Središnji državni ured za *e*-Hrvatsku

Stručna skupina za informacijsku sigurnost

NACIONALNI PROGRAM INFORMACIJSKE SIGURNOSTI U REPUBLICI HRVATSKOJ

Zagreb, ožujak 2005.

1. Naslov dokumenta
   Nacionalni program informacijske sigurnosti u Republici Hrvatskoj
2. Svrha dokumenta
   Ovaj dokument definira ciljeve informacijske sigurnosti na razini Republike Hrvatske, nadležnosti i poslove pojedinih institucija u području informacijske sigurnosti, kao i potrebnu međusobnu koordinaciju svih čimbenika informacijske sigurnosti. Nacionalni program informacijske sigurnosti stvara čvrstu osnovu za razvoj suvremenog informacijskog društva i prosperitet građana, gospodarstva i države te pretpostavke za međunarodne integracije u Europsku uniju i Sjevernoatlantski savez (NATO). Program razrađuje četverogodišnji ciklus postupnog uvođenja mjera informacijske sigurnosti u različite segmente društva, a u provedbenom dijelu predviđa potrebne faze i mehanizme praćenja predviđenih aktivnosti i projekata. Dokument se veže na odrednice Programa eEurope 2005 Europske unije, Inicijative *e*-Jugoistočna Europa (eSEE Initiative) pod okriljem Pakta o stabilnosti te Akcijskog plana za članstvo u NATO-u (MAP) u kojima Republika Hrvatska aktivno sudjeluje.
3. Oznaka
   SDUeH-InfSig-01
4. Status
   Konačni tekst
5. Verzija
   V 3.0
6. Datum verzije
   30. 03. 2005.
7. Izvor
   Središnji državni ured za *e*-Hrvatsku,
   Stručna skupina za informacijsku sigurnost sastavljena od predstavnika institucija:
   Središnji državni ured za *e*-Hrvatsku (SDUeH),
   Ministarstvo obrane RH (MORH) i Vojna sigurnosna agencija (VSA),
   Ministarstvo unutarnjih poslova (MUP),
   Ministarstvo vanjskih poslova i europskih integracija (MVPEI),
   Protuobavještajna agencija (POA),
   Obavještajna agencija (OA),
   Zavod za informacijsku sigurnost i kripto-zaštitnu tehnologiju (ZISKZT),
   Ured Vijeća za nacionalnu sigurnost (UVNS),
   Fakultet elektrotehnike i računarstva (FER),
   Hrvatska akademska i istraživačka mreža (CARNet)
8. Autorsko pravo:

SADRŽAJ:

SAŽETAK PROGRAMA

Nacionalni program informacijske sigurnosti u Republici Hrvatskoj definira ciljeve informacijske sigurnosti na razini Republike Hrvatske, nadležnosti i poslove pojedinih institucija u području informacijske sigurnosti, kao i potrebnu međusobnu koordinaciju svih čimbenika informacijske sigurnosti. Program stvara čvrstu osnovu za razvoj suvremenog informacijskog društva i prosperitet građana, gospodarstva i države te pretpostavke za međunarodne integracije u Europsku uniju (EU) i Sjevernoatlantski savez (NATO). Program razrađuje četverogodišnji ciklus postupnog uvođenja mjera informacijske sigurnosti u različite segmente društva, a u provedbenom dijelu predviđa potrebne faze i mehanizme praćenja predviđenih aktivnosti i projekata. Dokument se veže na odrednice programa eEurope 2005 Europske unije, Inicijative *e*-Jugoistočna Europa (eSEE inicijative) pod okriljem Pakta o stabilnosti te Akcijskog plana za članstvo u NATO-u (MAP), u kojima Republika Hrvatska aktivno sudjeluje.

Nacionalni program informacijske sigurnosti u Republici Hrvatskoj bavi se prvenstveno organizacijskim i upravljačkim aspektima uvođenja sustava informacijske sigurnosti u Republici Hrvatskoj, polazeći od preduvjeta potrebnih za sustavni razvoj zakona, propisa, metoda, postupaka i tehničkih sustava u području informacijske sigurnosti.

Temeljna operativna zadaća ovog Nacionalnog programa jest započeti sustavni proces uvođenja informacijske sigurnosti u Republici Hrvatskoj. To podrazumijeva donošenje nacionalne politike informacijske sigurnosti te niza provedbenih propisa po užim sigurnosnim područjima (sigurnosne provjere osoblja, fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava, sigurnost pristupa trećih strana i vanjske suradnje). Na takav način propisuju se koordinirani postupci, tj. sustav obveza i odgovornosti pojedinih tijela državne vlasti u ovom procesu. Nakon donošenja temeljnih dokumenata od strane Hrvatskog sabora i Vlade RH slijedi donošenje nacionalnih pravilnika i smjernica od strane središnjih sigurnosnih tijela u RH.

Strateška zadaća ovog Nacionalnog programa je postupno širenje procesa informacijske sigurnosti na državu u cjelini, uvođenjem odgovarajućih minimalnih sigurnosnih kriterija u državni i javni sektor te razvojem sigurnosne kulture najširih slojeva stanovništva.

1 UVOD

Uvođenje informacijske sigurnosti u sve segmente jedne zemlje predstavlja uvjet stvaranja informacijskog društva. Stvaranje informacijskog društva, gledano u širem kontekstu, bit će ne samo preduvjet uključenja zemlje u međunarodne integracijske procese, već iznad svega način za opstanak zemlje u društvu razvijenih. Ključni čimbenici informacijskog društva su državna uprava, gospodarstvo i građanstvo, a temelj razvoja informacijskog društva je povjerenje i sigurnost ovih čimbenika u interaktivne elektroničke usluge i elektroničko poslovanje.

Uspostavljanjem sustava informacijske sigurnosti i upravljanjem ovim sustavom u svim segmentima potrebnim za jednu suvremenu zemlju, državna uprava izvršava svoju ulogu u okviru izgradnje informacijskog društva. Takvu ulogu državna uprava ima i u okviru tradicionalnog društva. Organizacija tradicionalnog društva počiva na prevenciji potencijalnih ugroza društva te na brizi o razvoju zaštitnih i represivnih mjera. Na sličan način informacijska sigurnost predstavlja temelje za stvaranje i organizaciju informacijskog društva. Razvojem informacijske sigurnosti državna uprava uspostavlja preventivne mjere te stvara organizacijsko-tehničke pretpostavke za sustavni razvoj zaštitnih i represivnih postupaka u okviru informacijskog društva. Analogno tradicionalnom društvu, sustavom informacijske sigurnosti državna uprava stvara i temelje za formalni razvoj istražnih metoda i postupaka temeljenih na metodama računalne forenzike, ali i za tranziciju kaznenog zakonodavstva iz tradicionalnih okvira u informacijsko društvo. Sve ove procese nije moguće uspješno provesti bez dobro razvijene informacijske sigurnosti na nacionalnoj razini. U tom procesu nužna je uloga državne vlasti, kao čvrste pokretačke snage ovakvog procesa, koji treba doprijeti u sve pore jednog suvremenog društva.

Istraživanja provedena u razvijenim zemljama Europske unije (EU) i svijeta, pokazuju da financijske investicije i tehnološka dostignuća nisu dovoljni za stvaranje informacijskog društva te se sve razvijene zemlje posljednjih godina ubrzano i intenzivno okreću programima informacijske sigurnosti u svim segmentima državnog i gospodarskog sektora (razvoj preventivnih i represivnih postupaka), ali i programima razvoja sigurnosne kulture u najširima slojevima stanovništva. Ako se uspoređuje iskustvo tradicionalnog društva sa suvremenim informacijskim društvom kojem težimo, lako je uočiti da je razvoj tradicionalnog društva prošao sve ove faze te ih se ne može izbjeći niti u razvoju informacijskog društva. Za usporedbu možemo uzeti tradicionalno područje prometa, u kojemu razvoj i primjenu prometnih tehnologija i resursa nije moguće odvojiti od područja sigurnosti u prometu, a preventivne i represivne mjere, međusobno se prožimaju i ravnopravno razvijaju te su prisutne u životu svakog građanina počevši od njegove najranije dobi i predškolskih programa.

Nacionalni program informacijske sigurnosti (Nacionalni program) u Republici Hrvatskoj bavi se prvenstveno organizacijskim i upravljačkim aspektima uvođenja sustava informacijske sigurnosti u Republici Hrvatskoj (RH), polazeći od preduvjeta potrebnih za sustavni razvoj zakona, propisa, metoda, postupaka i tehničkih sustava u području informacijske sigurnosti.

Temeljna operativna zadaća ovog Nacionalnog programa jest započeti sustavni proces uvođenja informacijske sigurnosti u RH. To podrazumijeva donošenje

nacionalne politike informacijske sigurnosti te niza provedbenih propisa po užim sigurnosnim područjima (sigurnosne provjere osoblja, fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava, sigurnost pristupa trećih strana i vanjske suradnje). Na takav način propisuju se koordinirani postupci, tj. sustav obveza i odgovornosti pojedinih tijela državne vlasti u ovom procesu. Nakon donošenja temeljnih dokumenata (okvirni zakon o informacijskoj sigurnosti i nacionalna politika ili strategija informacijske sigurnosti) od strane Hrvatskog sabora, slijedi donošenje uredbi, pravilnika i smjernica od strane Vlade i središnjih sigurnosnih tijela u RH. Svi ovi dokumenti, sigurnosna politika, provedbene uredbe, pravilnici i smjernice, donose se na najvišoj državnoj razini i primjenjuju na središnja tijela izvršne vlasti – tijela Skupine A prema definiciji u Nacionalnom programu. Na temelju ovakvih propisa svako pojedino tijelo Skupine A razrađuje svoje detaljne procedure postupanja (naputke), koje su u ovakvom sustavu u visokoj mjeri međusobno usklađene. Ovako koncipirani propisi imaju za cilj uvesti minimalne sigurnosne kriterije na razini središnje državne vlasti RH, što je jedan od temeljnih zahtjeva Sjevernoatlantskog saveza (NATO) u okviru Akcijskog plana za članstvo (MAP). Nacionalnim programom planira se dostizanje stupnja informacijske sigurnosti u Republici Hrvatskoj sukladnog NATO standardima do kraja 2006. godine.

Aktualne promjene u zakonodavstvu EU u posljednjih nekoliko godina, usmjerene su uvelike na razvoj sigurnosne politike EU i slijede iskustvo sigurnosnog modela NATO-a, stečeno u dugogodišnjem multinacionalnom okruženju. Stoga će i za sve buduće članice EU prepoznavanje važnosti ovog područja, te sustavan pristup sigurnosti na nacionalnoj razini biti jedan od kriterija zrelosti zemlje kandidata. Obzirom na aktualne integracijske procese koje RH provodi prema NATO-u i EU, Nacionalni program temeljen je na sukladnosti sigurnosnih modela koje primjenjuju NATO i EU. Proces harmonizacije hrvatskog zakonodavstva sa zakonodavstvom EU, neumitno će vremenom dovesti do sukladnosti svih nacionalnih propisa sa zahtjevima EU, pa tako i u području informacijske sigurnosti. Međutim, u dijelu hrvatskih propisa, koji su koncepcijski zastarjeli i onemogućavaju početak uvođenja informacijske sigurnosti u institucije državne vlasti RH, potrebno je izvršiti koordinirane i brze zakonske promjene unutar rokova zadanih Nacionalnim programom.

Strateška zadaća Nacionalnog programa je postupno širenje procesa informacijske sigurnosti na državu u cjelini, uvođenjem odgovarajućih minimalnih sigurnosnih kriterija u državni i javni sektor te razvojem sigurnosne kulture najširih slojeva stanovništva. Ovaj proces je iznimno važan jer ljudsko društvo danas prolazi kroz fundamentalnu transformaciju iz industrijskog u informacijsko društvo. Tehnologije informacijskog doba preuzimaju postupno sve industrijske i socijalne aktivnosti i ubrzavaju globalizaciju ekonomija. Izgradnja informacijskog društva danas nije stvar izbora, niti samo jedan od uvjeta međunarodnih integracija. Izgradnja informacijskog društva prvenstveno je uvjet opstanka u društvu razvijenih.

Državna vlast ima temeljnu ulogu u stvaranju informacijskog društva. Prvi korak u tome je stvaranje zajedničke arhitekture informacijskih sustava državne uprave kroz projekte elektroničke državne uprave. Elektronička državna uprava podrazumijeva interaktivne elektroničke usluge državne uprave te najrasprostranjenijih javnih usluga, kao što su zdravstvo, obrazovanje itd. Elektronička državna uprava predstavlja okosnicu razvoja informacijskog društva, osobito u smislu stvaranja povjerenja i sigurnosti građanstva i poslovnog sektora u ovakav način poslovanja, ali

i povjerenja u državnu upravu koja provodi takvu modernizaciju. Upravo stoga suvremena državna uprava mora sustavno uvoditi mjere informacijske sigurnosti.

U stvaranju informacijskog društva nužno je postaviti određene sigurnosne okvire ne samo u tijela središnje izvršne vlasti – tijela Skupine A prema Nacionalnom programu, već u državnu vlast u širem smislu, ostale stupove i razine vlasti te u javni sektor – tijela Skupine B prema Nacionalnom programu. Ovaj dio procesa stvaranja informacijskog društva predstavlja nadgradnju prethodno opisanih okvira za središnju izvršnu vlast. U ovom dijelu su manje izraženi posebni zahtjevi informacijske sigurnosti (NATO, EU), a naglasak se stavlja na primjenu općih zahtjeva informacijske sigurnosti (međunarodne tehničke i sigurnosne norme te metode najbolje prakse). Programi informacijske sigurnosti za tijela Skupine B temelje se stoga na međunarodnim tehničkim i sigurnosnim normama te sadrže neke uže dijelove nacionalnih propisa informacijske sigurnosti za tijela Skupine A. Zbog primjene na tijela u različitim stupovima i razinama vlasti u državi, programi informacijske sigurnosti za tijela u Skupini B sadržajno se razlikuju od programa Skupine A. Izvršavanjem ovog dijela Nacionalnog programa Republika Hrvatska se osposobljava za provedbu niza inicijativa u sklopu pridruživanja EU, kao što je program eEurope 2005, te stvara ključne pretpostavke interoperabilnosti i mogućnosti korištenja podataka javnog sektora. Nacionalnim programom planira se u Republici Hrvatskoj dostići stupanj razvoja, potreban za provođenje strateških informacijskih projekata EU do kraja 2007. godine.

Nacionalni program predviđa inicijative državne vlasti Republike Hrvatske koje su usmjerene prema privatnom sektoru, odnosno gospodarstvu u cjelini – tijela Skupine C prema Nacionalnom programu. Inicijative se provode kroz različite oblike javno-privatnog partnerstva, danas uobičajenog u području informacijske sigurnosti u svijetu. Ovdje se primarno radi o interesu države da postojeće sigurnosne investicije u gospodarstvu, koje su i kod nas, primjerice u financijskom sektoru, na relativno visokoj razini, sustavno usmjeri na dobrobit svih čimbenika u državi. Primjer za to je javno-privatno partnerstvo na definiranju skupa organizacijsko-tehničkih protokola i metoda informacijske sigurnosti za gospodarske subjekte, čime se može postići niz dobiti za sve zainteresirane strane, poput olakšica na police osiguranja, učinkovite procedure istražnih i računalno-forenzičkih postupaka, manjeg broja elektroničkih provala, zloporaba i sl.

U smislu konkurentnosti gospodarstva i privlačnosti zemlje za inozemne investitore, neuspjeh u uspostavi informacijske sigurnosti na nacionalnoj razini može biti poguban za RH već krajem ovog desetljeća, osobito zbog uznapredovalih procesa informacijske sigurnosti u razvijenim zemljama i zemljama EU. Uzme li se u obzir da Nacionalni program informacijske sigurnosti u RH, kao i slični programi u drugim državama, predviđa minimalno trajanje od četiri godine, jasno je da vrijeme raspoloživo za priključenje RH razvijenim zemljama EU i svijeta u izgradnji informacijskog društva polako ističe.

1.1 Organizacija dokumenta

Nacionalni program informacijske sigurnosti u RH sadrži 10 poglavlja.

U poglavlju **2. Informacijska sigurnost** uvodi se pojam informacijske sigurnosti, definiraju osnovni pojmovi koji se susreću u daljnjem tekstu, objašnjavaju pojedina područja informacijske sigurnosti kao što su sigurnosne provjere osoblja, fizička sigurnost, sigurnost podataka, sigurnost informacijskih sustava, te sigurnost pristupa trećih strana i vanjske suradnje. Prikazan je i proces upravljanja sustavom informacijske sigurnosti, te kako treba organizirati sustav informacijske sigurnosti.

U poglavlju **3. Zahtjevi informacijske sigurnosti i međunarodni odnosi** predstavljeni su zahtjevi informacijske sigurnosti u okviru integracijskih procesa u Europskoj uniji i Sjevernoatlantskom savezu, sadržani u programima NATO-a Partnerstvo za mir (PfP) i Akcijskom planu za članstvo (MAP), Sporazumu o stabilizaciji i pridruživanju u EU (SSP) te u sigurnosnim politikama NATO-a i EU, kao i pratećim provedbenim dokumentima sigurnosne politike.

U poglavlju **4. Stanje informacijske sigurnosti u RH** prikazani su zakonodavni, institucionalni i infrastrukturni okviri koji predstavljaju osnovu za daljnju razradu Nacionalnog programa informacijske sigurnosti u RH. U sklopu zakonodavnog okvira odabrana su zakonska područja koja su ključna za proces uvođenja suvremenog koncepta informacijske sigurnosti u RH. Posebno su istaknuti propisi koji nisu usklađeni s temeljnim načelima informacijske sigurnosti (npr. ZZTP) ili pak uopće ne poznaju pojam informacijske sigurnosti (npr. Uredsko poslovanje). Naveden je prijedlog konkretnih potreba za izmjenama i dopunama propisa koji su nedostatni s aspekta informacijske sigurnosti, nositelji i rokovi sukladni potrebama ovog Nacionalnog programa informacijske sigurnosti. U sklopu institucionalnog okvira predstavljena su tijela koja čine osnovu organizacije sustava informacijske sigurnosti u RH. Također je predstavljen i kritički osvrt na postojeći infrastrukturni okvir za provedbu Nacionalnog programa.

U poglavlju **5. Razgraničenje nadležnosti u odnose na podatke i informacijsku infrastrukturu u RH** definirane su nadležnosti za ključne funkcionalnosti u području informacijske sigurnosti. Po načinu upravljanja informacijskom sigurnošću i nadležnostima za ključne funkcionalnosti u području informacijskom sigurnošću prepoznate su tri skupine pravnih osoba:

- **Skupinu A** čine tijela središnje izvršne vlasti, tijela sustava nacionalne sigurnosti te drugih institucija koje obavljaju vitalne i zajedničke funkcije za tijela iz Skupine A;
- **Skupinu B** čine tijela koja predstavljaju ostale stupove i razine državne vlasti u RH, javnog sektora te drugih institucija koje obavljaju vitalne i zajedničke funkcije za tijela iz Skupine B;
- **Skupinu C** čini privatni sektor u širem smislu. Ovdje pripadaju sve ostale pravne osobe u RH i sva trgovačka društva u RH, neovisno o tipu vlasništva (privatno, državno ili mješovito) ili osnivaču.

U poglavlju **6. Sigurnosna politika** predstavljeni su propisi informacijske sigurnosti i nadležnosti donošenja za pojedine skupine, definirane u petom poglavlju. Propisi

informacijske sigurnosti se dijele na krovne, provedbene i izvršne propise, te norme i preporuke.

U poglavlju **7. Edukacija i razvoj sigurnosne kulture** predstavljene su mjere, te nositelji planiranja i provedbe razvoja sigurnosne kulture, kao i prijedlog informatičkog obrazovanja i sigurnosne kulture uz nositelje planiranja i provedbe, a dani su i vremenski rokovi provedbe pojedinih faza.

U poglavlju **8. Provedba Nacionalnog programa informacijske sigurnosti u RH** razrađene su predradnje i faze provedbe Nacionalnog programa informacijske sigurnosti u RH te predviđene odgovarajuće metode praćenja provedbe Nacionalnog programa. U tu svrhu praćenje će biti organizirano kroz posebnu stručnu skupinu koja će na kvartalnoj i godišnjoj razini procjenjivati provedbu Nacionalnog programa, dok će državna tijela, koja sukladno Nacionalnom programu preuzimaju središnju državnu ulogu u informacijskoj sigurnosti, procjenjivati kontinuiranu provedbu Nacionalnog programa.

Poglavlje **9. Literatura** daje popis korištene literature.

U poglavlju **10. Stručna skupina za informacijsku sigurnost** navedeni su članovi stručne skupine koja je radila na izradi prijedloga Nacionalnog programa informacijske sigurnosti u Republici Hrvatskoj.

U **Prilogu A** nalazi se popis mjera provedbe Nacionalnog programa s nositeljima, sudionicima i rokovima izvršenja.

Prilog B daje popis korištenih kratica.

2 INFORMACIJSKA SIGURNOST

2.1 Pojam informacijske sigurnosti

Pojam informacijske sigurnost u ovom dokumentu obrađuje se na način kakav je danas prihvaćen u razvijenim zemljama svijeta i koji osigurava sukladnost s konceptom informacijske sigurnosti NATO-a i EU. Sustav informacijske sigurnosti obuhvaća ljude, procese, organizaciju i tehnologiju. Taj se sustav sastoji od uravnoteženog skupa sigurnosnih mjera: sigurnosne provjere osoblja, fizičke sigurnosti, sigurnosti podataka, sigurnosti informacijskih sustava; te koordiniranog uvođenja formalnih procedura poput procjene rizika, certifikacije osoblja i uređaja, kao i akreditacije tehničkih sustava za primjenu u određenom segmentu poslovnog procesa državne uprave. Uravnoteženost i koordinacija bitnih mjera i postupaka postižu se organizacijom i upravljanjem informacijskom sigurnošću.

2.1.1 Osnovni pojmovi

Prije opisa i objašnjenja sigurnosnih mjera potrebno je definirati osnovne pojmove koji se koriste u ovom tekstu, tj. definirati što je to podatak, informacija, informacijski sustav, itd.

Podatak je skup prepoznatljivih znakova zapisanih na određenom mediju.

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

Informacijski sustav je svaki sustav kojim se prikupljaju, pohranjuju, čuvaju, obrađuju, prikazuju, dohvaćaju i isporučuju informacije tako da budu dostupne i upotrebljive za svakoga tko ima pravo njima se koristiti.

Informatička oprema su svi fizički uređaji i/ili sredstva koji čine informacijski sustav.

Informacijska sigurnost se definira kao očuvanje:

a) povjerljivosti – osiguranje da je informacija dostupna samo onima koji imaju ovlašteni pristup istoj,
b) integriteta – zaštita postojanja, točnosti i kompletnosti informacije kao i procesnih metoda,
c) raspoloživosti – osiguranje da autorizirani korisnici imaju mogućnost pristupa informaciji i pripadajućim sredstvima kada se usluga zahtijeva.

Zaštita je skup mjera za očuvanje sigurnosti.

Nadzor je provjera da li je sustav zaštite učinkovit.

Odgovornost je ponašanje po zadanom skupu pravila.

Ovlaštenje je pravo postupanja u zadanim okvirima.

Vlasnici podataka odgovorni su za sve radnje s podacima u njihovoj nadležnosti, tijekom životnog ciklusa podataka. Pri tome, radnje s podacima podrazumijevaju nastajanje, obrađivanje, pohranjivanje i arhiviranje podataka.

Informacijska infrastruktura obuhvaća svu infrastrukturu u određenom državnom tijelu ili pravnoj osobi koja na bilo koji način utječe na temeljna svojstva povjerljivosti, dostupnosti ili cjelovitosti podataka i u okviru koje podaci nastaju, obrađuju se ili pohranjuju.

Vlasnici informacijske infrastrukture odgovorni su za planiranje i implementaciju organizacijskih i tehničkih mjera u skladu s važećim propisima informacijske sigurnosti.

Pravo pristupa i korištenja informacijskih resursa određuje se isključivo po načelu poslovne potrebe («need to know»), a ne po hijerarhijskom konceptu ranga radnog mjesta.

Sigurnosna akreditacija.

Akreditacija je općenito postupak u kojem mjerodavno neovisno akreditacijsko tijelo službeno potvrđuje pravnoj ili fizičkoj osobi da je sposobno provoditi određene poslove. Sigurnosna akreditacija se odnosi na provjeru sposobnosti pravnih osoba za provođenje procesa informacijske sigurnosti, sukladno mjerodavnim propisima informacijske sigurnosti. Proces informacijske sigurnosti sastoji se od niza propisanih mjera i metoda implementiranih u obliku organizacijskih i tehničkih kontrola u poslovne procese određene pravne osobe ili državnog tijela.

Sigurnosno akreditacijsko tijelo.

Akreditacijsko tijelo je neovisna pravna osoba ovlaštena zakonom ili akreditirana od strane određenog središnjeg akreditacijskog tijela, koja vrši provjeru sposobnosti pravnih osoba za provođenje procesa informacijske sigurnosti u okviru vlastitog poslovnog procesa.

Potvrda o sigurnosnoj akreditaciji

Akreditacijsko tijelo općenito izdaje potvrdu o akreditaciji pravnoj ili fizičkoj osobi za koju se utvrdi da ispunjava zahtjeve akreditacijskog procesa. Potvrda o sigurnosnoj akreditaciji označava zadovoljavanje propisanih zahtjeva procesa informacijske sigurnosti od strane određene pravne osobe ili državnog tijela. Potvrda o akreditaciji izdaje se uvijek na ograničeni vremenski rok. Uobičajeni rokovi za sigurnosne akreditacije su dvije, četiri i pet godina. Istekom akreditacijskog roka provodi se ponovna provjera, koja osim propisanih zahtjeva procesa informacijske sigurnosti ima za cilj utvrditi i kvalitetu upravljanja životnim ciklusom podataka, informacijske infrastrukture, fizičke sigurnosti i osoblja. Potvrdom o sigurnosnoj akreditaciji daje se ovlast za obavljanje određenih poslova.

Sigurnosni certifikat

Certifikat je općenito potvrda o sukladnosti određenog proizvoda, procesa ili usluge s nacionalnom normom ili formalnim tehničkim zahtjevima za proizvode, procese ili usluge. Sigurnosni certifikat odnosi se na osobe, proizvode ili sustave informacijske sigurnosti. Sigurnosnim certificiranjem se omogućava korištenje pojedinih tržišnih proizvoda u propisanim uvjetima s ciljem sustavne realizacije projekata informacijske infrastrukture. Primjerice proizvod tvrtke X, model Y, tip Z u inačici W, može se koristiti za razmjenu podataka u državnoj upravi do stupnja tajnosti «službena tajna – tajno».

Sigurnosno certifikacijsko tijelo
Certifikacijsko tijelo ili općenito tijelo za ocjenu sukladnosti je laboratorij neovisan o dobavljaču, potvrdbeno tijelo, nadzorno ili drugo tijelo koje sudjeluje u postupku ocjenjivanja sukladnosti. Sigurnosno certificiranje za potrebe tijela državne vlasti uobičajeno se organizira u središnjim državnim tijelima za sigurnost komunikacija (NCSA – National Communications Security Authority). Temeljni posao sigurnosnog certifikacijskog tijela je formiranje i redovito ažuriranje liste certificiranih proizvoda za upotrebu u nacionalnom sustavu informacijske sigurnosti. Postupci provođenja certificiranja sastoje se od laboratorijskih provjera i/ili preuzimanja određenih međunarodnih lista certifikata po utvrđenoj metodologiji. Liste certificiranih proizvoda koriste se u procesu sigurnosnog akreditiranja.

Tijela javne vlasti su državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave, pravne osobe s javnim ovlastima i druge osobe na koje su prenesene javne ovlasti.

2.1.2 Sigurnosne provjere osoblja

Sigurnosna provjera osoblja, osim primarnih mjera kojima se procjenjuje mogućnost dodjele ovlaštenja podrazumijeva i aktivnu brigu oko usmjeravanja, edukacije i kontrole ispravnog postupanja svakog pojedinca.

Sigurnosna provjera osoblja ponajprije obuhvaća procjenu da li se za nekog pojedinca u pogledu lojalnosti, povjerljivosti, pouzdanosti i vjerodostojnosti može dati ovlaštenje za pristup povjerljivim informacijama, a da to ne predstavlja neprihvatljiv rizik za sigurnost informacije. Procjena proizlazi kao rezultat obavljene sigurnosne provjere (provjere pouzdanosti) za one osobe čije zapošljavanje ili napredovanje podrazumijeva pristup povjerljivim informacijama. Sigurnosnu provjeru je potrebno provesti i za ugovorne strane i za osobe koje su samo privremeno u doticaju s povjerljivim informacijama. Sigurnosne provjere provode se u opsegu propisanom za dostupnu razinu povjerljivosti te uz znanje i pristanak provjeravane osobe.

Sigurnosna provjera osoblja podrazumijeva i pravovaljanu sigurnosnu informiranost, obrazovanje i obuku. Osoblje treba biti upoznato sa svojim sigurnosnim obavezama i propisanim postupcima, te biti redovito informirano o sigurnosnoj politici. Mora također biti upoznato i sa službenom procedurom izvješćivanja za slučaj sigurnosnih incidenata ili nepravilnosti, ali i sa sankcijama za sigurnosne prekršaje.

Putem programa sigurnosnog obrazovanja potrebno je razviti svijest o sigurnosnim prijetnjama i brizi za informaciju, te sposobnost pružanja podrške sigurnosnoj politici tijekom obavljanja svog redovnog posla.

2.1.3 Fizička sigurnost

Fizička sigurnost obuhvaća primjenu fizičkih i tehničkih mjera zaštite na mjestima, u zgradama i prostorima koji zahtijevaju zaštitu od gubitaka ili kompromitacije povjerljivih informacija. Uloga ovih mjera je sprječavanje nedopuštenog i nasilnog ulaska neovlaštenih osoba, te odvraćanje, otkrivanje i reagiranje na djelovanje neovlaštenih osoba.

Mjere fizičke sigurnosti obuhvaćaju i zaštitu informacija (infrastrukture) uslijed prirodnih pojava (požara, poplave, potresa, oluje), ali i brigu oko osiguranja adekvatnih uvjeta (temperatura, vlaga, neprekidno napajanje, zračenje) i odabira pozicije prostorija.

Definiranje obima fizičkih i tehničkih mjera zaštite treba biti usklađeno sa stupnjem tajnosti podataka, vjerojatnošću prijetnje i količinom informacija koje se moraju zaštititi. U prostorima u kojima se rukuje povjerljivim podacima utvrđuju se načela klasifikacije prostora na sigurnosne zone i administrativne zone. Fizička sigurnost provodi se ugradnjom fizičkih prepreka, sustava za otkrivanje neovlaštenog pristupa te sustava za kontrolu ulaska i izlaska. Fizička sigurnost provodi se nadalje angažiranjem stražarske službe te vršenjem pretresa, pratnje i nadzora posjetitelja.

2.1.4 Sigurnost podataka

Sigurnost podataka se ostvaruje na temelju zakona sustavnom primjenom propisanih sigurnosnih i zaštitnih mjera i postupaka za ovlašteni način prikupljanja, obrade, korištenja te za čuvanje, sprječavanje i oporavak od gubitka, ili neovlaštenog objavljivanja podataka.

Prvi i osnovni korak u ostvarenju sigurnosti podataka je klasifikacija ili razredba podataka obzirom na stupanj rizika i potrebne mjere zaštite sigurnosti podataka. Klasifikacija podataka propisana je zakonima i njima odgovarajućim provedbenim aktima koji zajedno omogućuju jednoznačno određivanje nazivne klase ili razreda podatka, odgovarajuće obvezatne oznake i tome odgovarajuće djelatne postupke, metode, sredstva i izvršitelje, ali i pravne (kaznene) sankcije za svaki odmak od propisanog postupka unutar klase i unutar određenog pravnog prostora. Klasifikacija treba biti bar onog stupnja kojeg je najviši povjerljivi dio, ali treba izbjegavati i pretjerano i preoskudno klasificiranje u interesu učinkovite sigurnosti i djelotvornosti. Klasifikacija sama po sebi nije zaštita, već smjernica koja ukazuje na potrebu posebnih mjera rukovanja i zaštite. Klasificirana informacija mora se zaštititi kroz svoj ciklus trajanja do razine koja je u skladu s njenom razinom klasifikacije. S njom se mora rukovati na način da je primjereno označena, jasno određena kao klasificirana i da ostaje klasificirana samo toliko dugo koliko je to potrebno. Odgovornost za dodjelu klasifikacije i njeno periodičko revidiranje treba ostati u okviru imenovanog vlasnika informacije. Po isteku potrebe za klasifikacijom potrebno je izvršiti deklasifikaciju. Oznaka neklasificirano ili nepostojanje nikakve klasifikacijske oznake ne podrazumijeva poimanje tog podatka kao javnog i ne predstavlja odobrenje za njegovu objavu. Objava neklasificiranih podataka mora se vršiti posebno propisanim formalnim procedurama.

