VAROVANJE OSEB, KI IMAJO DOSTOP DO TAJNIH PODATKOV

Janez Rozman

V vsakem organu se mora v skladu s tem zakonom in predpisi, sprejetimi na njegovi podlagi, vzpostaviti sistem postopkov in ukrepov varovanja tajnih podatkov, ki ustreza določeni stopnji tajnosti in onemogoča njihovo razkritje nepoklicanim osebam (prvi odstavek 38. člena zakona o tajnih podatkih, Uradni list RS, št. 135/03 – UPB1, v nadaljevanju: ZTP). Varovanje oseb, ki imajo dostop do tajnih podatkov, je ena od alinej drugega odstavka 38. člena ZTP. Gre za nalogo, ki v nobenem od predpisov, sprejetih na podlagi ZTP, ni doživela podrobnejše ureditve.

Menim, da gre za eno pomembnejših nalog v nizu postopkov in ukrepov varovanja tajnih podatkov. Tajni podatki so zagotovo najbolj ranljivi v fazi fizične obravnave in od trenutka, ko podatek preide v človeški spomin. Pravilen nabor postopkov in ukrepov, ki zagotavljajo ustrezno in učinkovito varovanje oseb (predvsem oseb, ki imajo dostop do tajnih podatkov TAJNO in STROGO TAJNO), je verjetno ključni element ustreznega varovanja tajnih podatkov nasploh. Namen prispevka je, da se vzpodbudijo aktivnosti na tem področju, da se vendarle nekaj premakne na ravni predpisov, predvsem pa v praksi.

Sistem varovanja tajnih podatkov je kompleksno področje. Običajno se postopki in ukrepi delijo na organizacijske, fizične in tehnične postopke in ukrepe. V vseh sistemih je temelj varnosti varnostno preverjanje zaposlenih in drugih oseb, ki bodo dostopale do tajnih podatkov. Zakon o tajnih podatkih v 2. členu pojasnjuje izraz dostop in pravi: »dostop je seznanitev osebe s tajnim podatkom ali možnost osebe pridobiti tajni podatek na podlagi dovoljenja za dostop do tajnih podatkov«. Pravilno razumevanje in uporaba izraza dostop je osnova za določitev kroga oseb, ki se mora zaradi »dostopa« podvreči postopku varnostnega preverjanja in kasneje skrbno izvajati postopke in ukrepe za zagotavljanje varnosti tajnih podatkov do katerih ima dostop in s katerimi je seznanjen.[1]

1 DOLOČITEV DELOVNIH MEST

Dostop do tajnih podatkov je povezan z nalogami, ki se opravljajo na posameznem delovnem mestu. Vsaka od podpisnic zagotovi, da so vse osebe, ki so njeni državljani in ki pri izvajanju svojih uradnih dolžnosti potrebujejo dostop oziroma lahko imajo dostop do tajnih podatkov stopnje CONFIDENTIONAL ali višje stopnje, pred nastopom svojih dolžnosti ustrezno varnostno preverjene (Zakon o ratifikaciji sporazuma med pogodbenicami Severnoatlantske pogodbe p varnosti podatkov – MSPSV, Uradni list RS, št. 22/04 – mednarodne pogodbe). Dokument C-M(2002)49 določa, da morajo države članice in civilni ter vojaški organi Nata zagotoviti, da se za varovanje tajnih podatkov pred izgubo njihove zaupnosti, celovitosti in razpoložljivosti uporabljajo temeljna varnostna načela in minimalni varnostni standardi, določeni v tem dokumentu[2]. Ta dokument v nadaljevanju določa načelo, da se morajo tajni podatki varovati z uravnoteženim sklopom varnostnih ukrepov, ki zajemajo ukrepe za varnostno preverjenost osebja, fizično varnost, varnost podatkov in informacijsko varnost (INFOSEC). Ta sklop ukrepov se uporablja za vse osebe, ki imajo dostop do tajnih podatkov, za vse medije, ki vsebujejo takšne podatke, in za vse prostore, kjer se nahajajo takšni podatki. V prilogi C – varnostna preverjenost osebja, je med drugim zapisano, da se dodelitev dovoljenja za dostop do tajnih podatkov za osebje (personnel security clearance – PSC)[3] ne sme razumeti kot zadnje stopnje v procesu varnostnega preverjanja osebja, saj je treba zagotoviti konstantno primernost posamezne osebe za dostop do Natovih tajnih podatkov. To primernost se doseže tako, da osebje neprestano ocenjujejo varnostni organi in vodje, pa tudi z izobraževanjem osebja o varnosti ter programom o varnostni ozaveščenosti, ki posameznike opominjajo na njihove varnostne odgovornosti in na potrebo po obveščanju svojih vodij in varnostnega kadra o podatkih, ki bi lahko vplivali na njihov varnostni status. V poglavju – varnostna ozaveščenost - je določeno, da morajo biti osebe poučene o varnostnih postopkih ter varnostnih obveznostih. S podpisom posebne izjave potrdijo, da so seznanjene s predpisi, ki urejajo varovanje tajnih podatkov in se zavezujejo ravnati v skladu s temi predpisi in da se zavedajo posledic, ki bi nastale v primeru, da bi prišlo do posredovanja tajnega podatka nepoklicani osebi namerno ali iz malomarnosti. Te osebe, ki bodo dostopale do tajnih podatkov morajo biti že na

