STRATEGIJA KRIPTOLOGIJE

REPUBLIKE SLOVENIJE

Avgust 2015

Predgovor

Z razvojem informacijskih tehnologij in s tem povezanim razvojem obdelave informacij je danes sorazmerno enostavno prestreči in spremeniti digitalne zapise podatkov, zato so se povečale zahteve po njihovi varnosti, ko se obravnavajo in prenašajo po komunikacijsko-informacijskih sistemih. Poleg običajnih ukrepov varnosti v sistemih (npr. vstopno uporabniško ime in geslo, protivirusni programi, programske ali strojne požarne pregrade itd.) je pri zaščiti sistemov in podatkov ključna uporaba kriptografije.

Kriptografija je znanstvena veda, ki ima številne praktične uporabnosti. Pojavlja se v številnih šifrirnih rešitvah, ki so prosto dostopne na trgu, državljani razvitih držav jo uporabljamo dnevno. Prisotna je pri overjanju in šifriranju (bančne kartice, brezžični telefoni, e-poslovanje, plačljiva TV), nadzoru dostopov (sistemi za zaklepanje vozil, smučarske vozovnice), plačevanju (predplačniške telefonske kartice, e-denar) in lahko postane temeljni instrument za demokracijo z vpeljavo sistemov za elektronsko glasovanje.

Kriptografija odgovarja na problem varnega komuniciranja ob prisotnosti tretje osebe, ki se jo obravnava kot prisluškovalca oziroma kot nezakonitega udeleženca komunikacije (lahko je to naš nasprotnik, sovražnik). Beseda kriptografija izhaja iz grških besed κρυπτός (skrito, tajno) in γράφειν (pisanje) in pomeni skrito oziroma tajno pisanje. Zaradi zgodovinskih razlogov je še danes izraz »šifriranje« pogosto sinonim za kriptografijo. Šifriranje je proces preoblikovanja digitalnega zapisa informacije iz berljive oblike v neberljivo.

Kriptografija opremlja oblikovalce informacijskih tehnologij z orodji, ki neposredno ali posredno pripomorejo k zagotavljanju varnostnih servisov, kot so: zaupnost, celovitost, razpoložljivost, avtentičnost in nezatajljivost. Med slednjimi je zaupnost najpogostejši varnostni servis, ki se ga doseže s šifriranjem. Pri tem je potreben šifrirni ključ, s katerim lahko prejeta šifrirana sporočila dešifriramo v berljivo obliko. Šifrirni ključ je tudi ključni parameter, ki mora biti ustrezno varovan. Kompromitacija šifrirnega ključa pomeni, da je postal javen in posledično ne zagotavlja več varnostnega servisa zaupnosti. Varnost ne sme temeljiti le na tajnosti kriptografskih mehanizmov, temveč predvsem na tajnosti šifrirnega ključa. Drugo vprašanje je, kakšna je dejanska kriptografska varnost šifrirnega ključa. Odgovor na to vprašanje nam da kriptoanaliza kriptografskih mehanizmov. Kriptografija in kriptoanaliza skupaj sta poznani pod imenom kriptologija.

Sprejetje strategije kriptologije je za Republiko Slovenijo pomembno zaradi več razlogov in mora postati trajnostno. Gre za nacionalni dokument, ki opredeljuje področje kriptologije in priporoča uporabo nacionalnih šifrirnih rešitev. Obstoječa zakonodaja sicer zahteva uporabo šifrirnih rešitev, vendar kljub temu še vedno nimamo enotnih stališč, ki bi jim lahko trajnostno sledili. Državni organi in organizacije so pogosto prepuščeni sami sebi in lastnim usmeritvam.

Postavili smo strokovno izhodišče, da se šifrirne rešitve, ki se uporabljajo za varovanje podatkov, ne bi nabavljale v tujini. S takimi nabavami se dejansko razkrijejo vsi načini varovanja podatkov najmanj prodajalcu šifrirne rešitve, s tem pa se posredno poveča možnost napada na naš sistem. Pristop do kriptologije, zasnovan v strategiji, temelji na predpostavki, da država razvija lastne šifrirne rešitve tako za namene varovanja tajnih podatkov kot tudi za varovanje ostalih podatkov. Tako politiko ima večina držav članic zveze NATO in EU. K sprejemu zakonskih okvirjev za ustrezno uporabo kriptografskih mehanizmov na vseh področjih nas zavezujejo tudi usmeritve združenja OECD[1] in priporočila evropske agencije ENISA[2]. Področje

[1] OECD (Organisation for Economic Co-operation and Development) je mednarodna gospodarska organizacija razvitih držav, ki sprejemajo načela predstavniške demokracije in svobodnega trga. Slovenija je od leta 2010 članica organizacije OECD.