U poslovnom procesu (uredsko poslovanje) sigurnost podataka podrazumijeva postojanje sigurnosnih procedura za prijem, rukovanje, pohranjivanje, arhiviranje, uništavanje, distribuciju, umnožavanje, prepisivanje, prevođenje, izdavanje, uvid i objavljivanje podataka. Sigurnosne procedure uključuju i postojanje evidencijskog sustava o kontroli pristupa i izvršenim radnjama, te kretanju (kolanju) i mjestu podataka.

2.1.5 Sigurnost informacijskih sustava – INFOSEC

Sigurnost informacijskih sustava (INFOSEC) podrazumijeva sigurnost podataka na elektroničkim medijima i računalima (COMPUSEC), sigurnost podataka u sustavima za prijenos podataka (COMSEC) te sigurnost informacijske infrastrukture u posebnim kategorijama prostora od različitih vrsta pasivnog ili aktivnog prisluškivanja (TECSEC).

Sigurnost informacijskih sustava obuhvaća primjenu mjera za zaštitu podataka koji su u obradi, ili su pohranjeni, ili je u tijeku njihov prijenos, od gubitka povjerljivosti, cjelovitosti i raspoloživosti, te radi sprječavanja gubitaka cjelovitosti ili raspoloživosti samih sustava. Sigurnosne mjere uključuju mehanizme i procedure koje trebaju biti implementirane u svrhu odvraćanja, prevencije, detektiranja i oporavka od utjecaja incidenata koji djeluju na povjerljivost, cjelovitost i raspoloživost podataka i pratećih sistemskih servisa i resursa, uključujući i izvješćivanje o sigurnosnim incidentima.

Sigurnost informacijskih sustava je dinamičan proces tijekom cijelog životnog ciklusa sustava te se on treba razmatrati od faze njegovog planiranja, razvoja, provedbe, operativnosti, rasta do rashodovanja i uništavanja prema potrebi. To je zapravo proces upravljanja rizikom koji se koristi za procjenu, nadgledanje, ukidanje, izbjegavanje, prijenos ili prihvaćanje rizika. Upravljanje rizikom je vještina koja stavlja u ravnotežu troškove primjene dodatnih sigurnosnih protumjera s koristi koja od toga proizlazi. Svrha procesa upravljanja rizikom je osiguranje permanentne funkcionalnosti sigurnosnih ciljeva povjerljivosti, cjelovitosti i raspoloživosti podataka.

Životni ciklus informacijskog sustava neizbježno prati i dokumentacija koja se odnosi na sigurnost. Ona podrazumijeva uzajamno djelovanje između svih strana uključenih u rad informacijskog sustava, od korisnika preko tijela odgovornih za planiranje, implementaciju i operativnost, do tijela za davanje sigurnosne akreditacije za rad. U dokumentaciju koja se odnosi na sigurnost spadaju elaborat o sigurnosti, sigurnosna prosudba, naputci za operativnu upotrebu sustava, te naposljetku suglasnost za upotrebu sustava. Sigurnosna akreditacija sustava odredit će da je dostignuta zadovoljavajuća razina zaštite informacijskog sustava i da se ona treba održavati.

Općenito se može reći da sigurnost informacijskih sustava obuhvaća sve što i informacijska sigurnost u širem smislu, samo primijenjeno u užim tehnološkim okvirima.

2.1.6 Sigurnost pristupa trećih strana i vanjske suradnje

Pristup trećih strana obuhvaća uobičajene postupke nabave, razvoja i održavanja opreme (tehnologije), u okviru čega postoji razmjena određenih podataka o organizaciji i/ili tehnologiji između državnog tijela i ponuđača. Pri tom odgovornost za obradu podataka ostaje u nadležnosti državnog tijela (npr. razvoj ili kupnja programa za praćenje poslovanja za potrebe državnog tijela). Vanjska suradnja je dublji oblik suradnje u kojoj vanjski poslovni subjekt ima odgovornost za obradu podataka određenog državnog tijela (npr. najam usluge za obradu podataka u nekom segmentu poslovanja državnog tijela, kao što su plaće ili stvaranje neke druge namjenske baze podataka i sl.).

U okviru svakog pristupa trećih strana, a naročito u okviru vanjske suradnje, potrebno je identificirati rizik. Procjena rizika obuhvaća elemente kao što su način pregovaranja i odobravanja povjerljivih ugovora, način pristupa vanjskog osoblja opremi i prostoru, utvrđivanje razloga i potrebe za pristupom, potreba provođenja sigurnosne provjere tvrtke i osoblja, izbor oblika ugovora, utvrđivanje sigurnosnih zahtjeva u ugovorima, razrada procedure razmjene povjerljivih podataka i sl.

Kada govorimo o sigurnosti pristupa trećih strana i vanjske suradnje u okviru NATO programa koristi se termin INDUSTRIJSKA SIGURNOST, koji između ostalog podrazumijeva i sigurnosnu provjeru tvrtke i osoblja (FSC – Facility Secure Clearance i PSC - Personnel Security Clerance) koje na nacionalnoj razini surađuju na NATO programima, uz potpisivanje prethodnih ugovora o prihvaćanju obaveza prema sporazumu o sigurnosti informacija.

U okviru ovog područja sigurnosti pojavljuju se i neke suvremene kategorije, čiji je smisao i dalje sigurnost suradnje s trećim stranama. To su različite inicijative za prevencijom monopola u pojedinim područjima državne nabave, obzirom da monopoli mogu uzrokovati ozbiljne sigurnosne posljedice. Najznačajnija takva inicijativa danas je inicijativa za ravnopravnim tretmanom programske podrške otvorenog izvornog koda od strane državne vlasti (Open Source Software – OSS, različite inačice operativnih sustava temeljenih na Linuxu i pratećih programskih aplikacija). U ovom području postoji formalna inicijativa EU te formalno ocjenjivanje uspješnosti OSS inicijative potencijalnih zemalja pristupnica u EU. U području izgradnje informacijsko-komunikacijskih sustava, uslijed liberalizacije tržišta telekomunikacija, ali i općenito zbog kvalitete razvoja projekata, nužno je u državnu upravu uvesti praksu ugovora o razini usluge (SLA – Service Level Agreement). Takvi ugovori obuhvaćaju sporazum s pružateljem usluge o kakvoći, prioritetima, rokovima, odgovornostima i sl., a posljedica su složenog poslovnog odnosa u kojem se radi o kompleksnim uslugama ili uslugama koje realizira više tvrtki, od kojih posljednja u nizu sklapa ugovor s krajnjim korisnikom, u ovom slučaju s državnim tijelom.

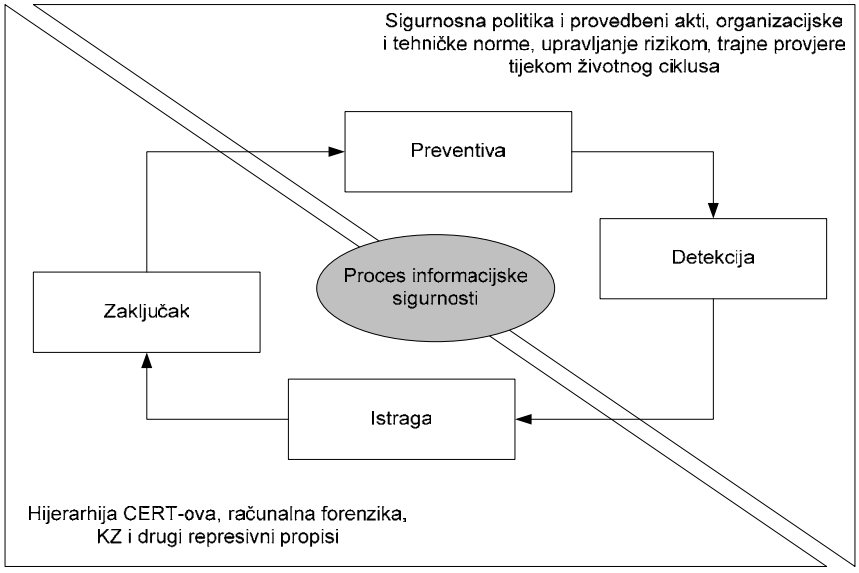
2.2 Upravljanje sustavom informacijske sigurnosti

Uspješna primjena informacijske sigurnosti unutar državnih tijela, ili općenito u okviru bilo kakve poslovne organizacije, zahtjeva sustavno upravljanje različitim aspektima informacijske sigurnosti, podržano odgovarajućom zakonskom podlogom. Upravo zbog važnosti i nužnosti ujednačavanja postupaka i procedura informacijske sigurnosti u svim tijelima državne uprave, upravljanje informacijskom sigurnošću mora biti usklađeno s organizacijskom hijerarhijom same državne uprave. Svi propisi informacijske sigurnosti donose se na najvišoj izvršnoj razini, bilo da se radi o državi ili o poslovnom subjektu. Na taj način se osigurava obvezatna primjena tih akata po svim hijerarhijskim organizacijskim razinama, što omogućava postizanje minimalnih sigurnosnih kriterija cijelog sustava (države ili poslovne korporacije). Stoga, u slučaju informacijske sigurnosti jedne države, donošenje akata i upravljanje mora se provoditi na nacionalnoj razini. Uobičajeno je to razina Vlade, odnosno stručnih tijela nacionalnog sigurnosnog sustava i Vlade. Isto vrijedi i za informacijsku sigurnost gospodarskih subjekata, koja također počinje na vršnoj razini same uprave poduzeća ili korporacije.

Proces upravljanja informacijskom sigurnošću odgovoran je za trajno usavršavanje zakonskog okvira počevši od sigurnosne politike, preko provedbenih uredbi, pravilnika i smjernica, do detaljnih procedura postupanja pojedinih tijela državne uprave. Upravljanje informacijskom sigurnošću obuhvaća postupke kao što su identifikacija resursa, klasifikacija podataka, upravljanje rizikom, planiranje i implementacija mjera, postupci certifikacije osoblja i uređaja, postupci akreditacije sustava za rad, nadzor implementacije i učinkovitosti mjera i postupaka, praćenje informacijskih sustava tijekom životnog ciklusa, sustavna edukacija i sl.

Na Slici 1. prikazan je procesni pogled na informacijsku sigurnost, prema kojem je vidljiv gornji desni dio koji karakteriziraju proaktivne mjere informacijske sigurnosti. Proaktivne mjere su one koje se primjenjuju «prije događanja sigurnosnih incidenata» i cilj im je spriječiti događanje incidenata. Ovaj dio mjera predstavlja suštinu sustava informacijske sigurnosti, a sastoji se od sigurnosne politike i provedbenih akata, organizacijskih i tehničkih normi, procjene i upravljanja rizikom, periodičnih revizijskih procesa i sl. U donjem lijevom dijelu Slike 1. prikazane su reaktivne mjere. Reaktivne mjere su one koje se primjenjuju «nakon događanja sigurnosnih incidenata» i cilj im je izvršiti procjenu i oporavak od šteta uzrokovanih sigurnosnim incidentima, revidirati organizacijske i tehničke dijelove sustava u svrhu budućeg sprječavanja sličnih incidenata te provesti prikupljanje dokaznog materijala za otkrivanje i zakonsko procesuiranje počinitelja određenog sigurnosnog incidenta.

Dobro organiziran sustav upravljanja informacijskom sigurnošću jedne zemlje ima neposredno preventivni utjecaj na ukupno stanje sigurnosti zemlje te čini temelj za razvoj učinkovitih represivnih postupaka suvremenog informacijskog društva.



Slika 1. Procesni pogled na informacijsku sigurnost

2.3 Organizacija sustava informacijske sigurnosti

Organizacija usklađenog sustava odgovornosti državnih tijela ključni je faktor za provođenje kompleksnog procesa upravljanja informacijskom sigurnošću. U cilju međusobne sukladnosti i zadovoljavajuće učinkovitosti takve organizacije u raznim zemljama, u svijetu se koristi generički model organizacijskih tijela, u okviru kojih su grupirani pojedini funkcionalni zahtjevi koji proizlaze iz općenitog procesa informacijske sigurnosti.

Pojam informacijske sigurnosti može se odnositi na međunarodne asocijacije (npr. NATO), pojedinačne države ili državne saveze kao što je EU, pri čemu postoje i vrlo velike razlike u ustroju državne vlasti pojedinih zemalja. Stoga je uobičajeno organizaciju informacijske sigurnosti definirati korištenjem generičkog modela organizacijskih tijela. Analizom funkcionalnih zahtjeva organizacijskih tijela u generičkom modelu i primjenom određenih načela tzv. generičke nadležnosti pridjeljuju se konkretnim nacionalnim tijelima. Tako se osigurava međusobna sukladnost sustava informacijske sigurnosti različitih zemalja (ili asocijacija), uz istovremeno poštivanje različitosti uređenja državne vlasti pojedinih zemalja. Kod raspodjele funkcionalnih zahtjeva primjenjuju se načela delegiranja odgovornosti na vršnu razinu organizacije, razdvajanja razvojnih i operativnih funkcionalnosti u cilju međusobnog poticanja kvalitetnijih rješenja, usklađenosti rada sigurnosnog i civilnog sektora državne uprave, primarne odgovornosti samih državnih tijela za vlastite implementacije i sl.

Osnovni skup generičkih organizacijskih tijela, kojima se osigurava međusobna sukladnost različitih nacionalnih modela organizacije informacijske sigurnosti i koji je primjeren zahtjevima NATO-a i EU-a, sadržava sljedeća generička organizacijska tijela:

Središnje državno sigurnosno tijelo odgovorno za usklađenost općih sigurnosnih mjera u državi
(**NSA** – National Security Authority);

Središnje državno komunikacijsko sigurnosno tijelo, odgovorno za usklađenost tehničkih sigurnosnih mjera
(**NCSA** – National Communications Security Authority);

Središnje državno tijelo za sigurnosne akreditacije komunikacijsko-informacijskih sustava ili više povezanih državnih tijela u nacionalnu hijerarhiju
(**SAA** – Security Accreditation Authority);

Državna tijela ili ustrojstvene jedinice u državnim tijelima odgovorne za nadzor operativnosti mjera INFOSEC-a u komunikacijsko-informacijskim sustavima
(**CIS OA** – Communications and Information System Operating Authority);

Državna tijela ili ustrojstvene jedinice u državnim tijelima odgovorne za planiranje i implementaciju mjera INFOSEC-a u komunikacijsko-informacijskim sustavima
(**CIS PIA** – Communications and Information System Planning and Implementation Authority);

Središnje državno tijelo i nacionalna hijerarhija državnih i privatnih tijela ili ustrojstvenih jedinica tijela, odgovornih za sigurnosne incidente na Internetu i drugim mrežama temeljenim na javnoj komunikacijskoj infrastrukturi
(**CERT** – Computer Emergency Response Team).

3 ZAHTJEVI INFORMACIJSKE SIGURNOSTI I MEĐUNARODNI ODNOSI

U okviru različitih integracijskih procesa uobičajeno je razlikovati eksplicitne i implicitne zahtjeve prema zemljama pristupnicama. Eksplicitni zahtjevi se navode u dokumentima koje potpisuju zemlje pristupnice i izražavaju se u obliku određene vrste partnerskih ciljeva. Implicitni zahtjevi sadržani su u nizu formalno-pravnih procedura i propisa određene zajednice i treba ih iščitavati i harmonizirati paralelno s dogovorenim integracijskim ciljevima. Takav posao obavljaju stručni timovi zemalja pristupnica, a rezultati tog posla, iako često nisu istaknuti kao eksplicitni ciljevi integracijskog procesa, preduvjet su ostvarenja tih ciljeva.

U području informacijske sigurnosti također susrećemo obje vrste zahtjeva integracijskih procesa. Primjer aktualnih eksplicitnih zahtjeva informacijske sigurnosti su minimalni sigurnosni kriteriji na nacionalnoj razini u okviru MAP programa NATO-a kojem je Hrvatska pristupila 2002. godine.

Nadalje, tu je Konvencija o kibernetičkom kriminalu Vijeća Europe koju je Hrvatska potpisala 23.11.2001., ratificirala 17.10.2002. i koja je stupila na snagu 1.7.2004. godine (NN, Međunarodni ugovori, 04/04). Konvencija o zaštiti pojedinaca pri automatskoj obradi osobnih podataka Vijeća Europe na snazi je od 1.10.1985. Republika Hrvatska potpisala je konvenciju 5.6.2003., ali je još nije ratificirala.

Implicitni zahtjevi informacijske sigurnosti vrlo su kompleksni i proizlaze iz niza propisa, u našem slučaju EU i NATO-a. Prvenstveno su to propisi poznati kao sigurnosna politika i provedbeni akti, ali i različiti zakoni, uredbe, rezolucije te akcijski programi u području projekata elektroničke državne uprave i informacijskog društva.

U okviru integracijskih procesa RH u EU i NATO, zahtjevi informacijske sigurnosti sadržani su u programima NATO-a Partnerstvo za mir (PfP) i Akcijski plan za članstvo (*MAP*), Sporazumu o stabilizaciji i pridruživanju u EU (SSP) te u sigurnosnoj politici NATO-a i EU, kao i pratećim provedbenim dokumentima sigurnosne politike. Nadalje, ti zahtjevi osobito su izraženi u programu eEurope 2005, kroz odluke, rezolucije i druge programske dokumente Vijeća Europske unije i Europske komisije u području informacijskog društva. Cijeli proces harmonizacije nacionalnog i EU zakonodavstva u mnogim područjima doticat će se problematike koja pripada u okvire ili se dotiče okvira informacijske sigurnosti (reforma državne uprave, uredsko poslovanje, osuvremenjivanje kaznenog zakonodavstva i sl.).

Prema Europskoj komisiji, sigurnost je preduvjet punog razvoja informacijskog društva, ključna komponenta vizije Interneta slijedeće generacije te jedan od šest prioriteta programa eEurope 2005. Sigurnost nije samo tehnološki izazov već u visokoj mjeri obuhvaća ljude i poslovne procese te je samim time sastavni dio suvremenog društva.

Područje informacijske sigurnosti se osim u okviru spomenutih integracijskih procesa spominje i u okviru međunarodnih bilateralnih Sporazuma o uzajamnoj zaštiti tajnih podataka. Tim se sporazumima države usaglašavaju oko istovjetnosti stupnjeva tajnosti, označavanju tajnih podataka, prosljeđivanju tajnih podataka, poduzimanju mjera za zaštitu tajnih podataka, povredi propisa o uzajamnoj zaštiti, nadležnosti

tijela i slično. Sporazumi tako reguliraju da prosljeđivanje tajnih podataka preko zaštićenih informacijsko komunikacijskih sustava podrazumijeva postojanje akreditacije za te sustave. Sporazumima se regulira da jedna strana od druge može zatražiti uvjerenje za neku stranku na njezinom državnom teritoriju u smislu postojanja ovlaštenja za pristup tajnim podacima s određenim stupnjem tajnosti. Nadležna tijela za provedbu ovih sporazuma su tijela navedena u unutarnjem zakonodavstvu tih država. Sporazume o uzajamnoj zaštiti tajnih podataka potpisuju Vlade, a u RH potpisivanje ovih Sporazuma prati i donošenje zakona o njihovom potvrđivanju temeljem Zakona o sklapanju i izvršavanju međunarodnih ugovora (NN 28/96).

3.1 Ugradnja harmonizacijskih očekivanja NATO i EU u zakonodavne i institucionalne okvire u RH

Problem informacijske sigurnosti jedna je od strateških odrednica Europske unije, ali je prepoznat i kao međunarodni problem. Vijeće Europe je usvojilo konvencije, europske sporazume i pripadajuće protokole, te preporuke kojima se nastoji, između ostalog, regulirati i pitanje informacijske sigurnosti. Strategija EU prema sigurnosnoj problematici određena je Odlukom Vijeća Europske unije o prihvaćanju sigurnosne politike [7] i Odlukom Europske komisije o provođenju sigurnosne politike [3].

Europska unija je izvršila i daljnju razradu sigurnosnog pristupa u području mrežne sigurnosti informacijskih sustava te pristupa razvoju informacijskog društva dokumentima kao što su [1,2,8,9,10]. Jasna sigurnosna strategija daje osnovu za izgradnju informacijske infrastrukture na kojoj će se temeljiti suvremeno informacijsko društvo te omogućava razvoj sigurnosne kulture javnog i privatnog sektora, ali i najširih slojeva građanstva. Ovakav pristup rezultirao je glavnim ciljevima i pripadnim aktivnostima koje su unesene u same temelje Akcijskog Plana eEurope 2005.[4,5]

Jedan od temeljnih vanjskopolitičkih ciljeva Republike Hrvatske jest ulazak RH u punopravno članstvo u EU. Potpisivanjem Sporazuma o stabilizaciji i pridruživanju (SSP) između Republike Hrvatske, s jedne strane, i Europskih zajednica i njihovih država članica, s druge strane [36], Republika Hrvatska je i službeno preuzela obvezu usklađivanja nacionalnog zakonodavstva s pravnom stečevinom EU (*Acquis Communautaire*), usporedo s obvezama uspostave političkog dijaloga, promicanja gospodarskih odnosa, razvoja zone slobodne trgovine, osiguranja regionalne suradnje te poticanja suradnje u nizu drugih područja. Iz toga proizlazi da će se i zakonodavstvo RH također morati usklađivati sa potrebama i zahtjevima u području informacijske sigurnosti. Potpisivanjem SSP-a Republika Hrvatska se, između ostalog, obvezuje da će «osnažiti suradnju na daljnjem razvijanju informacijskog društva, pripremu društva za digitalno doba, međusobno funkcioniranje mreža i usluga, izraditi plan usvajanja zakonodavstva EU na području informacijskog društva».

Neke od obveze informacijske sigurnosti za zemlje članice EU, dakle i za buduće zemlje pristupnice, mogu se vidjeti iz sljedećih dokumenata:

Rezolucijom Vijeća Europske unije 2002/C 43/02 od 28/01/2002 [7] definiraju se specifične aktivnosti u području mrežne i informacijske sigurnosti za zemlje članice EU. To su primjerice:

- povećanje svijesti o mrežnoj i informacijskoj sigurnosti putem odgovarajuće edukacije;
- promoviranje korištenja standarda ISO – 15408 (Common Criteria) s ciljem međusobnog priznavanja povezanih područja certificiranja;
- primjena učinkovitih interoperabilnih sigurnosnih rješenja temeljenih na prepoznatljivim normama, što uključuje i primjenu programske podrške otvorenog koda (Open Source Software – OSS), u projektima elektroničke Vlade i elektroničke javne nabave, kao i primjenu digitalnih potpisa i jake autentikacije za sve javne interaktivne usluge;
- učinkoviti odgovor na sigurnosne incidente (CERT – Computer Emergency Response Team) te međusobna razmjena podataka i suradnja na području mrežne i informacijske sigurnosti.

Akcijskim Planom eEurope 2005 [4] predlažu se slijedeće aktivnosti:

- osnivanje Cyber security task force (CSTF) s punom funkcionalnošću do sredine 2003. g.;
- postizanje «kulture sigurnosti» u dizajnu i implementaciji informacijskih i komunikacijskih proizvoda do kraja 2005. g.;
- ostvarenje sigurne komunikacije za razmjenu klasificiranih vladinih informacija do kraja 2003. g.

Kako je područje informacijske sigurnosti od strateškog interesa za EU, postavljeni su i formalni programi kao što je MODINIS [10], kojim se područje primjene mjera informacijske sigurnosti širi na Europsko ekonomsko područje (zemlje EEA) i zemlje pristupnice u EU. Program MODINIS se sastoji u praćenju mjera poboljšanja mrežne i informacijske sigurnosti u okviru Akcijskog Plana eEurope 2005 i nacionalnih inačica istog, ali i općenitog utvrđivanja stanja sigurnosne kulture i mjera za poticanje sigurnosne kulture i primjene dobre sigurnosne prakse u nacionalnim okvirima.

U okviru Akcijskog plana za članstvo u NATO-u (MAP), koji je također strateški interes RH, potrebno je naglasiti formalni partnerski cilj PG G 0360 I – «Nacionalni program za sigurnosnu kooperaciju s NATO-om», koji do 2006. godine podrazumijeva uspostavu minimalnih sigurnosnih kriterija na nacionalnoj razini RH i to u četiri osnovna sigurnosna područja: fizička sigurnost, sigurnosna provjera osoblja, sigurnost podataka i INFOSEC. Sadržaj ovog zahtjeva definiran je sigurnosnom politikom i provedbenim dokumentima sigurnosne politike NATO-a, a svodi se na donošenje nacionalne sigurnosne politike sukladne NATO-ovoj u temeljnim sigurnosnim pitanjima i principima upravljanja sigurnošću.

Kako bi se opisani sigurnosni zahtjevi EU i NATO-a mogli provesti na nacionalnoj razini u Republici Hrvatskoj, potrebno je organizirati usklađeni sustav odgovornosti državnih tijela, koji će provoditi kompleksan proces upravljanja informacijskom sigurnošću. Nacionalna organizacija informacijske sigurnosti RH, u cilju međusobne sukladnosti s EU i NATO organizacijom, treba zadovoljavati generički model organizacijskih tijela, u okviru kojih su grupirani pojedini funkcionalni zahtjevi koji proizlaze iz sigurnosne politike i provedbenih dokumenata EU i NATO-a, odnosno iz njihovog procesa informacijske sigurnosti.

3.2 Organizacijski zahtjevi NATO-a

Međusobne političke konzultacije, suradnja i planiranje obrane podrazumijevaju razmjenu klasificiranih informacija među potpisnicima NATO saveza i budućim članicama tog saveza. Ta se suradnja ne odnosi samo na vojna tijela, već i na državna tijela te javni i privatni sektor. Sukladno odredbama o međusobnoj zaštiti i čuvanju NATO klasificiranih dokumenata donesen je Sporazum o sigurnosti informacija koji definira okvir i sadržaj sigurnosnih standarda, a obuhvaća dokumente sigurnosne politike, smjernice i implementacijske direktive kao potporu ovim dokumentima.

Potpisnice ovog sporazuma moraju osigurati :

1. Prilagodbu nacionalnih zakonskih propisa kako bi se NATO informacija štitila u skladu s NATO pravilima, što se prvenstveno odnosi na propise iz područja:
   - SIGURNOSNA PROVJERA OSOBLJA – za sve osobe koje imaju ovlašten pristup NATO klasificiranim informacijama treba izvršiti odgovarajuću sigurnosnu provjeru i dodijeliti adekvatno sigurnosno ovlaštenje (PSC – Personal Security Clearance);
   - FIZIČKA SIGURNOST – osigurati primjenu tehničkih mjera zaštite za mjesta, prostorije i zgrade u kojima se rukuje NATO klasificiranim informacijama (NATO registri i podregistri u tijelima državne uprave);
   - SIGURNOST INFORMACIJA – osigurati ispravno klasificiranje i označavanje povjerljivih NATO informacija i materijala, te osigurati evidencijski sustav za primanje, evidentiranje, rukovanje, distribuiranje i uništavanje informacija;
   - SIGURNOST INFORMACIJSKIH SUSTAVA (INFOSEC) – svi sustavi koji rukuju NATO klasificiranim informacijama trebaju biti podložni procesu sigurnosnog odobrenja, koji se temelji na sigurnosnim ciljevima povjerljivosti, cjelovitosti i dostupnosti;
   - INDUSTRIJSKA SIGURNOST – treba izvršiti provjeru za ustanove (FSC – Facility Secure Clearance) koje na nacionalnoj razini surađuju na NATO programima te potpisivanje prethodnih ugovora o prihvaćanju obaveza prema sporazumu o sigurnosti informacija.
2. Osnivanje tijela vlasti za nacionalnu sigurnost nadležnog za NATO aktivnosti, koje će provoditi zaštitne sigurnosne mjere.

Bitno je naglasiti da dokumenti NATO sigurnosne politike ne zahtijevaju da se osnivaju nova tijela koja obavljaju funkcije generičkih organizacijskih tijela, već samo dodjelu funkcionalnosti tih tijela nekom od postojećih tijela nacionalne vlasti.

Dokumenti NATO-ve politike identificiraju ova nacionalna tijela vlasti povezana sa sigurnošću:

NSA – National Security Authority

Središnje državno sigurnosno tijelo koje predstavlja najvišu razinu sigurnosne vlasti i ima ulogu središnjeg tijela za kontakt s NATO uredom za sigurnost (NOS).

NSA je odgovoran za koordinaciju svih pitanja koja se tiču NATO sigurnosne politike unutar države i za praćenje njihove primjene kako bi se osigurao

zajednički stupanj zaštite klasificirane informacije. Odgovornosti NSA uključuju i brigu o održavanju sigurnosti NATO klasificiranih informacija u državnim, vojnim i civilnim tijelima, brigu oko provođenja periodičkih inspekcija te brigu o provođenju sigurnosne provjere za sve njene državljane koji imaju pristup informacijama klasificiranim s NATO POVJERLJIVO i iznad toga.

NCSA – National Comunications Security Authority

Središnje državno tijelo za sigurnost komunikacija koje treba zajamčiti (potvrditi) da su kriptografski sustavi, proizvodi i mehanizmi za zaštitu NATO informacije, djelotvorno i efikasno odabrani, vođeni i održavani. NCSA treba kontrolirati kriptografske tehničke podatke koji se odnose na zaštitu NATO informacija unutar države, te izvještavati o NATO komunikacijskoj sigurnosti i za to vezanim INFOSEC pitanjima.

NCSA surađuje s pripadnim NSA.

NDA – National Distribution Authority

Središnje državno tijelo (ili više državnih tijela povezanih u nacionalnu hijerarhiju), odgovorno za rukovođenje NATO kriptomaterijalima unutar svoje države. Uloga je tog tijela osigurati primjerene procedure za sigurnosno rukovanje, čuvanje, distribuciju i evidenciju cjelokupnog kriptomaterijala.

NDA djeluju u koordinaciji s pripadnim NSA.

SAA – Security Accreditation (Approval) Authority

Središnje državno tijelo (ili više državnih tijela povezanih u nacionalnu hijerarhiju) odgovorno za izdavanje sigurnosnog odobrenja za sustave koji pohranjuju, procesuiraju i distribuiraju NATO klasificirane informacije.

CIS Operating Authority

Državna tijela ili ustrojstvene jedinice u državnim tijelima odgovorne za nadzor operativnosti mjera INFOSEC-a u komunikacijsko-informacijskim sustavima koji pohranjuju, procesuiraju i distribuiraju NATO klasificirane informacije.

CIS Planning and Implementation Authority

Državna tijela ili ustrojstvene jedinice u državnim tijelima odgovorne za planiranje i implementaciju mjera INFOSEC-a u komunikacijsko-informacijskim sustavima koji pohranjuju, procesuiraju i distribuiraju NATO klasificirane informacije.

3.3 Organizacijski zahtjevi EU

Organizacijski zahtjevi EU u području informacijske sigurnosti izraženi su prvenstveno u okviru sigurnosne politike EU i provedbenih propisa [1,2,3,7,8,9,10], a dodatno su razrađeni i predstavljaju preduvjete realizacije niza drugih EU dokumenata i programa spomenutih u poglavlju 3.1.

Osnovni skup generičkih organizacijskih tijela, koji proizlazi iz EU sigurnosne politike i strategije pristupa informacijskoj sigurnosti, sadržava sljedeća generička organizacijska tijela:

NSA – National Security Authority

Središnje državno sigurnosno tijelo koje predstavlja najvišu razinu sigurnosne vlasti i ima ulogu središnjeg tijela za kontakt s Glavnim tajništvom Vijeća EU (GSC – General Secretariat of the Council) i daje predstavnika u Odbor za sigurnost (SC – Security Committee).

NSA je odgovoran za koordinaciju svih pitanja koja se tiču EU sigurnosne politike unutar svoje države i za nadzor primjene sigurnosnih mjera kako bi se osigurao zajednički stupanj zaštite klasificirane informacije. Odgovornosti NSA uključuju i brigu o održavanju sigurnosti EU klasificiranih podataka u državnim tijelima, brigu oko provođenja periodičkih inspekcija te brigu o provođenju odgovarajućeg certificiranja za sve državljane koji imaju pristup EU klasificiranim podacima.

SAA – Security Accreditation (Approval) Authority

Središnje državno tijelo za sigurnosne akreditacije komunikacijsko-informacijskih sustava (ili više državnih tijela povezanih u nacionalnu hijerarhiju) odgovorno za izdavanje sigurnosnih odobrenja za sustave koji pohranjuju, procesuiraju i distribuiraju EU klasificirane podatke. Potrebnu tehničku pomoć osigurava u koordinaciji sa pripadajućim IA.

