REPUBLIKA HRVATSKA
UREDVIJEĆA ZA NACIONALNU SIGURNOST

NACRT PRIJEDLOGA

ZAKONA O SUSTAVU INFORMACIJSKE SIGURNOSTI

Zagreb, siječanj 2007.

I. USTAVNA OSNOVA ZA DONOŠENJE ZAKONA

Ustavna osnova za donošenje ovog Zakona sadržana je u odredbama članka 37. stavak 2. Ustava Republike Hrvatske.

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

a) Ocjena stanja

Područje koje se ovim zakonskim prijedlogom treba urediti djelomično 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 utvrđivanju mjerila za određivanje tajnih podataka obrane te posebnim i općim postupcima za njihovo čuvanje (NN 70/91). Na taj način se ovo važno područje tajnosti podataka po prvi puta u Republici Hrvatskoj uredilo Zakonom, kojim su postavljena načela tajnosti podataka, vrste tajnosti i klasifikacija, postupci za određivanje tajnosti, nadležnosti tijela te zaštitne mjere. U području načela tajnosti podataka ovaj Zakon propisao je niz rješenja preuzetih iz 80-tih godina dvadesetog stoljeća, koja nisu u skladu sa suvremenim standardima tajnosti podataka zemalja EU-a, članica NATO-a i drugih razvijenih demokratskih zemalja svijeta. Primjerice, to su neodgovarajuća klasifikacija prema stupnjevima i vrstama tajnosti za državne podatke, nepostojanje elementarnih načela za pristup tajnim podacima kao što su poslovna ili službena potreba (need-to-know) i sigurnosna provjera s certifikatom za osobe s pravom pristupa tajnim podacima te neprimjereno tretiranje temeljnih demokratskih standarda kao što su zaštita osobnih podataka i pojam privatnosti općenito. Dio ove materije koji se odnosi na sve pravne i fizičke osobe u Republici Hrvatskoj, u međuvremenu 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 međunarodno prihvaćen način tretirati pojmove klasificiranih i neklasificiranih podataka državne uprave, stupnjeve i principe klasificiranja, kao i načela pristupa tajnim podacima.

Zakon o zaštiti tajnosti podataka (NN 108/96) nadalje propisuje način određivanja zaštitnih mjera za zaštitu tajnosti podataka i to na način da čelnicima javnih tijela i ovlaštenim dužnosnicima Republike Hrvatske daje ovlast za određivanje 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 neodgovarajuće stanje u kojemu se Republika Hrvatska danas nalazi, a to je nepostojanje nacionalnih standarda za zaštitu podataka, neprimjeren pristup tajnosti podataka u državnoj upravi i samim time loša percepcija javnosti o pojmovima privatnosti i tajnosti. Rezultat ovakvih odredbi Zakona je da tijela državne uprave samostalno donose vlastite mjere i standarde zaštite tajnosti podataka koji stoga na državnoj razini nisu standardizirani. U tijelima u kojima su takvi propisi doneseni i implementirani to je rezultiralo različitom učinkovitošću zaštitnih mjera i međusobno nesukladnim organizacijskim i tehničkim sigurnosnim rješenjima. Poseban problem na koji se svih ovih godina nije obraćala pažnja je i to što je samo mali broj tijela državne uprave uopće

osposobljen za donošenje i implementaciju mjera i standarda zaštite tajnosti podataka. U praksi su ovi podzakonski propisi doneseni, i barem u određenoj mjeri provedeni, uglavnom samo u tijelima sigurnosnog sustava u širem smislu (sigurnosno-obavještajne agencije, te ministarstva obrane, unutarnjih i vanjskih poslova). Najveći 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 tehničkih zahtjeva, kao i upitne primjerenosti državnim potrebama. Zaključno se može reći da problem postoji na dvije razine. Prva su nedovoljni kadrovski resursi i potrebna znanja za koncipiranje sigurnosnih mjera za zaštitu podataka u većini tijela, a druga je da i pri definiranim standardima zaštite podataka veliki broj tijela nema stručno-kadrovske potencijale za implementaciju, održavanje i unapređivanje zaštitnih mjera.

Ovakvo stanje predstavlja sigurnosni problem za Republiku Hrvatsku, ali i vrlo skup pristup, u kojem se na nekoordiniran i nesustavan način realiziraju i financiraju različita organizacijska i tehnička sigurnosna rješenja u tijelima državne uprave. U takvom stanju Republika Hrvatska ne može uspostaviti i osigurati minimalne zahtjeve informacijske sigurnosti na nacionalnoj razini, što je temeljni zahtjev NATO-a i EU-a u aktualnim integracijskim procesima. U tom smislu može se jasno reći da postojeći zakonski okvir u području informacijske sigurnosti nije usklađen sa zahtjevima NATO-a i EU-a, a međunarodno standardiziran i zahtijevan institucionalni okvir u području informacijske sigurnosti u Republici Hrvatskoj praktično 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 članstvo u NATO-u (MAP) 2002. godine. Ovim Zakonom je osnovan Ured Vijeća za nacionalnu sigurnost, nadležan između ostalog za provedbu sigurnosnih mjera potrebnih za zaštitu povjerljivih informacija i dokumenata u razmjeni između Republike Hrvatske i stranih obrambenih organizacija te Središnji registar za prijem i pohranu dokumenata. Pored toga, Ured je postao nadležan za tehničke poslove u području informacijske sigurnosti do osnivanja posebnog tehničkog tijela, Zavoda za informacijsku sigurnost i kripto-zaštitnu tehnologiju, koje Uredu u tim poslovima treba pružati tehničku potporu. Ovakvim propisom Republika Hrvatska je započela izgradnju zajedničke organizacije na nacionalnoj razini za potrebe suradnje s NATO-om, sukladno zahtjevima NATO-a. Ovim Zakonom u Republici Hrvatskoj uvedeni su međunarodno prihvaćeni standardi za postojanje središnjeg državnog tijela za informacijsku sigurnost (National Security Authority – NSA) i središnjeg državnog tijela za tehnička područja informacijske sigurnosti (National Communication Security Authority – NCSA ili Infosec Authority – IA). U razdoblju od donošenja ovog Zakona 2002. godine do danas, Ured je preuzeo i proveo većinu svojih nadležnosti u ovom području, dok je formiranje Zavoda tek započeto. Zbog pravnih nedorečenosti u odredbama Zakona, Zavod nikada nije formiran, inicijalna proračunska sredstva nisu korištena, a poslove Zavoda u okviru suradnje s NATO-om obavljali su privremeni ravnatelj Zavoda i Ured Vijeća za nacionalnu sigurnost. Najveći 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. S vremenom se, kroz provedbu Akcijskog plana za članstvo 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 području informacijske sigurnosti sa zahtjevima ne samo NATO-a, već i EU-a.