[2] ENISA (European Network and Information Security Agency) je evropska agencija za varnost omrežij in informacij.

zaupanja in varnosti je tudi eden izmed sedmih stebrov Digitalne agende za Evropo, ki jo je leta 2010 objavila Evropska komisija z namenom, da bi omogočila izhod iz krize in gospodarstvo EU pripravila na izzive naslednjega desetletja (Evropa 2020 – strategija za pametno, trajnostno in vključujočo rast).

1 Uvod

Delo na področju kriptologije je interdisciplinarno in zahteva povezovanje profilov strokovnjakov, kot so inženirji za programsko in strojno računalniško opremo in matematiki. Republika Slovenija bo s tem podprla tudi razvoj in uvedbo varnih storitev v kibernetskem prostoru na ozemlju Republike Slovenije, ki bodo podprte s šifrirnimi rešitvami na vseh področjih (tajni podatki, osebni podatki, e-identitete, e-podpis, e-transakcije ipd.) tako v smislu postavljanja tehnoloških zahtev za storitve kot tudi podpore domačemu razvojno-raziskovalnemu sektorju in proizvajalcem varnih storitev. Uporabnik in ponudnik teh storitev bosta tako javni kot zasebni sektor. Slednje je mogoče le, če so znanja pametno izkoriščena. Znanja, veščine in kompetence strokovnjakov so tisti ključni dejavniki, ki omogočajo, da se raziskovalni, razvojni in tržni potenciali lahko izkoristijo in prispevajo k povečanju produktivnosti in inovativnosti.

V slovenskih predpisih so šifrirne rešitve opredeljene kot šifrirna oprema (strojna in programska) in sistemi, ki se uporabljajo za šifrirno varovanje podatkov v komunikacijsko-informacijskih sistemih, v katerih se obravnavajo tajni, osebni in drugi občutljivi podatki. Med šifrirne rešitve spadajo tudi vsi moduli, ki so vgrajeni v posameznih delih sistemov in so namenjeni šifrirnemu varovanju podatkov. Šifrirno ovrednotenje je postopek, v katerem se ugotovi varnostno ustreznost predlagane šifrirne rešitve za varovanje prenosa tajnih podatkov določene stopnje tajnosti.

Pri šifrirnem ovrednotenju tujih šifrirnih rešitev se Urad Vlade Republike Slovenije za varovanje tajnih podatkov srečuje s problemom dostopa do varnostno kritičnih elementov, ker slednjih tuji proizvajalci oziroma pristojni organ države proizvajalke zaradi zaščite lastnih interesov niso pripravljeni razkriti v celoti. Posledično se za varovanje tajnih podatkov, osebnih podatkov in ostalih občutljivih podatkov uporabljajo tuje šifrirne rešitve, za katere ne vemo natančno, kako delujejo oziroma ne poznamo načina delovanja posameznih varnostno kritičnih elementov. Razlog temu sta pomanjkanje državne podpore za razvoj in proizvodnjo domačih šifrirnih rešitev in pomanjkanje nacionalne zavesti po uporabi domačih šifrirnih rešitev. V Republiki Sloveniji je tako s strani države opažena odsotnost iniciative za razvoj domačih šifrirnih rešitev. Gre večinoma za unikatne produkte z zelo ozkim krogom uporabnikov in specifičnimi zahtevami. Za nacionalno varnost države sta trajnostni razvoj in proizvodnja domačih šifrirnih rešitev bistvenega pomena.