SAA djeluju u koordinaciji s nadležnim NSA.

IA – INFOSEC Authority

Središnje državno tijelo za sigurnost komunikacija. Nositelj poslova predlaganja i usklađivanja tehničkih dokumenata politike informacijske sigurnosti, daje tehničke savjete i podršku nacionalnom procesu sigurnosne akreditacije (SAA), ispomaže izradu i revidira sistemske sigurnosne zahtjeve (SSRS), provodi poslove obuke i edukacije na nacionalnoj razini, daje tehničke savjete u okviru istraga INFOSEC incidenata, donosi tehničke smjernice i brine se o propisivanju autorizirane programske podrške. Surađuje s relevantnim tijelima EU i zemalja članica po pitanju mrežne i komunikacijske sigurnosti.

Rad IA odvija se koordinirano s nadležnim NSA.

ITSOA – IT System Operational Authority

Državna tijela ili ustrojstvene jedinice u državnim tijelima koje imaju odgovornost za implementaciju mjera INFOSEC-a u svojim informacijsko-komunikacijskim sustavima tijekom njihovog životnog ciklusa. Odgovorna su nacionalnom IA. U tijelima je moguće odgovornost ITSOA delegirati na IT odjele ili posebno tehničko tijelo. U okviru EU prakse odgovornost ITSOA uobičajeno je pridijeljena vlasniku tehničkog sustava (TSO – Technical Systems Owner).

U domeni vlasništva podataka vlasnik podataka (IO – Information Owner) razlikuje se od TSO, koji je odgovoran za postavljanje zahtjeva za pristup podacima, pri čemu se ova odgovornost može delegirati na određenog

upravitelja podacima (Information Manager) ili upravitelja bazama podataka (Database Manager) unutar njihove nadležnosti.

CISO i LISO koordinatori informacijske sigurnosti

Na nacionalnim sustavima se određuju CISO (Central Information Security Officer) koordinatori informacijske sigurnosti, a pojedina tijela prema potrebi određuju LISO koordinatore informacijske sigurnosti (Local Information Security Officer). Ovi koordinatori su odgovorni za operativnost mjera informacijske sigurnosti u informacijskim sustavima za koje su nadležni. U tijelima je moguće odgovornost za operativnost mjera informacijske sigurnosti pridijeliti nadležnom koordinatoru informacijske sigurnosti (officers/site officers), uz uvjet samostalnosti koordinatora informacijske sigurnosti, odnosno nezavisnosti od nadležne ITSOA ustrojstvene jedinice. Svi CISO i LISO koordinatori odgovorni su nacionalnom IA, koji se brine za uspostavu nacionalne mreže koordinatora informacijske sigurnosti.

CERT – Computer Emergency Response Team

Središnje državno tijelo i nacionalna hijerarhija državnih i privatnih tijela ili ustrojstvenih jedinica tijela, odgovornih za sigurnosne incidente na Internetu i drugim mrežama temeljenim na javnoj komunikacijskoj infrastrukturi. Hijerarhija se uobičajeno sastoji od vršnog nacionalnog CERT-a, zatim hijerarhije unutar državnih tijela (vršni CERT državne uprave i CERT-ovi specifičnih ministarstva kao MORH i MUP) te različitih gospodarskih (TK operatori i ISP-ovi, financijske institucije i sl.). Svrha hijerarhije je međusobno izvještavanje o incidentima po vertikali, horizontalna komunikacija sa svojim funkcionalnim parom u inozemstvu te podrška istragama incidenata na najvišoj potrebnoj nacionalnoj ili višoj razini.

3.3.1 Europska agencija za mrežnu i informacijsku sigurnost – ENISA

Europski Parlament, Vijeće Europske unije i Europska komisija zastupaju stajalište da je potrebna jača europska koordinacija s obzirom na informacijsku sigurnost. Da bi se postigao taj cilj bilo je potrebno uspostaviti agenciju s pravnom ovlasti na području EU. U skladu s Uredbom Europskog Parlamenta i Vijeća Europske unije [32] ustrojena je Europska agencija za mrežnu i informacijsku sigurnost (European Network and Information Security Agency – ENISA).

Ova Agencija bi trebala uživati povjerenje javnih tijela i institucija, kao i privatnog sektora u zemljama članicama. Glavni cilj Agencije je kreirati zajedničko razumijevanje u Europi o problemima koji se odnose na informacijsku sigurnost, što je neophodno da bi se osigurala raspoloživost i sigurnost mreža i informacijskih sustava u EU. Agencija bi trebala pružati pomoć nadležnim nacionalnim tijelima u primjeni mjera EU koje se odnose na mrežnu i informacijsku sigurnost. Agencija će imati savjetodavne i koordinacijske funkcije, a u njoj će se skupljati i analizirati podaci koji se odnose na informacijsku sigurnost. Agencija će biti otvorena za sudjelovanje trećih zemalja koje imaju sporazume sa EU. ENISA je formalno osnovana 15. ožujka 2004., 6. listopada 2004. imenovan je izvršni direktor, a tijekom 2005. započeti će s radom.

Tijekom organiziranja sustava informacijske sigurnosti u RH u 2005. godini, nadležne nacionalne institucije u području mrežne i informacijske sigurnosti RH, trebale bi uspostaviti suradnju s ENISA-om. U okviru takve suradnje, bit će moguće pospješiti proces harmonizacije zakonodavstva po pitanju informacijske sigurnosti te ubrzati organizaciju informacijske sigurnosti u RH.

4 STANJE INFORMACIJSKE SIGURNOSTI U RH

U Republici Hrvatskoj ne postoji tradicija sustavnog provođenja informacijske sigurnosti u državnoj upravi i društvu u cjelini. Prvo pravno uvođenje ovog pojma bilo je 2002. godine u Zakonu o sigurnosnim službama (ZOSS – NN 32/02 i 38/02), iako je od osamostaljenja Republike Hrvatske u nekim službama ostvarena visoka razina zaštite tajnosti podataka. Pojam informacijske sigurnosti u hrvatsku praksu je uveden nekoliko godina prije donošenja ZOSS-a, u okviru zahtjeva programa Partnerstva za mir (PfP) i suradnje s NATO-om. U tom smislu jedino i postoji određeno stručno i organizacijsko iskustvo u RH, koje je ostvareno kroz stručne skupine MORH-a, Tim za INFOSEC i Stručni tim za postupak osnivanja Zavoda za informacijsku sigurnost i kripto-zaštitnu tehnologiju, koje su provodila dijelove programa PfP te kasnije programa Akcijskog plana za članstvo u NATO-u (MAP).

Reguliranje informacijske sigurnosti samo jednim nacionalnim zakonom ni približno nije dovoljno za sustavno uređenje tog kompleksnog multidisciplinarnog područja. Stoga Hrvatskoj u ovom području predstoji sustavna razrada zakonodavstva te određena prilagodba i reorganizacija državne uprave, kako bi ovo područje moglo biti uspostavljeno po standardima EU i NATO-a. Temeljni smisao informacijske sigurnosti je postizanje minimalnih, a zatim i adekvatnih sigurnosnih kriterija na razini državne uprave RH. Da bi se to postiglo potrebno je donijeti nacionalnu politiku informacijske sigurnosti te provedbene akte i smjernice za državnu upravu i sukladno tome, poticati tehničku normizaciju i javno-privatno partnerstvo u izgradnji informacijskog društva u cjelini. Kroz proces uvođenja informacijske sigurnosti mora se, između ostaloga, osuvremeniti sustav sigurnosne klasifikacije dokumenata i ujednačiti načini postupanja s podacima te razgraničiti podatke u vlasništvu državne uprave od javnih podataka, odnosno uvesti jasne i transparentne procedure objavljivanja u tijelima državne vlasti.

Sadašnje stanje u RH je takvo da su sigurnosni kriteriji u nekim tijelima vjerojatno i znatno viši od minimalnih koje zahtijevaju EU ili NATO, ali istovremeno u nizu državnih tijela sigurnosne mjere gotovo i ne postoje. U nekim gospodarskim sektorima, kao što je npr. financijski sektor, znatna su ulaganja u područje informacijske sigurnosti, ali ne postoje inicijative, mjere i standardi koji bi takva ulaganja usmjeravali i osigurali primjenu relevantnih sigurnosnih normi, već to ovisi isključivo o poslovnoj politici svake pojedine tvrtke ili vlasnika. Upravo je provođenje inicijativa, donošenje mjera i preporuka te poticanje normizacije u području informatizacije i informacijske sigurnosti, temeljni zadatak državne uprave u suvremenom informacijskom društvu.

Razvoj informacijske tehnologije i infrastrukture u državi mora biti uvjetovan razvojem sigurnosno-zaštitnih mjera upotrebe tih tehnologija i infrastrukture, ali i razvojem sigurnosne kulture najširih skupina građanstva. Takav pristup donosi kategoriju povjerenja svih čimbenika informacijskog društva u razvoj novih e-usluga. Upravo nedostatak povjerenja najširih skupina građanstva, uz nerazvijenost infrastrukture, jedan je od ključnih razloga sporog razvoja novih e-usluga. To je posebno izraženo u tranzicijskim zemljama, a važi i za Republiku Hrvatsku, te ima visok utjecaj na sporost razvoja elektroničke trgovine i usluga. Osposobljavanjem državne uprave u području informacijske sigurnosti i razvojem sigurnosne kulture građanstva, može se bitno umanjiti stupanj nepovjerenja najširih skupina građanstva u suvremene

tehnološke usluge. Takvim pristupom državna uprava u suvremenom informacijskom društvu pruža građanstvu i pravnim subjektima potrebnu zaštitu, na način kako to čini i u tradicionalnim elementima organizacije društva.

4.1 Zakonodavni okvir

U ovom poglavlju prikazana su zakonska područja koja su ključna za proces uvođenja suvremenog koncepta informacijske sigurnosti u RH. Naveden je prijedlog konkretnih potreba za izmjenama i dopunama propisa koji su nedostatni s aspekta informacijske sigurnosti te nositelji i rokovi sukladni potrebama ovog Nacionalnog programa, a u svjetlu usklađivanja hrvatskih propisa (Zakon o zaštiti tajnosti podataka i Uredba o uredskom poslovanju) s propisima EU i NATO-a.

4.1.1 Zakon o zaštiti tajnosti podataka (ZZTP)

Zakon o zaštiti tajnosti podataka (NN 108/96) propisuje vrste i stupnjeve tajnosti te mjere i postupke za utvrđivanje, uporabu i zaštitu tajnosti podataka.

Prema tom zakonu, podaci prema vrsti tajne mogu biti državna, vojna, službena, poslovna i profesionalna tajna, a prema stupnju tajnosti podaci mogu biti državna tajna, vrlo tajni, tajni i povjerljivi.

Zakon ne definira sigurnosnu oznaku za neklasificirane podatke (neklasificirano) i jasnu oznaku za podatke koji se smiju objaviti (objavljivo). Zakon u slučaju državne, vojne i službene tajne ne utvrđuje nužnost provođenja postupka sigurnosne provjere i certificiranja osoblja.

U zakonu također nedostaje definicija sukladnosti vrsta i stupnja tajnosti u RH, u odnosu prema međunarodnim sigurnosnim oznakama (TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, UNCLASSIFIED), što bi konkretno trebalo preuzeti iz MAP programa.

Zakon o zaštiti tajnosti podataka propisuje obavezu prema kojoj su čelnici javnih tijela i ovlašteni dužnosnici RH dužni donijeti posebne propise o utvrđivanju stupnja i vrste tajnosti, načina i mjesta označavanja tajni, trajanja tajnosti te drugih mjera zaštite tajnih podataka, ovisno o djelokrugu rada odnosno mjestu nastanka, obrade ili čuvanja tajnih podataka.

Posljedica ovakvog pristupa zaštiti tajnih podataka, u kojem državna tijela samostalno propisuju mjere zaštite tajnih podataka kroz interne pravilnike o zaštiti tajnih podataka i kroz pravilnike o informacijskoj sigurnosti, je nepostojanje zajedničkih minimalnih sigurnosnih kriterija na nacionalnoj razini u RH. S tim u vezi, nemoguće je ispuniti zahtjeve NATO-a i EU za minimalnim sigurnosnim standardima jer pristup sigurnosti u državnim tijelima nije izbalansiran i nisu određeni minimalni sigurnosni kriteriji koje moraju zadovoljiti sva državna tijela i kompletna korištena infrastruktura u RH (koja nije više samo u državnom vlasništvu).

Treba imati na umu da je ovaj zakon donesen prije 8 godina i da tada nije bilo moguće tako jasno, kao što je to danas, sagledati činjenicu da se zaštita tajnih podataka, pogotovo onih u informacijsko komunikacijskim sustavima, ne može

razmatrati isključivo na razini pojedinog tijela, već da je treba sagledati u potpunosti, na nacionalnoj razini. Potrebno je stoga izvršiti korekciju ovog zakona kako bi se nadležnost za propisivanje zajedničkih zaštitnih mjera podigla na nacionalnu razinu koja bi bila obvezujuća za sva državna tijela. U Zakonu o sigurnosnim službama stoji da su tijela državne vlasti dužna primjenjivati norme zaštite tajnosti podataka koje usvoji Savjet za koordinaciju sigurnosnih službi te je stoga potrebno uskladiti postojeće odredbe ovih dvaju zakona.

Zakon o zaštiti tajnosti podataka propisuje da nadzor nad provedbom zaštite tajnih podataka obavlja čelnik tog tijela ili osoba koju on za to ovlasti. U Zakonu o sigurnosnim službama stoji da nadzor provođenja i organizaciju informacijske sigurnosti u tijelima državne vlasti provodi Protuobavještajna agencija pa bi i u tom smislu usklađivanjem odredaba ovih dvaju zakona trebalo razjasniti tko, pod kojim uvjetima i u kojoj mjeri provodi nadzor. U svakom slučaju, operativne i nadzorne nadležnosti moraju biti razdvojene.

Plan aktivnosti usklađivanja s Nacionalnim programom informacijske sigurnosti

1. Na prijedlog Savjeta za koordinaciju sigurnosnih službi, potrebno je izvršiti izmjene i dopune Zakona o zaštiti tajnosti podataka u smislu:
   - uvođenja sigurnosne oznake za neklasificirane podatke i procedura za podatke koji se smiju objaviti
   - definiranja sukladnosti vrste i stupnja tajnosti podataka u RH s međunarodnim sigurnosnim oznakama (TOP SECRET, SECRET, CONFIDENTIAL, RESTRICTED, UNCLASSIFIED) prema MAP programu
   - definiranja nadležnosti za propisivanje zajedničkih zaštitnih mjera (minimalnih sigurnosnih kriterija) u RH i obavezu usklađivanja i primjene tih mjera od strane državnih tijela
   - definiranje nadležnosti i opsega provođenja nadzora u provedbi zaštite tajnih podataka
   - propisivanje nužnosti certificiranja osoblja i provođenja postupka sigurnosne provjere

4.1.2 Zakon o zaštiti osobnih podataka (ZZOP)

Demokratsko društvo utemeljeno je na zaštiti pojedinca – građana. To je odgovornost države i standard bez kojeg se ne može ući u međunarodne integracije. Iako se u ovom slučaju radi o segmentu koji nije u okviru državne uprave u užem smislu, propisivanje jasnih mjera informacijske sigurnosti u zaštiti osobnih podataka građana, odgovornost je države.

Zakon o zaštiti osobnih podataka (NN 103/03) regulira način i uvjete obrade osobnih podataka, obrade posebnih kategorija osobnih podataka, obvezu informiranja ispitanika, povjeravanje poslova obrade osobnih podataka, iznošenje osobnih podataka iz RH, zaštitu rada ispitanika, obrade podataka u novinarske svrhe, te nadzor nad djelovanjem sustava obrade osobnih podataka.

Zakonom je izvršeno usklađivanje s Direktivom 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u pogledu obrade osobnih podataka i slobodnog kretanja tih podataka [11].

U svrhu provođenja Zakona o zaštiti osobnih podataka Vlada RH donijela je Uredbu o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka (NN 105/04) i Uredbu o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (NN 139/04).

Tijekom izgradnje sustava informacijske sigurnosti u RH, ovakvi namjenski propisi obuhvatit će se nacionalnim propisima informacijske sigurnosti u RH. Na taj način će se u budućnosti uvesti sustavni pristup informacijskoj sigurnosti, umjesto ovakvih posebnih propisa, čime će se ostvariti izbalansiranost sigurnosnih mjera i već spomenuti minimalni sigurnosni kriteriji na državnoj razini RH.

4.1.3 Zakon o pravu na pristup informacijama

Zakon o pravu na pristup informacijama (NN172/03) propisuje uvjete pod kojima je potrebno osigurati pravo na pristup informacijama. Pravo na pristup informacijama obuhvaća pravo ovlaštenika prava na informaciju (svaka domaća ili strana fizička ili pravna osoba koja zahtijeva pristup informaciji) na traženje i dobivanje informacija koje posjeduju, raspolažu ili nadziru tijela javne vlasti, kao i obvezu tijela javne vlasti da omogući pristup zatraženoj informaciji, odnosno da objavljuje informacije kada za to i ne postoji poseban zahtjev već takvo objavljivanje predstavlja njihovu obvezu određenu zakonom ili drugim općim propisom.

Pravo na pristup informacijama ne isključuje potrebu zaštite tih informacija i brigu o njihovoj sigurnosti i ne znači da svi imaju pravo pristupa svim informacijama, već podrazumijeva načelo poslovne potrebe ("need to know") od strane zainteresiranih ovlaštenika prava na informaciju. Tijela javne vlasti uskratiti će pravo na pristup informaciji ako je informacija zakonom ili na osnovi kriterija utvrđenih zakonom proglašena državnom, vojnom, službenom, profesionalnom ili poslovnom tajnom, te ako je zaštićena zakonom kojim se uređuje područje zaštite osobnih podataka. Pravo na pristup informacijama može se u određenim situacijama privremeno uskratiti (npr. sprječavanje i otkrivanje kaznenih dijela), ali ih je po prestanku važenja tih razloga potrebno učiniti dostupnim. Pravo na pristup informacijama ostvaruje se redovnim objavljivanjem (ako je propisana obveza objavljivanja), neposrednim pružanjem informacije ovlašteniku koji je podnio zahtjev, uvidom u dokumente koji sadrže traženu informaciju ili dostavom preslike tražene informacije. Zahtjev za ostvarivanje prava na pristup informaciji može se podnijeti u usmenoj i pismenoj formi, a tijela javne vlasti dužna su ga realizirati najkasnije u roku od 15 dana. Ovlaštenik koji raspolaže informacijom dobivenom od tijela javnih vlasti, ima pravo tu informaciju javno iznositi. Zakon o pravu na pristup informacijama osigurava pravo pristupa informacijama svim ovlaštenicima pod jednakim uvjetima, i svi su ravnopravni u njegovom ostvarivanju. Tijela javne vlasti stoga moraju osigurati ravnopravne tržišne uvjete svim pravnim osobama u pristupu državnim informacijama za koje postoji tržišni interes (npr. statistički podaci, izvodi iz državnih baza podataka i sl.), odnosno interes građana (analitička izvješća, npr. o broju i vrstama registriranih automobila).

Radi osiguranja provedbe ovog zakona, tijela javne vlasti obavezna su odrediti mjerodavnu službenu osobu za rješavanje ostvarivanja prava na pristup informacijama tzv. službenika za informiranje koji između ostalog ima i obvezu unapređivanja načina obrade, klasificiranja, čuvanja i objavljivanja informacija koje su sadržane u službenim dokumentima koji se odnose na rad tijela javne vlasti.

Tijela javne vlasti dužna su voditi poseban službeni upisnik o zahtjevima, postupcima i o ostvarivanju prava na pristup informacijama, a koji je razrađen Pravilnikom o ustroju, sadržaju i načinu vođenja službenog upisnika o ostvarivanju prava na pristup informacijama (NN 137/04).

4.1.4 Zakon o sigurnosnim službama RH (ZOSS)

Zakon o sigurnosnim službama (NN 32/02 i NN 38/02) uvodi pojam informacijske sigurnosti u zakonodavstvo RH i definira okvire organizacije informacijske sigurnosti unutar tijela državne vlasti. Okviri postavljeni zakonom sukladni su europskoj i svjetskog praksi prema kojoj je informacijska sigurnost tijela državne vlasti osigurana unutar okvira sigurnosnog sustava i kao dio tog sustava brine se o disperziji sigurnosne politike na nacionalnoj razini.

Model organizacije informacijske sigurnosti proizlazi iz čl. 87. zakona koji predviđa osnivanje Zavoda za informacijsku sigurnost i kripto-zaštitnu tehnologiju (ZISKZT) kao tijela odgovornog za predlaganje normi zaštite tajnosti podataka, a koje su tijela državne vlasti dužna primjenjivati. Sigurnosne službe sukladno čl. 29. nadziru njihovu organizaciju i provođenje.

Zakon o sigurnosnim službama u čl. 6. st. 2. definira i provedbu sigurnosnih mjera potrebnih za zaštitu povjerljivih informacija i dokumenata, u razmjeni između RH i stranih obrambenih organizacija (pogotovo se odnosi na NATO), te distribuciju tih informacija i dokumenata među tijelima državne vlasti. Provedba tih mjera u nadležnosti je Ureda Vijeća za nacionalnu sigurnost unutar kojeg se ustrojava i Središnji registar za pohranu takovih informacija.

Pojmovi 'ustanova' i 'norme' kako su definirani u čl. 87. ovog Zakona odstupaju od predviđenih funkcionalnosti Zavoda, te ih je stoga potrebno zamijeniti pojmovima 'tijelo državne vlasti' ili 'tijelo sigurnosnog sustava' i 'dokumenti sigurnosne politike informacijske sigurnosti u RH'. S tim u svezi potrebno je sadržajno uobličiti i članak 87. stavak 2. i 4. Zakona.

U čl. 6. st. 2. bilo bi prikladno uz pojam 'stranih obrambenih organizacija' dodati i 'drugih stranih organizacija', kako bi se pri Uredu Vijeća za nacionalnu sigurnost objedinila funkcionalnost NSA za NATO, EU, ali i dodati takav tekst kojim će se nedvosmisleno prepoznati uloga UVNS-a kao NSA za RH.

<u>Plan aktivnosti usklađivanja s Nacionalnim programom informacijske sigurnosti</u>

1.Po usvajanju ovog dokumenta od strane Vlade, Stručni tim za postupak osnivanja Zavoda i Ured Vijeća za nacionalnu sigurnost trebaju predložiti Savjetu za koordinaciju sigurnosnih službi potrebne izmjene i dopune Zakona o sigurnosnim službama

4.1.5 Kazneno zakonodavstvo

Kazneni zakon RH (NN 110/97, NN 27/98, NN 129/00, NN 51/01) usklađen je s odredbama Konvencije o kibernetičkom kriminalitetu i u isti su uključena nova kaznena djela i to: Kompjuterska prijevara, Kompjutersko krivotvorenje, Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa ili sustava i Dječja pornografija na računalnom sustavu ili mreži, a opisani članci Kaznenog zakona stupili su na snagu Zakonom o izmjenama i dopunama Kaznenog zakona (NN 105/04) od 1.10.2004. godine. U tijeku su pripreme odgovarajućih izmjena Zakona o kaznenom postupku (NN 62/03), i to u onome dijelu koji se odnosi na provođenje kriminalističkih obrada, prvenstveno presretanje i nadzor komunikacija na Internetu, prekogranični pristup podacima, kao i način obavljanja provjera korisnika Interneta u hitnim slučajevima.

Odredbama važećeg Zakona o kaznenom postupku u članku 180. donekle je riješen dio ove problematike (u stavku 1. predviđa se nadzor telefona kao i drugih uređaja za komunikaciju na daljinu), ali od stupanja na snagu ovog zakona u 1998. godini ništa nije napravljeno kako bi se mogla nadzirati i presretati komunikacija počinitelja kaznenih djela na Internetu, kako putem e-maila tako i putem svih drugih oblika komunikacije na Internetu. Dakle, osim stvaranja organizacijsko-tehničkog sustava koji će obavljati opisane zadaće bit će potrebno izmijeniti određene članke Zakona o kaznenom postupku, kako bi se sukladno odredbama Konvencije o kibernetičkom kriminalu, mogućnost korištenja ovakvih mjera, u slučajevima izdavanja Naloga od strane nadležnih sudova proširilo i na kaznena djela koja se navode u Konvenciji. U konkretnom slučaju ovo bi se odnosilo na naprijed opisana četiri nova kaznena djela, kao i na sva kaznena djela koja se odnose na povrede autorskih prava, koja su također eksplicitno navedena u ovoj Konvenciji.

Na taj način bit će usklađen veći dio formalnih zahtjeva koje RH treba uskladiti u sklopu borbe protiv računalnog kriminala. Potrebno je naglasiti da će u sklopu primjene spomenutih propisa biti potrebno obraditi kompleksno područje računalne forenzike. U tom dijelu je preostao veliki dio posla i nužno ga je riješiti u koordinaciji Ministarstva pravosuđa i Ministarstva unutarnjih poslova RH s nositeljima ključnih dijelova Nacionalnog programa informacijske sigurnosti u RH (NSA, NCSA, CERT).

Nadalje, bit će potrebno implementirati nova rješenja i izvršiti dodatne pravne pomake u zaštiti nacionalnog gospodarstva u okviru suvremenih trendova informacijskog društva. Ovdje ćemo navesti dva ključna područja povezana s programom informacijske sigurnosti. Prvo područje je sve više primjenjivano kriptiranje podataka od strane krajnjih korisnika – pravnih osoba (virtualne privatne mreže i sl.). Danas se u svijetu primjenjuje zakonsko propisivanje postupaka kao što je evidentiranje, certificiranje i akreditiranje kriptografske opreme za korištenje (u Republici Hrvatskoj dijelom predviđeno u ZISKZT). Ovdje je iznimno značajna uloga ZISKZT kao inicijatora pristupa ovom području na nacionalnoj razini, prvo kroz preventivne regulativne postupke te kasnije kao stručnog tijela za ispomoć Ministarstvu pravosuđa i Ministarstvu unutarnjih poslova u razvoju ovog područja. Drugo značajno područje pojavljuje se u okviru suvremenog pristupa reviziji poslovanja tvrtki. Ovaj proces se, obzirom na informatiziranost gotovo svih poslovnih subjekata, neumitno prebacuje u digitalno područje (propisi o čuvanju e-pošte, e-transakcijama, pohrani kripto ključeva i sl., npr. kao u Sarbanes-Oxley zakonu iz

SAD). Stoga će u idućem srednjoročnom razdoblju trebati planirati pravne pomake u zaštiti nacionalnog gospodarstva, povezane s područjem informacijske sigurnosti.

Plan aktivnosti usklađivanja s Nacionalnim programom informacijske sigurnosti:

1. Izmjene Zakona o kaznenom postupku u skladu s provedenim promjenama Kaznenog Zakona prema planu Ministarstva pravosuđa.
2. Razvoj i implementacija organizacijsko-tehničkog sustava za tajni nadzor usluga i prometa na Internetu, sukladno postojećem zakonodavstvu, od strane mjerodavnih državnih tijela i davatelja Internet usluga u RH (ISP), prema planu sigurnosnog sustava.
3. Planiranje pravnih pomaka u zaštiti nacionalnog gospodarstva u okviru suvremenih trendova informacijskog društva, analiza potreba i mogućnosti tijekom 2005. godine, u koordinaciji Ministarstva pravosuđa, Ministarstva gospodarstva i Ministarstva unutarnjih poslova, uz suradnju tijela nositelja Nacionalnog programa informacijske sigurnosti.

4.1.6 Arhive, registri i uredsko poslovanje

U slučaju informacija koje se nalaze na nekom fizičkom mediju, neovlašteni pristup uglavnom znači krađu medija. To znači da legitimni vlasnik ili korisnik ostaje bez medija što se lako uočava. Čak i kada je riječ o fotografiranju, fotokopiranju ili nekoj vrsti presnimavanja informacija s fizičkog medija, izvorniku čovjek mora fizički pristupiti, a što se sprečava metodama tehničke i fizičke zaštite. Međutim, kad se radi o informacijama u digitalnom obliku, spremljenim na računalima i prenošenim telekomunikacijskim putovima krađa je «nevidljiva» i mora se sprečavati novim, drugačijim sredstvima. Štoviše, dok je kod «klasičnih» medija vrlo teško izmijeniti dio informacije, kod digitalnih podataka je to onoliko lako ili teško koliko i kopirati podatke.

Danas praktički sve informacije nastaju u digitalnom obliku. Otisnute na papir već su u svom sekundarnom obliku koji je izgubio mnoge atribute koje izvornik ima. Takvo stanje pri kojem se dnevno uništavaju ogromne količine izvornih oblika informacija u digitalnom obliku, jer se većinom čuva sekundarna papirnata informacija, je neprihvatljivo. Stoga je temeljni zadatak sustava informacijske sigurnosti osigurati čuvanje informacija u njihovom izvornom digitalnom obliku. U tijeku je izrada Zakona o elektroničkom dokumentu koji će biti usklađen sa zahtjevima Europske unije.

Zakon o arhivskom gradivu i arhivima (NN 105/97) obvezuje na čuvanje informacija. Potrebno je izvršiti usklađivanje ovog i drugih propisa kako bi se sustavno počela prikupljati arhivska građa u elektroničkom obliku, pri čemu bi se obveza prikupljanja elektroničkog oblika trebala odnositi i na građu kojoj je originalni oblik tiskani ili analogni, a postoji elektronička kopija, kao i na građu kojoj je originalni oblik elektronički. Pri tom je tehničkim metodama (kriptiranjem, elektroničkim potpisom i sl.) potrebno osigurati zaštitu nepromjenjivosti izvorne informacije.

Javne publikacije čine velik dio nacionalnog informacijskog prostora. Zakonom o knjižnicama (NN 105/97) propisana je obveza dostavljanja tzv. «Obveznog primjerka» Nacionalnoj i sveučilišnoj knjižnici koja ga je obvezna čuvati. Nažalost,

iako i javne publikacije nastaju u digitalnom obliku pa se tek onda umnažaju u tiskanom obliku, ne postoji obveza niti čuvanja niti dostavljanja NSK-u digitalnog oblika publikacije. Stoga je nužno dopuniti Zakon o knjižnicama tako da, uz dostavu tiskanog primjerka, izdavača obvezuje i na dostavu propisanog digitalnog oblika publikacije. Strukovno udruženje Arhive-Knjižnice-Muzeji (AKM), vrlo je aktivno u uvođenju ovih važnih društvenih područja u suvremeno informacijsko društvo.

Za građane je od velikog značaja sigurnost njihovih osobnih, primjerice medicinskih podataka. I ti podaci danas u gotovo svim dijagnostičkim postupcima nastaju prvo u digitalnom obliku. No, kao što je građanima vitalno važna točnost tih podatka, a i poseban je interes za njihovom tajnošću, jednako je vitalan interes građana za trajnom dostupnošću tih podataka i to u digitalnom obliku. Stoga je nužno pokrenuti uspostavu nacionalnog medicinskog arhiva. I opet, ne radi se nužno o fizičkom objedinjavanju podataka, već o sustavu koji će omogućiti čuvanje, povezivanje i dohvat podataka. Ti su podaci ključni i za epidemiološka i druga znanstvena istraživanja.

Čak i kad informacije postoje u digitalnom obliku, prednosti takvog oblika informacija ne mogu se iskoristiti ukoliko iste nisu međusobno računalno povezane. Usprkos pionirskim poduhvatima još od prije više desetljeća (JMBG, matice) te sporadičnih nastojanja u objedinjavanju pojedinih registara i evidencija (DZS, DGU), RH nema tri temeljna središnja državna registra: prostornih jedinica, poslovnih subjekata i osoba. Podaci koji bi se u njima nalazili raštrkani su u nekoliko registara i evidencija, ili čak niti ne postoje (npr. registar tijela državne uprave). Stoga je nužno omogućiti jednoznačnu i računalnu identifikaciju i povezivanje podataka o pravnim osobama, fizičkim osobama i prostornim jedinicama. Objedinjavanje podataka u temeljne središnje registre ne pretpostavlja njihovo fizičko smještanje u jednu bazu podataka ili na isti fizički medij. Čak ne podrazumijeva niti nadležnost jednog tijela nad njihovim prikupljanjem, obradom i čuvanjem. Objedinjavanje prije svega znači središnju brigu za organizaciju i strukturiranje podataka, definiranje pristupa te nadzor nad provedbom. Primjerice, registri trgovačkih društava, obrta, udruga građana, političkih stranaka, vjerskih zajednica, poljoprivrednika, slobodnih zanimanja i drugi, pojedinačno mogu biti pod nadležnošću različitih tijela, uskladišteni na različitim računalima ili sustavu distribuiranih računala, ali sustav identifikacije i pristupa tim podacima mora biti planiran i objedinjen.