začetku seznanjene in periodično ponovno opominjane na varnostna tveganja, ki izhajajo iz nediskretnih razgovorov z osebami, ki nimajo potrebe po seznanitvi s temi podatki (need to know), in z njihovim odnosom do medijev ter na grožnje, ki jih predstavljajo dejavnosti obveščevalnih služb, katerih cilj so zveza Nato in države, ki so njene članice. Posamezniki morajo biti o teh nevarnostih temeljito poučeni in morajo ustrezne varnostne organe nemudoma obvestiti o kakršnemkoli poskusu pristopa ali dejanju, ki se jim zdi sumljiv ali neobičajen. To so načelna izhodišča, ki jih mora Slovenija kot članica Nata upoštevati. ZTP in predpisi, sprejeti na njegovi podlagi tega ne urejajo. Uredba o načinih in oblikah označevanja tajnih podatkov ter fizičnih, organizacijskih in tehničnih ukrepih ter postopkih za varovanje tajnih podatkov (Uradni list RS, št. 70/02) v 25. členu določa, da za načrtovanje, organiziranje in izvajanje usposabljanja in izpopolnjevanja zaposlenih za delo, povezano z varovanjem tajnih podatkov, skrbi UVTP. Predlog nove uredbe EVA 2004-1535-0001, te določne ne vsebuje več, kar pomeni, da se vprašanje usposabljanja in izpopolnjevanja prepušča organom in organizacijam. Verjetno bo treba s spremembami in dopolnitvami ZTP[4] urediti to vprašanje. Da trenutne razmere na tem področju niso dobre je realnost s katero se moramo soočiti in storiti vse potrebno, da se stanje izboljša. Verjetno je ena večjih težav v sposobnosti izvajanja teh ukrepov. Ali imamo dovolj strokovno usposobljenega kadra za izvajanje teh nalog? Drugo pomembno vprašanje je, ali je število sistemiziranih delovnih mest na katerih se zahteva dovoljenje za dostop do tajnih podatkov realno?[5] Dejstvo je, da se mora krog oseb, ki bodo imele dostop do tajnih podatkov najvišje stopnje tajnosti še zmanjšati. Temeljni problem je bil, da z uveljavitvijo ZTP nismo imeli organa, ki bi bil odgovoren za njegovo uveljavitev. S sklepom vlade (Uradni list RS, št. 6/02) je bil ustanovljen UVTP, vendar njegove pristojnosti in pooblastila segajo predvsem na zagotavljanje izpolnjevanja prevzetih obveznosti z vstopom v Nato in EU, v praksi pa tudi tistih pristojnosti ki jih ima, ne opravlja v skladu s potrebami in pričakovanji[6]. Ne samo zaradi tega, vendar pa tudi zaradi tega, je praksa izvajanja ZTP dokaj različna – neenotna. Trdim, da je delovnih mest za katera se zahteva dovoljenje za dostop do tajnih podatkov mnogo preveč, kar pomeni, da bodo v »sistem varovanja« vključeni tudi zaposleni, ki v praksi dejansko sploh nimajo opravka s tajnimi podatki in od tistih, ki obdelujejo tajne podatke, je zelo malo takih, ki obdelujejo tajne podatke stopnje TAJNO in višje, zato bo treba ločevati med zaposlenimi, ki imajo dovoljenje za dostop do tajnih podatkov in s tajnimi podatki ne rokujejo oziroma rokujejo s tajnimi podatki stopenj INTERNO ali ZAUPNO in tistimi, ki obdelujejo tajne podatke TAJNO in višje. Očitno je dovoljenje postalo tudi statusni simbol - simbol pomembnosti.

