijelima javne vlasti),
- sigurnosna podrucja informacijske sigurnosti (sigurnosne provjere, fizicka sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost vanjske suradnje ili industrijska sigurnost),
- kompleksnu hijerarhiju propisa informacijske sigurnosti (nacionalna politika, uredbe, pravilnici, interni akti za nadzor i provedbu),
- poslove i ovlasti središnjih državnih tijela za informacijsku sigurnost (Ured Vijeca za nacionalnu sigurnost, Zavod za sigurnost informacijskih sustava),
- osnivanje tijela za odgovore na racunalne ugroze (CERT-a) i nacin upravljanja i koordinacije,
- nacin provedbe informacijske sigurnosti, te
- nacin nadzora informacijske sigurnosti.

c) <u>Posljedice koje ce donošenjem Zakona proisteci</u>

Donošenjem predloženog Zakona uvodi se u sustav državne uprave nova vrsta tijela – središnja državna tijela za informacijsku sigurnost, cije ovlasti preuzimaju Ured Vijeca za nacionalnu sigurnost kao glavno koordinacijsko tijelo i Zavod za sigurnost informacijskih sustava kao tijelo za tehnicka podrucja informacijske sigurnosti. Kako bi ova tijela mogla obavljati propisane poslove predlaganja akata i donošenja odgovarajucih pravilnika za primjenu u tijelima javne vlasti, bit ce potrebno provesti izmjene i dopune Zakona o sustavu državne uprave, po uzoru na promjene koje su provedene u prosincu 2003. godine, tijekom uvodenja središnjih državnih ureda u sustav državne uprave (NN 199/2003).

Donošenjem Zakona cjelovito ce se urediti potpuno novo podrucje u Republici Hrvatskoj. Zakonom propisan sustav informacijske sigurnosti u Republici Hrvatskoj sacinjavaju središnja državna tijela za informacijsku sigurnost: Ured Vijeca za nacionalnu sigurnost (UVNS) i Zavod za sigurnost informacijskih sustava (ZSIS), kao okosnica i kljucni elementi sustava, zatim Nacionalni CERT u okviru Hrvatske akademske i istraživacke mreže (CARNet) kao tijelo nadležno za prevenciju i koordinaciju sigurnosnih racunalnih incidenata na javnim racunalnim mrežama, Središnji državni ured za e-Hrvatsku i Ministarstvo znanosti, obrazovanja i športa kao središnja tijela za planiranje i implementaciju propisanih mjera i standarda informacijske sigurnosti u državnom, odnosno obrazovnom i akademskom sektoru, te sigurnosno-obavještajne službe i koordinatori informacijske sigurnosti u svojstvu nadzora propisanih mjera i standarda informacijske sigurnosti u tijelima javne vlasti.

Zakonom se, pored redovitog nadzora informacijske sigurnosti, kojim se osigurava stalni ciklus planiranja, provodenja, provjere i dorade (PDCA) propisa i stanja informacijske sigurnosti u tijelima, po prvi puta uvodi i periodicni proces sigurnosne akreditacije informacijskih sustava i mreža tijela javne vlasti. Ovi aspekti dugorocno ce iznimno povoljno utjecati na bolje planiranje i sustavniju provedbu projekata u tijelima javne vlasti, kako u podrucju informatizacije, tako i u podrucju adaptacije i izgradnje objekata. Tu se primarno misli na uvodenje dodatnih kriterija u nabavi i projektiranju, kriterija koji prate, ne samo sigurnosne aspekte uporabe razlicitih uredaja i sustava i korištenja vanjskih usluga, vec prije svega na mjerila kvalitete i pouzdanosti tijekom njihovog životnog ciklusa. U tom smislu utjecaj mjera i standarda informacijske sigurnosti na troškove informatizacije, adaptacije ili izgradnje objekata ne treba promatrati odvojeno od same funkcionalnosti sustava, objekata, procesa ili osoba na koje se odnose, jer te mjere i standardi moraju predstavljati nužan uvjet realizacije pojedinih projekata i poslovnih procesa. Pri tome, je sadržaj i doseg mjera i standarda informacijske sigurnosti bitno razlicit i primjeren odgovarajucim segmentima tijela javne vlasti.

Prijedlog Zakona ureduje podrucje informacijske sigurnosti u Republici Hrvatskoj u skladu sa stvarnim i predvidenim potrebama Republike Hrvatske, kako u aspektu vlastite nacionalne sigurnosti i razvoja informacijskog društva, tako i u aspektu zahtjeva medunarodnih integracijskih procesa, odnosno sukladnosti sa sigurnosnim politikama NATO-a i EU.

U metodološkom smislu zakonski Prijedlog koncipira sustav instrumenata raspoloživih u sustavima informacijske sigurnosti zemalja EU i NATO-a, te optimalan s aspekta potreba Republike Hrvatske. Prijedlog u potpunosti slijedi strukovne potrebe i zahtjeve za ucinkovitošcu mjera i standarda informacijske sigurnosti u uvjetima naraslih i izmijenjenih prijetnji i izazova uslijed tehnološke i informacijske revolucije koja se odvija. Nužnost razlicitih oblika državnih ili vojnih integracija, medunarodne suradnje na suzbijanju ugroza kao što su organizirani kriminal ili terorizam, pa do razlicitih pojavnih oblika racunalnog i kibernetickog kriminala kojima smo vec sada okruženi, traži uvodenje minimalnih sigurnosnih zahtjeva informacijske sigurnosti u svakoj državi koja želi participirati u medunarodnoj zajednici, te osposobljenu i medunarodno usklađenu nacionalnu organizaciju nadležnih tijela, koja ce takve minimalne zahtjeve ne samo uspostaviti vec i trajno održavati.