Županije, općine, naselja, ulice, katastarske čestice i objekti nužno moraju imati jedinstvene identifikacije i biti dohvatljivi u digitalnom obliku, na jednom mjestu. Osim tehničkih mjera, potrebno je uskladiti zakone i druge propise na taj način da oni koji imaju pravo i obvezu stvarati i ukidati prostorne jedinice te donositi i mijenjati njihove nazive i oznake imaju obvezu o tome obavijestiti upravitelja registra prostornih jedinica. Treba propisati da njihova odluka stupa na snagu danom objave u središnjem državnom registru prostornih jedinica.

Registar poslovnih subjekata ili registar pravnih osoba mora biti integralan te, iako različiti dijelovi državne uprave i lokalne uprave imaju nadležnost nad različitim pravnim osobama, njihova identifikacija mora biti jedinstvena, a dohvat podataka osiguran kroz jedinstveno sučelje.

Registar osoba ili registar fizičkih osoba treba obuhvatiti sve osobe koje dolaze u kontakt i razmjenjuju osobne informacije s Republikom Hrvatskom. Danas su ti

podaci u maticama rođenih, umrlih, vjenčanih te državljana nad kojima ima nadležnost Središnji državni ured za upravu, evidencijama boravišta i prebivališta koje vodi Ministarstvo unutarnjih poslova, poreznih obveznika koje vodi Ministarstvo financija, zaposlenika koje vodi Ministarstvo gospodarstva, rada i poduzetništva. Pojedine osobe nalaze se u jednom, nekoliko ili svim navedenim registrima i evidencijama. Ove podatke treba objediniti na način kao kod poslovnih subjekata.

Relativno dobra povezanost podataka na nacionalnoj razini na osnovi JMBG razbijena je i onemogućena Zakonom o izmjenama i dopunama Zakona o matičnom broju (NN 66/02). Taj je Zakon potrebno žurno revidirati uvođenjem zamjenskog mehanizma povezanosti podataka, koji će istovremeno u potpunosti štititi privatnost i osobne podatke građana.

Uredba o uredskom poslovanju je stara više od desetljeća i ne prepoznaje činjenicu da svi dokumenti u državnoj upravi nastaju u digitalnom obliku. Taj zastarjeli model ne poznaje niti pojam informacijske sigurnosti niti minimalne sigurnosne standarde na nacionalnoj razini. Sve to predstavlja lošu podlogu za aktualnu informatizaciju državne uprave. Tako primjerice ne postoje tehnički zahtjevi koje bi programska aplikacija urudžbenog zapisnika trebala zadovoljiti niti propisani format podataka u urudžbenom zapisniku. Uredsko poslovanje predstavlja segment informacijske sigurnosti na nacionalnoj razini i mora se koordinirati s nacionalnim programom informacijske sigurnosti. Obzirom da je u Središnjem državnom uredu za upravu u tijeku izrada novih propisa o uredskom poslovanju, potrebno ih je koordinirati s područjem informacijske sigurnosti, tako da ovi novi propisi o uredskom poslovanju budu usklađeni s konceptom informacijske sigurnosti i sadržavaju potrebne teme iz ovog područja u dijelu propisa, ali i u okviru organizirane edukacije i ispitnih tema za državne službenike i namještenike. Stoga je nužno izmijeniti Uredbu o uredskom poslovanju na način da obvezuje čuvanje svih dokumenata i informacija u digitalnom obliku te njihovo povezivanje sa svim ostalim podacima u tijelima državne uprave elektroničkim putem u skladu s otvorenim standardima zapisa (npr. «Open Archive Initiative»).

Plan aktivnosti usklađivanja s Nacionalnim programom informacijske sigurnosti:

1. Donošenje novih propisa o uredskom poslovanju potrebno je uskladiti s ovim programom tijekom 2005. godine (SDUU)
2. Reviziju Zakona o izmjenama i dopunama Zakona o matičnom broju (NN 66/02) potrebno je uskladiti s ovim Programom u drugom kvartalu 2005. godine (MUP, SDUeH)
3. Planiranje koncepta državnih registara potrebno je provesti tijekom 2005. godine (SDUU, SDUeH)
4. Kroz harmonizaciju propisa s EU potrebno je u smislu ovog prijedloga uskladiti Zakon o arhivskom gradivu i arhivima i Zakon o knjižnicama tijekom 2005. i 2006. godine (SDUU, Državni arhiv, MK)

4.1.7 Normizacija u području računalne i komunikacijske tehnologije i informacijske sigurnosti u RH

Razvoj informacijskog društva oslanja se na tehnološku podršku, u okviru koje razlikujemo aplikacijsku i infrastrukturnu podršku. Tehnološka razina potrebna za iskorištenje potencijala informacijskog društva ne može se postići ukoliko se ne osigura odgovarajuća interoperabilnost aplikacijske i infrastrukturne podrške. Upravo to je uloga procesa normizacije koji predstavlja temelj razvoja otvorenog tržišta i ravnopravnog natjecanja svih sudionika informacijskog društva. Učinkovita normizacija služi na dobrobit i korisnicima i industriji, a time i državi u cjelini.

Tradicionalni pristup normizaciji kroz proces usklađivanja u tehničkim odborima i preuzimanja međunarodnih normi (ISO, ITU, IEEE i druge) u području računalne i komunikacijske tehnologije (ICT-a), pokazao se nedostatnim. Razlog je prvenstveno u iznimnoj dinamici, ali i kompleksnosti ICT područja. Stoga se u području ICT-a često javljaju određene nekonzistentnosti na nacionalnoj razini, u smislu nepokrivenosti pojedinih područja ili pak ograničenja i kolizije pojedinih normi uslijed brzog razvoja tehnologije. Alternativni pristupi normizaciji ICT-a u svijetu temelje se na vlasničkim i otvorenim standardima. U modelu vlasničkih standarda određena interesna grupacija tvrtki usuglašava nove ili preuzima privatne norme pojedine tvrtke. Takav pristup može dovesti do tržišne polarizacije, selektivnosti i netransparentnosti, ali i ograničenja tržišnog natjecanja. Upravo zbog opisanih razloga danas se u razvijenim zemljama, koje su u procesu stvaranja informacijskog društva, naglašava važnost otvorenih standarda koji se razvijaju u okviru nekomercijalnih strukovnih organizacija i omogućavaju ravnopravan pristup do tehničke dokumentacije svim zainteresiranim stranama. Zadatak države u ovakvim normizacijskom procesima je stvaranje okvira i pretpostavki za učinkovit proces nacionalne normizacije, kao i poticanje usvajanja otvorenih standarda i međunarodnih normi. Glavni čimbenici u procesu normizacije moraju biti gospodarski subjekti i državna stručna tijela.

Stoga i EU u okviru stvaranja informacijskog društva kroz program eEurope 2005, ima poseban prateći normizacijski program. Cilj takvog programa je koordinacija europskih normizacijskih tijela (CEN, CENELEC, ETSI), poticanje primjene otvorenih standarda te sustavna analiza postojećih normi na području EU, s ciljem revizije i dopune normi s aspekta potreba područja ICT-a i informacijske sigurnosti, odnosno programa eEurope 2005.

Krajem 2003. godine u SAD-u je pokrenuta posebna inicijativa od strane Ministarstva domovinske sigurnosti (DHS) te je formiran široki program nacionalne normizacije sa sigurnosnog aspekta u cjelini (ne samo ICT područje), tzv. ANSI-HSSP (American National Standards Institute – Homeland Security Standards Panel). Ovu inicijativu SAD-a prati i EU proširenim normizacijskim programom Zaštite i sigurnosti građana. Potrebno je napomenuti da se oba spomenuta normizacijska programa SAD-a i EU, trenutno najveći procesi normizacije u svijetu, sastoje u stvari od područja informacijske sigurnosti i tradicionalnog sigurnosnog područja civilne zaštite u približno podjednakom omjeru. Osim na ovom primjeru, značaj normizacije informacijske sigurnosti vidi se i kroz javna područja kakvo je zdravstvo, odnosno kroz informatizacijske procese zdravstva u razvijenim zemljama, koji se temelje upravo na normama ICT-a i informacijske sigurnosti (programi SAD-a u okviru HIPAA temelje se na normizaciji ICT-a, podataka i informacijskoj sigurnost). Sve navedeno

utječe i na tradicionalni proces međunarodne normizacije tako da je ISO, međunarodna organizacija za normizaciju, pokrenula dugoročni program Sigurnosne tehnike u informacijskoj tehnologiji (ISO/IEC JTC 1/SC27), koji ima za cilj uspješnu normizacijsku strategiju razvijenih zemalja usmjeriti prema međunarodnoj normizaciji.

Proces informacijske sigurnosti zahtijeva dva povezana segmenta normizacije. Prvi segment čini normizacija samih informacijsko-komunikacijskih tehnologija (ICT), a drugi segment čini normizacija sigurnosnih tehnika ICT-a. Dosadašnja formalna aktivnost u ovim područjima normizacije u RH slaba je, odnosno gotovo i ne postoji. Proces normizacije u RH provodi normizacijsko tijelo RH. Do kraja 2004. godine posao normizacijskog tijela u RH obavlja Državni zavod za normizaciju i mjeriteljstvo (DZNM). Počevši od 1. siječnja 2005. godine s radom treba započeti Hrvatsko nacionalno normirno tijelo (NN 163/03), kao pravni sljednik DZNM-a. Uredbom o osnivanju Hrvatskog zavoda za norme (NN 154/04) osnovana je javna ustanova za ostvarivanje ciljeva normizacije i obavljanje poslova i zadataka nacionalne normizacije pod nazivom Hrvatski zavod za norme (HZN).

Potrebu za normizacijom pojedinih područja iskazuju mjerodavna tijela državne vlasti i druge stručne ustanove u RH. U okviru Zajedničkog tehničkog odbora za informacijsku tehnologiju pri Hrvatskom zavodu za norme predloženo je formiranje Pododbora za sigurnost podataka (DZNM/TO Z1/PO 4 – koji pokriva područja pododbora ISO/IEC JTC 1/SC 27 IT Security techniques i ISO/IEC JTC 1/SC 37 Biometrics).

Središnji državni ured za *e*-Hrvatsku uključen je u međunarodni projekt PETTEP (Privacy enhanced technologies testing and evaluation project) čiji je cilj priprema prijedloga ISO norme za provjeru i certifikaciju informacijskih sustava i tehnologija koji podržavaju zaštitu osobnih podataka.

Plan aktivnosti usklađivanja s Nacionalnim programom informacijske sigurnosti u RH:

Nakon osnivanja tijekom prve polovine 2005. godine ZISKZT se treba uključiti u rad Pododbora za sigurnost podataka (DZNM/TO Z1/PO 4) i putem Hrvatskog zavoda za norme u rad ISO/IEC pododbora za sigurnosne tehnike u IT-u ISO/IEC JTC 1/SC27 u kojem djeluje niz susjednih zemalja i zemalja pristupnica u EU.

4.1.8 Interoperabilnost

Bitan preduvjet učinkovite primjene informacijske i komunikacijske tehnologije u složenim sustavima kakva je državna uprava je uspostavljanje interoperabilnosti na tehničkoj, semantičkoj i organizacijskoj razini. Nezavisan i nekoordiniran razvoj, bez usvajanja tehničkih normi koje bi informacijski sustavi morali zadovoljavati, doveo je do toga da je tehnička interoperabilnost informacijskih sustava različitih ustanova, a katkad i unutar jedne iste ustanove, u državnoj upravi problematična. Semantička interoperabilnost praktično ne postoji, jer nikad nisu uvedeni standardi zapisa i značenja pojedinih podataka u informacijskim strukturama. U području informacijske sigurnosti postavljaju se zahtjevi i na najvišu razinu interoperabilnosti –

organizacijsku interoperabilnost (koncepcija sigurnosne politike i minimalnih sigurnosnih kriterija), naravno uz pretpostavku zadovoljenja prvih dviju razina.

Vlada Republike Hrvatske usvojila je Strategiju Programa One Stop Shop [37] koja postavlja temeljna načela interoperabilnosti informacijskih sustava s ciljem uspostavljanja zajedničke arhitekture informacijskih sustava u državnoj upravi. Strategijom se predviđa uspostavljanje Centra znanja i izvrsnosti za upravljanje Referentnim popisom normi i standarda, Repozitorijem otvorenih standarda i Repozitorijem modela dokumenata, organizacijskih shema i postupaka te za razmjenu iskustava i podršku radu informatičara u državnoj upravi. S aspekta informacijske sigurnosti potrebno je naglasiti značaj organizacijske interoperabilnosti koja se obično zanemaruje (npr. to je usklađivanje funkcionalnosti pojedinih tijela u procesu informacijske sigurnosti u ovom dokumentu).

Za potrebe uspostavljanja interoperabilnosti nužne za razmjenu podataka unutar EU Europska komisija je pokrenula program IDAbc [6] u okviru kojeg se postavlja Europski okvir za interoperabilnost i pokreću pilot projekti aplikacija za razmjenu podataka između državnih uprava zemalja članica EU. Posebna se važnost daje uspostavljanju elektroničkog identiteta i interoperabilnih sustava za identifikaciju i autorizaciju pristupa zajedničkim resursima.

4.1.9 Pregled ostalog zakonodavstva povezanog s područjem informacijske sigurnosti

Obzirom na karakteristike informacijske sigurnosti, koja kao i suvremena informacijska i komunikacijska tehnologija zadire u sve pore društvenog života, jasno je da ogroman broj područja na određeni način dolazi u doticaj s područjem informacijske sigurnosti. U Nacionalnom programu cilj je odrediti ključne dijelove postojećeg zakonodavstva u Republici Hrvatskoj koji su značajni za uspostavu nacionalnog sustava informacijske sigurnosti. To uključuje s jedne strane postojeće propise koji su koncepcijski neusklađeni sa suvremenim društvenim procesima, a s druge strane neke suvremene elemente zakonodavstva RH koji nisu do sada u praksi u potpunosti provedeni.

Prioritet Nacionalnog programa je u brzoj proceduri izmijeniti samo onaj dio propisa koji priječi uvođenje suvremenog organizacijskog modela informacijske sigurnosti u RH, sukladno međunarodnim, prvenstveno EU i NATO, standardima. Ostali dio propisa i prakse postupanja u nekim područjima koja su s aspekta uvođenja informacijske sigurnosti manje važna, mijenjat će se i prilagođavati u okviru sveobuhvatnog procesa usklađivanja hrvatskog zakonodavstva s EU zakonodavstvom, kroz Nacionalni program RH za pridruživanje EU Vlade Republike Hrvatske, a čiju izradu i provedbu koordinira MVPEI. Jedan od takvih primjera je Zakon o elektroničkom potpisu (NN 10/02) [47], čija potpuna primjena će biti omogućena tek osiguranjem okruženja kojim se bavi ovaj Nacionalni program informacijske sigurnosti. Nadalje, tu je i Zakon o telekomunikacijama (NN 172/03, 60/04) [57] koji je djelomično usklađen sa pravnom stečevinom EU u području liberalizacije telekomunikacijskog tržišta, te će se taj postupak i nadalje nastaviti.

4.2 Institucionalni okvir

4.2.1 Ured Vijeća za nacionalnu sigurnost u ulozi Središnjeg sigurnosnog tijela (NSA) u RH

4.2.1.1 Ured Vijeća za nacionalnu sigurnost kao NSA za NATO i druge strane obrambene organizacije

Ured Vijeća za nacionalnu sigurnost (UVNS) je Zakonom o sigurnosnim službama dobio dvojnu ulogu. Pored stručnih i administrativnih poslova za Vijeće za nacionalnu sigurnost i Savjet za koordinaciju sigurnosnih službi, te poslova za Vijeće oko usmjeravanja i nadzora rada sigurnosnih službi , UVNS prema čl. 6. točka 2. obavlja i poslove nužne za provedbu sigurnosnih mjera za zaštitu povjerljivih informacija i dokumenata u razmjeni između RH i stranih obrambenih organizacija, te distribuciju tih informacija i dokumenata među tijelima državne vlasti.

Potpisivanjem Sigurnosnog sporazuma RH i NATO-a, a sukladno propisanim obvezama iz čl. 6. ZOSS-a, UVNS preuzima u svibnju 2003. ulogu koordinatora za usklađivanje sigurnosnih standarda između RH i NATO-a, a predstojnik UVNS-a posebnom je Odlukom (predsjednika Vlade i predsjednika RH) imenovan Nacionalnim koordinatorom za sigurnosne standarde u kontekstu NATO-a.

Ova dužnost nije u Odluci izravno vezana na naziv NSA (National Security Authority) i nije kao takva definirana u Zakonu o sigurnosnim službama, no potpisivanjem Sigurnosnog sporazuma RH i NATO-a ova je uloga utemeljena na međunarodnom sporazumu. Osnovna uloga UVNS-a kao NSA za NATO kompatibilna je s odgovarajućim istovrsnim tijelima zemalja članica NATO-a. Prema postojećoj nacionalnoj i sigurnosnoj politici NATO-a, UVNS kao hrvatski NSA za NATO dobio je ovlasti i dužnosti u slijedećim područjima:

- prilagodba nacionalne i sigurnosne politike NATO-a,
- koordinacija na nacionalnoj razini u pitanjima NATO sigurnosnih standarda,
- donošenje i provedba zakonske podloge potrebne za provedbu prihvaćene NATO sigurnosne politike,
- nacionalna točka kontakta za Ured za sigurnost NATO-a, te budućeg istovrsnog tijela EU po sigurnosnim i drugim pitanjima proisteklih iz sigurnosne politike,
- odgovornost za punu provedbu prihvaćenih sigurnosnih standarda i NATO sigurnosne politike u Republici Hrvatskoj, te provedba svih odredbi Sigurnosnog sporazuma RH i NATO-a u područjima sigurnosne zakonske podloge, sigurnosti informacija i dokumenata, sigurnosnih provjera osoblja, sigurnosti informacijskih sustava (INFOSEC), fizičke sigurnosti, industrijske sigurnosti,
- nadzor provedbe NATO sigurnosnih standarda na nacionalnoj razini za državni sustav,
- izdavanje sigurnosnih certifikata za osobe, te ostale subjekte i sustave čije se certificiranje zahtijeva od NATO-a,
- odgovornost za ustrojavanje i funkcioniranje sustava prijema, evidencije, distribucije i pohrane klasificiranih dokumenata i informacija u razmjeni između NATO-a i Republike Hrvatske.

UVNS u svojstvu hrvatskog NSA za NATO u skladu s gornjim ovlastima i u ispunjenju dužnosti koordinira sa Uredom za sigurnost NATO-a, a na nacionalnoj razini sa

Savjetom za koordinaciju sigurnosnih službi, ravnateljima hrvatskih sigurnosnih agencija, te sa svim ministarstvima i TDU u kojima se provode sigurnosne mjere i standardi nužni za komunikaciju s NATO-om. To se prvenstveno odnosi na provedbu standarda u Ministarstvu vanjskih poslova, Ministarstvu obrane, Glavnom stožeru OSRH, Ministarstvu unutarnjih poslova, te Uredu predsjednika RH. Prema prvim dostupnim naznakama sigurnosne i vanjske politike EU-a, slični zahtjevi će biti postavljeni i prema članicama EU, te kandidatima za prijem u EU.

Radi sustavne provedbe NATO sigurnosnih standarda i na nižim razinama, ustrojen je sustav NATO registara za prijem, evidenciju, distribuciju i pohranu informacija i dokumenata NATO-a u gore navedenim tijelima državne vlasti, koji je koordiniran od strane Središnjeg registra ustrojenog u Uredu Vijeća za nacionalnu sigurnost. Neposredan nadzor rada sustava NATO registara obavlja Središnji NATO registar koji je dio Ureda Vijeća za nacionalnu sigurnost.

4.2.1.2 Ured Vijeća za nacionalnu sigurnost kao NSA za RH

Postojeći zakonski okvir informacijske sigurnosti definiran Zakonom o sigurnosnim službama ne prepoznaje funkcionalnost središnjeg državnog sigurnosnog tijela (NSA - National Security Authority) odgovornog za usklađenost općih sigurnosnih mjera informacijske sigurnosti u RH (NSA za RH). Prema ZOSS-u, UVNS ovu funkcionalnost ima isključivo prema stranim obrambenim organizacijama (npr. NATO), pa tako ostaje otvoreno pitanje ove nadležnosti unutar RH, ali i prema drugim stranim neobrambenim organizacijama (npr. EU).

Sukladno praksi u svijetu koja je zapravo ekvivalenta zahtjevima sigurnosne politike NATO i EU, funkcionalnost središnjeg državnog sigurnosnog tijela (NSA) neke zemlje je uobičajeno obuhvaćena unutar krovnog ili koordinacijskog tijela sigurnosnog sustava. Definiranje UVNS-a kao NSA za RH bilo bi na tragu uspostavljenih nadležnosti unutar sigurnosnog sustava u RH i opće prihvaćenog modela sustava informacijske sigurnosti. Objedinjavanjem NSA za NATO, NSA za EU i NSA za RH unutar jednog tijela (UVNS-a), stvorili bi se temelji za učinkovito, koordinirano i sveobuhvatno djelovanje na polju informacijske sigurnosti u RH, ali i u okvirima međunarodnih integracijskih procesa i u međunarodnoj suradnji.

Definiranje UVNS-a kao zajedničkog NSA unutar RH (NATO, EU, RH) potrebno je uobličiti izmjenama ZOSS-a. Takvu inicijativu, a na tragu Nacionalnog programa, trebao bi Vladi predložiti sam UVNS, koji bi se, angažiranjem dodatnog stručnog kadra kroz izmjenu Uredbe o unutarnjem ustrojstvu, trebao osposobiti za takvo djelovanje.

Konačno definiranje tijela koje će preuzeti funkcionalnost zajedničkog NSA unutar RH i stavljanje tog tijela u funkciju od presudne je važnosti za RH. NSA je pokretač aktivnosti u cjelokupnom sustavu informacijske sigurnosti, i nositelj je izrade nacionalne politike informacijske sigurnosti, strateškog dokumenta koji inicira sve daljnje regulacijske procese iz područja informacijske sigurnosti jedne zemlje.

4.2.2 Zavod za informacijsku sigurnost i kripto-zaštitnu tehnologiju u ulozi Središnjeg tijela za sigurnost komunikacija (NCSA / IA) i Središnjeg tijela za sigurnosne akreditacije (SAA) u RH

Zavod za informacijsku sigurnost i kripto-zaštitnu tehnologiju tijelo je koje se osniva temeljem čl. 87. Zakona o sigurnosnim službama. Tim je člankom Zavod definiran kao ustanova za obavljanje djelatnosti istraživanja i razvoja protokola, opreme, sredstava i tehnologije namijenjene za zaštitu tajnih podataka u informacijskim i telekomunikacijskim sustavima, kao i informacijskih i telekomunikacijskih mreža i kanala kojima se ti podaci razmjenjuju u sustavu nacionalne sigurnosti RH. Prema istom članku proizlazi da je Zavod nadležan i za predlaganje normi zaštite tajnosti podataka koja su tijela državne vlasti dužna primjenjivati.

Zavod je još uvijek samo tijelo na papiru jer se model informacijske sigurnosti prema čl. 87. ZOSS-a pokazao kao nejasan i nedorečen, i kao takav je naposljetku onemogućio i daljnji postupak osnivanja Zavoda. Stoga će u nastavku ovog poglavlja biti naglasak na tome što je unutar postojećeg zakonodavstva potrebno korigirati kako bi Zavod uspio saživjeti u prijeko potrebnim okvirima informacijske sigurnosti, te ispunio očekivanja Nacionalnog programa.

- Umjesto da Zavod predlaže norme, a čija je izrada i predlaganje u nadležnosti tijela za normizaciju (Hrvatski zavod za norme – HZN), i koje se prvenstveno odnose na javni i privatni sektor, Zavod treba predlagati i donositi "dokumente sigurnosne politike u području informacijske sigurnosti u RH", a koji se odnose na tijela državne vlasti. Takvi dokumenti su uredbe i organizacijsko tehničke smjernice (pravilnici, preporuke, referentne liste međunarodnih i nacionalnih tehničkih normi) iz područja informacijske sigurnosti.
- Predlaganje uredbi i donošenje organizacijsko tehničkih smjernica koje obvezuju tijela državne vlasti izvan je nadležnosti ustanova te proizlazi da Zavod ne može biti ustanova, već državno tijelo u okviru sigurnosnog sustava RH.
- Djelokrugom rada Zavoda trebaju biti obuhvaćene funkcionalnosti informacijske sigurnosti sukladno zahtjevima integracijskih procesa EU i NATO:
    - funkcionalnost Zavoda kao središnjeg državnog tijela za sigurnost komunikacija (NCSA),
    - funkcionalnost Zavoda kao središnjeg državnog tijela odgovornog za rukovođenje kriptomaterijalima (NDA)
    - funkcionalnost Zavoda kao središnjeg državnog tijela za sigurnosne akreditacije informacijsko komunikacijskih sustava (SAA).
- Funkcionalnosti vezane uz informacijsku sigurnost, a koje se odnose na tijela državne vlasti uglavnom se ostvaruju unutar sigurnosnog sustava i takva je praksa opće prihvaćena u svijetu (NATO, EU, SAD i sve razvijene zapadne zemlje). Sigurnosne službe u RH sukladno Zakonu o sigurnosnim službama ne mogu preuzeti te funkcionalnosti te se one ostvaruju u Zavodu, kao zasebnom tijelu. U slučaju reorganizacije sigurnosnog sustava Zavod treba ostati tijelo sigurnosnog sustava odvojeno od operativnih službi. Time se u potpunosti postiže organizacijsko načelo razdvajanja razvojnih, operativnih i nadzornih funkcija u okviru informacijske sigurnosti na Zavod, tijela državne vlasti i sigurnosne službe.

Daljnje aktivnosti oko formiranja Zavoda vezane su prvenstveno uz konačni sadržaj ovog dokumenta jer je predviđeno da se po njegovom usvajanju relevantni zaključci

ugrade u osnivačke akte Zavoda. To se odnosi na prijedlog izmjena i dopuna Zakona o sigurnosnim službama te Uredbu o osnivanju i Uredbu o unutarnjem ustrojstvu, sukladno kojoj je potrebno izraditi i Pravilnik o unutarnjem redu. Usuglašavanje navedenih akata potrebno je realizirati unutar okvira zadanih rokova osnivanja Zavoda (drugi kvartal 2005. g.).

Uspješna implementacija procesa osnivanja Zavoda podrazumijeva u konačnici i osiguranje adekvatnog prostora i uvjeta za rad, te zapošljavanje prvenstveno visoko kvalificiranog stručnog kadra iz domene informacijske sigurnosti.

Plan aktivnosti usklađivanja s Nacionalnim programom informacijske sigurnosti

1. Izrada Prijedloga izmjena i dopuna Zakona o sigurnosnim službama u dijelu koji se odnosi na informacijsku sigurnost i Prijedloga Uredbe o osnivanju Zavoda (Stručni tim za postupak osnivanja Zavoda, UVNS)
2. Izrada Prijedloga Uredbe o unutarnjem ustrojstvu Zavoda, usklađene sa zakonskim promjenama (Stručni tim za postupak osnivanja Zavoda).
3. Imenovanje čelnika Zavoda (Vlada RH)
4. Izrada i usvajanje Pravilnika o unutarnjem redu Zavoda (čelnik Zavoda).
5. Početak rada Zavoda (osiguranje prostora, uvjeta za rad i financijskih sredstava i zapošljavanje službenika i namještenika)

4.2.3 Središnji državni CERT u RH

4.2.3.1 CARNet CERT

U okviru Hrvatske akademske i istraživačke mreže - CARNet osnovan je 1996. godine Centar za prevenciju i otklanjanje problema vezanih uz sigurnost računalnih mreža - CARNet CERT (CARNet Computer Emergency Response Team). Hrvatska akademska i istraživačka mreža CARNet bavi se razvojem, izgradnjom i održavanjem računalne komunikacijske infrastrukture koja povezuje akademske i znanstveno-istraživačke ustanove u Hrvatskoj u jedinstveni informatički sustav. CARNet CERT financira se iz sredstava Državnog proračuna koja su u razdjelu Ministarstva znanosti, obrazovanja i športa planirana za redovnu djelatnost Hrvatske akademske i istraživačke mreže CARNet čiji je CERT dio.

Svrha djelovanja CARNet CERT-a jest pomaganje korisnicima Interneta u Hrvatskoj u primjeni proaktivnih mjera za smanjivanje rizika od nastanka računalnih sigurnosnih incidenata te pružanje pomoći u suzbijanju posljedica nastalih računalnih sigurnosnih incidenata. Iako djelatnost CARNet CERT-a prvenstveno pokriva akademsku mrežu, obrađuju se svi prijavljeni incidenti u kojima je barem jedna uključena strana iz Hrvatske.

U djelokrug rada CARNet CERT-a nije uključeno operativno rješavanje problema i briga o sigurnosti pojedinih sustava.

Informiranje najšire i stručne javnosti o značaju računalne sigurnosti ostvaruje se distribucijom vijesti, sigurnosnih preporuka i upozorenja, te preporuke za poboljšanje sigurnosti putem weba i mailing listi. U suradnji sa SANS institutom (SysAdmin, Audit, Network, Security Institute, Bethesda, SAD) redovito se prevodi brošura "Dvadeset najkritičnijih sigurnosnih ranjivosti", a povremeno i objavljuje u tiskanom obliku i, u suradnji s ostalim hrvatskim davateljima Internetskih usluga (ISP-ovima) distribuira administratorima mreža priključenih na Internet preko svih hrvatskih ISP-ova. U slučaju pojave značajnijih incidenata (npr. masovno širenje virusa, značajno uskraćivanje usluga i sl.) CARNet CERT izdaje objave za medije u kojima se upozorava na ove pojave i savjetuje kako se obraniti od mogućih problema.

Mrežnim i sistem administratorima unutar Hrvatske nudi se usluga registracije i posredovanja pri rješavanju računalno-sigurnosnih incidenata. Bilo da je druga strana uključena u incident iz ili izvan Hrvatske CARNet CERT kontaktira administratora nadležnog za izvor incidenta, ili nadležni CERT, te inicira rješavanje problema. Također, sistem administratori se mogu obratiti CERT-u s pitanjima vezanim za sigurnost i zatražiti savjet. Povremeno se organiziraju prezentacije, stručni seminari ili radionice (npr. za djelatnike MUP-a organizirana je radionica o osnovama mrežne forenzike na kojoj je sudjelovalo oko 50 djelatnika iz svih PU).

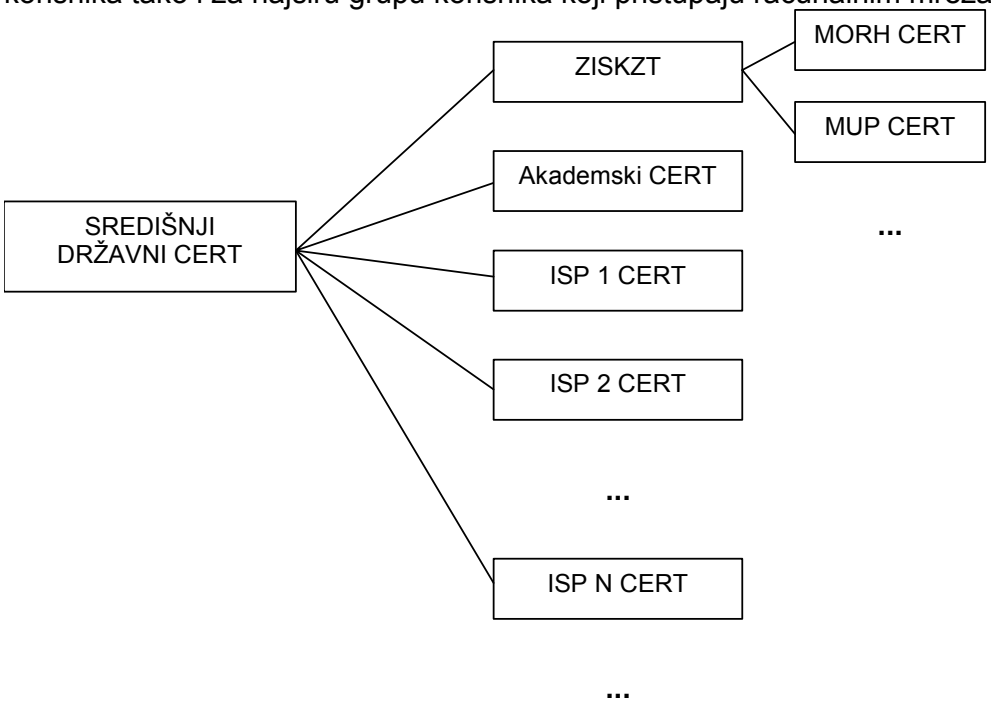
Kako je mrežna računalna sigurnost globalni problem i proces, CARNet CERT redovito surađuje s relevantnim svjetskim i europskim organizacijama i drugim CERT-ovima. CARNet CERT je član međunarodne organizacije FIRST (Forum of Incident Response Teams) od 1996. g. te redovito sudjeluje u radu TERENA CSIRT (Trans-European Research and Education Networking Association Computer Security Incident Response Teams) Task Force organizacije, a od 2002. godine ima status "akreditiranog tima" – najviši status u sustavu klasifikacije europskih CSIRT (CERT) timova u TERENA projektu Trusted Introducer.