Godine 2004. stručna skupina sastavljena od relevantnih stručnjaka državnog i akademskog sektora, u organizaciji Središnjeg državnog ureda za e-Hrvatsku, započela 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 EU-a i članicama NATO-a. Nacionalni program informacijske sigurnosti u Republici Hrvatskoj, nakon javne rasprave održane 31. ožujka 2005., prihvatila je Vlada Republike Hrvatske (www.e-hrvatska.hr). Strateški, dugoročni cilj Programa je izgradnja čvrstih temelja za razvoj informacijskog društva u Republici Hrvatskoj (programi EU-a: e-Europe 2005 i 2010, program RH e-Hrvatska 2007), bez čega će biti upitan bilo kakav gospodarski prosperitet Republike Hrvatske u idućem desetljeću. Taktički, kratkoročno, programom je planiran niz mjera kojima će se postupno, u roku od nekoliko godina, uz najmanje moguće izmjene zakonodavnog i institucionalnog okvira, Republiku Hrvatsku dovesti do suvremenog, međunarodno prihvaćenog koncepta informacijske sigurnosti, kao temelja vlastitog sustava nacionalne sigurnosti, ali i razvoja društva u cjelini. Sukladnost zahtjevima međunarodnih integracijskih procesa u NATO i EU postavljena je kao uvjet u Nacionalnom programu te njegova provedba osigurava Republici Hrvatskoj uređenje nacionalnih pitanja iz područja informacijske sigurnosti na način 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 potječe 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, već i na građanstvo i privatni sektor. U tom smislu, Nacionalni program je obuhvatio planiranje mjera informacijske sigurnosti za stupove vlasti (izvršnu, zakonodavnu i sudbenu), razine vlasti (državna, lokalna), javne institucije, građanstvo i privatni sektor. Pri tom je način propisivanja te sadržaj i opseg mjera bitno različit i primjeren potrebama svakog od ovih segmenata društva. Predviđene su i mjere koje se odnose na sustavan pristup edukaciji i razvoju sigurnosne svijesti u najširim društvenim slojevima, u okviru kojih će u budućnosti biti potrebno uvesti odgovarajuće 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 preporučene su pripremne radnje kao minimalni skup mjera koje je potrebno provesti kako bi Republika Hrvatska uopće mogla započeti prilagodbu međunarodnim zahtjevima, standardima i praksi postupanja u području informacijske sigurnosti. Pripremnim radnjama označeni su međunarodno prihvaćeni standardi koji sve zemlje obvezuju na propisivanje zakonodavnog okvira koji se odnosi na pristup na nacionalnoj razini i državnu upravu u cjelini te na određivanje tijela s ovlastima za propisivanje i usmjeravanje sigurnosnih standarda na nacionalnoj razini. U tom smislu pripremne radnje odnose se na odgovarajuće zakonske promjene kojima treba potpuno izmijeniti Zakon o zaštititi tajnosti podataka iz 1996. godine, doraditi Zakon o sigurnosnim službama iz 2002. godine u području informacijske sigurnosti te međusobno uskladiti nove prijedloge zakona koji će činiti budući zakonski sustav informacijske sigurnosti u Republici Hrvatskoj. Predviđeno 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 međunarodno prihvaćen način mora tretirati pojmove klasificiranih i neklasificiranih podataka državne uprave, stupnjeve tajnosti i načela klasificiranja, kao i način i uvjete pristupa tajnim podacima.

Novi Zakon o sustavu informacijske sigurnosti treba definirati pet sigurnosnih područja za razvoj mjera i standarda informacijske sigurnosti (sigurnosna provjera osoblja, fizička 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 međusobne odnose i rokove u kojima ih nadležna tijela trebaju donijeti. Potrebno je i na međunarodno prihvatljiv način 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 će se kroz definiran sustav podzakonske hijerarhije i tijekom dvogodišnjeg procesa popunjavati sadržajima, od općih načela prema posebnim i od organizacijskih detalja prema tehničkim.

Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske potrebno je, u skladu s prethodna dva zakona ujednačiti pristup području informacijske sigurnosti unutar sigurnosnog sustava Republike Hrvatske s onim na nacionalnoj razini te prilagoditi ustroj i ovlasti pojedinih tijela sigurnosnog sustava koja u području informacijske sigurnosti imaju nadležnost na nacionalnoj razini u Republici Hrvatskoj. To su prvenstveno Ured Vijeća za nacionalnu sigurnost, kao središnje državno tijelo za informacijsku sigurnost, odgovorno za donošenje i usmjeravanje mjera i standarda informacijske sigurnosti, Zavod za sigurnost informacijskih sustava, kao središnje državno tijelo za tehnička područja informacijske sigurnosti te sigurnosne agencije, koje će imati odgovarajuću ulogu nadzora propisanih mjera i standarda informacijske sigurnosti. Predradnje moraju rezultirati potpuno funkcionalnim središnjim državnim tijelima za opća i tehnička područja informacijske sigurnosti (NSA, NCSA) sa svim potrebnim ovlastima te kadrovskom i ostalom infrastrukturom za rad, jer će ta tijela biti pokretač razvitka sustava informacijske sigurnosti, propisanog Zakonom o sustavu informacijske sigurnosti.

b) Osnovna pitanja čije se uređenje predlaže ovim Zakonom

Zakon o sustavu informacijske sigurnosti, kao novina u hrvatskom pravnom poretku, uređuje 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 međusobne odnose, način i smjer pojedinačnog i zajedničkog funkcioniranja te nadležnosti nadzora. Informacijsku sigurnost tijela iz članka 1. stavak 2. ovog Zakona predstavlja skup mjera i standarda koji služi očuvanju temeljnih svojstava povjerljivosti, cjelovitosti i raspoloživosti klasificiranih i neklasificiranih podataka u radu državne uprave. Cjelovitost i raspoloživost informacijskih sustava u kojima se podaci obrađuju, prenose ili pohranjuju, također mora biti primjereno zaštićena. Pri tome je važno uočiti kako i podaci koji nisu klasificirani mogu imati veliku važnost, pa se i za njih primjenjuje odgovarajući skup mjera i standarda koje služe očuvanju svojstava cjelovitosti i

raspoloživosti podataka koji nisu tajni (neklasificirani podaci, odnosno podaci čija je uporaba ograničena u službene svrhe). Sustav informacijske sigurnosti razrađuje se promatrajući sve mjere, standarde i nadležnosti tijela kroz podjelu na pet međunarodno prihvaćenih sigurnosnih područja informacijske sigurnosti u državnoj upravi: sigurnosne provjere, fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost vanjske suradnje ili industrijska sigurnost. Zakon predstavlja okvir sustava informacijske sigurnosti, koji će se popunjavati sadržajima (mjere i standardi) kroz razvoj kompleksne hijerarhije podzakonske regulative za koji je određen ukupan rok od 18 mjeseci (uključuje i prethodnu unutarnju organizaciju središnjih državnih tijela za informacijsku sigurnost). Daljnja tri mjeseca predviđena su za donošenje internih provedbenih akata te još šest mjeseci za njihovu provedbu u tijelima iz članka 1. stavak 2. ovog Zakona.