V komunikacijsko-informacijskih sistemih, v katerih se obravnavajo tajni podatki, je dovoljena uporaba tistih šifrirnih rešitev, za katere je bilo izdano potrdilo o varnostni ustreznosti. Slednje lahko izda Urad Vlade Republike Slovenije za varovanje tajnih podatkov ali drug z zakonom določen organ, in sicer na podlagi šifrirnega ovrednotenja za vsako šifrirno rešitev posebej. Za varovanje prenosa nacionalnih tajnih podatkov v komunikacijsko-informacijskih sistemih je treba v čim večji meri uporabljati šifrirne rešitve domačih proizvajalcev, saj je uporaba tujih šifrirnih rešitev lahko varnostno kritična.

2 Zasnova strategije in cilji

Vlada Republike Slovenije je zasnovala »Strategijo kriptologije Republike Slovenije« z opredeljenimi cilji, za dosego katerih so oblikovani okvirni načrti in ukrepi za:

- vrednotenje šifrirnih rešitev,
- spodbujanje razvoja in uporabe šifrirnih rešitev,
- zagotavljanje šifrirnih rešitev za potrebe varovanja tajnih podatkov,
- prodor na tuje trge,
- raziskovanje na področju kriptologije,
- zagotavljanje kadrovskih virov:
    - podeljevanje štipendij za področje kriptologije,
    - zaposlovanje kriptoloških strokovnjakov.

Navedeni cilji so v naslednjem poglavju vsebinsko podrobneje specificirani prek predstavitve obstoječega stanja, ki ji sledi opredelitev ciljnega stanja, ključnih nosilcev razvoja in deležnikov, ukrepov za doseganje ciljnega stanja in opredelitev tveganj.

3 Specifikacija ciljev

3.1 Vrednotenje šifrirnih rešitev

Obstoječe stanje

Vrednotenje šifrirnih rešitev je normativno urejeno in se izvaja z omejenim kadrom, kar posledično pomeni, da varnostnega vrednotenja ni mogoče izvajati poglobljeno.

Za potrebe varovanja tajnih podatkov postopke šifrirnih vrednotenj opravlja Urad Vlade Republike Slovenije za varovanje tajnih podatkov, za obrambne potrebe pa Ministrstvo za obrambo.

Ciljno stanje

- postavitev enotnega organa, pristojnega za opravljanje postopkov šifrirnih ovrednotenj, umeščenega v Urad Vlade Republike Slovenije za varovanje tajnih podatkov; za nemoteno opravljanje nalog mora imeti ustrezno kadrovsko zasedbo in biti primerno opremljen – kriptološki laboratorij (prostor, strojna in programska oprema); v okviru Urada Vlade Republike Slovenije za varovanje tajnih podatkov mora biti zagotovljena tudi podpora upravnemu poslovanju;
- uvajanje novih šifrirnih rešitev mora biti izvedeno na podlagi predhodno opravljenega šifrirnega vrednotenja;
- trajnostno usposabljanje zaposlenih strokovnjakov na področju kriptologije.

Nosilec

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov.

Ukrepi za doseganje ciljnega stanja

- z ustrezno kadrovsko politiko (premestitve, dodatne zaposlitve) je treba zagotoviti kadrovsko dopolnjenost;
- zagotoviti je treba ustrezen prostor in opremo;
- zagotoviti je treba tudi ustrezna finančna sredstva za izvajanje postopkov šifrirnih ovrednotenj.

Tveganja

- pomanjkanje ustreznega kadra;
- zagotavljanje finančnih virov;
- medresorska strokovna delovna skupina za komunikacijsko varnost opravlja svoje delo v okviru svojih možnosti (časovnih, kadrovskih in finančnih) in predstavlja tveganje za učinkovito izvajanje postopkov šifrirnih ovrednotenj.

3.2 Spodbujanje razvoja in uporabe šifrirnih rešitev

Obstoječe stanje

Republika Slovenija kot proizvajalka šifrirnih rešitev ni zadostno prepoznana v domačem in mednarodnem okolju. V večini primerov za prenos tajnih, občutljivih in osebnih podatkov uporabljamo šifrirne rešitve, ki niso ustrezno implementirane in za katere ni bil izveden postopek šifrirnega vrednotenja. Razvoj šifrirnih rešitev je nenačrten. V Republiki Slovenji trenutno ni državnega organa, ki bi podpiral in financiral razvoj šifrirnih rešitev. Z uporabo tujih šifrirnih rešitev se zanemarja domače znanje in posledično ne spodbuja razvoja domačega gospodarstva.