2 POSTOPKI IN UKREPI

Postopke in ukrepe bi lahko delili na ukrepe in postopke, ki jih izvaja služba[7] in ukrepe in postopke, ki jih izvaja posameznik, oboje pa je tesno medsebojno povezano, saj posamezniku ključna znanja s tega področja posreduje služba v obliki usposabljanj in izpopolnjevanj, razgovorov in podobno. V varnostni politiki Nata je v poglavju »varnostna ozaveščenost in poučenost posameznikov« zapisano: »Vse osebe, ki so pooblaščene za dostop do Natovih tajnih podatkov, ali osebe, ki morajo delati s takšnimi podatki, morajo biti že na začetku seznanjene in periodično znova opomnjene na varnostna tveganja, ki izhajajo iz nediskretnih razgovorov z osebami, ki nimajo potrebe po seznanitvi z vsebino takšnih podatkov, in iz njihovih odnosov z mediji, ter na grožnje, ki jih predstavljajo dejavnosti obveščevalnih služb, katerih cilj so zveza Nato in države, ki so njene članice. Posamezniki morajo biti o teh nevarnostih temeljito poučeni in morajo ustrezne varnostne organe nemudoma obvestiti o kakršnem koli poskusu pristopa ali dejanju, ki se jim zdi sumljiv ali neobičajen.« V Sklepu sveta (2001/264/EC) je v oddelku V »splošna pravila o načelu potrebe po seznanitvi s podatki zaradi opravljanja funkcije ali delovnih nalog« v poglavju »posebna navodila« zapisano:

»15. Osebe, od katerih se zahteva delo s tajnimi podatki EU, je treba ob prvem prevzemu nalog in nato v periodičnih presledkih opozarjati na:

(a) nevarnosti, ki jih za varovanje tajnosti pomenijo indiskretni pogovori;

(b) previdnostne ukrepe v njihovih stikih s tiskom;

(c) nevarnost, ki jo za EU in države članice v zvezi s tajnimi podatki in dejavnostmi EU predstavljajo dejavnosti obveščevalnih služb;

(d) obveznost takojšnjega poročanja ustreznim varnostnim organom o vsakem poskusu ali ravnanju, ki bi zbudil sum o vohunski dejavnosti, ali o kakršnihkoli nenavadnih okoliščinah v zvezi z varovanjem tajnosti.

16. Vse osebe, ki so običajno izpostavljene pogostim stikom s predstavniki držav, katerih obveščevalne službe imajo za cilj EU in države članice v zvezi s tajnimi podatki in dejavnostmi EU, se pouči o tehnikah, za katere je znano, da jih uporabljajo različne obveščevalne službe.