Zakonski prijedlog veliku pažnju posvećuje podzakonskom okviru, odnosno propisima informacijske sigurnosti. Stoga se detaljno razrađuje vrsta i hijerarhija propisa te nadležnost i rokovi njihova donošenja, kako uslijed kompleksnosti i višeslojnosti propisa ne bi došlo do međusobne kolizije ili nedostatka pojedinih propisa. Ovakav pristup je međunarodno pravno prihvaćen i osigurava sustavno uvođenje informacijske sigurnosti od općih prema posebnim propisima, kao i od funkcionalnih prema provedbenim te od organizacijskih prema tehničkim. Na taj način se, između ostalog, osigurava i trajnije prihvaćanje pojedinih općih načela informacijske sigurnosti i njihova što manja ovisnost o tehnološkim i organizacijskim promjenama pojedinih poslovnih procesa koje su česte i neizbježne. Složena hijerarhija propisa započinje 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 ujednačiti pristup informacijskoj sigurnosti u različitim segmentima tijela iz članka 1. stavak 2. ovog Zakona, ovisno o stupu (izvršna, zakonodavna, sudbena) i razini vlasti (državna, lokalna) kojoj pojedino tijelo pripada. Na taj način, na najvišoj razini vlasti, usklađuju se ciljevi i dosezi informacijske sigurnosti u svim tijelima iz članka 1. stavak 2. ovog Zakona. Nacionalna politika informacijske sigurnosti daje smjernice za sadržaj mjera informacijske sigurnosti koje će se provoditi u tijelima iz članka 1. stavak 2. ovog Zakona, 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 sa nacionalnim standardima informacijske sigurnosti, koji će se primjenjivati u realizaciji propisanih mjera, prijedlogom Zakona se definiraju tijela koja će imati ovlasti središnjih državnih tijela za informacijsku sigurnost, odgovornih za koordinaciju i usmjeravanje aktivnosti, predlaganje i donošenje propisa. Zakonskim Prijedlogom se propisuje da Ured Vijeća za nacionalnu sigurnost (UVNS) postaje središnje državno tijelo za informacijsku sigurnost koje u međunarodno pravnoj nomenklaturi zemalja članica NATO-a predstavlja: National Security Authority – NSA, tijelo odgovorno za koordinaciju svih aktivnosti oko primjene mjera i donošenja standarda informacijske sigurnosti u tijelima iz članka 1. stavak 2. ovog Zakona te za koordinaciju svih drugih tijela koja imaju nadležnost 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 tehnička područja informacijske sigurnosti (National Communication Security Authority – NCSA ili Infosec Authority - IA). Zavod djeluje u uskoj koordinaciji s Uredom, kao krovnim tijelom, a osim općih poslova na sigurnosti informacijskih sustava i mreža tijela iz članka 1. stavak 2. ovog Zakona, nadležan je i za sigurnosne akreditacije informacijskih sustava i mreža u tim tijelima (Security Accreditation

Authority - SAA), za upravljanje kriptomaterijalima (National Distribution Authority – NDA) te za poslove tijela za odgovornog za računalne ugroze (CERT-a - Computer Emergency Response Team) u tim tijelima.

Kako bi se potrebna pažnja posvetila prevenciji i otklanjanju sigurnosnih problema vezanih uz sigurnost javnih računalnih mreža u Republici Hrvatskoj, koje se nužno koriste i u realizaciji državnih komunikacijskih mreža te omogućila učinkovita međunarodna suradnja Republike Hrvatske u ovom području, zakonskim Prijedlogom osniva se nacionalni CERT[1]. Pored uključenja u EU, NATO i međunarodnu 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 računalne incidente u RH, a napose na državnim računalnim mrežama. Kao javna ustanova, organizirana na temeljima postojećeg, međunarodno afirmiranog akademskog CERT-a u okviru Hrvatske akademske i istraživačke mreže – CARNet, CERT će biti ključna institucija za promoviranje informacijske sigurnosti u najširim društvenim slojevima Republike Hrvatske, ali i međunarodnim okvirima.

Jedan od najvažnijih zadataka informacijske sigurnosti je osiguravanje sustavne primjene 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 građanstva i gospodarstva, ovdje se radi o propisivanju i provedbi obvezujućih propisa u tijelima iz članka 1. stavak 2. ovog Zakona. Stoga je nužno zakonom propisati koncept provedbe mjera informacijske sigurnosti koji će, između ostalog, osigurati sustavnu informatizaciju državne uprave, u okviru koje će mjere informacijske sigurnosti biti planirane i primijenjene na propisani način. Zakonskim Prijedlogom je propisan međunarodno prihvaćen način kojim se definiraju nadležna centralna tijela za potporu u poslovima planiranja i implementacije (CIS[2] Planning and Implementation), koja ove poslove obavljaju u tijelima iz članka 1. stavak 2. ovog Zakona, koja nemaju primjerene vlastite stručne 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 osnivači, omogućavaju SDUeH-u izvršnu potporu za ove poslove, kakva se za potrebe Ministarstva znanosti, obrazovanja i športa planira kroz Hrvatsku akademsku i istraživačku mrežu (CARNet) te Sveučilišni računski centar (SRCE).

Kako bi se osigurao stalni ciklus planiranja, provođenja, provjere i dorade (PDCA[3]), sustav mora uključiti element nadzora informacijske sigurnosti. Nadzor je predviđen na dva koncepcijski različita načina zbog različitih zahtjeva informacijske sigurnosti i karakteristika tijela iz članka 1. stavak 2. ovog Zakona na koje se odnose. Prvi način odnosi se na središnja tijela izvršne vlasti i sukladan je konceptu koji koristi NATO, pri čemu se definiraju institucije nadležne za ovaj proces nadzora (CIS Operating). Prijedlogom Zakona za ovaj posao određene su sigurnosno-obavještajne agencije, koje sukladno svojoj nadležnosti

[1] Naziv CERT, iako izvorno potječe od kratice engleskog jezika Computer Emergency Response Team, danas je međunarodno priznat kao naziv ove vrste poslova i upotrebljava se u nacionalnim nazivima tijela koja imaju ovlasti ove vrste u nacionalnim okvirima (EU, Austrija, Grčka, Malta, Italija, Švicarska, Portugal, Njemačka, Švedska, ...). Ovaj naziv je uvriježen i u RH jer je već 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, provođenja, provjere i dorade određenih standarda

(civilna i vojna), osiguravaju propisanu primjenu mjera i standarda informacijske sigurnosti u tijelima državne uprave. U svim ostalim tijelima iz članka 1. stavak 2. ovog Zakona koristi se drugi, nešto manje zahtjevan način, sukladan EU zahtjevima. U tim tijelima propisuje se obveza postavljanja odgovarajućih koordinatora informacijske sigurnosti koji mogu biti centralni, za više tijela, ili lokalni. Ove koordinatore imenuju ta tijela čiji su zaposlenici, ali prema uvjetima koja se određuju na nacionalnoj razini, u središnjem državnom tijelu za informacijsku sigurnost, koje je nadležno i za stručno usmjeravanje i praćenje rada ovih koordinatora, putem uredbe Vlade Republike Hrvatske . Poslovi koje obavljaju sigurnosno-obavještajne agencije i koordinatori, poslovi su inspekcijskog nadzora organizacije i implementacije propisanih mjera svih pet sigurnosnih područja informacijske sigurnosti u tijelima iz članka 1. stavak 2. ovog Zakona te izvještavanja čelnika tijela iz članka 1. stavak 2. ovog Zakona i središnjeg državnog tijela za informacijsku sigurnost, o stanju i učinkovitosti propisanih standarda u tijelima iz članka 1. stavak 2. ovog Zakona te o mogućim poboljšanjima. Smisao nadzora informacijske sigurnosti prvenstveno je u stalnom usmjeravanju propisanih mjera i standarda informacijske sigurnosti te ispomoći stručnog i sigurnosnog osoblja u samim tijelima iz članka 1. stavak 2. ovog Zakona, zaduženog za održavanje i administriranje organizacijskih i tehničkih mjera i sustava iz svih sigurnosnih područja informacijske sigurnosti, realiziranih u određenom tijelu. U tom smislu, nadzor se obavlja u unaprijed planiranim terminima, a o rezultatima nadzora donosi se izvješće koje se dostavlja čelniku tijela te središnjem državnom tijelu za informacijsku sigurnost. Središnje državno tijelo za informacijsku sigurnost (UVNS), uz pomoć tijela za tehnička područja informacijske sigurnosti (ZSIS), nadzornih tijela/koordinatora te tijela za planiranje i implementaciju, zaduženo je za koordinaciju postupka otklanjanja nepravilnosti u provedbi mjera ili nedostatnosti propisa. Čelnici tijela odgovorni su za otklanjanje utvrđenih nedostataka u svojoj nadležnosti. U slučaju utvrđenih nepravilnosti na informacijskom sustavu za koji je provedena periodična sigurnosna akreditacija, ZSIS u suradnji s UVNS-om, ovisno o vrsti nepravilnosti, utvrđuje daljnju valjanost akreditacije.