Propisivanjem sustava informacijske sigurnosti sa širokim zahvatom u sva tijela javne vlasti te dobrom koordinacijom središnjih državnih tijela za informacijsku sigurnost i nacionalnog CERT-a nadležnog za javne racunalne mreže u Republici Hrvatskoj, osigurava se temelj za daljnje poticanje informacijske sigurnosti u cjelokupnom društvu, kroz procese normizacije u Republici Hrvatskoj i javno-privatnog partnerstva. Na taj nacin osiguravaju se preduvjeti za

strateški nacionalni interes stvaranja informacijskog društva kao preduvjeta gospodarskog prosperiteta Republike Hrvatske u iducem desetljecu.

Ovaj zakonski Prijedlog predstavlja zakonski okvir za izgradnju nacionalnog sustava informacijske sigurnosti, koji definira nadležnosti tijela za razvoj i donošenje nacionalnih mjera i standarda informacijske sigurnosti cime ce se uz donošenje potrebne podzakonske regulative, uspostaviti sustav informacijske sigurnosti u Republici Hrvatskoj. Ovako koncipiran, sustav informacijske sigurnosti je važan dio šireg sustava nacionalne sigurnosti Republike Hrvatske, ali i neophodan temelj za izgradnju informacijskog društva i buduci gospodarski prosperitet Republike Hrvatske, te uvjet medunarodnih integracijskih procesa u NATO i EU.

Drugim rijecima zakonski Prijedlog garantira sljedece:

1. **Cjelovit i jedinstven, pravno ureden okvir sustava informacijske sigurnosti, kao dio šireg sustava nacionalne sigurnosti Republike Hrvatske**
2. **Racionalnu i jasnu podjelu funkcionalnih nadležnosti izmedu nadležnih tijela, te uspostavu središnjih državnih tijela za ucinkovitu koordinaciju i usmjeravanje informacijske sigurnosti i razvoj nacionalnih standarda informacijske sigurnosti**
3. **Sustav informacijske sigurnosti sa širokim zahvatom u tijela javne vlasti kao temelj za sustavnu izgradnju informacijskog društva u Republici Hrvatskoj i preduvjet buduceg gospodarskog prosperiteta**
4. **Medunarodno pravno uskladen pristup informacijskoj sigurnosti, prilagoden za uvjete i potrebe Republike Hrvatske, kao garancija sukladnosti sa temeljnim zahtjevima integracijskih procesa u NATO i EU.**

III. OCJENA POTREBNIH SREDSTAVA ZA PROVOĐENJE ZAKONA

Ocjenjuje se da donošenje i provedba ovog Zakona nece iziskivati osiguranje dodatnih sredstava u Državnom proracunu Republike Hrvatske.

Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske predvideno je osnivanje Zavoda za sigurnost informacijskih sustava (ZSIS) kao pravnog sljednika Zavoda za informacijsku sigurnost i kripto-zaštitnu tehnologiju, a Ured Vijeca za nacionalnu sigurnost i sigurnosno-obavještajne službe postojece su institucije, cije su nadležnosti iz Zakona o informacijskoj sigurnosti uskladene u novom Zakonu o sigurnosno-obavještajnom sustavu Republike Hrvatske.

Jedino novo tijelo je Nacionalni CERT, koji je nova ustrojstvena jedinica postojece ustanove Hrvatske akademske i istraživacke mreže (CARNet), i koji ce se temeljiti na postojecem CERT-u, vec niz godina nadležnom za akademski sektor. CARNet je proracunski u nadležnosti Ministarstva znanosti, obrazovanja i športa, s kojim je usuglašena potrebna promjena statuta, slijedom koje se ocekuje manje povecanje troškova uslijed proširenja kadrovske baze i djelokruga poslova postojeceg CARNet CERT-a.

IV. TEKST NACRTA PRIJEDLOGA ZAKONA O INFORMACIJSKOJ SIGURNOSTI S OBRAZLOŽENJEM

Tekst Nacrta prijedloga zakona dan je u obliku Nacrta prijedloga Zakona o informacijskoj sigurnosti s obrazloženjem.

NACRT PRIJEDLOGA

ZAKONA O INFORMACIJSKOJ SIGURNOSTI

I. TEMELJNE ODREDBE

Clanak 1.

(1) Ovim se Zakonom uredu ju instituti informacijske sigurnosti i informacijskog sustava, sigurnosna podrucja informacijske sigurnosti, te nadležna tijela za usmjeravanje, provedbu i nadzor informacijske sigurnosti.

(2) Ovaj Zakon se primjenjuje na državna tijela, tijela jedinica lokalne i podrucne (regionalne) samouprave, te pravne osobe s javnim ovlastima (u daljnjem tekstu – tijela javne vlasti).

(3) Ovaj Zakon se primjenjuje i na pravne i fizicke osobe koje prilikom poslovanja s tijelima javne vlasti Republike Hrvatske ili na neki drugi nacin ostvare pristup klasificiranim podacima.