17. Za zasebna potovanja osebja, ki je bilo glede dostopa do tajnih podatkov EU varnostno preverjeno, v katero koli smer, Svet ne predvideva predpisov o varovanju tajnosti. Vendarle pristojni varnostni organi uradnike in druge uslužbence, ki spadajo v njihovo pristojnost, seznanijo s pravili potovanja, ki jih bodo morali spoštovati v danih primerih. Pristojni uradniki za varovanje tajnosti so zadolženi za organiziranje sestankov, na katerih članom osebja osvežijo ta posebna navodila.«

2.1 Varnostno preverjanje

Posameznik se s tematiko tajnih podatkov »prvič« sreča v postopku varnostnega preverjanja (drugi odstavek 4. člena uredbe o načinu in postopku varnostnega preverjanja – Uradni list RS, št. 110/03). Predlagatelj je dolžan kandidata seznaniti s predpisi s področja varovanja tajnih podatkov, potrebo po pridobitvi dovoljenja za dostop do tajnih, obsegom varnostnega preverjanja ter vsebino in postopkom za pridobitev dovoljenja, mu izroči ustrezen vprašalnik in da v podpis izjavo o seznanitvi z zakonom in predpisi, izdanimi na njegovi podlagi. Na ta način se je odgovornost seznanjanja s tematiko varovanja tajnih podatkov prenesla na predlagatelja. Ali in v kakšnem obsegu in kako kvalitetno se to izvaja, je že drugo vprašanje. Glede na to, da gre za osnovna pravila varovanja, ki jih mora poznati vsak, ki dostopa do tajnih podatkov, bi bilo primerneje, da bi sistem oblikovali tako, da bi se organiziralo osnovna usposabljanja. Udeležba na tem usposabljanju bi bila eden od pogojev za začetek postopka varnostnega preverjanja.[8]

Za potrebe varovanja bo treba namen varnostnega preverjanja dopolniti. Podatki zajeti v vprašalnikih za varnostno preverjanje in podatki zbrani v postopku varnostnega preverjanja se smejo po veljavni ureditvi uporabiti zgolj v postopku varnostnega preverjanja za dostop do tajnih podatkov, potem pa organ shrani dovoljenje in pisno soglasje za varnostno preverjanje z izpolnjenim vprašalnikom v posebni del kadrovske mape osebe, ki se lahko uporablja le v zvezi z izvajanjem določb tega zakona oziroma predpisov, izdanih na podlagi tega zakona (28. člen ZTP). Podatki o varnostnem preverjanju se lahko uporabljajo le za namene, za katere so bili zbrani.[9] Hranijo se toliko časa, dokler ima oseba pravico dostopa do tajnih podatkov, nato se obravnavajo skladno z določili zakona, ki ureja arhivsko gradivo in arhive. Taka ureditev je bila morda v nekem obdobju dobra, za resno delo na področju varovanja tajnih podatkov, pa je ta določba toga. Postavi se vprašanje ali službi, ki je odgovorna za varnost dovoliti vpogled v podatke zbrane v postopku varnostnega preverjanja, če izhajamo iz temeljnega namena varnostnega preverjanja. Dejstvo je, da se okoliščine v času spreminjajo in da posameznik postane zanimiv za »vsiljivce«[10], ko pridobi dostop do tajnih podatkov. V postopku varnostnega preverjanja se preverjajo varnostno relevantni podatki za določeno časovno obdobje – 5 ali 10 let. Ugotovitve varnostnega preverjanja so neke vrste garancija, da je posameznik vreden zaupanja tudi v prihodnje. Dovoljenje se izda za obdobje 5 ali 10 let, to je relativno dolgo obdobje v katerem se lahko marsikaj spremeni. Iz vidika varovanja tajnih podatkov so relevantne spremembe podatkov iz varnostnih vprašalnikov[11]. Zakon ne zavezuje posameznika, da obvešča pristojni organ o spremembah podatkov iz varnostnih vprašalnikov. Zakon govori o vmesnem varnostnem preverjanju[12] in sloni na predpostavki, da bo nekdo te podatke posredoval odgovorni osebi. Verjetno bi bilo treba zavezati tudi posameznika, da podatke, ki pomenijo odstop od podatkov navedenih v vprašalnikih, sporoči organu[13], ki je pristojen za vodenje postopka varnostnega preverjanja. Opustitev dolžnosti sporočanja bi morda lahko uvrstili celo med razloge za preklic dovoljenja, zagotovo pa med razloge za vmesno varnostno preverjanje.