Drugim riječima, zakonskim Prijedlogom namjeravaju se propisati:

- sve sastavnice sustava informacijske sigurnosti, njihov djelokrug i međusobni odnosi (središnja državna tijela za informacijsku sigurnost, nacionalni CERT, tijela za planiranje i implementaciju, tijela za nadzor u tijelima državne uprave, koordinatori informacijske sigurnosti u ostalim tijelima iz članka 1. stavak 2. ovog Zakona),
- sigurnosna područja informacijske sigurnosti (sigurnosne provjere, fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava ili INFOSEC i sigurnost vanjske suradnje ili industrijska sigurnost),
- hijerarhija propisa informacijske sigurnosti (nacionalna politika, uredbe, pravilnici, interni akti za nadzor i provedbu),
- poslovi i ovlasti središnjih državnih tijela za informacijsku sigurnost (Ured Vijeća za nacionalnu sigurnost, Zavod za sigurnost informacijskih sustava),
- osnivanje tijela za odgovore na računalne ugroze (CERT-a) te način upravljanja i koordinacija,
- način provedbe informacijske sigurnosti te
- način nadzora informacijske sigurnosti.

c) *Posljedice koje će donošenjem Zakona proisteći*

Donošenjem predloženog Zakona u sustav državne uprave uvode se nove vrste tijela – središnja državna tijela za informacijsku sigurnost, čije ovlasti preuzimaju Ured Vijeća za nacionalnu sigurnost, kao krovno koordinacijsko tijelo, te Zavod za sigurnost informacijskih sustava, kao pomoćno tijelo za tehnička područja informacijske sigurnosti. Kako bi ova tijela mogla obavljati propisane poslove predlaganja akata i donošenja odgovarajućih pravilnika za primjenu u tijelima iz članka 1. stavak 2. ovog Zakona, biti će potrebno provesti izmjene i dopune Zakona o sustavu državne uprave, po uzoru na promjene koje su provedene u prosincu 2003. godine, tijekom uvođenja središnjih državnih ureda u sustav državne uprave (NN 199/2003).

Donošenjem Zakona cjelovito će se urediti potpuno novo područje u Republici Hrvatskoj. Zakonom propisan sustav informacijske sigurnosti u Republici Hrvatskoj sačinjavaju središnja državna tijela za informacijsku sigurnost: Ured Vijeća za nacionalnu sigurnost (UVNS) i Zavod za sigurnost informacijskih sustava (ZSIS), kao okosnica i ključni elementi sustava, zatim Nacionalni CERT u okviru Hrvatske akademske i istraživačke mreže (CARNet), kao tijelo nadležno za prevenciju i koordinaciju sigurnosnih računalnih incidenata na javnim računalnim 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 agencije i koordinatori informacijske sigurnosti u svojstvu nadzora propisanih mjera i standarda informacijske sigurnosti u tijelima iz članka 1. stavak 2. ovog Zakona.

Zakonom se, pored redovitog nadzora informacijske sigurnosti, kojim se osigurava stalni ciklus planiranja, provođenja, provjere i dorade (PDCA) propisa i stanja informacijske sigurnosti u tijelima, po prvi puta uvodi i periodični proces sigurnosne akreditacije informacijskih sustava i mreža tijela iz članka 1. stavak 2. ovog Zakona. Ovi aspekti dugoročno će iznimno povoljno utjecati na bolje planiranje i sustavniju provedbu projekata u tijelima iz članka 1. stavak 2. ovog Zakona, kako u području informatizacije, tako i u području adaptacije i izgradnje objekata. Tu se primarno misli na uvođenje dodatnih kriterija u nabavi i projektiranju, kriterija koji prate ne samo sigurnosne aspekte uporabe različitih uređaja i sustava te korištenja vanjskih usluga, već prije svega mjerila kvalitete i pouzdanosti tijekom njihova 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. Pritom je sadržaj i doseg mjera i standarda informacijske sigurnosti bitno različit i primjeren odgovarajućim segmentima tijela iz članka 1. stavak 2. ovog Zakona.

Prijedlog Zakona uređuje područje informacijske sigurnosti u Republici Hrvatskoj u skladu sa stvarnim i predviđenim potrebama Republike Hrvatske, kako u području vlastite nacionalne sigurnosti i razvoja informacijskog društva, tako i u skladu sa zahtjevima međunarodnih integracijskih procesa, odnosno sukladnosti sa sigurnosnim politikama NATO-a i EU-a.

U metodološkom smislu zakonski Prijedlog koncipira sustav instrumenata raspoloživih u sustavima informacijske sigurnosti zemalja EU-a i NATO-a te je optimalan sa stajališta potreba Republike Hrvatske. Prijedlog u potpunosti slijedi strukovne potrebe i zahtjeve za učinkovitošću mjera i standarda informacijske sigurnosti u uvjetima naraslih i izmijenjenih

prijetnji i izazova uslijed tehnološke i informacijske revolucije. Nužnost različitih oblika državnih ili vojnih integracija, međunarodne suradnje na suzbijanju ugroza kao što su organizirani kriminal ili terorizam, pa do različitih pojavnih oblika računalnog i kibernetičkog kriminala kojima smo već sada okruženi, traži uvođenje minimalnih sigurnosnih zahtjeva informacijske sigurnosti u svakoj državi koja želi participirati u međunarodnoj zajednici te osposobljenu i međunarodno usklađenu nacionalnu organizaciju nadležnih tijela, koja će takve minimalne zahtjeve ne samo uspostaviti već i trajno održavati.

Propisivanjem sustava informacijske sigurnosti sa širokim zahvatom u tijela iz članka 1. stavak 2. ovog Zakona te dobrom koordinacijom središnjih državnih tijela za informacijsku sigurnost i nacionalnog CERT-a nadležnog za javne računalne 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 se način osiguravaju preduvjeti za strateški nacionalni interes stvaranja informacijskog društva kao preduvjeta gospodarskog prosperiteta Republike Hrvatske u idućem desetljeću.

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, čime će se, uz donošenje potrebne podzakonske regulative, uspostaviti sustav informacijske sigurnosti u Republici Hrvatskoj. Ovako ustrojen, sustav informacijske sigurnosti je važan dio šireg sustava nacionalne sigurnosti Republike Hrvatske, ali i neophodan temelj za izgradnju informacijskog društva i budući gospodarski prosperitet Republike Hrvatske te uvjet međunarodnih integracijskih procesa u NATO i EU.