U Hrvatskoj CARNet CERT održava i koordinira komunikaciju s "abuse timovima" davatelja usluga pristupa na Internet u Hrvatskoj kao i s predstavnicima Ministarstva unutarnjih poslova koji se bave problematikom računalnog kriminaliteta i zlouporabe Interneta. Također redovito surađuje s akademskom zajednicom (npr. Fakultet elektrotehnike i računarstva Sveučilišta u Zagrebu), a povremeno i s privatnim tvrtkama.

4.2.3.2 Uspostava Središnjeg državnog CERT-a

Za preventivno djelovanje te učinkovitu koordinaciju pri rješavanju računalnih sigurnosnih incidenata na Internetu, potrebno je uspostaviti hijerarhijski organiziranu infrastrukturu CERT timova sa Središnjim državnim CERT-om kao vršnim koordinirajućim tijelom. Tijela državne vlasti uobičajeno imaju zasebni koordinacijski CERT TDV, funkciju kojeg će u RH obavljati ZISKZT. Pored toga mogu se radi učinkovitosti organizirati CERT-ovi u skopu specifičnih ministarstava kao što su MORH i MUP. Ostali članovi ove hijerarhijske infrastrukture su CERT-ovi ili slična organizacijska tijela koja ustrojavaju davatelji Internetskih usluga (ISP), TK operatori, financijske institucije te druge tvrtke koje imaju interes ili značajni utjecaj na funkcioniranje nacionalne informacijske infrastrukture. Ovako uspostavljena hijerarhija treba omogućiti razmjenu informacija o računalnim sigurnosnim problemima, rana upozorenja o računalno-sigurnosnim ugrozama te učinkovitu komunikaciju pri istragama i rješavanju računalno-sigurnosnih incidenata kako unutar

Hrvatske tako i s odgovarajućim tijelima izvan Hrvatske. Također je potrebno usuglasiti zajedničke promotivne i edukativne djelatnosti kako za pojedine grupe korisnika tako i za najširu grupu korisnika koji pristupaju računalnim mrežama.



Slika 2. Nacionalna CERT infrastruktura

Središnji državni CERT potrebno je ustrojiti potrebnim aktima, osigurati mu potrebne resurse i dati potrebne ovlasti da bi mogao obavljati slijedeće poslove:

Uspostava nacionalne CERT infrastrukture – posebno je značajno uspostaviti nacionalnu strukturu CERT-ova unutar relevantnih ustanova i privatnih pravnih osoba te osigurati njihovo koordinirano djelovanje. Središnji državni CERT treba definirati pravila i način rada nacionalne CERT infrastrukture te raditi na poticaju njezine uspostave:

- poticanje i pomoć pri uspostavi ostalih CERT-ova u nacionalnoj CERT infrastrukturi, kroz suradnju s upravom, savjetovanje i edukaciju osoblja – članova CERT-ova,
- pomoć pri uključivanju ostalih CERT-ova u međunarodne organizacije i udruge CERT-ova,
- definiranje osnovnih potrebnih funkcionalnosti CERT-ova, njihove međusobne komunikacije kao i odnosa prema Središnjem državnom CERT-u (izvješćivanje, razmjena informacija između CERT-ova te s drugim relevantnim tijelima izvan RH),
- koordinacija zajedničke suradnje prema ostalim relevantnim TDV.

Reagiranje na ozbiljne sigurnosne incidente – u slučaju pojave značajnih incidenata ili incidenata koji prelaze okvire djelovanja pojedinih CERT-ova:

- koordiniranje rješavanja sigurnosnih incidenata koji svojim opsegom ili tipom ugrožavaju funkcioniranje Interneta ili moguće za život opasne aktivnosti,

- koordiniranje rješavanja incidenata koji ne spadaju u nadležnost niti jednog od ostalih CERT-ova, a barem jedna od uključenih strana je iz RH,

Prevencija računalno-sigurnosnih incidenata – podrška podizanju opće razine računalne sigurnosti u državnim ustanovama, privatnim poduzećima i najširem krugu korisnika:

- informiranje najšire javnosti o značaju i unapređenju računalne sigurnosti kroz izdavanje edukativnih materijala te javno djelovanje,
- informiranje stručne javnosti i ostalih CERT-ova kroz savjetovanje, izdavanje stručnih materijala i ranih upozorenja o ranjivostima računalnih sustava,
- organizacija i provođenje akcija i postupaka koje će upozoriti na postojeće propuste u računalno-komunikacijskoj infrastrukturi, a koji mogu biti iskorišteni za ugrožavanje njezinog funkcioniranja te davanje preporuka o načinima uklanjanja ovih propusta.

Na osnovu dosadašnjeg djelovanja, prikupljenih znanja i iskustva, funkciju Središnjeg državnog CERT-a treba preuzeti CARNet CERT – na taj će se način osigurati njegov brzi ustroj uz optimalno ulaganje resursa. Za osnivanje, ustroj i funkcioniranje Središnjeg državnog CERT-a potrebno je osigurati potrebne financijske (u proračunu RH ili adekvatne izvore financiranja) i druge resurse koji će omogućiti Središnjem državnom CERT-u učinkovito djelovanje. SDUeH, MZoŠ i CARNet trebaju poduzeti potrebne zakonsko-pravne i organizacijske korake za osnivanje, ustroj i funkcioniranje Središnjeg državnog CERT-a koji mora biti organizacijski i funkcionalno odvojen od postojećeg CARNet-ovog akademskog CERT-a.

Plan aktivnosti usklađivanja s Nacionalnim programom informacijske sigurnosti

1. Osnivanje Središnjeg državnog CERT-a (SDUeH, MZOŠ, CARNet).

4.2.4 Središnji državni ured za e-Hrvatsku i Agencija za potporu informacijskih sustava u ulozi tijela za planiranje i implementaciju mjera informacijske sigurnosti (ITSOA / CIS Planning and implementation») u RH

U sklopu cjelokupnog djelovanja subjekata u okruženju djelatnosti informacijskog društva, Središnji državni ured za e-Hrvatsku je izravno nadležan za razvoj informatičke infrastrukture u državnoj upravi, povezivanje informacijskih sustava tijela državne uprave uz racionalizaciju uporabe informatičkih resursa u državnoj upravi. Uz ovu primarnu nadležnost, Središnji državni ured za e-Hrvatsku je nadležan i za utvrđivanje i izradu stručnih i zakonskih podloga pridruživanja Republike Hrvatske Europskoj uniji u području razvoja informacijskog društva i primjene informacijske i komunikacijske tehnologije (eEurope).

Jedna od glavnih zadaća Programa e-Hrvatska 2007. je poduzimanje mjera za uspostavljanje sigurnosti informacijskih i komunikacijskih sustava državne uprave i na nacionalnoj razini. U skladu s time, SDUeH je inicirao osnivanje stručne skupine za izradu prijedloga Nacionalnog programa informacijske sigurnosti u RH (ovaj dokument) čije su zadaće izraditi okvir za razgraničenje nadležnosti u odnosu na

podatke i informacijsku infrastrukturu u RH te izradu sigurnosne politike, kao i utvrditi potrebne preduvjete za ustroj Zavoda za informacijsku sigurnost i kripto-zaštitnu tehnologiju i Središnjeg državnog CERT-a temeljeno na postojećim rješenjima, odnosno institucijama.

Za učinkovitu provedbu informatizacije državne uprave nužno je osigurati potporu informacijskim sustavima u institucionalnom obliku. Operativnim planom provedbe Programa e-Hrvatska 2007. za 2004. godinu predviđeno je formiranje Agencije za potporu informacijskih sustava, uspostavljanje mrežnog operacijskog centra za tijela državne uprave, te izrada projekta centralnog portala uz autentikaciju i autorizaciju pristupa informacijskim resursima državne uprave.

Uloga Agencije za potporu informacijskih sustava bila bi razvijanje i praćenje implementacije smjernica, normi i politike za razvoj e-uprave, davanje podrške tijelima državne uprave u razvoju vlastite strategije e-poslovanja, razvijanje i podupiranje zajedničke računalno-komunikacijske i aplikacijske infrastrukture, promoviranje primjene najboljih iskustava u upravljanju informacijskim sustavima, uključujući i zaštitu osobnih podataka, razvijanje zajedničkih elektroničkih usluga i centralni pristup informacijskim resursima državne uprave uz odgovarajuću autorizaciju i autentikaciju, te koordiniranje i planiranje cjeloživotnog obrazovanja državnih službenika u primjeni informacijske i komunikacijske tehnologije.

Obzirom na veliki broj djelatnosti i specifičnih tijela koje svaka državna vlast ima, uobičajeno je da neka od tih TDV nemaju adekvatne informacijsko-komunikacijske ustrojstvene jedinice. Stoga je predviđeno da SDUeH, kao središnje državno tijelo u procesu informatizacije državne uprave, bude nositelj organizacijske i nadzorne odgovornosti vlasnika informacijske infrastrukture u takvim tijelima. Ovakvim postupkom država dio lokalne infrastrukture, za koju se ne može osigurati adekvatna briga na lokalnoj razini ili to nije ekonomično, uključuje u zajedničku infrastrukturu (vlasništvo) s ciljem sustavne brige i razvoja cjelokupne infrastrukture u životnom ciklusu. Po analogiji s TDV i unutarnjim IT odjelima, SDUeH bi prenio izvršnu odgovornost vlasnika infrastrukture na Agenciju za potporu informacijskih sustava (APIS). Na ovaj način bi se u smislu informatičke potpore reorganizirala sva TDV koja nemaju vlastite organizacijske jedinice s određenim minimalnim brojem stručnih informatičkih djelatnika. Ovakva reorganizacija podrazumijeva preuzimanje brige od strane SDUeH i APIS-a o kompletnom životnom ciklusu opreme, dakle sve od planiranja i projektiranja, preko financiranja i nabave, upravljanja i održavanja te na kraju rashoda i uništenja opreme. Ovakvom organizacijom bi se postojeći informatički kadar iz manjih TDV u smislu radno-pravnog statusa formalno prebacio u APIS. Pri tome bi APIS i SDUeH preuzeli odgovornost za daljnju kadrovsku politiku i dodatno zapošljavanje nedostajućih informatičkih stručnjaka u državnoj upravi.

Ovakvim pristupom država s jedne strane postiže bolju konkurentnost u zapošljavanju informatičara, što je u proteklom periodu bio nepremostiv problem, a s druge strane postiže neophodne stručne kompetencije kako bi državna uprava uopće bila u stanju provesti izgradnju informacijskog društva. Upravo ove dvije komponente, čvrsto definirana organizacija i kadrovske kompetencije, preduvjet su uspostavljanju informacijske sigurnosti u državnoj upravi.

4.2.5 Agencija za zaštitu osobnih podataka

Temeljem Zakona o zaštiti osobnih podataka osnovana je Agencija za zaštitu osobnih podataka koja, u okviru javne ovlasti, nadzire provođenje zaštite osobnih podataka te ukazuje na uočene zlouporabe u prikupljanju i obradi osobnih podataka, sastavlja listu država i međunarodnih organizacija koje imaju odgovarajuće uređenu zaštitu osobnih podataka i rješava povodom zahtjeva za utvrđivanje povrede prava zajamčenih ovim Zakonom.

U obavljanju poslova javne ovlasti, Agencija ima pravo rješenjem narediti da se nepravilnosti uklone u određenom roku, privremeno zabraniti prikupljanje, obradu i korištenje osobnih podataka koji se prikupljaju, obrađuju ili koriste suprotno zakonu, narediti brisanje osobnih podataka prikupljenih bez pravne osnove, zabraniti iznošenje osobnih podataka iz Republike Hrvatske ili davanje na korištenje osobnih podataka drugim korisnicima ako se osobni podaci iznose iz Republike Hrvatske ili se daju na korištenje drugim korisnicima suprotno Zakonu, zabraniti povjeravanje poslova prikupljanja i obrade osobnih podataka izvršiteljima obrade ako ne ispunjavaju uvjete u pogledu zaštite osobnih podataka ili je povjeravanje navedenih poslova provedeno suprotno Zakonu. Agencija može predložiti pokretanje postupka kaznene ili prekršajne odgovornosti pred nadležnim tijelom.

Agencija obavlja i slijedeće poslove: prati uređenje zaštite osobnih podataka u drugim zemljama i surađuje s tijelima nadležnim za nadzor nad zaštitom osobnih podataka u drugim zemljama, nadzire iznošenje osobnih podataka iz Republike Hrvatske, izrađuje metodološke preporuke za unapređenje zaštite osobnih podataka i dostavlja ih voditeljima zbirki osobnih podataka, daje savjete u svezi s uspostavom novih zbirki osobnih podataka osobito u slučaju uvođenja nove informacijske tehnologije, daje mišljenja u slučaju sumnje smatra li se pojedini skup osobnih podataka zbirkom osobnih podataka u smislu ovog Zakona, prati primjenu organizacijskih i tehničkih mjera za zaštitu osobnih podataka te predlaže poboljšanje tih mjera, daje prijedloge i preporuke za unapređenje zaštite osobnih podataka, surađuje s nadležnim državnim tijelima u izradi prijedloga propisa koji se odnose na zaštitu osobnih podataka, daje prethodno mišljenje o tome sadrže li određeni načini obrade osobnih podataka specifične rizike za prava i slobode ispitanika, te obavlja i druge poslove određene zakonom.

4.3 Infrastrukturni okvir

Nacionalna politika informacijske sigurnosti te njeni provedbeni akti, moraju osigurati sustavan pristup svim dijelovima vitalne državne infrastrukture pa tako i onim dijelovima koji se unajmljuju od telekomunikacijskih (TK) operatora ili davatelja Internetskih usluga (ISP). Liberalizacija telekomunikacija u RH, iako postupno vodi ciljevima kao što su tržišno nadmetanje i deregulacija, donosi i niz pratećih sigurnosnih problema s kojima se suvremena državna uprava mora znati nositi. Tipični problemi koji nastaju pri liberalizaciji TK sektora poznati su u nizu tranzicijskih zemalja. Jedan od važnijih je intencija inozemnih vlasnika TK operatora za udaljenim, prekograničnim upravljanjem TK mrežama, čime se za vlasnika smanjuju troškovi, ali se ugrožava nacionalno gospodarstvo odljevom radnih mjesta te su osobni podaci građana u TK prometu, koji na taj način nekontrolirano cirkuliraju preko granica i

pohranjuju se u trećim zemljama, najčešće izvan dosega bilo kakvog zakonodavstva. Krupan problem je i ekstrateritorijalni Internetski promet koji se događa i unutar nacionalne komunikacije uzrok kojeg je financijska zarada, tržišna borba ili jednostavno nebriga TK operatora ili ISP-a. Rezultat takvog stanja je da poruka poslana e-poštom na odredište unutar istog grada može, prije krajnjeg odredišta, proći jednu ili više državnih granica jer postoji mogućnost da TK operator ili ISP, koji ima podružnice u više susjednih država, ima privatne vodove koji povezuju te podružnice i u određenom trenutku može mu se isplatiti centralizirati sustav u samo jednu od tih zemalja po svom izboru. Slična situacija može se, s daljnjom liberalizacijom tržišta u međunarodnom javnom govornom prometu RH, očekivati i u telefoniji, prvenstveno mobilnoj. Zadatak sigurnosne evaluacije informacijsko-komunikacijskih projekata državne uprave jest prepoznati i izbjeći ovakve ugroze, dok je zadatak nacionalne politike informacijske sigurnosti postaviti ciljeve koji će omogućiti razvoj mehanizama zaštite i prevencije (regulativnih, organizacijskih i/ili tehničkih) od ugroza, na dobrobit svih čimbenika informacijskog društva – građanstva, gospodarstva i države u cjelini.

Jedan od tipičnih problema koji treba strateški riješiti kroz nacionalnu politiku informacijske sigurnosti je i pristup telekomunikacijskoj infrastrukturi u RH. To pretpostavlja jasno definirano vlasništvo nad postojećim telekomunikacijskim kanalima i vodovima u RH te strategiju korištenja takvih vodova od strane državne uprave, kao i poštivanje određenih sigurnosnih pravila za sve privatne vlasnike infrastrukture. Uz TK kanale i vodove, koji se uglavnom tretiraju kao vlasništvo bivšeg državnog TK operatora, postoji i kabelska infrastruktura u vlasništvu HEP-a ili HŽ-a, potencijalno iskoristiva za projekte kao što je Računalno-komunikacijska mreža tijela državne uprave (RKMTDU). Pored toga postoji i kvalitetna bežična infrastruktura u vlasništvu HEP-a i Odašiljača i veza, koja također može biti temelj za interventne službe RH (Hitna pomoć, Vatrogastvo, Policija, Služba spašavanja i sl.). Pokazuje se da problemi konfuznog pristupa TK infrastrukturi traju u RH već niz godina, a proces liberalizacije telekomunikacija u RH koji je započeo 1999. godine donošenjem Zakona o telekomunikacijama i privatizacijom HT-a, samo je dodatno zakomplicirao neriješene probleme. Donošenje nacionalne politike informacijske sigurnosti jedan je od najboljih načina kako suvremena država može postupno i sustavno riješiti ovakve probleme.

Primjena informacijske i komunikacijske tehnologije danas je jedan od glavnih preduvjeta za povećanje učinkovitosti poslovanja, kako u privatnom sektoru, tako i u državnoj upravi. Međutim tehnologija nije i ne može biti sama sebi svrhom. Iskustva provedbe Akcijskog plana eEurope 2005. pokazuju da je moguće utrošiti velika financijska sredstva, a da učinak bude znatno manji od očekivanog. Informacijska tehnologija mora biti prije svega osnova i poticaj za restrukturiranje poslovnih procesa u državnoj upravi i međusobnu koordinaciju resora državne izvršne vlasti.

Svaki informacijski sustav mora se postupno i sustavno nadograđivati te kvalitetno upravljati i održavati kroz cijeli životni ciklus, u svakoj svojoj fazi od inicijacije i idejnog projekta, preko razvoja, implementacije, korištenja pa sve do rashoda. Sigurnosna evaluacija mora biti dio svih tih faza životnog ciklusa. Izgradnja Računalno-komunikacijske mreže tijela državne uprave (RKMTDU) nužna je za ostvarivanje elektroničkih usluga za građanstvo i poslovne subjekte te za međusobnu povezanost državnih tijela (Projekt e-Hrvatska 2007.). Obzirom da je projekt RKMTDU u neuspješnoj realizaciji već gotovo čitavo desetljeće, ponovno se provodi tehnička

revizija RKMTDU. Uz tehničku reviziju, nužna je i sigurnosna evaluacija projekta RKMTDU, kako bi se izgradnja ove vitalne infrastrukture ispravno usmjerila. Sigurnosna evaluacija projekta RKMTDU nije moguća do pune uspostave sustava informacijske sigurnosti u RH (sigurnosna politika i provedbeni dokumenti, organizirana provedbena tijela u RH) što je dodatni razlog za ubrzano uspostavljanje sustava informacijske sigurnosti u RH.

RKMTDU mora biti integralna infrastruktura državne uprave RH, jer samo tako ima smisla i može donijeti poboljšanja i osuvremenjivanje. Dosadašnji koncept nepovezanih projekata informacijske infrastrukture u RH donosi, vremenom, ogromne troškove zbog neumitnih zahtjeva interoperabilnosti. Čak i tradicionalna poslovna telefonska mreža državne uprave nije uspjela zaživjeti kao integralna telefonska mreža, već je većina državnih tijela doživljava i koristi kao svoju internu. Rezultat je slaba optimizacija poslovne telefonske mreže na državnoj razini što poskupljuje poslovanje, ali i loš pristup korisnika, koji razgovarajući posredstvom javne mreže povećavaju troškove i potencijalno narušavaju sigurnost. Glavni razlog zašto projekt kao što je RKMTDU ne uspijeva jest to što u državnoj upravi RH nikada nije formalno uspostavljen nacionalni pristup izgradnji informacijsko-komunikacijske infrastrukture. Upravo takav pristup dio je nacionalne politike informacijske sigurnosti kojom se država osposobljava za tzv. horizontalnu komunikaciju među tijelima državne vlasti i pristup tijelima kao resursima zajedničkog nacionalnog sustava. Dosadašnji pristup organizaciji državne uprave u RH izrazito je tradicionalan i u potpunosti vertikalno organiziran po resorima, čime uvelike blokira zajedničke infrastrukturne inicijative, umjesto da ih potiče, pa čak i propisuje. Prihvaćanjem načela informacijske sigurnosti stvaraju se i/ili reorganiziraju državna tijela koja imaju nacionalnu odgovornost nad izgradnjom, upravljanjem i korištenjem sveukupne državne informacijske infrastrukture. Pri tome odgovornost upravljačkih tijela treba biti raspodijeljena, kako bi se onemogućila zloporaba uslijed kumuliranih nadležnosti pojedinih tijela.

5 RAZGRANIČENJE NADLEŽNOSTI U ODNOSU NA PODATKE I INFORMACIJSKU INFRASTRUKTURU U RH

Suvremeni sustav informacijske sigurnost traži jasno određivanje nadležnosti pojedinih tijela koja upravljaju ovom kompleksnom organizacijom. Pri tome je nužno provesti razdvajanje nadležnosti između ključnih funkcionalnosti u sustavu informacijske sigurnosti, postići organizacijsku i tehničku kompetentnost svih tijela u upravljačkom lancu informacijske sigurnosti te uskladiti potrebne propise na najvišoj državnoj razini. Ovaj Nacionalni program daje načelne kriterije i preporuke za organizacijski model sustava informacijske sigurnosti RH, ali tek donošenje nužnih akata i pokretanje ključnih tijela u RH stvara temelj za postupanje i stvarne promjene u ovom području u RH.

Sustav informacijske sigurnosti gledan s aspekta suvremene državne uprave, zahtijeva podjelu na više skupina tijela i pravnih osoba. Općenito to bi bile središnja izvršna vlast, ostali stupovi i razine državne vlasti, javni i privatni sektor. Razlog formiranja više skupina tijela je prvenstveno bitno različit tretman informacijske sigurnosti u svakoj pojedinoj skupini (ciljevi, potrebe, zahtjevi), ali i bitno različit koncept zakonske regulacije područja informacijske sigurnosti unutar ovakvih skupina državnih tijela i pravnih osoba.

Sustav informacijske sigurnosti u RH primijenit će se provođenjem različitih aktivnosti i mjera na sljedeće tri skupine državnih tijela, odnosno pravnih osoba:

- **Skupina A**, sastoji se od tijela središnje izvršne vlasti, tijela sustava nacionalne sigurnosti te drugih institucija koje obavljaju vitalne i zajedničke funkcije za tijela iz Skupine A;
- **Skupina B**, sastoji se od tijela koja predstavljaju ostale stupove i razine državne vlasti u RH, javnog sektora te drugih institucija koje obavljaju vitalne i zajedničke funkcije za tijela iz Skupine B;
- **Skupina C**, sastoji se od privatnog sektora u širem smislu, tj. ovdje pripadaju sve ostale pravne osobe u RH i sva trgovačka društva u RH, neovisno o tipu vlasništva (privatno, državno ili mješovito) ili osnivaču.

Podjela na Skupine A, B i C definira minimalne kriterije informacijske sigurnosti za pravne osobe iz svake pojedine Skupine. Pored postavljanja minimalnih kriterija, država posjeduje i dodatnu mogućnost formiranja posebnih skupina pravnih osoba s aspekta nacionalne sigurnosti.

Ovakve posebne skupine država određuje na temelju procjene kritične nacionalne infrastrukture u smislu opasnosti od terorizma, rata i svih potencijalnih ugroza s nacionalnim značenjem. Proces određivanja kritične nacionalne infrastrukture odvija se u okviru sustava nacionalne sigurnosti, a popis kritične nacionalne infrastrukture redovito se objavljuje u okviru strategije nacionalne sigurnosti i treba biti dostupan javnosti. Vijeće za nacionalnu sigurnost može na prijedlog nadležne sigurnosne službe, usklađen s nadležnim ministarstvom, odrediti posebnu skupinu tijela i tvrtki iz bilo koje od Skupina A, B i C, čija je djelatnost od vitalnog značenja za određenu kritičnu nacionalnu infrastrukturu (primjerice elektroenergetski sustav RH). Za takvu posebnu skupinu uobičajeno se uz niz drugih mjera, definira i poseban skup minimalnih kriterija informacijske sigurnosti, u suradnji nadležnih tijela sigurnosnog

sustava, mjerodavnog ministarstva te predstavnika pravnih osoba koje spadaju u određenu posebnu skupinu tijela. Razlika u odnosu na Skupinu C je u tome što se ovdje minimalni sigurnosni kriteriji postavljaju neovisno o volji samih pravnih osoba na koje će se propisi odnositi, ali se svima na koje se odnose ovakvi kriteriji pruža mogućnost aktivnog sudjelovanja u oblikovanju ovakve posebne politike i provedbenih akata informacijske sigurnosti.

Nadalje, kako bi se definirao sustav upravljanja informacijskom sigurnošću u državi, potrebno je za svaku od prethodno definiranih Skupina utvrditi nekoliko temeljnih kategorija kao što su: vlasnici podataka, vlasnici informacijske infrastrukture, posebni propisi informacijske sigurnosti koji reguliraju tu skupinu, te nadležna tijela u upravljanju informacijskom sigurnošću u svakoj od tih skupina. Kroz analizu odabranih Skupina A, B i C, bit će utvrđene ove temeljne kategorije za svaku odabranu skupinu.

Vlasnici podataka odgovorni su za sve radnje s podacima u njihovoj nadležnosti, tijekom životnog ciklusa podataka te za planiranje i implementaciju organizacijskih i tehničkih mjera u skladu s važećim propisima informacijske sigurnosti i u okviru svoje nadležnosti. Pri tome, radnje s podacima podrazumijevaju nastajanje, obrađivanje, pohranjivanje i arhiviranje podataka. Informacijska infrastruktura obuhvaća svu infrastrukturu u određenom državnom tijelu ili pravnoj osobi koja na bilo koji način utječe na temeljna svojstva povjerljivosti, dostupnosti ili cjelovitosti podataka i u okviru koje podaci nastaju, obrađuju se ili pohranjuju. Vlasnici informacijske infrastrukture odgovorni su za informacijsku infrastrukturu tijekom životnog ciklusa infrastrukture te za planiranje i implementaciju organizacijskih i tehničkih mjera, u skladu s važećim propisima informacijske sigurnosti i u okviru svoje nadležnosti.

Informacijska sigurnost regulirana je općim zakonskim aktima kao što je primjerice Zakon o zaštiti osobnih podataka, koji se odnosi na sve tri skupine državnih tijela i pravnih osoba, ali i posebnim zakonskim aktima, koji mogu biti zajednički ili specifični za svaku pojedinu skupinu. Obzirom na stanje informacijske sigurnosti u RH te na potrebe procijenjene ovim Nacionalnim programom, nužno je na početku ovog procesa donijeti okvirni zakon o informacijskoj sigurnosti u RH koji će biti krovni propis za omogućavanje organizacije informacijske sigurnosti u sve tri skupine tijela. Pri tome će se u okviru razrade propisa nižim podzakonskim aktima informacijske sigurnosti, voditi računa o specifičnostima, potrebama i zahtjevima svake pojedine skupine tijela i pravnih osoba. Okvirni zakon o informacijskoj sigurnosti treba odrediti nadležnosti i djelatnosti upravljačkih tijela u sustavu informacijske sigurnosti, kako bi se moglo pristupiti izradi strukturiranog skupa nacionalnih propisa informacijske sigurnosti tijekom čega će se morati mijenjati i prilagođavati neki postojeći zakoni u RH. Pored ovakvog okvirnog zakona o informacijskoj sigurnosti, bit će nužno donijeti nacionalnu strategiju ili politiku informacijske sigurnosti kao temeljni krovni propis koji postavlja osnovna sigurnosna načela, područja i dosege primjene te izražava potporu najviše državne vlasti u provedbi informacijske sigurnosti u RH. Svi ostali propisi informacijske sigurnosti u RH (uredbe, pravilnici, naputci, smjernice i sl.), neovisno o tome na koju skupinu tijela i pravnih osoba se primjenjuju, moraju biti potpuno usklađeni s okvirnim zakonom o informacijskoj sigurnosti i nacionalnom strategijom ili politikom informacijske sigurnosti, čime se osigurava konzistentnost cijelog sustava.

Više je razloga zašto se donose skupovi propisa za svaku pojedinu skupinu tijela i pravnih osoba. Osnovni razlog je da su zahtjevi informacijske sigurnosti na Skupinu

A neusporedivo oštriji od zahtjeva na Skupinu B. Specifičnost Skupine B je da u okviru provedbe traži dugotrajne koordinacije i konzultacije između različitih stupova vlasti i javnog sektora, što nije moguće provesti bez uređenog stanja informacijske sigurnosti u Skupini A i određenog iskustva države u ovom području. Skupina C pak traži višu razinu svijesti ne samo u državnim tijelima, već i kod najširih slojeva društva, da bi se uopće mogao inicirati postupak javno-privatnog partnerstva u ovom kompleksnom području informacijske sigurnosti. Ta razina svijesti postiže se kroz proces uređenja Skupina A i B, koji sam po sebi traži dobro organizirane prateće programe edukacije i razvoja sigurnosne kulture te stvara preduvjete za osuvremenjavanje nacionalnih školskih programa s aspekta povezansti informatike i informacijske sigurnosti.

Sustav informacijske sigurnosti neposredno je ovisan o poslovnim procesima u pojedinim državnim tijelima i pravnim osobama. Obzirom na česte promjene i prilagodbe poslovnih procesa, koje diktira brz razvoj tehnologije i globalizacija, sustav informacijske sigurnosti mora upravljati promjenama statusa i pripadnosti pojedinih tijela određenim skupinama u smislu informacijske sigurnosti. Odluku o tome uobičajeno donosi Središnje državno sigurnosno tijelo (NSA), za RH UVNS, a to vrijedi i za slučaj uključivanja novih tijela u sustav informacijske sigurnosti. Što se tiče ostalih nadležnih tijela u upravljanju informacijskom sigurnošću, postoje određene sličnosti između ove tri skupine tijela, ali i bitne razlike koje će biti utvrđene u sljedećim poglavljima. Posebni propisi informacijske sigurnosti bit će detaljnije opisani u poglavlju 6. Sigurnosna politika.

5.1 Skupina A

Skupina A sastoji se od tijela središnje izvršne vlasti, tijela sustava nacionalne sigurnosti te drugih institucija koje obavljaju vitalne i zajedničke funkcije za tijela iz Skupine A. Stoga Skupina A u smislu ovog dokumenta podrazumijeva sljedeće državne institucije u RH:
Predsjednik RH s pratećim službama, Vlada RH, Uredi Vlade RH, Ministarstva, Središnji državni uredi, Državno odvjetništvo, tijela sigurnosnog sustava RH (UVNS, POA, OA, VSA, ZISKZT), diplomatsko-konzularna predstavništva RH. U smislu obavljanja vitalnih i zajedničkih funkcija za tijela iz skupine A, ovdje spadaju, na način opisan u ovom poglavlju, i Vrhovni sud, APIS i FINA.