Clanak 2.

(1) Informacijski sustav u smislu ovog Zakona je svaki komunikacijski, racunalni ili drugi elektronicki sustav u kojem podaci nastaju, obraduju se, pohranjuju se ili se prenose, tako da budu dostupni i upotrebljivi za ovlaštene korisnike.

(2) Informacijska sigurnost u smislu ovog Zakona predstavlja skup propisanih mjera i standarda zaštite tajnosti i ogranicenja uporabe podataka, u cilju postizanja odgovarajuce povjerljivosti, cjelovitosti i raspoloživosti podataka te cjelovitosti i raspoloživosti informacijskih sustava u kojima podaci nastaju, obraduju se, pohranjuju se ili se prenose.

II. SIGURNOSNA PODRUCJA INFORMACIJSKE SIGURNOSTI

Clanak 3.

Zaštita tajnosti i ogranicenje uporabe podataka provode se primjenom propisanih mjera i standarda u okviru sigurnosnih podrucja informacijske sigurnosti:

- sigurnosne provjere osoblja,
- fizicka sigurnost,
- sigurnost podataka,
- sigurnost informacijskih sustava i
- sigurnost vanjske suradnje (industrijska sigurnost).

Clanak 4.

(1) Sigurnosne provjere osoblja iz clanka 3. ovog Zakona, obuhvacaju postupke:

- izdavanja uvjerenja o sigurnosnoj provjeri osobe (u daljnjem tekstu certifikat), koje provodi središnje državno tijelo za informacijsku sigurnost, na zahtjev tijela javne vlasti, a za osobe koje imaju poslovnu potrebu pristupati klasificiranim podacima u tim tijelima;

- provedbe sigurnosne provjere osoba iz alineje 1. ovog stavka, koju vrši nadležna sigurnosno-obavještajna služba na zahtjev središnjeg državnog tijela za informacijsku sigurnost.

(2) Fizicka sigurnost iz clanka 3. ovog Zakona obuhvaca postupke:

- sigurnosne kategorizacije objekata i prostora, koju u svrhu primjene odgovarajucih mjera fizicke i tehnicke zaštite objekata i prostora, provode tijela javne vlasti koja u svom radu koriste ili pohranjuju klasificirane podatke;

- provedbe mjera sprjecavanja, odvracanja i otkrivanja pokušaja neovlaštenog pristupa, te reagiranja na takve pokušaje neovlaštenog pristupa u objekte i prostore iz alineje 1. ovog stavka, kao i mjera osiguranja odgovarajucih uvjeta za pohranu klasificiranih podataka u tim objektima i prostorima.

(3) Sigurnost podataka iz clanka 3. ovog Zakona obuhvaca postupke:

- utvrdivanja sigurnosnih mjera i standarda za pristup i postupanje s klasificiranim i neklasificiranim podacima u poslovnim procesima (uredsko poslovanje) tijela javne vlasti;

- provedbe mjera sigurnosti klasificiranih podataka primjenom postupaka iz stavaka 1., 2., 4. i 5. ovoga clanka.

(4) Sigurnost informacijskih sustava iz clanka 3. ovog Zakona obuhvaca postupke:

- utvrdivanja sigurnosnih mjera i standarda u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskih sustava tijela javne vlasti, u kojima klasificirani i neklasificirani podaci nastaju, obraduju se, pohranjuju se ili se prenose;

- provedbe mjera sigurnosti informacijskih sustava iz alineje 1. ovog stavka te primjena postupaka iz stavaka 1., 2., 3. i 5. ovoga clanka na informacijske sustave i osoblje koje radi na poslovima vezanim za te informacijske sustave.

(5) Sigurnost vanjske suradnje iz clanka 3. ovog Zakona obuhvaca postupke:

- primjene propisanih sigurnosnih mjera u poslovanju fizickih i pravnih osoba s tijelima javne vlasti u okviru kojeg te fizicke i pravne osobe ostvaruju pristup klasificiranim podacima;

- izdavanja certifikata fizickih i pravnih osoba iz alineje 1. ovog stavka, koje izdaje središnje državno tijelo za informacijsku sigurnost, na zahtjev tijela javne vlasti i uz suglasnost fizicke i pravne osobe iz tocke 1. ovog stavka;

- provedbe sigurnosnih provjera fizickih i pravnih osoba iz alineje 1. ovog stavka, koju provodi nadležna sigurnosno-obavještajna služba, na zahtjev središnjeg državnog tijela za informacijsku sigurnost.

Clanak 5.

(1) Usmjeravanje svih aktivnosti, mjera i standarda iz clanka 4. stavaka 1., 2., 3. i 5. ovog Zakona, u tijelima javne vlasti i pravnim i fizickim osobama iz clanka 1., stavka 3. ovog Zakona, provodi središnje državno tijelo za informacijsku sigurnost, u suradnji s drugim tijelima u Republici Hrvatskoj nadležnim za poslove propisane ovim Zakonom.

(2) Usmjeravanje svih aktivnosti, mjera i standarda iz clanka 4., stavka 4. ovog Zakona, u tijelima javne vlasti provodi središnje državno tijelo za tehnicka podrucja informacijske sigurnosti, u suradnji sa središnjim državnim tijelom za informacijsku sigurnost iz stavka 1. ovog clanka i drugim tijelima u Republici Hrvatskoj nadležnim za poslove propisane ovim Zakonom.