Drugim riječima, zakonski Prijedlog osigurava sljedeće:

1. **Cjelovit i jedinstven pravno uređen okvir sustava informacijske sigurnosti, kao dio šireg sustava nacionalne sigurnosti Republike Hrvatske;**
2. **Racionalnu i jasnu podjelu funkcionalnih nadležnosti između nadležnih tijela te uspostavu središnjih državnih tijela za učinkovitu koordinaciju i usmjeravanje informacijske sigurnosti i razvoj nacionalnih standarda informacijske sigurnosti;**
3. **Sustav informacijske sigurnosti sa širokim zahvatom u tijela iz članka 1. stavak 2. ovog Zakona, kao temelj za sustavnu izgradnju informacijskog društva u Republici Hrvatskoj i preduvjet budućeg gospodarskog prosperiteta;**
4. **Međunarodno-pravno usklađen pristup informacijskoj sigurnosti, prilagođen uvjetima i potrebama Republike Hrvatske, kao jamstvo sukladnosti s temeljnim zahtjevima integracijskih procesa u NATO i EU.**

III. OCJENA POTREBNIH SREDSTAVA ZA PROVOĐENJE ZAKONA

Ocjenjuje se da donošenje i provedba ovog Zakona neće zahtijevati osiguranje dodatnih sredstava u Državnom proračunu Republike Hrvatske.

Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske predviđeno je osnivanje Zavoda za sigurnost informacijskih sustava (ZSIS) kao pravnog sljednika Zavoda za informacijsku sigurnost i kripto-zaštitnu tehnologiju, a Ured Vijeća za nacionalnu sigurnost i sigurnosno-obavještajne agencije postojeće su institucije, čije su nadležnosti iz Zakona o informacijskoj sigurnosti usklađene s novim Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske (NN 79/06).

Jedino novo tijelo je Nacionalni CERT, koji je nova ustrojstvena jedinica postojeće ustanove Hrvatske akademske i istraživačke mreže (CARNet) i koji će se temeljiti na postojećem CERT-u, već niz godina nadležnom za akademski sektor. CARNet je proračunski u nadležnosti Ministarstva znanosti, obrazovanja i športa, s kojim je usuglašena potrebna promjena statuta, slijedom koje su planirani dodatni troškovi uslijed proširenja kadrovske baze i djelokruga poslova postojećeg CARNet CERT-a. Ovi troškovi su planirani u Državnom proračunu za 2007. godinu pod stavkom 080 75 – 1444 – A628063 REDOVNA DJELATNOST NACIONALNOG CERTA, 1.530667 kn, te stavkom 080 75 – 1444 – K628066 NACIONALNI CERT – ZAJEDNIČKA RK INFRASTRUKTURA, 1.850.000 kn.

IV. TEKST NACRTA PRIJEDLOGA ZAKONA O SUSTAVU INFORMACIJSKE SIGURNOSTI S OBRAZLOŽENJEM

Tekst Nacrta prijedloga Zakona dan je u obliku Nacrta prijedloga Zakona o sustavu informacijske sigurnosti s obrazloženjem.

NACRT PRIJEDLOGA

ZAKONA O SUSTAVU INFORMACIJSKE SIGURNOSTI

I. OSNOVNE ODREDBE

Članak 1.

(1) Ovim Zakonom se utvrđuje pojam informacijske sigurnosti, propisi informacijske sigurnosti te nadležna tijela za donošenje, provođenje i nadzor mjera i standarda informacijske sigurnosti.

(2) Ovaj Zakon se primjenjuje na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima, koje u svom djelokrugu koriste klasificirane i neklasificirane podatke.

(3) Ovaj Zakon se primjenjuje i na pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima.

Članak 2.

Pojmovi koji se koriste u ovom Zakonu imaju sljedeće značenje:

- Informacijska sigurnost - skup mjera i standarda zaštite tajnosti i ograničenja uporabe podataka, u cilju postizanja odgovarajuće povjerljivosti, cjelovitosti i raspoloživosti podataka te cjelovitosti i raspoloživosti informacijskih sustava u kojima se podaci obrađuju, pohranjuju ili prenose.
- Informacijski sustav - svaki komunikacijski, računalni ili drugi elektronički sustav u kojem se podaci obrađuju, pohranjuju ili prenose tako da budu dostupni i upotrebljivi za ovlaštene korisnike.
- Sustav informacijske sigurnosti - podrška za realizaciju i održavanje propisanih mjera i standarda informacijske sigurnosti, obuhvaća organizacijsku strukturu, odgovornost, način (politike) postupanja, aktivnosti planiranja, provedbe, provjere i dorade mjera i standarda te utvrđenu praksu i procedure postupanja u okviru poslovnih procesa i resursa.
- Mjere informacijske sigurnosti - opća pravila zaštite tajnosti i ograničenja uporabe podataka koja se primjenjuju u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona, koja u svom djelokrugu koriste klasificirane podatke određenog stupnja tajnosti i neklasificirane podatke, pri čemu te mjere mogu biti realizirane na fizičkoj, tehničkoj ili organizacijskoj razini.
- Standardi informacijske sigurnosti - organizacijske i tehničke procedure i rješenja namijenjena sustavnoj i ujednačenoj realizaciji propisanih mjera informacijske sigurnosti u različitim tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona.
- Sigurnosna područja informacijske sigurnosti - predstavljaju podjelu kompleksnog područja informacijske sigurnosti s ciljem omogućavanja jasne, sustavne i učinkovite realizacije donošenja, primjene i nadzora mjera i standarda informacijske sigurnosti, koristeći pri tome međunarodno prihvaćenu podjelu na pet sigurnosnih područja informacijske sigurnosti u državnoj upravi (sigurnosna provjera osoblja, fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost vanjske suradnje).

- Sigurnosna akreditacija informacijskih sustava - postupak provjere sposobnosti tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona za upravljanje sigurnošću vlastitog informacijskog sustava, koji se provodi utvrđivanjem usklađenosti implementiranih mjera i standarda informacijske sigurnosti na određenom informacijskom sustavu, s mjerodavnim propisima informacijske sigurnosti (organizacijska, tehnička i fizička razina).

II. PROPISI INFORMACIJSKE SIGURNOSTI

Članak 3.

(1) Nacionalna politika informacijske sigurnosti u Republici Hrvatskoj je dokument kojim Hrvatski sabor utvrđuje temeljne ciljeve, načela i dosege primjene informacijske sigurnosti u Republici Hrvatskoj, nužne za sustavno kreiranje i provedbu mjera i standarda informacijske sigurnosti u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona, čime se osigurava uvođenje zajedničkih kriterija i minimalnih zahtjeva informacijske sigurnosti u svim tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona.

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

Članak 4.

(1) Zaštita tajnosti i ograničenje uporabe klasificiranih i neklasificiranih podataka provodi se propisivanjem mjera i standarda informacijske sigurnosti, u okviru sigurnosnih područja informacijske sigurnosti:

- sigurnosna provjera osoblja,
- fizička sigurnost,
- sigurnost podataka,
- sigurnost informacijskih sustava,
- sigurnost vanjske suradnje.

(2) Uredbom o mjerama informacijske sigurnosti, koju donosi Vlada Republike Hrvatske, propisuju se mjere za sigurnosna područja informacijske sigurnosti iz stavka 1. ovog članka te obveza primjene tih mjera na klasificirane podatke odgovarajućeg stupnja tajnosti i neklasificirane podatke, sukladno ovom Zakonu i Nacionalnoj politici informacijske sigurnosti iz članka 3. ovog Zakona.

III. SREDIŠNJA DRŽAVNA TIJELA ZA INFORMACIJSKU SIGURNOST

Ured Vijeća za nacionalnu sigurnost

Članak 5.