Kategorije bitne za organizaciju i upravljanje informacijskom sigurnošću u Skupini A prikazane su u Tablici 1.:

Tablica1. Skupina A

Skupina A – Organizacija i upravljanje informacijskom sigurnošću -			
Vlasnici podataka	**Vlasnici informacijske infrastrukture**	**Posebni propisi informacijske sigurnosti**	**Upravljačka tijela**
TDV / čelnici tijela	TDV / ustrojstvena jedinica, a za TDV bez IT	Zakon o informacijskoj sigurnosti (okvirni) i	***Središnje državno sigurnosno tijelo u RH (NSA):*** UVNS

Skupina A – Organizacija i upravljanje informacijskom sigurnošću -			
Vlasnici podataka	**Vlasnici informacijske infrastrukture**	**Posebni propisi informacijske sigurnosti**	**Upravljačka tijela**
	ustrojstvene jedinice: SDUeH / APIS	Nacionalna strategija ili politika informacijske sigurnosti – Hrvatski sabor Provedbene uredbe po sigurnosnim područjima - Vlada RH Pravilnici i smjernice - Sigurnosni sustav: UVNS (NSA), ZISKZT (NCSA, SAA), u suradnji s POA, OA, VSA (CIS Op.) Navedenim aktima utvrđene tehničke i sigurnosne norme i otvoreni standardi - Normizacijsko tijelo RH, SDUeH, ZISKZT, UVNS)	***Središnje tijelo za sigurnost komunikacija u RH (NCSA / IA):*** ZISKZT ***Središnje tijelo za sigurnosne akreditacije (SAA):*** Središnji državni SAA je ZISKZT , a lokalni SAA za specifične programe ministarstava su VSA za MORH, OA za DKP MVP-a ***Tijela za nadzor operativnosti mjera inf. sig. u RH (CIS Operating / CISO/LISO koordinatori):*** POA, OA ili VSA, u skladu s nadležnostima definiranim u ZOSS-u ***Tijela za planiranje i implementaciju mjera inf. sig. (CIS Planning & Implementation / ITSOA):*** TDV / ustrojstvena jedinica ili SDUeH / APIS (vlasnik informacijske infrastrukture)

Odgovornost vlasnika podataka u Skupini A mora biti jasno definirana i postavljena na čelnika svakog pojedinog tijela državne vlasti (TDV). Pri tome ova odgovornost podrazumijeva rukovodnu odgovornost za uspostavljanje potrebnih procedura i organizacijsku kontrolu funkcioniranja i usklađenosti tih procedura informacijske sigurnosti. Osim čelnika koji predstavlja najodgovorniju osobu za organizaciju informacijske sigurnosti, ovakva organizacija mora unutar tijela definirati izvršnu odgovornost rukovodne hijerarhije i svakog službenika i namještenika TDV. Odgovornost u okviru informacijske sigurnosti se uobičajeno procesuira na dvije pravne razine: kroz kaznene postupke sukladno definiranim kaznenim djelima u RH, te kroz disciplinske postupke u okviru disciplinskih i stegovnih sudova za državne službenike i namještenike, ovlaštene službene osobe, vojne osobe itd. Nije uobičajeno, niti primjereno, donositi posebne prekršajne odredbe u okviru sustava informacijske sigurnosti, jer dio prekršaja u ovom segmentu mora biti kazneno sankcioniran, a dio spada u redovne propise radno-pravne stege. Tretirati prekršaje informacijske sigurnosti izvan ova dva spomenuta područja kaznenog i radnog prava protivno je temeljnim principima sigurnosti i njenom integralnom shvaćanju u okviru suvremenog društva.

Vlasnici informacijske infrastrukture u Skupini A vode brigu o informacijsko-komunikacijskoj opremi tijekom cjelokupnog životnog ciklusa opreme (planiranje, projektiranje, nabava, opremanje, upravljanje, održavanje, rashod, uništavanje). Pri tome se primjenjuju pozitivni propisi državne uprave u smislu nabave i izvršenja državnog proračuna. Vlasnici informacijske infrastrukture su redovito sama TDV, odnosno ta odgovornost može biti prenesena na unutarnje ustrojstvene jedinice tehničkog profila s odgovarajućim nadležnostima informacijsko-komunikacijskog karaktera.

Za TDV koja nemaju adekvatne informacijsko-komunikacijske ustrojstvene jedinice je predviđeno da SDUeH, kao središnje državno tijelo u procesu informatizacije državne uprave, bude nositelj organizacijske i nadzorne odgovornosti vlasnika informacijske infrastrukture u takvim tijelima. Po analogiji s TDV i unutarnjim IT odjelima, SDUeH bi prenio izvršnu odgovornost vlasnika infrastrukture na Agenciju za potporu informacijskih sustava (APIS). Na ovaj način bi se u smislu informatičke potpore reorganizirala sva TDV koja nemaju vlastite organizacijske jedinice s određenim minimalnim brojem stručnih informatičkih djelatnika. S aspekta informacijske sigurnosti APIS mora pripadati Skupini A te je, ovisno o pravnom statusu APIS-a, potrebno donijeti odredbe koje će pravno obvezivati APIS na posebnu regulativu informacijske sigurnosti u Skupini A.

Bitno je naglasiti da koncept vlasnika informacijske infrastrukture mora biti jednoznačno definiran, to znači da za svako tijelo u Skupini A vlasnik mora biti ili unutarnja IT ustrojstvena jedinica ili APIS, nikako oboje. Pri tome vlasnik informacijske infrastrukture može sukladno propisima informacijske sigurnosti koristiti usluge trećih strana ili vanjsku suradnju.

Zahtjevi na upravljačka tijela skupine A postavljeni su kroz sigurnosnu politiku EU i NATO-a, ali su danas na ovakav način organizirani sustavi informacijske sigurnosti u gotovo svim razvijenim zemljama svijeta. Poštivanjem ovakvih zahtjeva postiže se za svaku državu iznimno važna karakteristika u međunarodnim integracijskim procesima i međunarodnoj suradnji – organizacijska interoperabilnost. Stoga je cilj organizaciju informacijske sigurnosti u RH prilagoditi međunarodnim standardima, ali istovremeno

i zadržati dio nadležnosti uspostavljenih u nacionalnom zakonodavstvu RH, koji je sukladan ciljanom konceptu informacijske sigurnosti. NSA (National Security Authority) ili središnje državno sigurnosno tijelo je uobičajeno krovno ili koordinacijsko tijelo sigurnosnog sustava i u slučaju RH to bi bio UVNS (Ured Vijeća za nacionalnu sigurnost). Sukladno ZOSS-u UVNS obavlja i funkciju NDA (National Distribution Authority) ili Središnjeg distribucijskog tijela za povjerljive materijale NATO-a. NCSA (National Comunications Security Authority) ili Središnje tijelo za sigurnost komunikacija uobičajeno predstavlja tehničko tijelo sigurnosnog sustava, u našem slučaju ZISKZT (Zavod za informacijsku sigurnost i kripto zaštitnu tehnologiju). SAA (Security Acreditation Authority) ili Središnje državno tijelo za sigurnosne akreditacije, uobičajeno predstavlja tehničko tijelo sigurnosnog sustava, u našem slučaju ZISKZT. Zbog velikog opsega poslova te zbog poboljšanja učinkovitosti u procesu sigurnosnih akreditacija, uobičajeno je od strane središnjeg SAA akreditirati lokalne SAA za pojedine specifične nacionalne programe. U slučaju RH, akreditacije za lokalnu SAA funkcionalnost trebao bi ZISKZT provesti za VSA za potrebe MORH-a, te za OA-u za potrebe diplomatsko-konzularnih predstavništava MVP-a. Akreditacijski proces podrazumijeva akreditiranje informacijsko-komunikacijskih procesa na određeni vremenski period (najčešće 2 do 4 godine) te kasnije redovito obnavljanje akreditacijskog procesa. Pored procesa sigurnosnih akreditacija, iznimno je važan operativni nadzor mjera informacijske sigurnosti (CIS Operating), koji provode sigurnosne službe (POA, OA, VSA), sukladno nadležnostima definiranim u ZOSS-u. Operativni nadzor se provodi nad TDV koja su propisno akreditirana za rad i njime se prati poštivanje propisanih procedura, te planiranje i upravljanje promjenama u sustavu, koje se neminovno događaju u periodu redovnog rada sustava, bilo zbog tehnoloških (npr. promjena poslužiteljske platforme) ili organizacijskih promjena (npr. spajanje nekih odjela u TDV).

U Skupini A, koja predstavlja srce sustava informacijske sigurnosti države, iznimno je značajno poštovati načelo razdvajanja nadležnosti pa je operativni nadzor u potpunosti razdvojen od procesa planiranja i implementacije. Proces planiranja i implementacije metoda i mjera informacijske sigurnosti (CIS Planning & Implementation) redovito obavlja vlasnik informacijske infrastrukture te u slučaju RH vrijedi pojašnjenje koje je već dano za vlasnike informacijske infrastrukture.

Obzirom na ulogu Vrhovnog suda koja proizlazi iz čl. 17. ZOSS-a (izdavanje naloga za provođenje mjera tajnog prikupljanja podataka) potrebno je ovu funkcionalnost tretirati u Skupini A. U tom smislu Vrhovni sud treba imati posebno organiziran poslovni proces izdavanja naloga za provođenje mjera tajnog nadzora, na koji se primjenjuju propisi Skupine A, dok se na ostale funkcionalnosti Vrhovnog suda mogu primjenjivati propisi Skupine B.

Sukladno odluci Vlade RH o postavljanju Financijske agencije (FINA-e) za nositelja poslova certificiranja elektroničkih potpisa (Certificate Authority – CA) za tijela državne uprave te za implementaciju računalno-komunikacijske mreže tijela državne uprave, FINA u smislu informacijske sigurnosti u RH mora spadati u Skupinu A (vitalna i zajednička infrastruktura tijela u Skupini A). Obzirom da FINA nije TDV te da se propisi iz Skupine A ne odnose na FINA-u, Vlada RH ovakvu obvezu mora uvesti kroz Uredbu kojom definira nositelja poslova certificiranja elektroničkih potpisa ili kroz ugovor s FINA-om o obavljanju ovih poslova. U okviru informacijske sigurnosti, moguće je pojedine funkcionalnosti nekih tijela, uz odgovarajuće organizacijske zahtjeve, tretirati u višoj sigurnosnoj skupini. U tom smislu FINA može imati posebno

organiziran poslovni proces certificiranja, na koji se primjenjuju propisi Skupine A, dok ostali dijelovi FINA-e mogu primjenjivati propise Skupine B. Tijekom perioda izgradnje sustava informacijske sigurnosti RH, poslove certificiranja elektroničkog potpisa će trebati sustavno sagledati kao jednu od vitalnih komponenti tog sustava.

5.2 Skupina B

Skupina B sastoji se od tijela koja predstavljaju ostale stupove i razine državne vlasti u RH, javnog sektora te drugih institucija koje obavljaju vitalne i zajedničke funkcije za tijela iz Skupine B. Stoga, Skupina B u smislu ovog dokumenta podrazumijeva sljedeće državne institucije u RH:
Hrvatski sabor s pratećim službama, pravosudna vlast u RH (Vrhovni sud, Ustavni sud te područni i ostali sudovi), Hrvatska narodna banka (HNB), državne upravne organizacije (npr. DZS), javni sektor (npr. HZMO, CARNet, FINA, itd.), uredi državne uprave u županijama, područna (regionalna) uprava i lokalna samouprava (županije, gradovi, općine) te sve pravne i fizičke osobe s javnim ovlastima.

Kategorije bitne za organizaciju i upravljanje informacijskom sigurnošću u Skupini B prikazane su u Tablici 2.:

Tablica 2. Skupina B

Skupina B – Organizacija i upravljanje informacijskom sigurnošću -			
Vlasnici podataka	**Vlasnici informacijske infrastrukture**	**Posebni propisi informacijske sigurnosti**	**Upravljačka tijela**
TDV / čelnici tijela ili Pravna osoba / ravnatelj	TDV / ustrojstvena jedinica, za TDV bez IT ustrojstvene jedinice: SDUeH / APIS, za znanstveni, visokoškolski i obrazovni sustav: MZOŠ / Srce, odnosno CARNet a za ostale: pravna osoba	Zakon o informacijskoj sigurnosti (okvirni) i Nacionalna strategija ili politika informacijske sigurnosti – Hrvatski sabor Provedbene uredbe po sigurnosnim područjima - Vlada RH Pravilnici i smjernice - Sigurnosni sustav: UVNS (NSA), ZISKZT (NCSA, SAA), u suradnji s POA, OA, VSA (CIS Op.)	**Središnje državno sigurnosno tijelo u RH (NSA):** UVNS **Središnje tijelo za sigurnost komunikacija u RH (NCSA / IA):** ZISKZT **Tijela za sigurnosne akreditacije (SAA):** Akreditacijsko tijelo RH, a lokalni SAA za specifične TDV je ZISKZT **Tijela za nadzor operativnosti mjera inf. sig. u**

Skupina B – Organizacija i upravljanje informacijskom sigurnošću -			
Vlasnici podataka	**Vlasnici informacijske infrastrukture**	**Posebni propisi informacijske sigurnosti**	**Upravljačka tijela**
		Opće tehničke i sigurnosne norme, prihvaćene u okviru nacionalnih normizacijskih procesa i otvoreni standardi - Normizacijsko tijelo RH, SDUeH, ZISKZT, UVNS	**RH (CIS Operating / CISO/LISO koordinatori):** hijerarhija koordinatora informacijske sigurnosti usklađenih od strane NCSA/IA **Tijela za planiranje i implementaciju mjera inf. sig. (CIS Planning & Implementation / ITSOA):** vlasnik informacijske infrastrukture (TDV/ustrojstvena jedinica, SDUeH/APIS, MZOŠ/CARNet ili pravna osoba)

Odgovornost vlasnika podataka u Skupini B mora biti uvijek jasno definirana i postavljena na čelnika svakog pojedinog tijela državne vlasti (TDV) ili pravne osobe (ravnatelj i sl.). Pri tome ova odgovornost podrazumijeva rukovodnu odgovornost za uspostavljanje potrebnih procedura i organizacijsku kontrolu funkcioniranja i usklađenosti tih procedura informacijske sigurnosti. Osim čelnika, koji predstavlja najodgovorniju osobu za organizaciju informacijske sigurnosti, ovakva organizacija mora unutar tijela definirati izvršnu odgovornost rukovodne hijerarhije i svakog službenika TDV, odnosno zaposlenika pravne osobe. Odgovornost se uobičajeno procesuira na više pravnih razina. Sukladno Skupini A, i u Skupini B dio prekršaja informacijske sigurnosti spada pod kaznene sankcije, a dio spada u redovne postupke radno-pravnog zakonodavstva. U Skupini B zbog interakcije državnih upravnih organizacija i javnog sektora s privatnim sektorom, može doći do, također redovitih, gospodarskih pravnih mehanizama, koji se primjenjuju u okviru sudova časti Hrvatske gospodarske komore (primjerice kršenje odredbi poslovne tajne). Stoga, niti u Skupini B nije uobičajeno tretirati prekršaje informacijske sigurnosti izvan spomenutih područja kaznenog i radnog prava, odnosno pravnih mehanizama gospodarske komore.

Vlasnici informacijske infrastrukture u Skupini B vode brigu o informacijsko-komunikacijskoj opremi tijekom cjelokupnog životnog ciklusa opreme (planiranje,

projektiranje, nabava, opremanje, upravljanje, održavanje, rashod, uništavanje). Pri tome se primjenjuju pozitivni propisi u smislu nabave i izvršenja državnog proračuna ili sredstava pravne osobe. Vlasnici informacijske infrastrukture moraju biti jednoznačno definirani. To mogu biti sama TDV, odnosno unutarnje ustrojstvene jedinice tehničkog profila s odgovarajućim nadležnostima informacijsko-komunikacijskog karaktera. Obzirom na veliki broj djelatnosti i specifičnih tijela koje svaka državna vlast ima, uobičajeno je da mnoga od tih TDV nemaju adekvatne informacijsko-komunikacijske ustrojstvene jedinice. Stoga se može, na način predviđen u okviru Skupine A, koristiti SDUeH, središnje državno tijelo u procesu informatizacije državne uprave, kao nositelja organizacijske i nadzorne odgovornosti vlasnika informacijske infrastrukture u takvim tijelima. Po analogiji s TDV i unutarnjim IT odjelima, SDUeH bi prenio izvršnu odgovornost vlasnika infrastrukture na Agenciju za potporu informacijskih sustava (APIS). Na ovaj način bi se u smislu informatičke potpore reorganiziralo sva TDV u Skupini B, koja nemaju vlastite organizacijske jedinice s određenim minimalnim brojem stručnih informatičkih djelatnika. Ovakva reorganizacija odnosi se na kompletan životni ciklus opreme, dakle na sve faze od planiranja i projektiranja, preko financiranja i nabave, upravljanja i održavanja te na kraju rashoda i uništenja opreme.

Nadalje, nužno je u okviru znanstvenog i obrazovnog sustava definirati koncept vlasnika informacijske infrastrukture. Ovdje se primjenjuje potpuna analogija s prethodno opisanim pristupom TDV u Skupini A. Pri tome dio znanstvenih i obrazovnih institucija (to su prvenstveno znanstvene institucije i fakulteti) mogu imati vlastite ustrojstvene jedinice koje su adekvatno popunjene informatičkim stručnjacima i vlasnici su informacijske infrastrukture. Drugi dio institucija su one koje nemaju adekvatne unutarnje ustrojstvene jedinice (to su prvenstveno obrazovne ustanove i neke znanstvene i visokoškolske ustanove) i koje će lokalnu podršku dobivati preko zajedničke infrastrukture od MZOŠ i Srca, odnosno CARNet-a. Pri tome su uloga i međusobni odnos MZOŠ i Srca, odnosno CARNet-a analogni ulozi i odnosu SDUeH i APIS-a opisanom u Skupini A.

Prijedlog o tome koja će tijela biti koncipirana kao vlasnici informacijske infrastrukture donose nadležna tijela, u ovom slučaju SDUeH i MZOŠ, i usklađuju s tijelima i institucijama na koje se odnosi odluka. Koordinaciju i potrebnu reorganizaciju u ovom smislu, s APIS-om, Srcem i CARNet-om također provode SDUeH i MZOŠ.

Skupina B obuhvaća tijela državne vlasti u širem smislu. Kako tu spadaju različiti stupovi državne vlasti te različite razine vlasti i javni sektor, organizacija informacijske sigurnosti ovog segmenta države nužno se provodi donošenjem posebnog zakona. Okvirni zakon o informacijskoj sigurnosti predstavlja, zajedno s nacinalnom strategijom ili politikom informacijske sigurnosti, krovne propise i za skupinu B. Zbog kompleksnosti skupine B, prije razrade propisa informacijske sigurnosti za ovu skupinu, potrebno je provesti detaljnu koordinaciju i usuglašavanje primjene mjera informacijske sigurnosti u okviru različitih stupova vlasti i javnog sektora, a s ciljem usklađenog sigurnosnog pristupa. U okviru toga nužno je prethodno uređenje informacijske sigurnosti skupine A te organiziranje pratećih programa edukacije i razvoja sigurnosne kulture.

Zahtjevi na upravljačka tijela Skupine B postavljeni su uglavnom kroz sigurnosnu politiku EU, ali danas su na ovakav način organizirani sustavi informacijske sigurnosti u gotovo svim razvijenim zemljama svijeta. Uz sve do sada navedene ciljeve, bitan

cilj je zadržati što je moguće veću jednostavnost upravljačkog sustava i što veću sukladnost između Skupina A i B. NSA (Središnje državno sigurnosno tijelo) je uobičajeno krovno ili koordinacijsko tijelo sigurnosnog sustava, te je i za Skupinu B odabran UVNS (Ured Vijeća za nacionalnu sigurnost). NCSA / IA (Središnje tijelo za sigurnost komunikacija) uobičajeno predstavlja tehničko tijelo sigurnosnog sustava, te je i za Skupinu B odabran ZISKZT (Zavod za informacijsku sigurnost i kripto zaštitnu tehnologiju). Za razliku od Skupine A, u Skupini B ulogu SAA (Središnje tijelo za sigurnosne akreditacije) mora imati Akreditacijsko tijelo RH, jer se ovdje radi dijelom o javnom sektoru te su primarni zahtjevi za jedinstvenim sustavom normizacijsko-akreditacijskih procesa države. Zbog važnosti pojedinih TDV s aspekta nacionalne sigurnosti (Hrvatski sabor, Vrhovni sud i sl.), ali i zbog poboljšanja učinkovitosti u procesu sigurnosnih akreditacija, uobičajeno je od strane Akreditacijskog tijela RH, formalno akreditirati lokalne SAA za određena TDV iz Skupine B. Sukladno odabiru SAA za Skupinu A, te nadležnostima tih tijela u RH, u Skupini B lokalni SAA za uži dio državne uprave treba biti ZISKZT. Akreditacijski proces podrazumijeva akreditiranje informacijsko-komunikacijskih procesa na određeni vremenski period (najčešće 2 do 4 godine) te redovito obnavljanje akreditacijskog procesa.

U okviru Skupine B procesi planiranja i implementacije mjera informacijske sigurnosti (CIS Planning & Implementation) te operativnog nadzora (CIS Operating), djelomice su pojednostavljeni zbog manje rigoroznih sigurnosnih zahtjeva za ovu skupinu tijela. Operativni nadzor informacijske sigurnosti (CIS Operating / CISO/LISO), provode centralni i lokalni koordinatori informacijske sigurnosti koji su zaposlenici svakog pojedinog TDV iz skupine B. To vrijedi i za TDV koja nemaju vlastitu IT ustrojstvenu jedinicu već za njih posao obavlja APIS. U slučaju tijela važnih s aspekta nacionalne sigurnosti (Hrvatski sabor, Vrhovni sud i sl.), operativni nadzor mjera informacijske sigurnosti provodi se na način predviđen za Skupinu A i od strane istih tijela te se usklađuje s radom nadležnih koordinatora informacijske sigurnosti u tim tijelima.

Koordinatori informacijske sigurnosti su stručni djelatnici zaposleni u TDV, koji zbog razdvajanja nadležnosti ne smiju biti odgovorni ustrojstvenoj jedinici TDV koja je nadležna za planiranje i implementaciju mjera informacijske sigurnosti, niti SDUeH i APIS-u. Koordinatori informacijske sigurnosti su operativno odgovorni čelniku ili upravi tijela (rang samostalnih koordinatora ili savjetnika za poslove informacijske sigurnosti u TDV), a stručno su odgovorni središnjem državnom tijelu za sigurnost komunikacija (ZISKZT). Organiziranje mreže koordinatora informacijske sigurnosti u nadležnosti je ZISKZT, koji svoje prijedloge usklađuje s tijelima i institucijama u Skupini B. Postoje centralni i lokalni koordinatori informacijske sigurnosti, a razlika je u tome da centralni nadziru rad više funkcionalno povezanih lokalnih i/ili obavljaju poslove nekoliko funkcionalno povezanih lokalnih koordinatora. Zadatak operativnog nadzora je, kao i u Skupini A, nadzor nad tijelima i pravnim osobama koja su propisno akreditirana za rad, pri čemu se prati poštivanje procedura, te planiranje i upravljanje promjenama u sustavu, koje se neminovno događaju u periodu redovnog rada sustava, bilo zbog tehnoloških (npr. promjena poslužiteljske platforme) ili organizacijskih promjena (npr. spajanje nekih odjela u TDV).

Proces planiranja i implementacije metoda i mjera informacijske sigurnosti (CIS Planning & Implementation / ITSOA) i u Skupini B redovito obavlja vlasnik informacijske infrastrukture te u slučaju RH vrijedi pojašnjenje koje je već dano za vlasnike informacijske infrastrukture.

Potrebno je napomenuti da u Skupini B postoje i pravne i fizičke osobe s javnim ovlastima (primjerice javni bilježnici). Sa stanovišta vlasništva podataka i informacijske infrastrukture na njih se ne postavljaju posebni zahtjevi već ih se smatra vlasnicima i podataka i informacijske infrastrukture, koji su dužni poštovati propise informacijske sigurnosti za Skupinu B. Stoga je i proces planiranja i implementacije metoda i mjera informacijske sigurnosti u nadležnosti same pravne osobe. Nadležno akreditacijsko tijelo je Akreditacijsko tijelo RH, a nadležni koordinator informacijske sigurnosti se postavlja u mjerodavnom državnom tijelu, tj. tijelu koje je pravnoj ili fizičkoj osobi dalo javnu ovlast (najčešće centralni koordinator informacijske sigurnosti ili više regionalnih).

5.3 Skupina C

Skupina C sastoji se od privatnog sektora u širem smislu, tj. ovdje pripadaju sve ostale pravne osobe u RH i sva trgovačka društva u RH, neovisno o tipu vlasništva (privatno, državno ili mješovito) ili osnivaču. U Skupinu C u smislu ovog dokumenta pripadaju sve pravne osobe u RH koje nisu obuhvaćene Skupinama A i B.

Kategorije bitne za organizaciju i upravljanje informacijskom sigurnošću u Skupini C prikazane su u Tablici 3:

Tablica 3. Skupina C

Skupina C – Organizacija i upravljanje informacijskom sigurnošću -			
Vlasnici podataka	**Vlasnici informacijske infrastrukture**	**Posebni propisi informacijske sigurnosti**	**Upravljačka tijela**
Pravne osobe / Uprava tvrtke	Pravne osobe / IT ustrojstvena jedinica	Zakon o informacijskoj sigurnosti (okvirni) i Nacionalna strategija ili politika informacijske sigurnosti – Hrvatski sabor **Javno-privatno partnerstvo** s ciljem dogovaranja zajedničke platforme informacijske sigurnosti Organizacijske i funkcionalne politike tvrtki, Procedure i kontrole, Norme, otvoreni standardi, smjernice -Tvrtke	**a) Vlada RH:** • SDUeH • ZISKZT • Min. gospodarstva • Min. financija • NBH • Normizacijsko tijelo RH • Akreditacijsko tijelo RH **b) Privatni sektor:** • HGK, HUP, … • Financijski sektor • Sektor osiguranja • Velike tvrtke u RH **c) Revizorske kuće**

Za Skupinu C ovaj Nacionalni program daje samo inicijalne preporuke za proces javno-privatnog partnerstva kojim bi se trebala sporazumno ugovoriti politika informacijske sigurnosti za ovu najširu skupinu. Unatoč tome, bitni koncepti informacijske sigurnosti trebali bi se i prije ovog procesa uvoditi u javnu kulturu RH od strane TDV.

Odgovornost vlasnika podataka u Skupini C mora biti uvijek jasno definirana i postavljena na upravu tvrtke. Ovakvo postavljanje odgovornosti temelj je svih suvremenih zakonskih akata iz područja korporativnog upravljanja tvrtkama te normi i preporuka za informacijsku sigurnost poslovanja tvrtki. Pri tome, ova odgovornost podrazumijeva rukovodnu odgovornost za uspostavljanje potrebnih procedura informacijske sigurnosti i organizacijsku kontrolu rada i usklađenosti tih procedura. Osim uprave tvrtke, koja predstavlja nositelja odgovornosti za organizaciju informacijske sigurnosti, ovakva organizacija mora unutar tvrtke definirati izvršnu odgovornost rukovodne hijerarhije i svakog djelatnika tvrtke. Odgovornost se uobičajeno procesuira na više pravnih razina. Najčešće se koriste redovni postupci radno-pravnog zakonodavstva (vezano za prava i obveze djelatnika u informacijskoj sigurnosti), zatim gospodarski pravni mehanizmi u okviru sudova časti Hrvatske gospodarske komore i trgovačkih sudova (prava i obaveze poslovnih partnera u suradnji, kršenje odredbi poslovne tajne) te kazneno zakonodavstvo, u slučajevima težih kršenja informacijske sigurnosti pri suradnji državnih i privatnih institucija (sigurnost pristupa trećih strana i vanjska suradnja).

Vlasnici informacijske infrastrukture u Skupini C vode brigu o informacijsko-komunikacijskoj opremi tijekom cjelokupnog životnog ciklusa opreme (planiranje, projektiranje, nabava, opremanje, upravljanje, održavanje, rashod, uništavanje). Pri tome se primjenjuju pozitivni propisi države i pravilnici o poslovanju same tvrtke. Vlasnici informacijske infrastrukture su redovito same tvrtke, odnosno to mogu biti unutarnje ustrojstvene jedinice tehničkog profila s odgovarajućim nadležnostima informacijsko-komunikacijskog karaktera. Odnedavno se počinju javljati potrebe i mogućnosti angažiranja vanjskih tvrtki koje daju uslugu dijela ili kompletne informacijsko-komunikacijske infrastrukture. Ova pojava za sada je uglavnom zabilježena kod malih i srednjih poduzeća, prvenstveno u segmentu infrastrukturne podrške, ali nije značajnije prisutna u segmentu informacijske sigurnosti (samo segmentarno, primjerice područje tehničke zaštita i sl.). Zbog načela razdvajanja nadležnosti, eventualna potpuna vanjska suradnja za jednu tvrtku bi svakako podrazumijevala dvije neovisne vanjske tvrtke za poslove informacijske infrastrukture i poslove informacijske sigurnosti.

Skupina C obuhvaća sve pravne osobe u RH, neovisno o vrsti trgovačkog društva, osnivaču ili vlasništvu. Kako se tu radi o najrazličitijim kombinacijama osnivača i vlasništva (privatno, državno ili mješovito) te o nekim infrastrukturnim poduzećima (telekomunikacije, elektroprivreda, komunalna poduzeća, željeznica, ceste, itd.), koja su u procesu privatizacije ili mogu biti u budućnosti, uobičajeno je primjenjivati sličan tretman kod ovakvih pravnih osoba. To znači da državna uprava, nakon ulaska u proces informacijske sigurnosti državnog sustava (Skupine A i B), treba izaći s idejnim konceptom javno-privatnog partnerstva u informacijskoj sigurnosti. Ovakvo javno-privatno partnerstvo ima za cilj u procesu informacijske sigurnosti aktivirati i sve preostale - nedržavne resurse, na dobrobit svih čimbenika suvremenog

informacijskog društva: građanstva, gospodarstva i državne uprave, ali i u cilju prosperiteta države u cjelini (konkurentnost i imidž države u svijetu).

Cilj javno-privatnog partnerstva je usuglasiti pristup sigurnosnoj politici u Skupini C, dakle između državnog, javnog i privatnog sektora. Rezultat javno-privatnog partnerstva može biti niz formalnih mjera (zakoni, norme, sporazumi i sl.), ali i neformalnih koordiniranih postupanja u različitim sektorima čitavog društva (popularizacija, edukacija, programi, akcije i sl.). Inicijativu javno-privatnog partnerstva treba formirati na temelju iskustva u organizaciji informacijske sigurnosti Skupina A i B te prijedloga nadležnih tijela iz tih Skupina. Ovdje se primarno radi o interesu države da postojeće sigurnosne investicije u gospodarstvu, koje su i kod nas, primjerice u financijskom sektoru, na relativno visokoj razini, sustavno usmjeri na dobrobit svih čimbenika u procesu. Primjer za to je javno-privatno partnerstvo na definiranju skupa organizacijsko-tehničkih protokola i metoda informacijske sigurnosti za gospodarske subjekte, čime se može postići niz dobiti za sve zainteresirane strane, poput olakšica na police osiguranja, učinkovite procedure istražnih i računalno-forenzičkih postupaka, manjeg broja računalnih provala i sl.

Potrebno je naglasiti da se u okviru procesa koji će se provoditi u skupinama A i B predviđa kontinuirana poslovna suradnja državnog i privatnog sektora na poslovima informacijske sigurnosti i informatizacije općenito. Međutim ti procesi su prvenstveno namijenjeni organizaciji državnih i javnih tijela. Poslovi u skupini C su pak zamišljeni kao sveukupno usklađivanje informacijskog društva i poticanje privatnog sektora (onog dijela koji to do tada nije učinio samoinicijativno) na preuzimanje i implementiranje određenih (dogovorenih) standarda informacijske sigurnosti.

Zahtjevi na upravljačka tijela Skupine C postavljeni su temeljem prakse pristupa ovom području u EU i SAD-u, što je danas način postupanja u okviru informacijske sigurnosti javnog i privatnog sektora u svim razvijenim zemljama svijeta. Cilj je organizaciju informacijske sigurnosti u RH učiniti sukladnom suvremenim zemljama svijeta te istovremeno i u što većoj mjeri koristiti uloženu investiciju u informacijsku sigurnost unutar pojedinih Skupina A, B i C. U tom smislu relevantni čimbenici s državne strane moraju osim nadležnih tijela iz Skupina A i B (prvenstveno SDUeH i ZISKZT) biti i ključna ministarstva (npr. Ministarstvo gospodarstva, rada i poduzetništva i Ministarstvo financija) te druge institucije važne za procese u Skupini C (Normizacijsko i Akreditacijsko tijelo RH te NBH). Vlada RH mora, institucionalno, biti nositelj aktivnosti. Privatni sektor trebaju predstavljati Hrvatska gospodarska komora i udruge poslodavaca, ali je nužno uključiti i najpropulzivnije gospodarske sektore u smislu informacijske sigurnosti (financijski sektor, sektor osiguranja, skupinu najvećih tvrtki u RH). Ključni čimbenik koji u poslovnom sektoru omogućava ekonomsko opravdanje investicija u informacijsku sigurnost su revizorske tvrtke, odnosno sve one koje obavljaju poslove IT revizije u RH (npr. u sklopu upravljanja rizikom i određivanja boniteta tvrtki na tržištu) i koje svakako treba uključiti u proces organizacije informacijske sigurnosti u RH.