2.2 Usposabljanje in izpopolnjevanje

Za vse osebe, ki dostopajo do tajnih podatkov mora država zagotoviti ustrezne oblike usposabljanja in izpopolnjevanja v obliki seminarjev, delavnic, predavanj, razgovorov na individualni ravni in drugo. To obvezo je treba zapisati v zakon, poleg tega pa naložiti vsem organom, da določijo osebo, ki bo odgovorna za varovanje tajnih podatkov v organu. Vsebine – teme seminarjev, razgovorov bodo zelo pestre, odvisno od ciljne skupine. Posameznik mora biti seznanjen s ključnimi metodami dela »vsiljivcev«, če želimo, da bo pravočasno zaznal okoliščine, ki kažejo na to, da je postal zanimiv. Zanimivo je, da nekatere tuje države na spletnih straneh objavlja članke v katerih nekako nalagajo svojim državljanom, kako naj se samozaščitno obnašajo, koga naj obvestijo, če ugotovijo, da so zaradi dela, ki ga opravljajo tarča tuje obveščevalne službe in drugo. Gre za zanimiv pristop preventivnega dela, bistveno teže pa je to prenesti v predpis – zakon in to zahtevati od državljanov. Prav iz teh razlogov trdim, da je sistem usposabljanja in izpopolnjevanja ključnega pomena za učinkovito varovanje tajnih podatkov.

Nacionalni varnostni organ, katerega poslanstvo se veže predvsem na izvajanje postopkov in ukrepov povezanih z obravnavanjem tajnih podatkov zveze Nato in EU bo moral v prihodnje prevzeti bistveno več odgovornosti tudi za zagotavljanje učinkovitega varovanja na nacionalni ravni ali pa se to poveri enemu od resorjev. Znanja s tega področja se morajo na ravni države združevati in dopolnjevati v povezavi z vsemi, ki imajo znanja s tega področja[14]. Poleg zaprosila za izdajo varnostnega potrdila za dostop do tajnih podatkov Nato in EU je treba podpisati posebno izjavo[15], s katero se posameznik moralno zaveže, da bo s tajnimi podatki ravnal pravilno, to pa je tudi bolj ali manj vse. Je sploh korektno, da se od posameznika zahteva podpis take izjave, če ga nihče ni poučil o nevarnostih, katerim je izpostavljen zaradi delovanja obveščevalnih služb, katerih cilj so podatki s katerimi razpolaga? Dejstvo je, da gre v tem primeru za formalnost, ki mora biti izpolnjena, kar pa za varno obravnavanje tajnih podatkov ni dobro. Raven varnostne kulture bo treba dvigniti na višjo raven, najprej na ključnih mestih, kjer se kroji politika varovanja tajnih podatkov in kjer nastajajo predpisi, ki urejajo to področje.

3 DOLŽNOSTI POSAMEZNIKA

S predpisi je treba določiti ustrezen nabor dolžnosti, ki jih mora posameznik izvajati v času, ko dostopa do tajnih podatkov in v nekaterih primerih tudi kasneje. Zagotovo sem sodi dolžnost obveščanja o spremembah vsebine odgovorov na vprašanja iz varnostnih vprašalnikov (nekdo lahko pridobi državljanstvo tretje države, spremembe osebnega imena, bivališča in drugo). Dolžnost obveščanja o stikih s predstavniki tujih varnostnih in obveščevalnih služb. Dolžnost obveščanja o težavah na finančno materialnem področju, ki so okoliščine, ki kažejo na prezadolženost.[16] Morda bi namesto dolžnost zapisali »možnost«. Zaposleni mora imeti možnost, da dobi ustrezno strokovno pomoč, še preden pregloboko zabrede v težave, dolžnost organizacije pa je, da vzpostavi sistem, ki bo zaposlene navajal na to in ki bo znal prepoznati dejavnike, ki kažejo na to, da je s posameznikom nekaj narobe.