III. PROPISI INFORMACIJSKE SIGURNOSTI

Clanak 6.

(1) Nacionalnu politiku informacijske sigurnosti u Republici Hrvatskoj donosi Hrvatski sabor, na prijedlog Vlade Republike Hrvatske, uz prethodnu suglasnost Predsjednika Republike Hrvatske.

(2) Nacionalna politika informacijske sigurnosti je dokument kojim Hrvatski sabor utvrduje temeljne ciljeve, nacela i dosege primjene informacijske sigurnosti u Republici Hrvatskoj, nužne za sustavno kreiranje i provedbu mjera i standarda sigurnosnih podrucja informacijske sigurnosti u tijelima javne vlasti, a cime se osigurava postojanost sustava javne vlasti u Republici Hrvatskoj te postiže uvodenje zajednickih kriterija i minimalnih zahtjeva informacijske sigurnosti u sva tijela javne vlasti.

Clanak 7.

Na temelju Nacionalne politike informacijske sigurnosti iz clanka 6. stavka 2., Vlada Republike Hrvatske uredbama propisuje skupove mjera za svako pojedino sigurnosno podrucje iz clanka 3., stavka 1., alineje 1. do 5. ovog Zakona, kao i primjenu tih mjera na odgovarajuce vrste klasificiranih i neklasificiranih podataka.

IV. SREDIŠNJA DRŽAVNA TIJELA ZA INFORMACIJSKU SIGURNOST

Ured Vijeca za nacionalnu sigurnost

Clanak 8.

Ured Vijeca za nacionalnu sigurnost (UVNS) je središnje državno tijelo za informacijsku sigurnost koje je odgovorno za koordinaciju aktivnosti vezanih za primjenu mjera i donošenje standarda informacijske sigurnosti u tijelima javne vlasti u Republici Hrvatskoj, kao i za uskladenost aktivnosti oko primjene mjera i standarda informacijske sigurnosti u razmjeni klasificiranih podataka izmedu Republike Hrvatske i stranih zemalja i organizacija.

Clanak 9.

(1) Ured Vijeca za nacionalnu sigurnost donosi pravilnike kojima se reguliraju standardi zaštite tajnosti i ogranicenja uporabe podataka u tijelima javne vlasti i pravnim i fizickim osobama iz clanka 1. stavka 3. ovog Zakona, a u okviru sigurnosnih podrucja informacijske sigurnosti koja su u njegovoj nadležnosti.

(2) Ured Vijeca za nacionalnu sigurnost uskladuje standarde iz stavka 1. ovog clanka sa zahtjevima integracijskih procesa koje provodi Republika Hrvatska i drugim medunarodnim standardima i preporukama informacijske sigurnosti, te sudjeluje u nacionalnoj normizaciji podrucja informacijske sigurnosti.

Clanak 10.

Ured Vijeca za nacionalnu sigurnost koordinira i uskladuje rad svih tijela javne vlasti koja sudjeluju u izradi i provedbi propisa informacijske sigurnosti, kao i tijela koja imaju odredene nadležnosti u podrucju informacijske sigurnosti.

Zavod za sigurnost informacijskih sustava

Clanak 11.

Zavod za sigurnost informacijskih sustava (ZSIS) je središnje državno tijelo za tehnicka podrucja informacijske sigurnosti koji skrbi o:

- sigurnosti informacijskih sustava i mreža tijela javne vlasti,
- sigurnosnim akreditacijama informacijskih sustava i mreža tijela javne vlasti,
- upravljanju kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka izmedu tijela javne vlasti te izmedu Republike Hrvatske i stranih zemalja i organizacija,
- koordinaciji prevencije i otklanjanja problema vezanih uz sigurnost racunalnih mreža u tijelima javne vlasti.

Clanak 12.

(1) Zavod za sigurnost informacijskih sustava donosi pravilnike kojima se reguliraju standardi zaštite tajnosti i ogranicenja uporabe podataka u tijelima javne vlasti, a u okviru sigurnosnog podrucja informacijske sigurnosti koje je u njegovoj nadležnosti.

(2) Zavod za sigurnost informacijskih sustava uskladuje standarde iz stavka 1. ovog clanka sa zahtjevima integracijskih procesa koje provodi Republika Hrvatska i drugim medunarodnim standardima i preporukama informacijske sigurnosti, te sudjeluje u nacionalnoj normizaciji podrucja informacijske sigurnosti.

Clanak 13.

Zavod za sigurnost informacijskih sustava obavlja poslove periodicne sigurnosne akreditacije informacijskih sustava i mreža državnih tijela i tijela lokalne i podrucne (regionalne) samouprave u Republici Hrvatskoj, a za pravne osobe s javnim ovlastima u Republici Hrvatskoj te poslove obavlja u koordinaciji sa Hrvatskom akreditacijskom agencijom (HAA).

Clanak 14.

Razrada poslova središnjih državnih tijela za informacijsku sigurnost iz clanaka 8. i 11. ovog Zakona uredit ce se uredbama Vlade Republike Hrvatske, na prijedlog celnika nadležnih tijela i u skladu s ovim Zakonom.

V. NACIONALNI CERT

Clanak 15.