6 SIGURNOSNA POLITIKA

Sigurnosna politika je hijerarhijski strukturiran skup dokumenta informacijske sigurnosti koji predstavlja temelj za implementaciju sustava informacijske sigurnosti. Općenito, dokumente sigurnosne politike možemo podijeliti na krovne, provedbene i izvršne te norme i preporuke.

Sigurnosnom politikom osigurava se uvođenje ponajprije minimalnih, a zatim i potrebnih sigurnosnih kriterija. Za Skupinu A, to je i jedan od temeljnih zahtjeva integracijskih procesa NATO-a i EU. U okviru sigurnosne politike tijela Skupine B i C, koristi se samo manji dio nacionalnog zakonodavnog okvira propisanog za Skupinu A, a u većoj mjeri se oslanja na svjetski priznate organizacijske i sigurnosne norme (npr. ISO 17799) te svjetska iskustva u javno-privatnim partnerstvima u području informacijske sigurnosti.

Krovni propisi

U ovu vrstu propisa spadaju zakoni, strategije ili politike kojima se informacijska sigurnost razmatra na općenitoj razini ne ulazeći u detalje njezine implementacije. Krovni propisi sadrže definiciju informacijske sigurnosti, njene opće ciljeve i razmjere i nije im svrha opisivanje stanja već donošenje odluka o potpori ciljevima informacijske sigurnosti. Krovni propisi moraju biti precizni i jasni te uravnoteženi između funkcionalnosti i sigurnosti. S ovim propisima trebaju biti upoznati svi na koje se odnose. Krovni propisi, između ostalog, podrazumijevaju i definiranje odgovornosti za upravljanje i provođenje informacijske sigurnosti.

Ako informacijsku sigurnost razmatramo na nacionalnoj razini, zajednički krovni dokument informacijske sigurnosti trebalo bi definirati zakonom. Takav bi okvirni zakon trebao jasno razgraničiti podjelu nadležnosti i djelatnosti upravljačkih tijela skupine A, B i C u sustavu informacijske sigurnosti. Prateći krovni dokument okvirnog zakona o informacijskoj sigurnosti trebala bi biti i nacionalna strategija ili politika informacijske sigurnosti koja definira osnovna sigurnosna načela, područja i dosege primjene, te izražava potporu najviše državne vlasti u provedbi informacijske sigurnosti u RH. U skupini C, osim navedenih krovnih propisa postoje i krovni propisi sigurnosne politike koje donosi uprava tvrtke.

Provedbeni propisi

Provedbeni propisi nastavak su razrade krovnih propisa na pojedina sigurnosna područja poput sigurnosne provjere osoblja, fizičke sigurnosti, sigurnosti podataka i INFOSEC-a, te daljnja razrada ovih sigurnosnih područja na organizacijsko tehničke specifikacije kojima se propisuju metode upravljanja sigurnošću u pojedinim područjima i razrađuju formalni postupci procjene rizika, certifikacije osoblja i uređaja te akreditacije.

Kad govorimo o Skupini A i Skupini B, provedbeni propisi su uredbe koje donosi Vlada RH na prijedlog središnjih državnih sigurnosnih tijela – UVNS i ZISKZT, kao nositelja izrade propisa, u suradnji s ostalim tijelima sigurnosnog sustava u širem smislu: POA, OA, VSA, MUP i MORH.

U provedbene propise Skupine A i skupine B spadaju i pravilnici koji uredbe razrađuju na organizacijsko tehničke specifikacije. Pravilnicima se vrši razrada pojedinih elementa sustava i daju opće organizacijsko tehničke smjernice. Pravilnike donose središnja državna sigurnosna tijela – UVNS i ZISKZT, u suradnji s ostalim tijelima sigurnosnog sustava u širem smislu: POA, OA, VSA, MUP i MORH.

TDV iz Skupine A i skupine B koja imaju specifične sigurnosne potrebe (npr. MUP, MORH, sigurnosne službe), više od minimalnih sigurnosnih kriterija propisanih na nacionalnoj razini, mogu umjesto provedbe nacionalnih pravilnika koji definiraju minimalne sigurnosne kriterije, izraditi i predložiti vlastite pravilnike. U tom slučaju suglasnost na primjenu takvih pravilnika daju UVNS (NSA) i ZISKZT (NCSA). Suglasnost se daje nakon utvrđivanja da predloženi pravilnik određenog tijela zadovoljava minimalne sigurnosne kriterije postavljene na nacionalnom nivou. Naputke o provedbi Pravilnika izrađuje svako TDV za sebe (vlasnik infrastrukture) i u slučaju primjene nacionalnog pravilnika, kao i u slučaju primjene vlastitog pravilnika

U provedbene propise Skupine C spadaju općenite organizacijske politike kao analogija uredbama, odnosno funkcionalne politike kao analogija pravilnicima. Provedbene propise Skupine C donosi uprava tvrtke na prijedlog sigurnosnog menađžmenta tvrtke.

Izvršni propisi

Izvršni propisi predstavljaju razradu provedbenih propisa i to u vidu naputaka koje kao posljednje u lancu egzaktno opisuju način na koji je potrebno implementirati postojeće pravilnike i funkcionalne politike. Donošenje naputaka u Skupinama A, B i C u nadležnosti je samih tijela, odnosno pojedinih segmenata tog tijela (npr. IT odjel ili vanjsko tijelo - APIS) i provodi se kroz njihovu međusobnu koordinaciju sa središnjim državnim sigurnosnim tijelom (NSA) UVNS i središnjim tijelom za sigurnost komunikacija (NCSA) ZISKZT u RH. Uobičajeno vrijedi da je izrada naputaka vezanih uz tehnologiju u nadležnosti IT struktura, izrada naputaka vezanih uz procese i organizaciju u nadležnosti upravljačkih struktura, a izrada naputaka vezanih uz osoblje u nadležnosti struktura za upravljanje ljudskim potencijalima.

Prilikom izrade ovih naputaka koriste se zadani elementi sigurnosne politike i provedbenih akata, raspoložive preporuke i tzv. metode najbolje prakse u pojedinom organizacijskom ili tehničkom procesu.

Norme

Norma je dokument odobren od mjerodavnog tijela koji za opću i višekratnu uporabu daje pravila, upute ili značajke za aktivnosti i njihove rezultate te jamči najbolji stupanj uređenosti u danim uvjetima.

Kad govorimo o informacijskoj sigurnosti, norme predstavljaju rješenje zajedničkih potreba gospodarstva za jedinstvenim sustavom upravljanja sigurnošću informacija. Poslovanje u skladu s normom (standardom) omogućava sigurno upravljanje informacijskom sigurnošću i stvara povjerenje u međuorganizacijskom poslovanju. Ovakve poslovne norme mogu postati i nacionalne norme. U tom smislu državna uprava u koordinaciji s privatnim sektorom treba pokrenuti inicijativu za usvajanje i

primjenu međunarodnih organizacijsko-tehničkih normi informacijske sigurnosti kroz nacionalne normizacijske procese. Da bi opće tehničke i sigurnosne norme, prihvaćene u okviru nacionalnih normizacijskih procesa, postale dijelom sigurnosne politike, moraju biti utvrđene odnosnom vertikalom propisa unutar Skupine A, B ili C na koju se odnose.

Preporuke

Preporuke definiraju preporučene načine zaštite sustava. Implementacija mjera definiranih preporukama poželjna je, no ne i nužna, što preporuke čini fleksibilnim elementom u primjeni sigurnosne politike. Preporuke se najčešće koriste na onim mjestima gdje sigurnost nije moguće, nije potrebno ili nije poželjno strogo definirati.

6.1 Skupina A

Sigurnosna politika koja se odnosi na tijela Skupine A sastoji se od okvirnog zakona o informacijskoj sigurnosti i nacionalne strategije ili politike informacijske sigurnosti, te niza provedbenih uredbi koje su dalje razrađene pravilnicima i detaljnim procedurama. Okvirni zakon o informacijskoj sigurnosti treba odrediti nadležnosti i djelatnosti upravljačkih tijela u sustavu informacijske sigurnosti. Krovne dokumente nacionalne politike informacijske sigurnosti donosi Hrvatski sabor i njima se izražava odlučnost u potpori ciljevima informacijske sigurnosti. Takvi su dokumenti nužni jer ujednačuju sigurnosno postupanje od strane različitih državnih tijela s ciljem uvođenja minimalnih sigurnosnih kriterija jedne države. On pokreće regulacijski proces izrade provedbenih akata, tzv. uredbi koje donosi Vlada RH a koji obvezuju sva tijela Skupine A, te čine temelj kasnijeg niza inicijativa koje se odnose na tijela iz Skupina B i C odnosno države u cjelini. Prilikom donošenja nacionalne politike informacijske sigurnosti, a napose prilikom izrade provedbenih uredbi, potrebno je provjeriti da li postojeći zakonodavni instituti na odgovarajući način definiraju sve potrebne ovlasti pojedinih tijela u sustavu informacijske sigurnosti, te prema potrebi provesti nužne korekcije postojećih zakona ili izradu novih zakona (primjerice područje sigurnosnih provjera).

Razrada provedbenih uredbi vrši se kroz organizacijsko tehničke smjernice u vidu obvezujućih pravilnika koje donose tijela sigurnosnog sustava sukladno zakonski propisanim nadležnostima (nacionalni pravilnici) ili pravilnika koje donose sama tijela (vlastiti pravilnici), i egzaktnih naputaka usklađenih s odnosnom vertikalom propisa, koje donose sama tijela, odnosno SDUeH/APIS za tijela koja ne posjeduju IT osoblje.

Na tijela iz Skupine A mogu se primjenjivati i važeće norme u RH, ali isključivo ako su prethodno utvrđene u nekoj od razina hijerarhije nacionalne sigurnosne politike.

Propisi informacijske sigurnosti koji se odnose na tijela Skupine A, s pripadajućim nadležnostima za njihovo donošenje, prikazani su u Tablici 4.:

Tablica 4. Skupina A – propisi i nadležnost donošenja

Skupina A **- Propisi i nadležnost donošenja -**

PROPISI		NADLEŽNOST DONOŠENJA
I krovni	**ZAKONI** Zakon o informacijskoj sigurnosti **STRATEGIJE** Nacionalna strategija ili politika informacijske sigurnosti	**Hrvatski sabor** na prijedlog Vlade RH nositelj izrade UVNS (NSA) i ZISKZT (NCSA), uz suradnju, POA, OA, VSA, MUP, MORH, SDUeH
II provedbeni	**UREDBE** zajednički obvezujući provedbeni dokumenti sigurnosne politike	**Vlada RH** na prijedlog središnjih državnih sigurnosnih tijela – UVNS i ZISKZT, uz suradnju POA, OA, VSA, MUP, MORH, SDUeH
	NACIONALNI PRAVILNICI zajedničke obvezujuće organizacijsko-tehničke smjernice	**Središnja državna sigurnosna tijela – UVNS i ZISKZT,** uz suradnju POA, OA, VSA, MUP, MORH
	VLASTITI PRAVILNICI specifične obvezujuće organizacijsko-tehničke smjernice za pojedino tijelo kao proširenje kriterija zahtijevanih nacionalnim pravilnicima	**Pojedina tijela za sebe** suglasnost na primjenu vlastitih pravilnika daju UVNS (NSA) i ZISKZT (NCSA)
III izvršni	**NAPUTCI** detaljne i specifične upute za rad, usklađene sa odnosnom vertikalom propisa	**Svako pojedino tijelo za sebe** (SDUeH/APIS za tijela bez IT osoblja), prema potrebi u suradnji s nadležnim tijelima sigurnosnog sustava
IV norme i preporuke	**NORME** opće tehničke i sigurnosne norme prihvaćene u okviru nacionalnih normizacijskih procesa i otvoreni standardi, sve utvrđeno odnosnom vertikalom propisa	**Tijelo za normizaciju** HZN u suradnji sa ZISKZT (NCSA), SDUeH
	PREPORUKE preporuke i tzv. metode najbolje prakse, usklađene odnosnom vertikalom propisa	UVNS (NSA), ZISKZT (NCSA), Središnji državni CERT, APIS (CIS Planning & Implementation / ITSOA)

6.2 Skupina B

Obzirom na usku povezanost Skupina A i B, Nacionalni program predviđa sličan zakonodavni i instuticionalni okvir za donošenje propisa informacijske sigurnosti ovih dviju skupina. Osnovna razlika Skupine A i B vidljiva je u sadržaju akata i u provedbenom segmentu informacijske sigurnosti gdje postoje različita upravljačka tijela za sigurnosne akreditacije i nadzor operativnosti mjera (5 poglavlje).

U Skupini B manje su izraženi posebni zahtjevi informacijske sigurnosti (NATO, EU), a naglasak se stavlja na primjenu općih zahtjeva informacijske sigurnosti (međunarodne tehničke i sigurnosne norme te metode najbolje prakse). Programi informacijske sigurnosti za tijela Skupine B temelje se stoga na međunarodnim tehničkim i sigurnosnim normama te sadrže neke uže dijelove nacionalnih propisa informacijske sigurnosti za tijela Skupine A. Zbog primjene na tijela u različitim stupovima i razinama vlasti u državi, programi informacijske sigurnosti za tijela u Skupini B sadržajno se razlikuju od programa Skupine A.

Propisi informacijske sigurnosti koji se odnose na tijela Skupine B, s pripadajućim nadležnostima za njihovo donošenje, prikazani su u Tablici 5.:

Tablica 5. Skupina B – propisi i nadležnost donošenja

Skupina B - Propisi i nadležnost donošenja -		
PROPISI		**NADLEŽNOST DONOŽENJA**
I krovni	**ZAKONI** Zakon o informacijskoj sigurnosti **STRATEGIJE** Nacionalna strategija ili politika informacijske sigurnosti	**Hrvatski sabor** na prijedlog Vlade RH nositelj izrade UVNS (NSA) i ZISKZT (NCSA), uz suradnju, POA, OA, VSA, MUP, MORH, SDUeH
II provedbeni	**UREDBE** zajednički obvezujući provedbeni dokumenti sigurnosne politike	**Vlada RH** na prijedlog središnjih državnih sigurnosnih tijela – UVNS i ZISKZT, uz suradnju POA, OA, VSA, MUP, MORH, SDUeH
	NACIONALNI PRAVILNICI zajedničke obvezujuće organizacijsko-tehničke smjernice	**Središnja državna sigurnosna tijela – UVNS i ZISKZT,** uz suradnju POA, OA, VSA, MUP, MORH
	VLASTITI PRAVILNICI specifične obvezujuće organizacijsko-tehničke smjernice za pojedino tijelo kao proširenje kriterija zahtijevanih nacionalnim pravilnicima	**Pojedina tijela za sebe** suglasnost na primjenu vlastitih pravilnika daju UVNS (NSA) i ZISKZT (NCSA)
III izvršni	**NAPUTCI** detaljne i specifične upute za rad, usklađene sa odnosnom vertikalom propisa	**Svako pojedino tijelo za sebe** (SDUeH/APIS za tijela bez IT osoblja), prema potrebi u suradnji s nadležnim tijelima sigurnosnog sustava

Skupina B - Propisi i nadležnost donošenja -		
PROPISI		**NADLEŽNOST DONOŽENJA**
IV norme i preporuke	**NORME** opće tehničke i sigurnosne norme prihvaćene u okviru nacionalnih normizacijskih procesa i otvoreni standardi, sve utvrđeno odnosnom vertikalom propisa	**Tijelo za normizaciju** HZN u suradnji sa UVNS (NSA), SDUeH, ZISKZT
	PREPORUKE preporuke i tzv. metode najbolje prakse, usklađene odnosnom vertikalom propisa	UVNS (NSA) ZISKZT (NCSA) Središnji državni CERT, APIS (CIS Planning & Implementation / ITSOA)

6.3 Skupina C

Na Skupinu C se uobičajeno utječe kroz norme te otvorene standarde prihvaćene u okviru nacionalnih, ali i međunarodnih normizacijskih procesa. Isto tako, uobičajeno je od strane države vršiti utjecaj na organizaciju i provođenje informacijske sigurnosti kroz određene oblike javno-privatnog partnerstva i traženja zajedničkih ciljeva države i privatnih tvrtki čime se postiže ujednačavanje razine informacijske sigurnosti između Skupina A, B i C, odnosno gospodarstva u cjelini. Na obaveze i nadležnosti po pitanju informacijke sigurnosti unutar skupine C država može utjecati i donošenjem okvirnog zakona o informacijskoj sigurnosti, te kroz nacionalnu strategiju ili politiku informacijske sigurnosti.

Dokumenti sigurnosne politike koji se odnose na privatni sektor su: krovni dokumenti sigurnosne politike (zakonski okviri i nacionalna strategija, sigurnosna politika uprave tvrtke), detaljne sigurnosne politike (opće organizacijske i funkcionalne politike) te procedure. Osnovni element politike je odluka koju donosi uprava, a kojom se izražava odlučnost uprave u potpori ciljevima informacijske sigurnosti.

Propisi informacijske sigurnosti koji se odnose na Skupinu C, s pripadajućim nadležnostima za njihovo donošenje, prikazani su u Tablici 6.:

Tablica 6. Skupina C – propisi i nadležnost donošenja

Skupina C - Propisi i nadležnost donošenja -		
PROPISI		**NADLEŽNOST DONOŠENJA**
O sporazumni	**JAVNO-PRIVATNO PARTNERSTVO**	**Vlada RH** inicira prema privatnom sektoru

Skupina C - Propisi i nadležnost donošenja -		
PROPISI		**NADLEŽNOST DONOŠENJA**
I krovni	**ZAKONI** Zakon o informacijskoj sigurnosti **STRATEGIJE** Nacionalna strategija ili politika informacijske sigurnosti	**Hrvatski sabor** na prijedlog Vlade RH nositelj izrade UVNS (NSA) i ZISKZT (NCSA), uz suradnju, POA, OA, VSA, MUP, MORH, SDUeH
	SIGURNOSNA POLITIKA krovni dokument sigurnosne politike tvrtke	**Uprava tvrtke** na prijedlog sigurnosnog menađžmenta
II provedbeni	**OPĆE ORGANIZACIJSKE I FUNKCIONALNE POLITIKE** organizacijsko tehničke smjernice	**Uprava tvrtke** na prijedlog sigurnosnog menađžmenta
III izvršni	**PROCEDURE** detaljne i specifične upute za rad, usklađene sa odnosnom vertikalom propisa	**Tvrtka** odjeli tvrtke
IV norme i preporuke	**NORME** opće tehničke i sigurnosne norme i otvoreni standardi prihvaćeni u okviru nacionalnih i svjetskih normizacijskih procesa koje su utvrđene odnosnom vertikalom propisa	**Tijelo za normizaciju** HZN u suradnji s predstavnicima vlasti i privatnog sektora
	PREPORUKE preporuke i tzv. metode najbolje prakse, usklađene odnosnom vertikalom propisa	UVNS (NSA) ZISKZT (NCSA) Središnji državni CERT, IT Privatnog sektora, Revizorske kuće

7 EDUKACIJA I RAZVOJ SIGURNOSNE KULTURE

Povoljna društvena klima temeljena na transparentnom protoku informacija ključna je za razvoj sigurnosne kulture u društvu. Sigurnosni standardi nisu tajna već temeljni zahtjev svakog radnog mjesta «od portira do predsjednika uprave» u tvrtki te «od građanina do predsjednika» u državi. Bez sigurnosne kulture nemoguće je provesti razvoj informacijskog društva. Potrebno je uvesti i stalno razvijati formalne informatičke obrazovne programe, od osnovnog, preko srednjeg pa do visokog školstva te obrazovnih programa prilagođenih za državnu upravu. Takvi informatički programi moraju sadržavati elemente sigurnosne kulture suvremenog informacijskog društva. Uz to, nužno je stalno djelovati prema širokim društvenim skupinama, kroz različite oblike publikacija, javnih tribina i sl. Pristup problemima informacijske sigurnosti mora biti integralni dio pristupa popularizaciji informatizacije i Interneta, odnosno informacijskog društva u cjelini.

7.1 Razvoj sigurnosne kulture

Kako je za zaštitu informacija bitna svaka osoba koja s njom odlazi u kontakt, svjesnost od mogućnosti zloupotrebe informacija te informiranost o postupcima i sredstvima zaštite ključna je za informacijsku sigurnost. Stoga je razvoj svijesti i informiranosti jednako važan kao i uvođenje samih mjera ili sredstava zaštite.

7.2 Skupine kojima treba razvijati sigurnosnu kulturu

Svijest o informacijskoj sigurnosti mora biti prisutna kod svakog građanina. No, prema njihovoj ulozi u korištenju, stvaranju i rukovanju informacijama te prema tipu informacija, razina i opseg potrebne svjesnosti se razlikuju. Stoga je potrebno definirati osnovne skupine na koje treba djelovati.

Građani

Svi građani moraju razumjeti kako informacija koju oni mogu koristiti nastaje, mijenja se, obrađuje, razmjenjuje i pohranjuje. Također moraju biti informirani kojim vlastitim postupcima ugrožavaju sigurnost informacija i koji su glavni izvori opasnosti za sigurnost informacija.

Rukovatelji informacijama

Rukovatelji informacijama u domeni svoje nadležnosti moraju dodatno biti svjesni i svoje osobne odgovornosti za tuđe informacije, mogućih grešaka koje mogu prouzročiti rukovanjem informacijama i načina na koji mogu svojim djelovanjem ugroziti njihovu sigurnost.

Državni službenici i namještenici

Svi državni službenici i namještenici su, u pravilu, rukovatelji određenim informacijama, koje su od posebne važnosti za građane. Stoga je i njihova odgovornost veća, te i razvoj svijesti treba biti usklađen s takvom odgovornošću i značajem informacija.

Dužnosnici i rukovoditelji u državnim tijelima

Rukovodna, strateška i nacionalna odgovornost treba biti u središtu aktivnosti za razvoj svijesti rukovoditelja i dužnosnika. Uz ovu kategoriju je najčešće vezan i pojam vlasnika podataka, dakle najodgovornijih osoba za određeni skup podataka. Pri strateškom planiranju, predlaganju i donošenju zakona i propisa, ulaganju u infrastrukturu i razvoj, posebna je odgovornost za planiranje i provođenje informacijske sigurnosti. Kao što se pri donošenju zakona mora voditi računa o njihovoj ekonomskoj utemeljenosti i provedivosti, tako se mora voditi računa i o nacionalnoj informacijskoj infrastrukturi i sigurnosti informacija.

7.3 Nadležni za razvoj sigurnosne kulture

Temeljni postulat jest da je pravo i dužnost svakog građanina da djeluje na razvoj svijesti o informacijskoj sigurnosti u svojoj okolini. Međutim, neka tijela imaju i specifične nadležnosti i obveze.

Nositelj planiranja programa razvoja sigurnosne kulture za sve skupine je UVNS (u svojstvu NSA) a suradnici u tom postupku su ZISKZT i Središnji državni CERT.

Nositelj provedbe programa razvoja sigurnosne kulture za građane i rukovatelje informacijama u RH je Središnji državni CERT, a za skupine državnih službenika i namještenika, te dužnosnika i rukovoditelja u državnim tijelima nositelji provedbe su UVNS i ZISKZT. To je sažeto prikazano u Tablici 7. s vremenskim rokovima izrade programa.

Tablica 7.

<table>
<tr><th></th><th>Skupine za razvoj sigurnosne kulture</th><th>Nositelji planiranja</th><th>Nositelji provedbe</th><th>Vremenski rokovi izrade programa</th></tr>
<tr><td>1.</td><td>Građani</td><td rowspan="4">Nositelj je UVNS (NSA), a suradnici su ZISKZT (NCSA) i Središnji državni CERT</td><td rowspan="2">Središnji državni CERT</td><td>2. kvartal 2007. g.</td></tr>
<tr><td>2.</td><td>Rukovatelji informacijama u RH</td><td>4. kvartal 2006. g.</td></tr>
<tr><td>3.</td><td>Državni službenici i namještenici</td><td rowspan="2">UVNS (NSA) i ZISKZT (NCSA)</td><td>2. kvartal 2006. g.</td></tr>
<tr><td>4.</td><td>Dužnosnici i rukovoditelji u državnim tijelima</td><td>4. kvartal 2005. g.</td></tr>
</table>

7.4 Programi edukacije

U RH ne postoje specijalizirane škole ili smjerovi za obuku stručnjaka za informacijsku sigurnost. Nema niti sustavne organizacije tečajeva ili drugih oblika cjeloživotnog obrazovanja. U RH ne postoji ni nacionalna udruga stručnjaka za informacijsku sigurnost. Stoga je nužno potaknuti osnivanje stručne udruge na nacionalnoj razini, uvođenje sustavnog obrazovanja stručnjaka te uvrštavanje tema iz informacijske sigurnosti u redovne školske programe.

Informatičko obrazovanje i sigurnosna kultura

Za uspješnost u društvu znanja ključno je informatičko obrazovanje cjelokupnog stanovništva. Prije svega treba osigurati da obrazovni sustav uvrsti potrebne sadržaje, ali i osigurati obrazovanje za stanovništvo koje je završilo svoj formalni obrazovni ciklus, najbolje putem tehnologije e-learninga.

Na sve razine obrazovanja od predškolskih programa do sveučilišnih studija, potrebno je propisati primjereno informatičko obrazovanje ujednačeno na nacionalnoj razini. Ono svakako mora sadržavati adekvatne teme iz područja informacijske sigurnosti. Potrebno je potaknuti sustav visokog školstva za uvođenje odgovarajućih dodiplomskih programa iz područja informacijske sigurnosti. Poticaj treba napraviti kroz pokretanje stručnih i znanstvenih poslijediplomskih studija u području informacijske sigurnosti.

e-Obrazovanje

Građani koji su završili tradicionalno obrazovanje trebaju imati mogućnost stjecanja potrebnog informacijskog obrazovanja i ovladavanja informacijskom sigurnosti. Kako se radi o potencijalno velikom broju građana, vrlo širokog spektra znanja i sposobnosti, taj se zadatak može riješiti jedino korištenjem novih obrazovnih tehnologija koje omogućavaju učeniku da bira mjesto, vrijeme i način obrazovanja, kao i njegov opseg i dubinu. Te se tehnologije danas nazivaju e-Obrazovanje.

Državni stručni ispit

U program državnog stručnog ispita, koji polažu državni službenici i namještenici treba uvrstiti sadržaje informatičkog obrazovanja koji moraju sadržavati i teme iz informacijske sigurnosti. Pored provjere znanja, potrebno je osigurati i kvalitetno obrazovanje. Obvezni seminari iz područja informacijske sigurnosti moraju se uvesti i za državne dužnosnike.

Obrazovanje informatičara u TDV

Za informatičare zaposlene u TDV potrebno je organizirati trajno informatičko obrazovanje s naglaskom na područje informacijske sigurnosti.

7.4.1 Nositelji planiranja informatičkog obrazovanja i sigurnosne kulture

Za sve razine formalnog obrazovanja, od osnovnog do visokoškolskog, nositelj neformalnih aktivnosti u okviru postojećih obrazovnih programa, putem predavanja i radionica, bi trebao biti MZOŠ do kraja 2006. godine. Zavod za školstvo bi bio nositelj buduće revizije obrazovnih programa. Formalni programi trebali bi se donijeti do kraja 2008. godine.

SDUeH bi trebao biti nositelj planiranja informatičkog obrazovanja i sigurnosne kulture za dužnosnike, službenike, službene i vojne osobe, te informatičare u državnim institucijama do kraja 2006. godine, kao i za planiranje adekvatnog e-Obrazovanja do kraja 2007. godine.

7.4.2 Nositelji provedbe plana informatičkog obrazovanja i sigurnosne kulture

Za sve razine formalnog obrazovanja, neformalne aktivnosti bi trebala provesti upravljačka tijela u sustavu informacijske sigurnosti, UVNS, ZISKZT, MZOŠ, CARNet, SDUeH i APIS. Formalne visokoškolske dodiplomske i poslijediplomske aktivnosti trebale bi se provesti putem MZOŠ-a, kroz postojeća i buduća iskustva ostvarena preko Fakulteta računarstva i elektrotehnike (FER) i ostale visokoškolske ustanove. Ostale formalne obrazovne aktivnosti u osnovnim, srednjim i visokim školama, išle bi kroz redovne izmjene programa i provedbu novih programa u tim institucijama.

Za dužnosnike, službenike, službene i vojne osobe u TDV nositelji provedbe bili bi SDUU, UVNS, ZISKZT, Središnji državni CERT, te Policijska akademija i Zapovjedništvo za združenu izobrazbu i obuku Ministarstva obrane RH. Za informatičare u državnim službama nositelji provedbe bi bili APIS i ZISKZT. Za provedbu e-learninga nositelj provedbe bi bio APIS.

7.5 Istraživanja

U okviru znanstvenog djelovanja na području informacijske i komunikacijske tehnologije, potrebno je pokrenuti i poticati kategorije projekata i istraživanja na području informacijske sigurnosti (ZISKZT, SDUeH, MZOŠ, MUP - Policijska akademija, MORH – Zapovjedništvo za združenu izobrazbu i obuku).

Tijela nadležna za informacijsku sigurnost u RH trebala bi međusobnim dogovorom napraviti godišnji i višegodišnji program poticanih istraživanja u RH u području informacijske sigurnosti. MZOŠ je nadležan za planiranje proračuna i ugovaranje pojedinih konkretnih projekata.

Tablica 8.

	Informatičko obrazovanje i sigurnosna kultura	**Nositelji planiranja**	**Nositelji provedbe**	**Vremenski rokovi izrade kataloga znanja**
1.	Osnovno obrazovanje	MZOŠ – nositelj neformalnih aktivnosti u okviru postojećih obrazovnih programa (predavanja i radionice) Zavod za školstvo – nositelj buduće revizije obrazovnih programa	Neformalne aktivnosti - Upravljačka tijela u sustavu inf. sig. UVNS, ZISKZT, MZOŠ/CARNet, SDUeH/APIS Formalne visokoškolske dodiplomske i poslijediplomske aktivnosti – MZOŠ/FER	Neformalne aktivnosti do kraja 2006. g. Formalni programi do kraja 2008. g.
2.	Srednje obrazovanje			
3.	Visoko obrazovanje			

	Informatičko obrazovanje i sigurnosna kultura	**Nositelji planiranja**	**Nositelji provedbe**	**Vremenski rokovi izrade kataloga znanja**
4.	Dužnosnici službenici, službene i vojne osobe	SDUeH	SDUU, UVNS, ZISKZT, Središnji državni CERT, Policijska akademija, Zapovjedništvo za združenu izobrazbu i obuku MORH-a	Do kraja 2006. g.
5.	Informatičari u državnim institucijama		APIS, ZISKZT	Do kraja 2006. g.
6.	e-Obrazovanje		APIS	Do kraja 2007. g.

8 PROVEDBA NACIONALNOG PROGRAMA INFORMACIJSKE SIGURNOSTI U RH

Potrebno je razraditi predradnje i faze provedbe Nacionalnog programa informacijske sigurnosti u RH te predvidjeti odgovarajuće metode praćenja provedbe Nacionalnog programa. U tu svrhu praćenje će biti organizirano kroz posebnu stručnu skupinu koja će na kvartalnoj i godišnjoj razini procjenjivati provedbu Nacionalnog programa, dok će državna tijela, koja sukladno Nacionalnom programu preuzimaju središnju državnu ulogu u informacijskoj sigurnosti, procjenjivati dnevnu provedbu Nacionalnog programa. U fazi početnih predradnji, tijekom 2005. g., ocjena provedbe će se temeljiti na provedbi pojedinih elemenata Nacionalnog programa. Postupnim uvođenjem posebne regulative informacijske sigurnosti, počevši od 2006. g., potrebno je primijeniti formalne procedure i metode ocjenjivanja, koje će se temeljiti na provedbi podjele nadležnosti i primjeni modela funkcionalnosti sukladno Nacionalnom programu i donesenoj posebnoj regulativi informacijske sigurnosti.

8.1 Faze provedbe

Faze provedbe Nacionalnog programa podrazumijevaju izradu i primjenu metoda i mjera informacijske sigurnosti na skupine tijela i pravnih osoba koje su definirane u Nacionalnom programu: Skupine A, B i C. Kako bi se Nacionalni program uopće mogao provoditi potrebno je izvršiti određene predradnje, koje će biti posebno istaknute jer predstavljaju preduvjet izvođenja faza.