Ciljno stanje

- uvrstitev Republike Slovenije na seznam proizvajalk šifrirnih rešitev;
- obstoj vsaj treh domačih podjetij, ki so sposobna razvijati lastne šifrirne rešitve za varovanje različnih vrst podatkov in e-storitev.

Nosilci in deležniki

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov (nosilec),
- Ministrstvo za gospodarski razvoj in tehnologijo in
- Javna agencija za spodbujanje podjetništva, inovativnosti, razvoja, investicij in turizma.

Kot vsebinski nosilci sodelujejo:

- Slovenska obveščevalno-varnostna agencija,
- Ministrstvo za obrambo,
- Ministrstvo za zunanje zadeve in
- Ministrstvo za javno upravo.

Ukrepi za doseganje ciljnega stanja

- Republika Slovenija mora prek razvojnih projektov zagotavljati finančno pomoč pri razvoju novih šifrirnih rešitev;
- Republika Slovenija mora razviti sposobnost oblikovanja jasnih kriterijev, ki proizvajalcem omogočajo razvijanje kakovostnih šifrirnih rešitev in jih k temu jasno usmerjajo;
- spodbude za razvoj novih šifrirnih rešitev morajo prihajati s strani države tudi prek javnih razpisov. Slovenska obveščevalno-varnostna agencija, Ministrstvo za obrambo, Ministrstvo za zunanje zadeve, Ministrstvo za javno upravo in Ministrstvo za notranje zadeve – Policija kot največji uporabniki šifrirnih rešitev in Urad Vlade Republike Slovenije za varovanje tajnih podatkov kot nacionalni varnostni organ, pristojen za izvajanje šifrirnih ovrednotenj, morajo sodelovati pri pripravi javnih razpisov za nove šifrirne rešitve. Javna agencija za spodbujanje podjetništva, inovativnosti, razvoja, investicij in turizma v razvojne programe redno vključuje projekte, povezane z razvojem šifrirnih rešitev.

Tveganja

- neobstoj domačih šifrirnih rešitev predstavlja veliko tveganje za nacionalno varnost Republike Slovenije;
- neobstoj državnih spodbud za razvojne projekte s področja kriptologije pomeni tveganje, da Republika Slovenija pride v stanje brez ustreznih kriptoloških strokovnjakov, ki so potrebni za razvoj novih šifrirnih rešitev;
- samostojen razvoj novih šifrirnih rešitev brez državne podpore predstavlja tudi tveganje za obstoj posameznega podjetja;
- pri šifrirnem ovrednotenju tujih šifrirnih rešitev se srečujemo s problemom možnosti seznanitve s ključnimi kriptografskimi mehanizmi, ker slednjih tuji proizvajalci oziroma

pristojni organi držav proizvajalk zaradi zaščite lastnih interesov niso pripravljeni razkriti. Nepoznavanje kriptografskih mehanizmov, ki se uporabljajo v nacionalnih komunikacijsko-informacijskih sistemih, predstavlja veliko tveganje za nacionalno varnost Republike Slovenije.

3.3 Zagotavljanje šifrirnih rešitev

Obstoječe stanje

V državni upravi se za prenos tajnih (in ostalih) podatkov skoraj izključno uporabljajo različne tuje šifrirne rešitve, kar je lahko varnostno kritično. Škodljiva je tudi odsotnost enotnega pristopa pri sprejemanju odločitev o izbiri posameznih šifrirnih rešitev. Posledici tovrstne razpršenosti nista le netransparentnost in slabša učinkovitost takšne zaščite, temveč tudi precejšnja finančna potratnost (manjše količine raznovrstnih rešitev, vzdrževalne pogodbe).

Urad Vlade Republike Slovenije za varovanje tajnih podatkov vodi seznam odobrenih šifrirnih rešitev za varovanje prenosa tajnih podatkov za različne stopnje tajnosti.

Ciljno stanje

- uporaba šifrirnih rešitev za varovanje prenosa vseh podatkov v komunikacijsko-informacijskih sistemih državnih organov;
- omogočanje uporabe šifrirnih rešitev za varen prenos podatkov tudi v širšem okolju (banke, poslovni subjekti, kritična infrastruktura).