(1) Poslove prevencije i otklanjanja problema vezanih uz sigurnost racunalnih mreža u Republici Hrvatskoj, obavlja nacionalno tijelo za prevenciju i odgovor na racunalne ugroze (u daljnjem tekstu CERT), koji se kao zasebna ustrojstvena jedinica ustrojava u Hrvatskoj akademskoj i istraživackoj mreži (u daljnjem tekstu CARNet).

(2) CERT je odgovoran za prevenciju i koordinaciju postupanja vezanih za sigurnosne racunalne incidente u Republici Hrvatskoj, kao i za one koji su povezani sa stranim zemljama i organizacijama.

(3) CERT je ovlašten za koordiniranje rada istovrsnih tijela koja rade na prevenciji i otklanjanju problema vezanih uz sigurnost racunalnih mreža u Republici Hrvatskoj, te odreduje pravila i nacine zajednickog rada takvih tijela u svrhu preventivnog djelovanja i ucinkovite koordinacije pri rješavanju problema vezanih uz sigurnost racunalnih mreža u Republici Hrvatskoj.

Clanak 16.

CERT suraduje s Zavodom za sigurnost informacijskih sustava u izradi propisa u okviru podrucja sigurnosti informacijskih sustava i mreža tijela javne vlasti, te izraduje i sudjeluje u izradi preporuka i normi u Republici Hrvatskoj iz podrucja sigurnosti informacijskih sustava.

Clanak 17.

(1) Ravnatelj CARNet-a, uz suglasnost celnika Ureda Vijeca za nacionalnu sigurnost, imenuje svog pomocnika zaduženog za upravljanje CERT-om.

(2) Razrada poslova CERT-a provest ce se na nacin propisan za izmjenu statuta CARNet-a, na prijedlog ravnatelja CARNet-a, uz prethodnu suglasnost celnika Ureda Vijeca za nacionalnu sigurnost i Zavoda za sigurnost informacijskih sustava te u skladu s ovim Zakonom.

(3) Za sve službenike CERT-a i ostale službenike CARNet-a, koji u svome poslu imaju potrebu pristupati klasificiranim podacima, provodi se propisani postupak sigurnosne provjere.

VI. PROVEDBA INFORMACIJSKE SIGURNOSTI

Clanak 18.

(1) Tijela javne vlasti, sukladno pravilnicima iz clanka 9., stavka 1. i clanka 12., stavka 1. ovog Zakona, dužna su provesti propisane standarde informacijske sigurnosti.

(2) Za tijela javne vlasti koja nemaju ustrojene odgovarajuce informaticke i tehnicke ustrojstvene jedinice, poslove iz stavka 1. ovog clanka, na njihov zahtjev, obavlja središnje tijelo državne uprave nadležno za razvitak informacijskog sustava državne uprave, a u okviru obrazovnog i akademskog sektora ove poslove obavlja središnje tijelo državne uprave nadležno za znanost i obrazovanje.

(3) Za obavljanje poslova iz stavka 2. ovog clanka središnje tijelo državne uprave nadležno za razvitak informacijskog sustava državne uprave koristi usluge posebnih tijela za potporu informacijskih sustava, a središnje tijelo državne uprave nadležno za znanost i obrazovanje za obavljanje poslova iz stavka 1. ovog clanka koristi usluge CARNet-a i Sveucilišnog racunskog centra (SRCE).

VII. NADZOR INFORMACIJSKE SIGURNOSTI

Clanak 19.

(1) Poslovi nadzora informacijske sigurnosti su poslovi redovitog nadzora organizacije, provedbe, stanja i ucinkovitosti propisanih mjera i standarda u okviru sigurnosnih podrucja informacijske sigurnosti u tijelima javne vlasti.

(2) Poslove nadzora iz stavka 1. ovog clanka, u središnjim tijelima državne uprave i tijelima za potporu informacijskih sustava iz clanka 18., stavka 3. ovog Zakona, provode nadležne sigurnosno-obavještajne službe, a u ostalim tijelima javne vlasti ovaj nadzor provode osobe imenovane za koordinatore informacijske sigurnosti u odredenim tijelima javne vlasti.

(3) Tijela javne vlasti obvezna su u svoje unutarnja ustrojstva ugraditi radna mjesta koordinatora informacijske sigurnosti.

(4) Sigurnosno-obavještajne službe donose interne akte za obavljanje poslova nadzora iz stavka 2. ovog clanka, uz suglasnost središnjih državnih tijela za informacijsku sigurnost i u skladu s ovim Zakonom i podzakonskim propisima.

(5) Vlada Republike Hrvatske donijeti ce na prijedlog Ureda Vijeca za nacionalnu sigurnost, a uz prethodno mišljenje Zavoda za sigurnost informacijskih sustava, u skladu s ovim Zakonom i podzakonskim propisima, uredbu o poslovima koordinatora informacijske sigurnosti u tijelima javne vlasti iz stavka 2. ovog clanka, kojim utvrduje uvjete i vrstu poslova za ova radna mjesta, te rokove u kojima ova tijela trebaju provesti imenovanja koordinatora, pri cemu tako odredeni koordinatori informacijske sigurnosti mogu biti lokalni za pojedino tijelo ili centralni za odgovarajucu grupu tijela javne vlasti.