8.1.1 Predradnje

Predradnje mogu započeti nakon prihvaćanja Nacionalnog programa informacijske sigurnosti od strane Vlade RH. Sastoje se od slijedećih poslova:

- Formiranje nove stručne skupine za praćenje provedbe Nacionalnog programa informacijske sigurnosti u RH, na temelju postojeće SSZIS. Nositelj je SDUeH, sudionici SSZIS, UVNS (NSA), ZISKZT (NCSA i SAA), POA, OA i VSA (CIS Operating), MORH, MUP, MF, MVPEI, APIS, MZOŠ, CARNet (CIS Planning and Implementation), Središnji državni CERT. Rok za osnivanje je travanj 2005. g.
- Donošenje okvirnog zakona o informacijskoj sigurnosti. Nositelj je UVNS u suradnji sa ZISKZT, sudionici SSZIS, SDUeH. Rok je drugi kvartal 2005. g.
- Izmjene Zakona o sigurnosnim službama RH u dijelu koji definira nadležnosti u području informacijske sigurnosti (UVNS, ZISKZT, sigurnosne službe). Nositelj je UVNS u suradnji sa ZISKZT i sigurnosnim službama. Rok je drugi kvartal 2005. g.
- Upućivanje Vladi RH osnivačkih akata Zavoda za informacijsku sigurnost i kriptozaštitnu tehnologiju (ZISKZT) usklađenih s Nacionalnim programom informacijske sigurnosti, te imenovanje ravnatelja Zavoda. Nositelj je UVNS i Stručni tim za postupak osnivanja Zavoda, sudionici sigurnosne službe i SDUeH. Rok je drugi kvartal 2005. g.
- Početak rada Zavoda za informacijsku sigurnost i kriptozaštitnu tehnologiju (ZISKZT). Nositelj je ravnatelj Zavoda. Rok je treći kvartal 2005. g.
- Osnivanje Agencije za potporu informacijskih sustava (APIS). Nositelj je SDUeH, sudionici FINA i TDV koja će koristiti usluge. Rok je treći kvartal 2005. g.

- Osnivanje Središnjeg državnog tijela za računalne incidente (Središnji državni CERT). Nositelj je CARNet u suradnji sa Srcem, sudionici SDUeH, MZOŠ, ZISKZT. Rok je treći kvartal 2005. g.
- Izmjene Zakona o zaštiti tajnosti podataka. Nositelj je UVNS, sudionici ZISKZT, sigurnosne službe, MORH, MUP i Državno odvjetništvo. Rok je treći kvartal 2005. g.
- Usklađivanje propisa o uredskom poslovanju s propisima informacijske sigurnosti. Nositelj je SDUU, sudionici su SDUeH, UVNS, ZISKZT i sigurnosne službe. Rok je četvrti kvartal 2005. g.
- Revizija Zakona o izmjenama i dopunama Zakona o matičnom broju. Nositelj je MUP u suradnji sa SDUeH, MP i SDUU. Rok je četvrti kvartal 2005. g.
- Usmjeravanje Projekta RKMTDU sa sigurnosnog aspekta. Nositelj ZISKZT, a sudionici SDUeH i MZOŠ. Rok je četvrti kvartal 2005. g.

8.1.2 Faza 1.

Prva faza može započeti nakon realizacije nužnih preduvjeta iz 8.1.1, tj. u drugom kvartalu 2005. g. Sastoji se od slijedećih poslova:

- Donošenje Nacionalne strategije ili politike informacijske sigurnosti. Nositelj je UVNS i ZISKZT, sudionici su sigurnosne službe, MUP, MORH, SSZIS, SDUeH. Rok je četvrti kvartal 2005. g.
- Uspostava osnovne funkcionalnosti od strane središnjih upravljačkih tijela u sustavu informacijske sigurnosti. Nositelji su UVNS (NSA), ZISKZT (NCSA i SAA) i Središnji državni CERT. Rok je četvrti kvartal 2005. g.
- Uspostava Referentne liste normi i standarda i uključivanje potrebnih normi i otvorenih standarda iz područja informacijske sigurnosti. Nositelji su SDUeH i ZISKZT. Rok je četvrti kvartal 2005. g.
- Donošenje Uredbi Vlade RH s ciljem provedbe Nacionalne politike informacijske sigurnosti. Nositelj je UVNS i ZISKZT, sudionici su sigurnosne službe, MUP, MORH. Rok je drugi kvartal 2006. g.
- Donošenje Pravilnika i Smjernica za pojedina sigurnosna područja. Nositelji su tijela sigurnosnog sustava sukladno nadležnosti. Rok je četvrti kvartal 2006. g.
- Organizacija ključnih procesa od strane ostalih upravljačkih tijela u sustavu informacijske sigurnosti. Nositelji su POA, OA i VSA (CIS Operating), SDUeH/APIS, MZOŠ/CARNet (CIS Planning and Implementation). Rok je četvrti kvartal 2006. g.
- Sigurnosna akreditacija Projekta RKMTDU. Nositelj je ZISKZT (SAA), a sudionici SDUeH, MZOŠ i APIS. Rok je četvrti kvartal 2006. g.
- Izrada programa razvoja sigurnosne kulture. Nositelj je UVNS (NSA), sudionici ZISKZT (NCSA) i CARNet (Središnji državni CERT). Rok je četvrti kvartal 2006. g.
- Planiranje pravnih pomaka u zaštiti građanstva i gospodarstva u okviru suvremenog informacijskog društva. Nositelj je MUP u suradnji s MP, Državnim odvjetništvom, UVNS, ZISKZT i Središnjim državnim CERT-om. Rok je četvrti kvartal 2006. g.

Dovršetak Faze 1. planira se do kraja 2006. g., čime bi RH ispunila zahtjeve NATO-a po pitanju informacijske sigurnosti.

8.1.3 Faza 2.

Druga faza može se djelomično preklapati s prvom fazom te može započeti u drugom kvartalu 2006. g., nakon donošenja najvažnijih propisa iz Faze 1. (Nacionalna politika informacijske sigurnosti i provedbene Uredbe). Sastoji se od slijedećih poslova:

- Dogovaranje i usuglašavanje pristupa politici informacijske sigurnosti u Skupini B. Nositelj su UVNS i ZISKZT, sudionici su sigurnosne službe, SSZIS, SDUeH, MZOŠ. Rok je četvrti kvartal 2006. g.
- Izrada edukacijskih programa za neformalne edukacijske aktivnosti u obrazovanju. Nositelj je MZOŠ, a suradnici su upravljačka tijela u sustavu informacijske sigurnosti: UVNS, ZISKZT, MZOŠ/CARNet, SDUeH/APIS. Rok je četvrti kvartal 2006. g.
- Donošenje Smjernica i Preporuka informacijske sigurnosti za Skupinu B. Nositelj je UVNS, sudionici su ZISKZT i sigurnosne službe. Rok je četvrti kvartal 2007. g.
- Uspostava mreže INFOSEC koordinatora za Skupinu B. Nositelj je ZISKZT, sudionici TDV u kojima se postavljaju SDUeH/APIS i MZOŠ/CARNet. Rok je četvrti kvartal 2007. g.
- Koordinacija SAA procesa za Skupinu B. Nositelj je Akreditacijsko tijelo RH, u suradnji sa ZISKZT. Rok je četvrti kvartal 2007. g.
- Izrada edukacijskih programa i kataloga znanja za obrazovanje državnih službenika i namještenika, informatičara u TDV te e-learning koncepta u RH. Nositelj je SDUeH, suradnici SDUU, APIS, ZISKZT, CARNet, Policijska akademija i Zapovjedništvo za združenu izobrazbu i obuku MORH-a. Rok je četvrti kvartal 2007. g.

Dovršetak Faze 2. planira se do kraja 2007. g., čime bi RH ispunila temeljne zahtjeve Programa eEurope 2005 i općenito zahtjeve EU po pitanju informacijske sigurnosti.

8.1.4 Faza 3.

Treća faza može se djelomično preklapati s drugom fazom te može započeti u četvrtom kvartalu 2006. g., nakon donošenja posebnog zakona o informacijskoj sigurnosti, koji regulira tijela iz Skupine B. Sastoji se od sljedećih poslova:

- Dogovaranje i usklađivanje pristupa javno-privatnom partnerstvu u informacijskoj sigurnosti u Skupini C. Nositelj je Vlada RH, a sudionici državne i privatne institucije predviđene Nacionalnim programom. Rok je četvrti kvartal 2007. g.
- Uvođenje formalnih i neformalnih inicijativa u okviru Skupine C. Nositelj je Vlada RH, a sudionici državne i privatne institucije predviđene Nacionalnim programom. Rok je četvrti kvartal 2008. g.
- Izrada edukacijskih programa i kataloga znanja za osnovno i srednje obrazovanje u RH. Nositelj je Zavod za školstvo, suradnici MZOŠ/CARNet. Rok je četvrti kvartal 2008. g.
- Izrada edukacijskih programa i kataloga znanja za visoko obrazovanje u RH (dodiplomsko i poslijediplomsko). Nositelj je FER, suradnici MZOŠ/CARNet, SDUeH/APIS, ZISKZT. Rok je četvrti kvartal 2008. g.

Dovršetak Faze 3. planira se do kraja 2008. g., čime bi RH ispunila sve zahtjeve za stvaranje suvremenog informacijskog društva, obuhvaćajući time sve bitne čimbenike, tj. državnu upravu, javni sektor, građanstvo i gospodarstvo.

8.2 Mehanizmi praćenja provedbe

Za praćenje procesa uspostave sustava informacijske sigurnosti u RH, u početnoj fazi tijekom 2005. g., do preuzimanja obveza od strane nadležnih tijela, bila bi zadužena novoformirana stručna skupina. Kako bi takav proces praćenja bio usklađen s informatizacijom u RH, rad ove skupine bi preko SDUeH trebao biti usklađen s izvršenjem akcijskog plana eHrvatska te ostalim važnim infrastrukturnim projektima (RKMTDU, APIS i veliki projekti informatizacije pravosuđa, zdravstva i sl.). Upravo iz tog razloga SDUeH, kao središnje tijelo u RH za poslove informatizacije, treba biti tijelo zaduženo za formiranje nove stručne skupine koja će tijekom 2005. pratiti provođenje Nacionalnog programa informacijske sigurnosti u RH. Tako bi se osigurala nužna koordiniranost aktualnih i budućih projekata informatizacije s tijekom postupnog uvođenja organizacije informacijske sigurnosti.

Novoformirana stručna skupina treba, radi kontinuiteta, biti utemeljena na sastavu stručne skupine koja je izradila Prijedlog Nacionalnog programa informacijske sigurnosti u RH, ali mora dodatno imati ciljano uključene članove iz svakog dolje navedenog tijela, koji će neposredno raditi na pripremi za preuzimanje propisanih poslova u okviru sustava informacijske sigurnosti RH. Tu spadaju sljedeća tijela:

- Središnje državno sigurnosno tijelo u RH - UVNS (NSA),
- Središnje državno tijelo za sigurnost komunikacija u RH - ZISKZT (NCSA / IA),
- Središnje tijelo za sigurnosne akreditacije - ZISKZT (SAA),
- Tijela za nadzor operativnosti mjera informacijske sigurnosti u TDV – POA, OA i VSA (CIS Operating / CISO),
- Tijela za planiranje i implementaciju mjera informacijske sigurnosti – MORH, MUP, MF, MVPEI, SDUeH/APIS, MZOŠ/CARNet (CIS Planning & Implementation / ITSOA),
- Središnji državni CERT – CARNet, Srce.
- Tijela nadležna za razvoj informacijskog društva, javnu upravu i zaštitu podataka (SDUeH, SDUU, MMTPR, MZOŠ, MP, AZOP)

Novoformirana stručna skupina bi tijekom 2005. g., kvartalno pratila uspostavu funkcionalnosti u pojedinim tijelima u RH. Ovdje spadaju prvenstveno sljedeća tijela, odnosno funkcije: UVNS (NSA), ZISKZT (NCSA/IA, NDA i SAA), POA, OA i VSA (CIS Operating/CISO), CARNet i Srce (Središnji državni CERT), te tijela zadužena za sustav zajedničke informacijske infrastrukture SDUeH/APIS i MZOŠ/CARNet (CIS Planning & Implementation/ITSOA). Preuzimanje upravljačkih funkcija informacijske sigurnosti u RH mora biti obavljeno do kraja 2005. g.

Od početka 2006. g. upravljačke funkcije u informacijskoj sigurnosti RH moraju se provoditi autonomno od strane nadležnih tijela i u skladu s Nacionalnim programom i Nacionalnom politikom informacijske sigurnosti u RH. Stručna skupina bi se tijekom sljedeće dvije godine, 2006. i 2007., sastajala u posljednjem kvartalu godine kako bi pripremila godišnje izvješće za Vladu RH. Godine 2008. bilo bi pripremljeno završno četverogodišnje izvješće, nakon čega bi trebala prestati potreba za radom ovakve stručne skupine, jer bi četverogodišnji proces obuhvatio punu uspostavu informacijske sigurnosti u sve tri definirane skupine tijela i pravnih osoba u RH (Skupine A, B i C).

9 LITERATURA

1. Commission Decision of 29 November 2001. 2001/844/EC,ECSC,Euratom: OJ L 317, 3.12.2001., pp 1-55. amending Rules of Procedure of the Commission [C(2000) 3614] OJ L 308, 8.12.2000., pp 26-34.
2. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890 final.
3. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Network and Information Security: Proposal for A European Policy Approach. COM/2001/0298 final.
4. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – eEurope 2005: An information society for all - An Action Plan to be presented in view of the Sevilla European Council, 21-22 June 2002, COM(2002) 0263 final.
5. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – eEurope 2005 Action Plan: An Update {SEC(2004) 607} {SEC(2004) 608}, COM(2004) 0380 final.
6. Corrigendum to Commission Decision 2004/387/EC of 28 April 2004 – Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDAbc) (OJ L 144, 30.4.2004) OJ L 181, 18.5.2004, pp 25-35.
7. Council Decision of 10 February 2004. (2004/194/EC) OJ L 63, 28.2.2004., pp 48-52. amending Council Decision of 19 March 2001. (2001/264/EC) adopting the Council's security regulations. OJ L 101, 11.4.2001., pp 1-66.
8. Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security (2002/C 43/02). OJ C 043, 16.2.2002. pp 2-4.
9. Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security (2003/C 48/01). OJ C 048, 28.2.2003., pp 1-2.
10. Decision 2256/2003/EC of the European Parliament and of the Council of 17 November 2003 adopting a multiannual programme (2003-2005) for the monitoring of the eEurope 2005 action plan, dissemination of good practices and the improvement of network and information security (MODINIS) (Text with EEA relevance), OJ L 336, 23.12.2003., pp 1-5. as amended by Decision No 787/2004/EC of the European Parliament and of the Council of 21 April 2004 amending Council Decision 96/411/EC and Decisions No 276/1999/EC, No 1719/1999/EC, No 2850/2000/EC, No 507/2001/EC, No 2235/2002/EC, No 2367/2002/EC, No 253/2003/EC, No 1230/2003/EC and No 2256/2003/EC with a view to adapting the reference amounts to take account of the enlargement of the European Union. OJ L 138, 30.4.2004., pp 12-16.

11. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, 23.11.1995, pp 31-50.
12. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). OJ L 201, 31.7.2002., pp 37-47.
13. Directive on Industrial Security: AC/35-D/2003, NATO, 2002.
14. Directive on Personnel Security: AC/35-D/2000, NATO, 2002.
15. Directive on Physical Security: AC/35-D/2001, NATO, 2002.
16. Directive on the Security of Information: AC/35-D/2002, NATO, 2002.
17. European Telecommunications Standardization Institute (ETSI), Response from CEN and ETSI to the "Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach", ETSI SR 002 298 V1.1.1, December 2003.
18. INFOSEC Managment Directive for CIS: AC/35-D/2005, NATO, 2002.
19. Kazneni zakon RH (NN 110/97, NN 27/98, NN 129/00, NN 51/01)
20. Klaić A. Informacijska sigurnost u RH, studija izvedivosti, prethodna analiza. Zagreb: Nacionalno povjerenstvo za sigurnost, studeni 2002.
21. Kok W. et al. Facing the challenge: The Lisbon strategy for growth and employment. Report from the High Level Group chaired by Wim Kok, November 2004.
22. Konvencija o kibernetičkom kriminalu Vijeća Europe (NN -MU 9/02).
23. Lebinac V., Klaić A. Informacijska sigurnost (INFOSEC). Zagreb: Nacionalno povjerenstvo za sigurnost, rujan 2000.
24. Norma BS 7799-2. BSI, 1999.
25. Norma ISO/IEC 15408 (Common Criteria V2.0). ISO, 1999.
26. Norma ISO/IEC 17799. ISO, 2000.
27. Operativni plan provedbe Programa *e*Hrvatska 2007. za 2004. godinu. Zagreb: Središnji Državni Ured za *e*Hrvatsku, lipanj 2004.
28. Pravilnik o informacijskoj sigurnosti Ministarstva obrane i Oružanih snaga Republike Hrvatske (NN 168/03).
29. Pravilnik o ustroju, sadržaju i načinu vođenja službenog upisnika o ostvarivanju prava na pristup informacijama (NN 137/04).
30. Prikaz kaznenog zakonodavstva s područja kompjuterskog kriminaliteta, CARNet, rujan 2003. g., CCERT-PUBDOC-2003-09-41.
31. Primary Directive on INFOSEC: AC/35-D/2004, NATO, 2002.
32. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). OJ L 077, 13.03.2004., pp 1-11.
33. Security in Government Departments. New Zealand: Department of the Prime
34. Minister and Cabinet, 1994.
35. Security within the NATO: C-M(2002)49, NATO, 2002.

36. Sporazum o stabilizaciji i pridruživanju između Republike Hrvatske, s jedne strane, i Europskih zajednica i njihovih država članica, s druge strane. potpisan 29. listopada 2001., ratificiran u Hrvatskom saboru, Europskom parlamentu i svim zemljama članicama 8. listopada 2004. (http://www.mei.hr/Download/ 2002/07/05/SSP_cjeloviti_tekst1.pdf)
37. Strategija Programa One Stop Shop. Zagreb: Središnji državni ured za *e*Hrvatsku, Središnji državni ured za upravu, Financijska agencija, prosinac 2004.
38. Upravljanje sigurnošću informacijskih sustava. Zagreb: CARNet, studeni 2003. (CCERT-PUBDOC-2003-11-49).
39. The National Strategy to Secure Cyberspace, The White House, USA, February 2003.
40. Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka (NN 139/04).
41. Uredba o načinu vođenja i obrascu evidencije o zbirkama osobnih podataka (NN 105/04).
42. Uredba o osnivanju Hrvatskog zavoda za norme (NN 154/04).
43. Uredbe o provedbi ZOSSa i reguliranju sigurnosnog sustava (NN 83/03).
44. Zakon o akreditaciji (NN 158/03).
45. Zakon o arhivskom gradivu i arhivima (NN 105/97).
46. Zakon o elektroničkoj trgovini (NN 173/03).
47. Zakon o elektroničkom potpisu (NN 10/02).
48. Zakon o izmjenama i dopunama Kaznenog zakona (NN 105/04).
49. Zakon o izmjenama i dopunama Zakona o matičnom broju (NN 66/02).
50. Zakon o kaznenom postupku (NN 62/03).
51. Zakon o knjižnicama (NN 105/97).
52. Zakon o normizaciji (NN 163/03).
53. Zakon o općoj sigurnosti proizvoda (NN 158/03).
54. Zakon o pravu na pristup informacijama (NN 172/03).
55. Zakon o sigurnosnim službama RH (NN 32/02 i 38/02).
56. Zakon o tehničkim zahtjevima za proizvode i ocjeni sukladnosti (NN 158/03).
57. Zakon o telekomunikacijama (NN 122/03 i 60/04).
58. Zakon o ustrojstvu i djelokrugu ministarstava i državnih upravnih organizacija (NN 199/03, 30/04).
59. Zakon o zaštiti osobnih podataka (NN 103/03).
60. Zakon o zaštiti tajnosti podataka (NN 108/96).

10 STRUČNA SKUPINA ZA INFORMACIJSKU SIGURNOST

Stručna skupina za informacijsku sigurnost okupljena je pri SDUeH u srpnju 2004. s ciljem pripreme prijedloga Nacionalnog programa informacijske sigurnosti u Republici Hrvatskoj. Stručna skupina aktivno djeluje do potpunog reguliranja područja informacijske sigurnosti u Republici Hrvatskoj i preuzimanja obveza od strane mjerodavnih institucija, što se planira do početka 2006. godine.

Članovi stručne skupine su:

Dr. sc. Diana Šimić, voditeljica
Dr. sc. Suzana Stojaković Čelustka, zamjenica voditeljice
Robert Butković
Albert Crismanich
Bojnik Stanko Ćavar
Draginja Dokmanović Ćurić
Boris Gaćina
Iva Jeličić
Mr. sc. Aleksandar Klaić
Mario Kauzlarić
Mr. sc. Predrag Pale
Mr. sc. Boris Posavec
Mr. sc. Vlado Pribolšan
Josip Trbuščić

PRILOG A

POPIS MJERA

Mjera	Nositelj	Sudionici	Rok izvršenja
Formiranje nove stručne Skupine za praćenje provedbe Nacionalnog programa informacijske sigurnosti u RH, na temelju postojeće SSZIS	SDUeH	SSZIS, UVNS, ZISKZT, POA, OA, VSA, MORH, MUP, MF, MVPEI, APIS, MZOŠ, CARNet, Središnji državni CERT	04/2005
Donošenje okvirnog zakona o informacijskoj sigurnosti	UVNS	SSZIS, SDUeH,	06/2005
Izmjene Zakona o sigurnosnim službama RH u dijelu koji definira nadležnosti u području informacijske sigurnosti (UVNS, ZISKZT, sigurnosne službe)	UVNS	ZISKZT, sigurnosne službe	06/2005
Upućivanje Vladi RH osnivačkih akata Zavoda za informacijsku sigurnost i kriptozaštitnu tehnologiju (ZISKZT) usklađenih s Nacionalnim programom informacijske sigurnosti, te imenovanje ravnatelja Zavoda	UVNS, Stručni tim za postupak osnivanja Zavoda	Sigurnosne službe, SDUeH	06/2005
Početak rada Zavoda za informacijsku sigurnost i kriptozaštitnu tehnologiju (ZISKZT)	Ravnatelj Zavoda		09/2005
Osnivanje Agencije za potporu informacijskih sustava (APIS)	SDUeH	FINA i TDV koja će koristiti usluge	09/2005
Osnivanje Središnjeg državnog tijela za računalne incidente (Središnji državni CERT)	CARNet	SDUeH, MZOŠ, ZISKZT	09/2005

Mjera	Nositelj	Sudionici	Rok izvršenja
Izmjene Zakona o zaštiti tajnosti podataka	UVNS	ZISKZT, sigurnosne službe, MORH, MUP i Državno odvjetništvo	09/2005
Usklađivanje propisa o uredskom poslovanju s propisima informacijske sigurnosti	SDUU	SDUeH, UVNS, ZISKZT i sigurnosne službe	12/2005
Revizija Zakona o izmjenama i dopunama Zakona o matičnom broju	MUP	SDUeH, MP, SDUU	12/2005
Usmjeravanje Projekta RKMTDU sa sigurnosnog aspekta	ZISKZT	SDUeH, MZOŠ	12/2005
Donošenje Nacionalne strategije ili politike informacijske sigurnosti	UVNS i ZISKZT	Sigurnosne službe, MUP, MORH, SSZIS, SDUeH	12/2005
Uspostava osnovne funkcionalnosti od strane središnjih upravljačkih tijela u sustavu informacijske sigurnosti	UVNS, ZISKZT, Središnji državni CERT		12/2005
Uspostava Referentne liste normi i standarda i uključivanje potrebnih normi i otvorenih standarda iz područja informacijske sigurnosti	SDUeH, ZISKZT		12/2005
Donošenje Uredbi Vlade RH s ciljem provedbe Nacionalne politike informacijske sigurnosti	UVNS i ZISKZT	Sigurnosne službe, MUP, MORH	06/2006
Donošenje Pravilnika i Smjernica za pojedina sigurnosna područja	UVNS i ZISKZT	Sigurnosne službe, MUP, MORH	12/2006
Organizacija ključnih procesa od strane ostalih upravljačkih tijela u sustavu informacijske sigurnosti	POA, OA, VSA, SDUeH/APIS, MZOŠ/CARNet		12/2006
Sigurnosna akreditacija Projekta RKMTDU	ZISKZT	SDUeH, MZOŠ i APIS	12/2006
Izrada programa razvoja sigurnosne kulture	UVNS	ZISKZT, CARNet (Središnji državni CERT)	12/2006

Mjera	Nositelj	Sudionici	Rok izvršenja
Planiranje pravnih pomaka u zaštiti građanstva i gospodarstva u okviru suvremenog informacijskog društva	MUP u suradnji s MP, Državnim odvjetništvom, UVNS, ZISKZT i Središnjim državnim CERT-om		12/2006
Dogovaranje i usuglašavanje pristupa politici informacijske sigurnosti u Skupini B	UVNS i ZISKZT	Sigurnosne službe, MUP, MORH, SSZIS, SDUeH, MZOŠ	12/2006
Izrada edukacijskih programa za neformalne edukacijske aktivnosti u obrazovanju	MZOŠ	UVNS, ZISKZT, CARNet, SDUeH/APIS	12/2006
Donošenje Smjernica i Preporuka informacijske sigurnosti za Skupinu B	UVNS i ZISKZT	Sigurnosne službe, MUP, MORH	12/2007
Uspostava mreže INFOSEC koordinatora za Skupinu B	ZISKZT	TDV u kojima se postavljaju, SDUeH/APIS i MZOŠ/CARNet	12/2007
Koordinacija akreditacijskog procesa za Skupinu B	Akreditacijsko tijelo RH	ZISKZT	12/2007
Izrada edukacijskih programa i kataloga znanja za obrazovanje državnih službenika i namještenika, informatičara u TDV te e-learning koncepta u RH	SDUeH	SDUU, APIS, ZISKZT, CARNet, Policijska akademija, Zapovjedništvo za združenu izobrazbu i obuku MORH-a	12/2007
Dogovaranje i usklađivanje pristupa javno-privatnom partnerstvu u informacijskoj sigurnosti u Skupini C	Vlada RH	državne i privatne institucije predviđene Nacionalnim programom	12/2007
Uvođenje formalnih i neformalnih inicijativa u okviru Skupine C	Vlada RH	državne i privatne institucije predviđene Nacionalnim programom	12/2008
Izrada edukacijskih programa i kataloga znanja za osnovno i srednje obrazovanje u RH	Zavod za školstvo	MZOŠ/CARNet	12/2008

Mjera	Nositelj	Sudionici	Rok izvršenja
Izrada edukacijskih programa i kataloga znanja za visoko obrazovanje u RH (dodiplomsko i poslijediplomsko)	FER	MZOŠ/CARNet, SDUeH/APIS, ZISKZT	12/2008

PRILOG B

POPIS KRATICA

Kratica	Hrvatski naziv	Izvorni naziv
ANSI	Američki nacionalni normizacijski zavod	American National Standards Institute
APIS	Agencija za potporu informacijskih sustava	Agency for ICT support
AZOP	Agencija za zaštitu osobnih podataka	
CARNet	Hrvatska akademska i istraživačka mreža	Croatian Academic and Research Network
CEN	Europski odbor za normizaciju	European Committee for Standardization
CENELEC	Europski odbor za tehničku normizaciju	European Committee for Technical Standardization
CERT	Centar za odgovor na računalne incidente	Computer Emergency Response Team
CIS	Komunikacijsko-informacijski sustav	Communication Information System
CISO	centralni koordinator informacijske sigurnosti	Central Information Security Officer
COMPUSEC	Sigurnost informacija u elektroničkim medijima i računalima	Computer Security
COMSEC	Sigurnost informacija u sustavima za prijenos podataka	Communication Security
CSIRT	Centri za računalnu sigurnost	Computer Security Incident Response Teams
CSTF	Radno tijelo za kibernetičku sigurnost	Cyber Security Task Force
DGU	Državna geodetska uprava	
DHS	Ministarstvo domovinske sigurnosti	Department of Homeland Security
DKP	diplomatsko-konzularno predstavništvo	
DZNM	Državni zavod za normizaciju i mjeriteljstvo	
DZS	Državni zavod za statistiku	
EC	European Communities	Europske zajednice
EEA	Europski gospodarski prostor	European Economic Area
ENISA	Europska agencija za mrežnu i informacijsku sigurnost	European Network and Information Security Agency
eSEE	e-Jugoistočna Europa	e(lectronic)South Eastern Europe
ETSI	Europski institut za telekomunikacijske norme	European Telecommunications Standards Institute
EU	Europska unija	European Union
FER	Fakultet elektrotehnike i računarstva	
FINA	Financijska agencija	
FIRST	Skup (forum) centara za računalnu sigurnost	Forum of Incident Response Teams
FSC	sigurnosna provjera objekta	Facility Secure Clearance
GSC	Glavno tajništvo Vijeća	General Secretariat of the Council
HGK	Hrvatska gospodarska komora	Croatian Chamber of Commerce
HIPAA	Dokument o prenosivosti i odgovornosti zdravstvenog osiguranja	Health Insurance Portability and Accountability Act
HNB	Hrvatska narodna banka	

Kratica	Hrvatski naziv	Izvorni naziv
HSSP	Nacionalni panel sigurnosnih standarda	Homeland Security Standards Panel
HUP	Hrvatska udruga poslodavaca	
HZMO	Hrvatski zavod za mirovinsko osiguranje	
HZN	Hrvatski zavod za norme	
IA	Tijelo za INFOSEC	INFOSEC Authority
ICT	informacijska i komunikacijska tehnologija	Information and Communication Technology
IEEE	Američki institut inženjera elektrotehnike i Institut radio inženjera	American Institute of Electrical Engineers and Institute of Radio Engineers
INFOSEC	Sigurnost informacijskih sustava	Information System Security
IO	vlasnik informacije	Information Owner
ISO	Međunarodna organizacija za normizaciju	International Organization for Standardization
ISP	davatelj internetskih usluga	Internet Service Provider
IT	informacijska tehnologija	Information Technology
ITSOA	tijelo nadležno za upravljanje IT sustavima	IT System Operational Authority
ITU	Međunarodna telekomunikacijska unija	International Telecommunication Union
KZ	kazneni zakon	
LISO	lokalni koordinator informacijske sigurnosti	Local Information Security Officer
MAP	Akcijski plan za članstvo	Membership Action Plan
MF	Ministarstvo financija	
MMPTR	Ministarstvo mora, turizma, prometa i razvitka	
MORH	Ministarstvo obrane RH	
MUP	Ministarstvo unutarnjih poslova	
MVPEI	Ministarstvo vanjskih poslova i europskih integracija	
MZOŠ	Ministarstvo znanosti, obrazovanja i športa	
MZT	Ministarstvo znanosti i tehnologije	
NATO	Sjevernoatlantski savez	North Atlantic Treaty Organization
NCSA	Središnje državno komunikacijsko-sigurnosno tijelo	National Communications Security Authority
NDA	Središnje državno tijelo odgovorno za distribuciju NATO kriptomaterijala	National Distribution Authority
NSA	Središnje državno sigurnosno tijelo	National Security Authority
NSK	Nacionalna sveučilišna biblioteka	National and University Library
OA	Obavještajna agencija	
OSS	softver s otvorenim (javno poznatim) kodom	Open Source Software
PfP	Partnerstvo za mir (NATO program)	Partnership for Peace
POA	Protuobavještajna agencija	
PSC	sigurnosna provjera pojedinca	Personnel Security Clearance
PU	policijska uprava	Police Directorate
RH	Republika Hrvatska	Republic of Croatia

Kratica	Hrvatski naziv	Izvorni naziv
RKMTDU	računalno-komunikacijska mreža tijela državne uprave	
SAA	Središnje državno tijelo za sigurnosne akreditacije	Security Accreditation Authority
SANS	Institut sistemskih administratora, revizije, mreža i sigurnosti	SysAdmin, Audit, Network, Security Institute
SC	Sigurnosni odbor	Security Committee
SDUU	Središnji državni ured za upravu	Central State Office for Administration
SDUeH	Središnji državni ured za eHrvatsku	
SLA	Ugovor o razini usluge	Service Level Agreement
Srce	Sveučilišni računski centar	
SSP	Sporazum o stabilizaciji i pridruživanju	Stability and Association Agreement
SSRS	Izjave o specifičnim sigurnosnim zahtjevima	System-Specific Security Requirements Statements
SSZIS	Stručna skupina za informacijsku sigurnost	
TDV	tijelo državne vlasti	
TECSEC	tehnička sigurnost	Technical Security
TK	Telekomunikacije	telecommunications
TSO	vlasnik tehničkog sustava	Technical Systems Owner
UVNS	Ured Vijeća za nacionalnu sigurnost	
VSA	Vojna sigurnosna agencija	
ZISKZT	Zavod za informacijsku sigurnost i kripto-zaštitnu tehnologiju	
ZOSS	Zakon o sigurnosnim službama	
ZZOP	Zakon o zaštiti osobnih podataka	
ZZTP	Zakon o zaštiti tajnosti podataka	