Ured Vijeća za nacionalnu sigurnost (UVNS) je središnje državno tijelo za informacijsku sigurnost koje je odgovorno za koordinaciju aktivnosti oko donošenja i primjene mjera i standarda informacijske sigurnosti u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona, kao i za koordinaciju aktivnosti oko primjene mjera i standarda informacijske sigurnosti u razmjeni klasificiranih i neklasificiranih podataka između Republike Hrvatske i stranih zemalja i organizacija.

Članak 6.

(1) Ured Vijeća za nacionalnu sigurnost donosi Pravilnik o standardima sigurnosne provjere osoblja, Pravilnik o standardima fizičke sigurnosti, Pravilnik o standardima sigurnosti podataka i Pravilnik o standardima sigurnosti vanjske suradnje, kojima se, u skladu s ovim Zakonom i Uredbom iz članka 4. stavak 2., u okviru sigurnosnih područja informacijske sigurnosti, reguliraju standardi zaštite tajnosti i ograničenja uporabe klasificiranih i neklasificiranih podataka u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona.

(2) Ured Vijeća za nacionalnu sigurnost usklađuje standarde iz stavka 1. ovog članka sa zahtjevima integracijskih procesa koje provodi Republika Hrvatska i drugim međunarodnim standardima i preporukama informacijske sigurnosti te sudjeluje u nacionalnoj normizaciji područja informacijske sigurnosti.

Članak 7.

(1) Ured Vijeća za nacionalnu sigurnost koordinira i usklađuje rad svih tijela i pravnih osoba koja, sukladno ovom Zakonu, imaju određene nadležnosti u području informacijske sigurnosti.

(2) Ured Vijeća za nacionalnu sigurnost surađuje s mjerodavnim institucijama stranih zemalja i organizacija u području informacijske sigurnosti te koordinira međunarodnu suradnju ostalih tijela i pravnih osoba iz stavka 1. ovog članka.

Zavod za sigurnost informacijskih sustava

Članak 8.

Zavod za sigurnost informacijskih sustava (ZSIS) je središnje državno tijelo za tehnička područja informacijske sigurnosti koje je zaduženo za:

- sigurnost informacijskih sustava tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona,
- sigurnosne akreditacije informacijskih sustava tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona,
- upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka između tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona te između Republike Hrvatske i stranih zemalja i organizacija,
- koordinaciju prevencije i otklanjanja problema vezanih uz sigurnost računalnih mreža u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona.

Članak 9.

(1) Zavod za sigurnost informacijskih sustava donosi Pravilnik o standardima sigurnosti informacijskih sustava kojim se, u skladu s ovim Zakonom, Uredbom iz članka 4. stavak 2. i Pravilnicima iz članka 6. stavak 1., u okviru sigurnosnog područja informacijske sigurnosti sigurnost informacijskih sustava, reguliraju standardi zaštite tajnosti i ograničenja uporabe podataka u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona.

(2) Zavod za sigurnost informacijskih sustava usklađuje standarde iz stavka 1. ovog članka sa zahtjevima integracijskih procesa koje provodi Republika Hrvatska i drugim međunarodnim standardima i preporukama informacijske sigurnosti te sudjeluje u nacionalnoj normizaciji područja informacijske sigurnosti.

Članak 10.

(1) Zavod za sigurnost informacijskih sustava obavlja poslove sigurnosne akreditacije informacijskih sustava u tijelima iz članka 1. stavak 2. ovog Zakona, u kojima se koriste klasificirani i neklasificirani podaci.

(2) Poslove iz stavka 1. ovog članka, za pravne osobe s javnim ovlastima u Republici Hrvatskoj, Zavod obavlja u koordinaciji s Hrvatskom akreditacijskom agencijom (HAA).

Članak 11.

Uredbom o poslovima središnjih državnih tijela za informacijsku sigurnost, Vlada će, na prijedlog čelnika nadležnih tijela i u skladu s ovim Zakonom, propisati poslove iz članaka 5. i 8. ovog Zakona.

IV. NACIONALNI CERT

Članak 12.

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

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

(3) CERT je ovlašten za koordinaciju rada istovrsnih tijela koja rade na prevenciji i otklanjanju problema vezanih uz sigurnost računalnih mreža u Republici Hrvatskoj te određuje pravila i načine zajedničkog rada takvih tijela u svrhu preventivnog djelovanja i učinkovite koordinacije pri rješavanju problema vezanih uz sigurnost računalnih mreža u Republici Hrvatskoj.

Članak 13.

CERT surađuje sa Zavodom za sigurnost informacijskih sustava u izradi propisa u okviru područja sigurnosti informacijskih sustava tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona te izrađuje i sudjeluje u izradi preporuka i normi u Republici Hrvatskoj iz područja sigurnosti informacijskih sustava.

Članak 14.

(1) Ravnatelj CARNet-a, uz suglasnost čelnika Ureda Vijeća za nacionalnu sigurnost, imenuje svog pomoćnika zaduženog za upravljanje CERT-om.

(2) Razrada poslova CERT-a provest će se na način propisan za izmjenu Statuta CARNet-a, na prijedlog ravnatelja CARNet-a, uz prethodnu suglasnost čelnika Ureda Vijeća 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 trebaju pristupati klasificiranim podacima, provodi se propisani postupak sigurnosne provjere.

V. PROVEDBA INFORMACIJSKE SIGURNOSTI

Članak 15.

(1) Tijela i pravne osobe iz članka 1. stavak 2. ovog Zakona, sukladno pravilnicima iz članka 6. stavak 1. i članka 9. stavak 1. ovog Zakona, dužni su provesti propisane standarde informacijske sigurnosti.

(2) Za tijela i pravne osobe iz članka 1. stavak 2. ovog Zakona, koje nemaju ustrojene odgovarajuće informatičke i tehničke ustrojstvene jedinice, poslove iz stavka 1. ovog članka, u području informacijskih sustava, 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 članka, središnje tijelo državne uprave nadležno za razvitak informacijskog sustava državne uprave koristi usluge Agencije za podršku informacijskim sustavima i informacijskim tehnologijama (APIS IT) i Financijske agencije (FINA), a središnje tijelo državne uprave nadležno za znanost i obrazovanje za obavljanje poslova iz stavka 2. ovog članka koristi usluge CARNet-a i Sveučilišnog računskog centra (Srce).

VI. NADZOR INFORMACIJSKE SIGURNOSTI

Članak 16.

(1) Poslovi nadzora informacijske sigurnosti su poslovi inspekcijskog nadzora organizacije, provedbe, stanja i učinkovitosti propisanih mjera i standarda informacijske sigurnosti u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona.

(2) Poslove nadzora iz stavka 1. ovog članka u tijelima državne uprave i tijelima za potporu informacijskih sustava iz članka 15. stavak 3. ovog Zakona, provode nadležne sigurnosno-obavještajne agencije, a u ostalim tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona, nadzor provode koordinatori informacijske sigurnosti u tim tijelima.

(3) Tijela i pravne osobe iz stavka 2. ovog članka, u kojima nadzor provode koordinatori informacijske sigurnosti, obvezna su u svoja unutarnja ustrojstva ugraditi radna mjesta koordinatora informacijske sigurnosti.

Članak 17.

(1) Sigurnosno-obavještajne agencije, uz suglasnost središnjih državnih tijela za informacijsku sigurnost i u skladu s ovim Zakonom i podzakonskim propisima, donose Pravilnik o nadzoru informacijske sigurnosti, za obavljanje poslova iz članka 16. stavak 1. ovog Zakona.