4 SKLEPNO

Prispevek je nastal v času, ko se pripravljajo spremembe in dopolnitve zakona o tajnih podatkih, v času, ko nastaja nova uredba o varovanju tajnih podatkov, ki se tega vprašanja sploh ne dotika, z namenom, da se vzpodbudi razmišljanje o tem kako in v kakšnem obsegu urediti to vprašanje v predpisih in v nadaljevanju, kako to izpeljati v praksi. Žal se v praksi sistem varovanja tajnih podatkov preveč gradi samo na tehniki (blagajne, signalno varnostne naprave, kamere in drugo). Sistem varovanja tajnih podatkov bo ustrezen takrat, ko bo ustrezno urejeno tudi varovanje oseb, ki dostopajo do tajnih podatkov. Predpisi EU in dokumenti Nata nam dajejo dovolj dobro osnovo, da se to vprašanje ustrezneje uredi tudi v nacionalnih predpisih.

OPOMBE

[1] Razlikovati moramo med izrazom dostop, ki je zapisan v 2. členu ZTP in dejansko seznanitvijo z vsebino tajnih podatkov. Postopki in ukrepi morajo zajeti tudi osebje, ki ima samo možnost dostopa (varnostno osebje, vzdrževalci …) in osebje, ki sicer rokuje s tajnimi podatki, vendar z vsebino niso seznanjeni (kurirji, osebje v glavni – sprejemni pisarni…). To so dejstva, ki jih morajo odgovorni za načrtovanje in izvajanje postopkov in ukrepov varovanja upoštevati. Sistem varovanja je skupek medsebojno povezanih postopkov in ukrepov, ki zajema vse, ki sodijo v kategorijo oseb, ki imajo dostop do tajnih podatkov.

[2] Tu je treba opozoriti, da temeljni dokument Nata določa temeljna varnostna načela in minimalne varnostne standarde, kar pomeni, da ne gre za "klasičen predpis«, ki bi bil neposredno uporabljiv, kot trdijo nekateri. Ta dokument postavlja načela in standarde, ki jih je treba upoštevati pri vzpostavljanju nacionalnega sistema varovanja, po katerem se bodo obravnavali tudi tajni podatki Nato.

[3] PSC je varnostno potrdilo s katerim nacionalni varnostni organ potrjuje, da je posameznik varnostno preverjen v skladu z nacionalno zakonodajo in da poseduje veljavno dovoljenje za dostop do tajnih podatkov določene stopnje.

[4] Ministrstvo za notranje zadeve je sprožilo postopek sprememb in dopolnitev ZTP. Delovna skupina je imenovana in mora pripraviti predlog sprememb in dopolnitev ZTP.

[5] Osebno menim, da je tu prišlo do pretiravanja in bo treba v nekaj letih to popraviti. Z nepremišljenimi koraki na tem področju je vse preveč zaposlenih "obremenjeno" z varnostnim preverjanjem, v nadaljevanju pa bomo ugotovili, da bo zelo težko zagotoviti ustrezno usposabljanje in izpopolnjevanje za tako maso zaposlenih.

[6] S spremembo ZTP v letu 2003 je zakonodajalec v spremenjenem prvem odstavku 43. člena zapisal, da vlada določi nacionalni varnostni organ, ki spremlja izvajanje tega zakona in drugih predpisov, sprejetih na njegovi podlagi, v prehodnih določbah pa je določil, da do določitve nacionalnega varnostnega organa njegove naloge0020opravlja UVTP. Vlada tega še ni storila, tako še vedno ni jasno, kdo bo v prihodnje opravljal naloge nacionalnega varnostnega organa.

[7] V Ministrstvu za obrambo je to Obveščevalno varnostna služba, ki ji zakon o obrambi v 4. poglavju »strokovne obveščevalne, protiobveščevalne in varnostne naloge obrambe« nalaga naloge tudi na tem področju«. Problem nastane v resorjih, ki takih »služb« nimajo.

[8] V okviru državne uprave bo treba določiti organ in vsebine osnovnega programa ter izvajalce. Posameznik bi po končanem usposabljanju dobil potrdilo o udeležbi na usposabljanju. Usposabljanja bi se lahko udeležil vsak delavec (po odobritvi in napotitvi nadrejenega). Usposabljanja bi morala biti brezplačna. V nadaljevanju bi se pripravili programi za dodatna "funkcionalna" usposabljanja (določanje podatkov za tajne – ocean možnih škodljivih posledic, dokumentiranje in evidentiranje, industrijska varnost, informacijska varnost, varnostno preverjanje in drugo). Tudi na ta način bi se združevala, dopolnjevala in nadgrajevala znanja s področja varovanja tajnih podatkov.