Nosilci in deležniki

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov (nosilec),
- Ministrstvo za obrambo,
- Slovenska obveščevalno-varnostna agencija,
- Ministrstvo za notranje zadeve,
- Ministrstvo za zunanje zadeve,
- Ministrstvo za javno upravo in
- Javna agencija za spodbujanje podjetništva, inovativnosti, razvoja, investicij in turizma.

Ukrepi za doseganje ciljnega stanja

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov izvaja šifrirno vrednotenje šifrirnih rešitev in objavlja seznam odobrenih šifrirnih rešitev na svoji spletni strani;
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov ob sodelovanju ostalih deležnikov koordinira in promovira uporabo šifrirnih rešitev za zagotavljanje varnih storitev v kibernetskem prostoru;
- državni organi (nosilci in deležniki) sodelujejo pri razvoju in izvedbi končnih šifrirnih rešitev za prenos tajnih podatkov za potrebe ostalih državnih organov; Urad Vlade Republike Slovenije za varovanje tajnih podatkov koordinira postopke z zunanjim izvajalcem;
- umestitev zahteve po uporabi kriptografskih mehanizmov za varovanje prenosa podatkov v predpise;
- izvajanje promocije uporabe šifrirnih rešitev v ostalih panogah, npr. bančni sektor, zavarovalništvo itd.;
- Javna agencija za spodbujanje podjetništva, inovativnosti, razvoja, investicij in turizma nudi pomoč domačim podjetjem na javnih razpisih za črpanje evropskih sredstev za razvoj in proizvodnjo šifrirnih rešitev.

Tveganja

- brez razvoja in proizvodnje domačih šifrirnih rešitev nimamo lastnih produktov za varovanje prenosa podatkov po komunikacijsko-informacijskih sistemih in posledično zaupamo varnost nacionalnih tajnih podatkov izključno tujim šifrirnim rešitvam oziroma drugim državam;
- pri vsaki šifrirni rešitvi, ki je ni možno preučiti do najmanjše podrobnosti, obstaja tveganje, da uporablja neustrezne kriptografske mehanizme ali ima celo vgrajena stranska vrata z namenom prestrezanja podatkov;
- z neobstojem domačih šifrirnih rešitev je onemogočen nastanek dodane vrednosti.

3.4 Razpoznavnost nacionalnih šifrirnih rešitev

Obstoječe stanje

Slovenske šifrirne rešitve, ki so odobrene za varovanje nacionalnih tajnih podatkov, na tujih trgih niso prisotne.

Urad Vlade Republike Slovenije za varovanje tajnih podatkov je pristojen za izvajanje postopkov šifrirnih ovrednotenj in je prepoznan v EU in zvezi NATO kot nacionalni varnostni organ Republike Slovenije.

Ciljno stanje

- vključitev domačih šifrirnih rešitev, ki so odobrene za varovanje nacionalnih tajnih podatkov, na seznam EU in NATO potrjenih šifrirnih rešitev.

Nosilci in deležniki

- Javna agencija za spodbujanje podjetništva, inovativnosti, razvoja, investicij in turizma (nosilec),
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov,
- Ministrstvo za obrambo in
- Ministrstvo za zunanje zadeve.

Ukrepi za doseganje ciljnega stanja

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov, Ministrstvo za obrambo in Ministrstvo za zunanje zadeve lahko nudijo pomoč domačim proizvajalcem pri prodaji modificiranih šifrirnih rešitev na tujih trgih;
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov se določi kot pristojen organ za koordiniranje aktivnosti pri drugem šifrirnem ovrednotenju za pridobitev potrdila za varovanje tajnih podatkov EU;
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov in Ministrstvo za obrambo se določita kot pristojna organa za koordiniranje aktivnosti za pridobitev potrdila za varovanje tajnih podatkov zveze NATO;
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov pripravi navodilo za postopek drugega šifrirnega ovrednotenja, ki je potreben za pridobitev potrdila za varovanje tajnih podatkov EU;
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov in Ministrstvo za obrambo pripravita navodilo za postopek pridobitve potrdila za varovanje tajnih podatkov zveze NATO;

- Urad Vlade Republike Slovenije za varovanje tajnih podatkov in Ministrstvo za obrambo ponudita domačim proizvajalcem šifrirnih rešitev možnost pridobitve potrdil za varovanje tajnih podatkov EU in zveze NATO;
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov in Ministrstvo za obrambo nadaljujeta z aktivnostmi v mednarodnih asociacijah v povezavi z evalvacijami šifrirnih rešitev, katerih članica je Republika Slovenija.