(2) Vlada Republike Hrvatske donijet će, na prijedlog Ureda Vijeća za nacionalnu sigurnost, a uz prethodno mišljenje Zavoda za sigurnost informacijskih sustava, u skladu s člankom 16. stavak 2. i 3. ovog Zakona i podzakonskim propisima, Uredbu o poslovima koordinatora informacijske sigurnosti u tijelima i pravnim osobama, kojom se utvrđuju uvjeti i vrsta poslova za ova radna mjesta te rokovi provedbe, kao i tijela i pravne osobe koje trebaju provesti imenovanja koordinatora, pri čemu tako određeni koordinatori informacijske sigurnosti mogu biti lokalni za pojedino tijelo i pravnu osobu ili centralni za odgovarajuću grupu tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona.

Članak 18.

(1) Nadležne sigurnosno-obavještajne agencije i koordinatori informacijske sigurnosti iz članka 16. stavak 2. ovog Zakona, o rezultatima svakog provedenog nadzora u tijelu ili pravnoj osobi, donose izvješće koje dostavljaju čelniku tijela ili pravne osobe odgovornom za poduzimanje mjera za otklanjanje svih uočenih nedostataka u određenom roku te središnjem državnom tijelu za informacijsku sigurnost

(2) Središnje državno tijelo za informacijsku sigurnost, temeljem uočenih nedostataka iz stavka 1. ovog članka, može pokrenuti postupak utvrđivanja odgovornosti za propuste, postupak preispitivanja daljnje valjanosti sigurnosne akreditacije informacijskog sustava određenog tijela ili pravne osobe iz članka 1. stavak 2. ovog Zakona te postupak izmjene propisa informacijske sigurnosti.

VII. PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 19.

(1) Vlada Republike Hrvatske, uz suglasnost Predsjednika Republike Hrvatske, predložit će Hrvatskom saboru donošenje Nacionalne politike informacijske sigurnosti u Republici Hrvatskoj iz članka 3. ovog Zakona u roku od šest mjeseci od dana stupanja na snagu ovog Zakona.

(2) Vlada Republike Hrvatske donijet će Uredbu iz članka 4. stavak 2. i članka 11. ovog Zakona u roku od devet mjeseci od dana stupanja na snagu ovog Zakona, a uredbu iz članka 17. stavak 2. ovog Zakona u roku od osamnaest mjeseci od dana stupanja na snagu ovog Zakona

(3) CARNet će provesti izmjene Statuta iz članka 14. stavak 2. ovog Zakona u roku od devet mjeseci od dana stupanja na snagu ovog Zakona.

(4) Ured Vijeća za nacionalnu sigurnost donijet će Pravilnike iz članka 6. stavak 1. ovog Zakona u roku od petnaest mjeseci od dana stupanja na snagu ovog Zakona.

(5) Zavod za sigurnost informacijskih sustava donijet će Pravilnik iz članka 9. stavak 1. ovog Zakona u roku od petnaest mjeseci od dana stupanja na snagu ovog Zakona.

Članak 20.

(1) Tijela iz članka 15. stavak 2. ovog Zakona, nadležna za poslove provedbe informacijske sigurnosti u drugim tijelima, dužna su, uz suglasnost središnjih državnih tijela za informacijsku sigurnost, donijeti Pravilnik o provedbi mjera i standarda informacijske sigurnosti u roku od osamnaest mjeseci od dana stupanja na snagu ovog Zakona.

(2) Tijela iz članka 16. stavak 2. ovog Zakona, nadležna za poslove nadzora informacijske sigurnosti u tijelima državne uprave, dužna su, uz suglasnost središnjih državnih tijela za informacijsku sigurnost, donijeti Pravilnik o nadzoru mjera i standarda informacijske sigurnosti u roku od osamnaest mjeseci od dana stupanja na snagu ovog Zakona.

(3) Tijela i pravne osobe iz članka 1. stavak 2. ovog Zakona dužna su u roku od tri mjeseca od dana donošenja mjerodavnih Pravilnika iz članka 19. stavak 4. i 5. ovog Zakona, donijeti Pravilnik tijela ili pravne osobe o provedbi mjera i standarda informacijske sigurnosti u svom djelokrugu, s rokom provedbe od šest mjeseci od dana donošenja.

Članak 21.

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

OBRAZLOŽENJE

Glava I., OSNOVNE ODREDBE

Prijedlogom nacrta Zakona o sustavu informacijske sigurnosti uvodi se i regulira novo područje informacijske sigurnosti u Republici Hrvatskoj. U članku 1. određuje se i djelokrug primjene Zakona na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te pravne osobe s javnim ovlastima. Zakon se primjenjuje i na pravne i fizičke osobe koje ostvare pristup ili postupaju s klasificiranim i neklasificiranim podacima. U članku 2. definiraju se pojmovi informacijske sigurnosti, podatka, sustava informacijske sigurnosti, informacijskog sustava, sustava informacijske sigurnosti, mjera, standarda i sigurnosnih područja informacijske sigurnosti te sigurnosne akreditacije informacijskih sustava. Informacijska sigurnost tako u smislu ovog Zakona predstavlja skup propisanih mjera i standarda zaštite tajnosti i ograničenja uporabe podataka, u cilju postizanja odgovarajuće povjerljivosti, cjelovitosti i raspoloživosti podataka te cjelovitosti i raspoloživosti informacijskih sustava u kojima se podaci obrađuju, pohranjuju ili se prenose. Uvodi se pojam sigurnosnih područja informacijske sigurnosti (sigurnosne provjere osoblja, fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava i sigurnost vanjske suradnje), u svrhu stvaranja sustavnih i međusobno koordiniranih skupova mjera i standarda, u okviru kojih se primjenjuju propisane mjere i standardi s ciljem zaštite tajnosti i ograničenja uporabe podataka.

Glava II., PROPISI INFORMACIJSKE SIGURNOSTI

Člankom 3. definira se temeljni propis za razradu podzakonskog sustava akata (mjere i standardi, provedba, nadzor), Nacionalna politika informacijske sigurnosti u Republici Hrvatskoj koju donosi Hrvatski sabor, na prijedlog Vlade Republike Hrvatske, i uz prethodnu suglasnost Predsjednika Republike Hrvatske, kojom se utvrđuju temeljni ciljevi, načela i dosezi primjene informacijske sigurnosti u Republici Hrvatskoj, nužni za sustavno kreiranje i provedbu mjera i standarda sigurnosnih područja informacijske sigurnosti u tijelima iz članka 1. stavak 2. ovog Zakona, čime se postiže uvođenje zajedničkih kriterija i minimalnih zahtjeva informacijske sigurnosti u svim tijelima iz članka 1. stavak 2. ovog Zakona. Člankom 4. stavak 1. definira se spomenutih pet sigurnosnih područja i način njihove uporabe u izgradnji nacionalnih propisa, a stavkom 2. propisuje se razrada mjera informacijske sigurnosti u skladu s ovim Zakonom i Nacionalnom politikom informacijske sigurnosti, koje donosi Vlada RH za sva sigurnosna područja informacijske sigurnosti.