[9] Zbrani so bili za izvedbo postopka varnostnega preverjanja. Zakon daje možnost vmesnega varnostnega preverjanja, kjer pa se preverja samo ugotovitve v okviru vprašanj iz 25. člena ZTP.

[10] Namenoma uporabljam izraz "vsiljivci", ker želim s tem zajeti najširši možni krog oseb, ki želijo priti do tajnih podatkov do katerih dostopa oseba, pa te pravice nimajo (od radovednega sodelavca, soseda, žene, do pripadnika tuje obveščevalne službe).

[11] Vsaka sprememba ima svoj pomen v času in prostoru in tako je treba tudi jemati vprašanje sporočanja sprememb. Sprememba bivališča verjetno nima večje teže, vendar če gre za osebo, ki bo obravnavala tajne podatke najvišje stopnje, je verjetno tudi ta podatek pomemben prav iz vidika izvajanja protiobveščevalnih ukrepov.

[12] Če je zoper osebo, ki ima dovoljenje za dostop do tajnih podatkov, sprožen disciplinski postopek zaradi kršitve pravil obravnavanja tajnih podatkov ali kazenski postopek zaradi suma storitve naklepnega kaznivega dejanja, ki se preganja po uradni dolžnosti, ali je podan sum varnostnega zadržka iz četrte ali pete alinee 27. člena tega zakona, se opravi vmesno varnostno preverjanje.

[13] Zakon o preprečevanju korupcije v 37. členu nalaga funkcionarjem, da vsako leto izkažejo podatke o letnih dohodkih in da sporočajo podatke o dohodnini in vsako spremembo premoženja, ki jo je treba po zakonu preprečevanju pranja denarja obvezno sporočiti.

[14] Fakulteta za policijsko-varnostne vede zagotovo sodi v ta krog.

[15] Podpisani/a _____, roj. _____ , posedujem veljavno dovoljenje za dostop do tajnih podatkov do stopnje tajnosti _____ št._____ izdano pri _____ dne_____ izjavljam, da sem seznanjen/a s postopki in ukrepi za varno dostopanje, obdelavo, posredovanje in hranjenje tajnih podatkov, ki so v lasti Republike Slovenije in zveze NATO ter se hkrati zavedam vseh odgovornosti in posledic, ki bi lahko nastale v primeru neprimernega, neodgovornega ali drugega protipravnega ravnanja, ki je v nasprotju z predpisi in veljavnim pravnim redom Republike Slovenije in zveze NATO, ki urejajo in določajo varovanje ukrepov in postopkov za varovanje tajnih podatkov. Enaka je vsebina izjave za dostop do tajnih podatkov EU. Predpisi EU so dostopni na spletnih straneh, dokumenti Nata pa so označeni »Nato unclassified« - brez stopnje tajnosti znotraj zveze Nato in niso dostopni širši javnosti, še znotraj uprave je dostop relativno omejen.

[16] Posameznik lahko zaide v finančne težave in s tem postane ranljiv. Če bo ta problem sporočil, bo dobil ustrezna navodila, kako ravnati, da se zavaruje pred morebitnim izsiljevanjem, "ugodnim" kreditom in drugo. Na spletni strani »http://rf-web.tamu.edu/security/SECGUIDE/spystory/Intro.htm#True%20Spy%20Stories« je objavljenih nekaj zanimivih prispevkov s tega področja.

O AVTORJU

Janez Rozman, univ. dipl. prav., sekretar za sistemska vprašanja v Sekretariatu generalnega sekretarja Ministrstva za obrambo - za ministrstvo opravlja naloge s področja usmerjanja in uveljavljanja skupnih osnov enotnega sistema določanja, varovanja in dostopa do tajnih podatkov.