(6) Tijela nadležna za nadzor, o rezultatima svakog nadzora donose izvješce koje dostavljaju celniku tijela javne vlasti, odgovornom za poduzimanje mjera za otklanjanje svih uocenih nedostataka, te središnjem državnom tijelu za informacijsku sigurnost odgovornom za pokretanje postupka utvrdivanja odgovornosti za propuste.

(7) Pored utvrdivanja odgovornosti za propuste središnje državno tijelo za informacijsku sigurnost temeljem uocenih nedostataka po potrebi potice postupak izmjene propisa informacijske sigurnosti, te provodi postupak preispitivanja daljnje valjanosti sigurnosne akreditacije informacijskih sustava i mreža u tijelu, u suradnji sa Zavodom za sigurnost informacijskih sustava.

VIII. PRIJELAZNE I ZAVRŠNE ODREDBE

Clanak 20.

(1) Vlada Republike Hrvatske, uz prethodnu suglasnost Predsjednika Republike Hrvatske, uskladuje Uredbu o unutarnjem ustrojstvu Ureda Vijeca za nacionalnu sigurnost prema odredbama ovog Zakona i u roku od šest mjeseci nakon stupanja na snagu ovoga Zakona.

(2) Vlada Republike Hrvatske, Savjet za koordinaciju sigurnosno-obavještajnih agencija i Ured Vijeca za nacionalnu sigurnost, osigurat ce potrebne materijalno-tehnicke i kadrovske preduvjete za pocetak rada Zavoda za sigurnost informacijskih sustava, a na nacin koji osigurava da ovaj Zavod preuzme poslove središnjeg državnog tijela za tehnicka podrucja informacijske sigurnosti u roku od šest mjeseci nakon stupanja na snagu ovog Zakona.

(3) CARNet utvrduje svoje unutarnje ustrojstvo na nacin koji osigurava osnivanje CERT-a i provedbu poslova sukladno clancima 15. do 17. ovog Zakona, u roku od devet mjeseci nakon stupanja na snagu ovog Zakona.

Clanak 21.

(1) Vlada Republike Hrvatske, uz suglasnost Predsjednika Republike Hrvatske, predložit ce Hrvatskom Saboru donošenje Nacionalne politike informacijske sigurnosti u Republici Hrvatskoj iz clanka 6. ovog Zakona, u roku od šest mjeseci nakon stupanja na snagu ovog Zakona.

(2) Vlada Republike Hrvatske donijet ce uredbe iz clanaka 7., 14. ovog Zakona, u roku od devet mjeseci nakon stupanja na snagu ovog Zakona, a uredbu iz clanka 19. stavka 5. ovog Zakona, u roku od osamnaest mjeseci nakon stupanja na snagu ovog Zakona

(3) CARNet ce provesti izmjene statuta iz clanka 17., stavka 2. ovog Zakona, u roku od devet mjeseci nakon stupanja na snagu ovog Zakona.

(4) Ured Vijeca za nacionalnu sigurnost donijet ce Pravilnike iz clanka 9., stavka 1. ovog Zakona, u roku od osamnaest mjeseci nakon stupanja na snagu ovog Zakona.

(5) Zavod za sigurnost informacijskih sustava donijet ce Pravilnike iz clanka 12., stavka 1. ovog Zakona, u roku od osamnaest mjeseci nakon stupanja na snagu ovog Zakona.

Clanak 22.

(1) Tijela nadležna za poslove provedbe informacijske sigurnosti iz clanka 18., stavka 2. i poslove nadzora informacijske sigurnosti iz clanka 19., stavka 2. ovog Zakona, dužna su, uz suglasnost središnjih državnih tijela za informacijsku sigurnost, donijeti odgovarajuce interne akte za obavljanje tih poslova, u roku od osamnaest mjeseci nakon stupanja na snagu ovog Zakona.

(2) Tijela javne vlasti i tijela nadležna za poslove provedbe informacijske sigurnosti iz clanka 18., stavka 3. ovog Zakona, dužna su u roku od tri mjeseca od donošenja mjerodavnih Pravilnika iz clanka 21., stavaka 4. i 5. ovog Zakona, donijeti odgovarajuce interne akte o provedbi informacijske sigurnosti u tijelu javne vlasti.

(3) Tijela javne vlasti i tijela nadležna za poslove provedbe informacijske sigurnosti dužna su provesti interne akte iz stavka 2. ovog clanka u roku od šest mjeseci od njihovog donošenja.

Clanak 23.

Ovaj Zakon stupa na snagu osmog dana od objave u Narodnim novinama.

OBRAZLOŽENJE

Glava I., TEMELJNE ODREDBE

Prijedlogom Nacrta Zakona o informacijskoj sigurnosti uvodi se i regulira novo podrucje informacijske sigurnosti u Republici Hrvatskoj. U clanku 1. odreduje se i djelokrug primjene Zakona na državna tijela, tijela jedinica lokalne i podrucne (regionalne) samouprave, te pravne osobe s javnim ovlastima (u daljnjem tekstu - tijela javne vlasti). Zakon se primjenjuje i na pravne i fizicke osobe koje prilikom poslovanja s tijelima javne vlasti ili na neki drugi nacin ostvare pristup klasificiranim podacima. U clanku 2. Definiraju se pojmovi informacijskog sustava i informacijske sigurnosti. Informacijska sigurnost tako u smislu ovog Zakona predstavlja skup propisanih mjera i standarda zaštite tajnosti i ogranicenja uporabe podataka, u cilju postizanja odgovarajuce povjerljivosti, cjelovitosti i raspoloživosti podataka te cjelovitosti i raspoloživosti informacijskih sustava u kojima podaci nastaju, obraduju se, pohranjuju se ili se prenose.