Glava III., SREDIŠNJA DRŽAVNA TIJELA ZA INFORMACIJSKU SIGURNOST

U člancima 5. do 7. određuju se nadležnosti UVNS-a kao središnjeg državnog tijela za informacijsku sigurnost (nacionalni NSA) koje je odgovorno za koordinaciju aktivnosti vezanih za donošenje i primjenu mjera i standarda informacijske sigurnosti u tijelima iz članka 1. stavak 2. ovog Zakona, kao i za usklađenost aktivnosti oko primjene mjera i standarda informacijske sigurnosti u razmjeni klasificiranih podataka između RH i stranih zemalja i organizacija. Tako se člankom 6. propisuje da UVNS donosi pravilnike iz sigurnosnih područja za koja je nadležan, a kojima se reguliraju standardi za provedbu mjera iz Vladine Uredbe iz članka 4. stavak 2. ovog Zakona. Također se člankom 6. stavak 2.

definira odnos prema nacionalnom normizacijskom procesu, a člankom 7. se utvrđuje UVNS kao krovno tijelo nadležno za koordinaciju aktivnosti donošenja i primjene mjera i standarda u svim područjima informacijske sigurnosti i koordinaciju svih drugih tijela s određenim nadležnostima u području informacijske sigurnosti.

U člancima 8. do 11. određuju se nadležnosti ZSIS-a kao središnjeg državnog tijela za tehnička područja informacijske sigurnosti (nacionalni NCSA), koje djeluje u koordinaciji s UVNS-om (NSA) i koje skrbi o sigurnosti informacijskih sustava tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona, sigurnosnim akreditacijama informacijskih sustava tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona, upravljanju kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka između tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona te između Republike Hrvatske i stranih zemalja i organizacija, kao i o koordinaciji prevencije i otklanjanja problema vezanih uz sigurnost računalnih mreža u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona. Tako se člankom 9. propisuje da ZSIS donosi Pravilnik o sigurnosti informacijskih sustava, kojim se reguliraju standardi za provedbu mjera iz Vladinih Uredbe iz članka 4. stavak 2., u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona. Također se člankom 9. i 10. definira odnos prema nacionalnom normizacijskom i akreditacijskom procesu te utvrđuje nadležnost ZSIS-a za poslove sigurnosnih akreditacija (nacionalni SAA) informacijskih sustava i mreža tijela i pravnih osoba iz članka 1. stavak 2. ovog Zakona. Člankom 11. propisuje se obveza uređivanja poslova središnjih državnih tijela za informacijsku sigurnost, UVNS-a i ZSIS-a, Uredbom Vlade Republike Hrvatske, na prijedlog čelnika tih tijela i u skladu s ovim Zakonom.

Glava IV., NACIONALNI CERT

U člancima 12. do 14. definira se novo nacionalno tijelo za prevenciju i odgovor na računalne ugroze (u daljnjem tekstu CERT) koje obavlja poslove prevencije i otklanjanja problema vezanih uz sigurnost računalnih mreža u Republici Hrvatskoj (prvenstveno javnih). CERT se, kao zasebna ustrojstvena jedinica, ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (u daljnjem tekstu CARNet). Člankom 13. se utvrđuje potrebna koordinacija CERT-a i ZSIS-a u području sigurnosti informacijskih sustava i normizaciji ovog područja u RH, a u članku 14. definiran je način postavljanja čelnog čovjeka i razrada poslova CERT-a, koji osiguravaju međusobnu usklađenost rada CERT-a i središnjih državnih tijela za informacijsku sigurnost UVNS-a i ZSIS-a.

Glava V., PROVEDBA INFORMACIJSKE SIGURNOSTI

Člankom 15. propisuje se obveza provođenja propisanih standarda informacijske sigurnosti temeljem pravilnika koje donose UVNS i ZSIS, a koji su usklađeni s Uredbom Vlade RH koja utvrđuje mjere informacijske sigurnosti. U stavku 2. definira se da u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona, koja nemaju ustrojene odgovarajuće informatičke i tehničke ustrojstvene jedinice, nadležnost za poslove provedbe sigurnosti informacijskih sustava ima Središnji državni ured za e-Hrvatsku, koji u tu svrhu koristi usluge APIS-a i FINA-e (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 Sveučilišnog računskog centra (Srce) (stavak 3.).

Glava VI., NADZOR INFORMACIJSKE SIGURNOSTI

Člankom 16. definiran je segment nadzora informacijske sigurnosti u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona, kao inspekcijski nadzor organizacije, provedbe, stanja i učinkovitosti propisanih mjera i standarda (stavak 1.). Poslove nadzora u središnjim tijelima državne uprave i tijelima za potporu informacijskih sustava provode nadležne sigurnosno-obavještajne agencije (civilna i vojna), a u ostalim tijelima iz članka 1. stavak 2. ovog Zakona, nadzor provode koordinatori informacijske sigurnosti u određenim tijelima (stavak 2.), koja su obvezna u svoja unutarnja ustrojstva ugraditi odgovarajuća radna mjesta koordinatora informacijske sigurnosti (stavak 3.). U Članku 17., stavcima 1. i 2., propisuju se potrebni akti za provođenje nadzora, te utvrđuje mogućnost da se koordinatori optimalno razmjeste po konceptu centralnih (za više tijela i/ili pravnih osoba) ili lokalnih koordinatora u tijelima i pravnim osobama. U članku 18., stavcima 1. i 2., utvrđuje se način izvješćivanja i postupanja vezano za rezultate nadzora.

Glava VII., PRIJELAZNE I ZAVRŠNE ODREDBE

Prijelaznim i završnim odredbama u člancima 19. i 20. definira se dinamika donošenja regulativnog okvira propisanog Zakonom u odnosu na vrijeme donošenja ovog Zakona. Potrebno je napomenuti da je dužina rokova uvjetovana činjenicom da se radi o potpuno novom području u RH za koji je potrebno međusobno koordinirati zajednički rad čitavog niza tijela koja do sada nisu postojala ili nisu obavljala ove poslove na nacionalnoj razini. Prijedlogom se želi prvo osigurati rad središnjih državnih tijela za informacijsku sigurnost (UVNS, ZSIS), kako bi ta tijela mogla razraditi i dalje predlagati donošenje nužne podzakonske regulative (uredbe, pravilnici, interni akti).

Članak 19. propisuje rokove za donošenje propisa informacijske sigurnosti u odnosu na vrijeme stupanja na snagu ovog Zakona. Nacionalna politika informacijske sigurnosti u Republici Hrvatskoj donosi se u roku od šest mjeseci, Uredbe Vlade RH o mjerama informacijske sigurnosti u okviru pojedinih područja informacijske sigurnosti donose se u roku od 9 mjeseci, jednako 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 i pravnim osobama iz članka 1. stavak 2. ovog Zakona treba se donijeti u roku od 18 mjeseci. UVNS i ZSIS moraju donijeti pravilnike o standardima informacijske sigurnosti u tijelima i pravnim osobama iz članka 1. stavak 2. ovog Zakona za sigurnosna područja za koja su nadležni, u roku od 15 mjeseci (članak 19. stavci 4. i 5.).

Članak 20. stavak 1., propisuje rokove za poslove provedbe, a stavak 2. za poslove nadzora informacijske sigurnosti u drugim tijelima, tako da se pravilnici tijela za te poslove trebaju donijeti u roku od 18 mjeseci. Sva tijela zadužena za provedbu (tijela i pravne osobe iz članka 1. stavak 2. ovog Zakona) dužna su u roku od 3 mjeseca od donošenja mjerodavnih pravilnika (članak 19., stavci 4. i 5.), donijeti Pravilnike tijela ili pravne osobe o provedbi mjera i standarda informacijske sigurnosti u pojedinom tijelu (stavak 3.). Za samu provedbu mjera i standarda informacijske sigurnosti u tim tijelima i pravnim osobama propisan je rok od daljnjih 6 mjeseci.