Tveganja

- postopek drugega šifrirnega ovrednotenja predstavlja tveganje in ne zagotavlja, da se bo proces zaključil s potrditvijo predlagane šifrirne rešitve za varovanje tajnih podatkov EU določene stopnje tajnosti;
- ravno tako postopek šifrirnega ovrednotenja za pridobitev odobritve za varovanje tajnih podatkov zveze NATO predstavlja tveganje in ne zagotavlja, da se bo tudi uspešno zaključil;
- tudi to, da bodo šifrirne rešitve ovrednotene s strani pristojnega organa NATO oziroma EU, ne pomeni, da bodo te rešitve v mednarodnem okolju prodane.

3.5 Raziskovanje na področju kriptologije

Obstoječe stanje

V Republiki Sloveniji so aktivne številne programske skupine, vendar med njimi ni nobene, ki bi delovala na področju kriptologije. V preteklosti so bili določeni raziskovalni projekti s področja kriptologije financirani s strani države (Javna agencija za raziskovalno dejavnost Republike Slovenije, Ministrstvo za obrambo in Slovenska obveščevalno-varnostna agencija).

Ciljno stanje

- spodbujanje in državno sofinanciranje razvojnih projektov na področju kriptologije.

Nosilci in deležniki

- Javna agencija za raziskovalno dejavnost Republike Slovenije (nosilec),
- Ministrstvo za izobraževanje, znanost in šport,
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov in
- Javna agencija za spodbujanje podjetništva, inovativnosti, razvoja, investicij in turizma.

Ukrepi za doseganje ciljnega stanja

- Javna agencija za raziskovalno dejavnost Republike Slovenije, ki opravlja strokovne, razvojne in izvršilne naloge v zvezi z izvajanjem sprejete Raziskovalne in inovacijske strategije Slovenije v okviru veljavnega proračunskega memoranduma in državnega proračuna in druge naloge pospeševanja raziskovalne dejavnosti, skladno z namenom ustanovitve skupaj z Uradom Vlade Republike Slovenije za varovanje tajnih podatkov, vključi projekte s področja kriptologije v okvir svojega delovanja;
- razvojni projekti se določajo na osnovi splošnih in posebnih potreb po šifrirnih rešitvah. Splošne potrebe so javno znane zahteve informacijske družbe. Posebne potrebe so specifične zahteve državnih organov, ki jih koordinira Urad Vlade Republike Slovenije za varovanje tajnih podatkov. Javna agencija za raziskovalno dejavnost Republike Slovenije, Javna agencija za spodbujanje podjetništva, inovativnosti, razvoja, investicij in turizma in

Urad Vlade Republike Slovenije za varovanje tajnih podatkov koordinirajo svoje aktivnosti s ciljem financiranja skupaj določenih razvojnih projektov na področju kriptologije.

Tveganja

- pri potrjevanju razvojnih projektov za kriptologijo obstaja tveganje, da predlagatelj projekta nima namena delovati na področju kriptologije;
- pri določitvi razvojnih projektov za kriptologijo obstaja tveganje, da se delo preusmeri na druga področja.

3.6 Zagotavljanje kadrovskih virov

3.5.1 Podeljevanje štipendij za področje kriptologije

Obstoječe stanje

Trenutni sistem štipendiranja ne predvideva posebnih štipendij na področju kriptologije.

Ciljno stanje

- Republika Slovenija na letni ravni štipendira vsaj štiri dodiplomske oziroma podiplomske študente/raziskovalce s področja kriptologije.

Nosilci in deležniki

- Ministrstvo za izobraževanje, znanost in šport,
- Ministrstvo za delo, družino, socialne zadeve in enake možnosti in
- Javna agencija za raziskovalno dejavnost Republike Slovenije.

Ukrepi za doseganje ciljnega stanja

- investiranje v izobraževanje kriptološkega kadra;
- nosilci in deležniki določijo kriterije za pridobitev štipendij;
- vsakega štipendista s področja kriptologije se vključi v programsko skupino za kriptologijo;
- Javna agencija za raziskovalno dejavnost Republike Slovenije zagotovi ustrezno politiko obstoja kadra za delo na področju kriptologije.