Glava II., SIGURNOSNA PODRUCJA INFORMACIJSKE SIGURNOSTI

U clanku 3. i 4. definiraju se sigurnosna podrucja informacijske sigurnosti: sigurnosne provjere osoblja, fizicka sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost vanjske suradnje (industrijska sigurnost), u okviru kojih se primjenjuju propisane mjere i standardi u svrhu zaštite tajnosti i ogranicenja uporabe podataka.

U clanku 5. utvrduje se primarna nadležnost središnjih državnih tijela za informacijsku sigurnost nad ovim sigurnosnim podrucjima informacijske sigurnosti, tako da je Ured Vijeca za nacionalnu sigurnost (UVNS) nadležan za sigurnosne provjere osoblja, fizicku sigurnost, sigurnost podataka i sigurnost vanjske suradnje (industrijska sigurnost), a Zavod za sigurnost informacijskih sustava (ZSIS) za sigurnost informacijskih sustava.

Glava III., PROPISI INFORMACIJSKE SIGURNOSTI

Clankom 6. se definira temeljni propis, Nacionalna politika informacijske sigurnosti u Republici Hrvatskoj, koju donosi Hrvatski sabor, na prijedlog Vlade Republike Hrvatske, uz prethodnu suglasnost Predsjednika Republike Hrvatske, kojom se utvrduje temeljne ciljeve, nacela i dosege primjene informacijske sigurnosti u Republici Hrvatskoj, nužne za sustavno kreiranje i provedbu mjera i standarda sigurnosnih podrucja informacijske sigurnosti u tijelima javne vlasti, a cime se osigurava postojanost sustava javne vlasti u Republici Hrvatskoj te postiže uvodenje zajednickih kriterija i minimalnih zahtjeva informacijske sigurnosti u svim tijelima javne vlasti.

Clankom 7. se propisuje razrada mjera informacijske sigurnosti, koje proizlaze iz ovog Zakona i Nacionalne politike informacijske sigurnosti, te koje donosi Vlada RH za pojedina sigurnosna podrucja informacijske sigurnosti.

Glava IV., SREDIŠNJA DRŽAVNA TIJELA ZA INFORMACIJSKU SIGURNOST

U clancima 8. do 10. odreduju se nadležnosti UVNS-a kao središnjeg državnog tijela za informacijsku sigurnost (nacionalni NSA) koje je odgovorno za koordinaciju aktivnosti vezanih za primjenu mjera i donošenje standarda informacijske sigurnosti u tijelima javne vlasti u RH, kao i za uskladenost aktivnosti oko primjene mjera i standarda informacijske

sigurnosti u razmjeni klasificiranih podataka izmedu RH i stranih zemalja i organizacija. Tako se clankom 9. propisuje da UVNS donosi pravilnike iz sigurnosnih podrucja za koja je nadležan, kojima se reguliraju standardi za provedbu mjera iz Vladinih uredbi u tijelima javne vlasti. Takoder se clankom 10. definira odnos prema nacionalnom normizacijskom procesu te utvrduje UVNS kao vršno tijelo nadležno za koordinaciju svih aktivnosti u podrucju informacijske sigurnosti i koordinaciju svih drugih tijela koja participiraju u podrucju informacijske sigurnosti.

U clancima 11. do 13. odreduju se nadležnosti ZSIS-a kao središnjeg državnog tijela za tehnicka podrucja informacijske sigurnosti (nacionalni NCSA) koji skrbi o sigurnosti informacijskih sustava i mreža tijela javne vlasti, sigurnosnim akreditacijama informacijskih sustava i mreža tijela javne vlasti, upravljanju kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka izmedu tijela javne vlasti te izmedu Republike Hrvatske i stranih zemalja i organizacija i koordinaciji prevencije i otklanjanja problema vezanih uz sigurnost racunalnih mreža u tijelima javne vlasti. Tako se clankom 12. propisuje da ZSIS donosi pravilnike iz sigurnosnih podrucja za koja je nadležan, kojima se reguliraju standardi za provedbu mjera iz Vladinih uredbi u tijelima javne vlasti. Takoder se clankom 12. i 13. definira odnos prema nacionalnom normizacijskom i akreditacijskom procesu te utvrduje nadležnost ZSIS za poslove sigurnosnih akreditacija (nacionalni SAA) informacijskih sustava i mreža tijela javne vlasti

Clankom 14. propisuje se obveza uredivanja poslova središnjih državnih tijela za informacijsku sigurnost, UVNS-a i ZSIS-a, uredbama Vlade Republike Hrvatske, na prijedlog celnika tih tijela i u skladu s ovim Zakonom.