Tveganja

- brez štipendiranja področja kriptologije tvegamo dolgoročno pomanjkanje ustreznega kadra za razvoj in proizvodnjo šifrirnih rešitev;

brez zagotavljanja novih kadrov na področju kriptologije je tvegano uresničevanje Strategije kriptologije Republike Slovenije.

3.5.2 Zaposlovanje kriptoloških strokovnjakov

Obstoječe stanje

Trenutni kadrovski sistem javnega sektorja nima opredeljenega področja zaposlovanja kriptoloških strokovnjakov.

Ciljno stanje

- povečati pretok kriptološkega znanja med javnim sektorjem, izobraževalnimi in raziskovalnimi ustanovami ter gospodarstvom in s tem podpreti javno-zasebno partnerstvo.

Nosilci in deležniki

- Ministrstvo za javno upravo (nosilec),
- Ministrstvo za obrambo,
- Slovenska obveščevalno-varnostna agencija,
- Ministrstvo za notranje zadeve,
- Ministrstvo za zunanje zadeve,
- Urad Vlade Republike Slovenije za varovanje tajnih podatkov in
- Ministrstvo za gospodarski razvoj in tehnologijo.

Ukrepi za doseganje ciljnega stanja

za uresničevanje Strategije kriptologije Republike Slovenije je treba omogočiti zaposlovanje kriptološkega kadra;

- Ministrstvo za obrambo, Slovenska obveščevalno-varnostna agencija, Ministrstvo za notranje zadeve, Ministrstvo za javno upravo in Ministrstvo za zunanje zadeve – kot največji uporabniki šifrirnih rešitev – morajo sodelovati z izobraževalnimi ustanovami pri pridobivanju kadra s področja kriptologije;
- nosilci in deležniki v sistemizaciji delovnih mest (njihovih organov) na področju informacijske zaščite kot pogoj določijo izobrazbo s področja kriptologije.

Tveganja

- brez vzpostavljenih primernih razmer za zaposlovanje kriptoloških strokovnjakov je tvegano uresničevanje Strategije kriptologije Republike Slovenije.
- brez vzpostavljenih primernih razmer za zaposlovanje kriptoloških strokovnjakov tvegamo odhod visoko strokovnega kadra v tujino.

4 Načrt uresničevanja strategije

4.1 Sodelovanje z deležniki in izvajanje strategije

Odgovorni nosilci in deležniki za izvedbo strategije kriptologije v roku pol leta od sprejetja strategije oblikujejo skupen akcijski načrt za posamezne cilje.

V akcijskem načrtu so opredeljeni časovni okvir za izvedbo ciljev in načini ter viri financiranja.

4.2 Spremljanje in vrednotenje izvajanja strategije

Urad Vlade Republike Slovenije za varovanje tajnih podatkov je zadolžen za spremljanje realizacije Strategije kriptologije Republike Slovenije. Za pridobivanje kadrovskih kazalcev sodeluje s slovenskimi univerzami. Raziskovalno aktivnost na področju kriptologije spremlja Javna agencija za raziskovalno dejavnost Republike Slovenije. Javna agencija za spodbujanje podjetništva, inovativnosti, razvoja, investicij in turizma spremlja vključenost domače industrije v razvoj in proizvodnjo šifrirnih rešitev.

Za dosego posameznih ciljev so zadolženi njihovi nosilci, ki izvajajo potrebne aktivnosti in na svojem področju opravljajo nadzor nad opravljenim delom. Posamezni nosilci Uradu Vlade Republike Slovenije za varovanje tajnih podatkov dvakrat letno poročajo o doseženem napredku.

5 Dejavniki tveganja za uresničevanje strategije

Dejavniki tveganja za uresničevanje zastavljenih strateških ciljev so:

- neugodne gospodarske razmere v državi in posledično pomanjkanje finančnih sredstev,
- vpliv politike na upravljanje s kadri in delovanje uprave,
- nezadostna podpora strokovnosti in kadrovanju v skladu z zahtevami delovnih procesov in ciljev organizacije,
- nestalnost institucionalnega okvira (spremembe ministrstev, institucij) in posledično pomanjkanje finančnih sredstev zaradi večjih stroškov in neobvladovanje organizacijskih težav.