Glava V., NACIONALNI CERT

U clancima 15. do 17. definira se novo nacionalno tijelo za prevenciju i odgovor na racunalne ugroze (u daljnjem tekstu CERT) koje obavlja poslove prevencije i otklanjanja problema vezanih uz sigurnost racunalnih mreža u Republici Hrvatskoj. CERT se kao zasebna ustrojstvena jedinica ustrojava u Hrvatskoj akademskoj i istraživackoj mreži (u daljnjem tekstu CARNet). Clankom 16. se utvrduje potrebna koordinacija CERT-a i ZSIS-a u podrucju sigurnosti informacijskih sustava i normizaciji ovog podrucja u RH, a u clanku 17. definiran je nacin postavljanja celnog covjeka i razrada poslova CERT-a, koji osiguravaju medusobnu usklađenost rada CERT-a i središnjih državnih tijela za informacijsku sigurnost UVNS-a i ZSIS-a.

Glava VI., PROVEDBA INFORMACIJSKE SIGURNOSTI

Clankom 18. propisuje se obveza provodenja propisanih standarda informacijske sigurnosti temeljem pravilnika koje donose UVNS i ZSIS, a koji su usklađeni s uredbama Vlade RH koje utvrduju mjere informacijske sigurnosti i Nacionalnom politikom informacijske sigurnosti kojom su definirani opci ciljevi i dosezi primjene informacijske sigurnosti. U stavku 2. definira se da u tijelima javne vlasti koja nemaju ustrojene odgovarajuce informaticke i tehnicke ustrojstvene jedinice, nadležnost za poslove provedbe informacijske sigurnosti ima Središnji državni ured za e-Hrvatsku, koji u tu svrhu koristi usluge posebnih tijela za potporu informacijskih sustava (stavak 3.), dok u okviru obrazovnog i akademskog sektora nadležnost za poslove provedbe informacijske sigurnosti ima Ministarstvo znanosti, obrazovanja i športa, koje u tu svrhu koristi usluge CARNet-a i Sveucilišnog racunskog centra (SRCE) (stavak 3.).

Glava VII., NADZOR INFORMACIJSKE SIGURNOSTI

Clankom 19. definiran je segment nadzora informacijske sigurnosti u tijelima javne vlasti, kao redoviti nadzor organizacije, provedbe, stanja i ucinkovitosti propisanih mjera i standarda (stavak 1.). Poslove nadzora u središnjim tijelima državne uprave i tijelima za potporu informacijskih sustava provode nadležne sigurnosno-obavještajne službe (civilna i vojna), a u ostalim tijelima javne vlasti ovaj nadzor provode osobe imenovane za koordinatore informacijske sigurnosti u odredenim tijelima javne vlasti (stavak 2.), koja su obvezna u svoja unutarnja ustrojstva ugraditi odgovarajuca radna mjesta koordinatora informacijske sigurnosti (stavak 3.). U stavcima 4. i 5. propisuju se potrebni akti za provodenje nadzora od strane tijela i koordinatora, te utvrduje mogucnost da se koordinatori optimalno razmjeste po konceptu centralnih ili lokalnih koordinatora u tijelima javne vlasti ili kombinirano. U stavcima 6. i 7. utvrduje se nacin izvješcivanja i postupanja vezano za rezultate nadzora

Glava VIII., PRIJELAZNE I ZAVRŠNE ODREDBE

Prijelaznim i završnim odredbama u clancima 20. do 22. definira se dinamika donošenja kompleksne hijerarhije podzakonske regulative propisane Zakonom u odnosu na vrijeme donošenja ovog Zakona.

Clanak 20. propisuje rokove za utvrdivanje unutarnjeg ustroja UVNS-a, ZSIS-a na 6 mjeseci, te CERT-a (CARNet-a) na 9 mjeseci. U stavku 2. utvrduje se obveza nadležnih tijela (UVNS, Savjet za koordinaciju sigurnosno-obavještajnih agencija, Vlada RH) da osiguraju potrebne materijalno-tehnicke i kadrovske preduvjete za pocetak rada Zavoda za sigurnost informacijskih sustava. Iako se Zavod osniva temeljem Zakona o sigurnosno-obavještajnom sustavu RH, to je potrebno zbog dinamike provedbe ovog Zakona.

Clanak 21. propisuje rokove za donošenje propisa informacijske sigurnosti. Nacionalna politika informacijske sigurnosti u Republici Hrvatskoj donosi se u roku od šest mjeseci, Uredbe Vlade o mjerama informacijske sigurnosti u okviru podrucja informacijske sigurnosti donose se u roku od 9 mjeseci, kao i uredbe Vlade o razradi poslova središnjih državnih tijela za informacijsku sigurnost te izmjene statuta CARNet-a u poslovima CERT-a. Uredba Vlade RH o poslovima koordinatora informacijske sigurnosti u tijelima javne vlasti treba se donijeti u roku od 18 mjeseci.

UVNS i ZSIS moraju donijeti pravilnike o standardima informacijske sigurnosti u tijelima javne vlasti, za sigurnosna podrucja za koja su nadležni, u roku od 18 mjeseci (clanak 21. stavci 4. i 5.).

Clanak 22. propisuje rokove za poslove provedbe i nadzora informacijske sigurnosti, tako da se interni akti tijela o nacinu provodenja tih poslova trebaju donijeti u roku od 18 mjeseci. Sva tijela zadužena za provedbu (tijela javne vlasti ili centralna tijela) u roku od 3 mjeseca od donošenja mjerodavnih pravilnika dužna su donijeti interne akte o konkretnoj provedbi u pojedinom tijelu javne vlasti (stavak 2.). Za samu provedbu informacijske sigurnosti propisan je rok od 6 mjeseci nakon toga.