

Zagotavljanje industrijske varnosti

Aleš Kotnik

Povzetek:

Namen prispevka:

V okviru prispevka bom predstavil kaj predstavlja danes pojem industrijske varnosti, kakšna je vloga industrijske varnosti glede na osebno varnost, fizično varnost, dokumentacijsko varnost in informacijsko varnost, kje je njeno mesto znotraj državnih organov in gospodarskih družb, pravno ureditev področja industrijske varnosti, zagotavljanje industrijske varnosti, vlogo industrijske varnosti v okviru MO in SV ter nakazal možnosti sodelovanje slovenskih gospodarskih družb in organizacij na mednarodnem področju znotraj EU in NATO.

Osnovni cilji:

1. Industrijska varnost kot sestavni del varnostne politike.
2. Ustrezna stopnja zaščite tajnih podatkov na vseh nivojih.
3. Potrebno dopolnjevanje notranjih pravnih aktov na področju industrijske varnosti.
4. Potrebno zagotavljanje sredstev za vzpostavitev pogojev za zagotavljanje industrijske varnosti.
5. Izboljšanje postopkov na področju industrijske varnosti.

Posebni cilji:

6. Razvoj modela za ocenjevanje ustreznosti sistemov varovanja na področju industrijske varnosti.
7. Izdelava priročnika na področju industrijske varnosti.

Metodologija:

Pri izdelavi prispevka sem uporabil naslednje metode:

- analize stanja na področju industrijske varnosti,
- analiza dokumentov, ki opredeljujejo industrijsko varnost,
- izkustveno metodo poznavanja sistemov,
- empirično raziskavo z izdelavo modela za ocenjevanje ustreznosti sistemov varovanja.

Ugotovitve:

Uspehi na področju industrijske varnosti so v veliki meri odvisni od sodelovanja državnih organov na tem področju. Bistvenega pomena za uveljavitev in doseganje standardov na področju industrijske varnosti je izdelava priročnika, ki bo namenjen gospodarskim družbam. Zagotovitev večje podpore industrijski varnosti z:

- Spremembami in dopolnitvami zakonodaje v kolikor se za to izkažejo potrebe.
- Izboljšanjem postopkov na področju industrijske varnosti (priročnik).
- Spodbujanjem gospodarskih družb, da si pridobijo oz. zagotovijo pogoje za pridobitev varnostnega dovoljenja, kar je lahko s pridobitvijo varnostnega dovoljenja do neke mere prednost na domačem in mednarodnem trgu, odvisno od trenutnega stanja.

Praktična uporabnost:

Prispevek je namenjen vsem zaposlenim v državnih organih, ki delajo na področju industrijske varnosti in zaposlenim v gospodarskih družbah, ki sodelujejo z državnimi organi v smislu izmenjave tajnih podatkov.

Izvirnost/pomembnost prispevka:

S prispevkom želim poudariti pomembnost izdelave priročnika na področju industrijske varnosti za potrebe in uporabo izven okvira državnih organov in nujnost izdelave modela za

ocenjevanje varnostnih postopkov, ki bi v skladu z obstoječo zakonodajo omogočal ustrezno stopnjo varovanja in večjo fleksibilnost.

Ključne besede: Industrijska varnost, varovanje tajnih podatkov državnih organov v gospodarskih družbah, pravna ureditev, mednarodna industrijska varnost

1 UVOD

Občutek ogroženosti in nevarnosti, ki prežijo na nas povzročajo škodo, socialne in ekonomske posledice, kar nasploh znižuje kakovost našega življenja. Stopnja zagotavljanja varnosti je pokazatelj kakovosti našega življenja, za kar je potrebno prizadevanje državnih organov in vseh organizacij ter posameznikov, ki so za to odgovorni.

Politični, gospodarski, družbeni, tehnični in drugi dejavniki zato zahtevajo tudi enotno obravnavanje varnosti na področjih osebne, fizične, tehnične, informacijske, dokumentacijske in **industrijske varnosti**.

V globalnem smislu prihaja ne samo do izmenjave podatkov med državnimi organi in gospodarskimi družbami znotraj države ampak do so sodelovanja in kontaktov med več državami, regijami in gospodarskimi družbami na mednarodnem prizorišču. Različni dejavniki vpliva dajejo temu sodelovanju odgovorno in občutljivo vlogo pri sodelovanju državnih organov z industrijo na različnih trgih. Industrijska varnost v tem pogledu pridobiva na veljavi in zahteva celovit pristop k reševanju varnostnih vprašanj na tem področju.

Po vstopu Slovenije v NATO in EU ter posledično delovanja Slovenske vojske in obrambnega sistema v zavezništvih se je okrepila tudi slovenska obrambna industrija in izboljšal tudi dostop do mednarodnih trgov drugih držav. Vse to nam omogoča sodelovanje v mreži ekspertov v industriji in gospodarstvu, kjer se pojavljajo tajni podatki državnih organov.

Vsaka gospodarska družba ima svoje vrednote od kadrov (delavci in vrhunski strokovnjaki), patentov, tehnologij do infrastrukture in strojev. Vse navedeno je potrebno varovati in zaščititi pred raznimi negativnimi dejavniki. V kolikor pa gospodarska družba razpolaga s tajnimi podatki državnih organov, pa mora zadostiti zakonskim določilom na področju varovanja tajnih podatkov in te zahteve obvezno vključiti svoj sistem fizičnega, tehničnega, informacijskega, dokumentacijskega in industrijskega varovanja.

2 METODOLOŠKI OKVIR

V okviru naloge bom v nadaljevanju skušal predstaviti kaj predstavlja danes pojem industrijske varnosti, kakšna je vloga industrijske varnosti glede na osebno varnost, fizično varnost, dokumentacijsko varnost in informacijsko varnost, kje je njeno mesto znotraj državnih organov in gospodarskih družb, pravno ureditev področja industrijske varnosti, zagotavljanje industrijske varnost, industrijsko varnost kot sestavni del varnostno logističnega okvirja, industrijska varnost kot sistem in njeni posamezni deli, vlogo industrijske varnosti v okviru MO in SV ter nakazal možnosti sodelovanje slovenskih gospodarskih družb in organizacij na mednarodnem področju znotraj EU oziroma Evropske obrambne agencije in NATO oziroma NATO agencije za vzdrževanje in oskrbo.

Razvoj industrijske varnosti pomembno vpliva na zagotavljanje višje stopnje varnosti, saj vključuje tako državne organizacije in gospodarske družbe v domačem in mednarodnem okolju in tako zajame velik del pri zagotavljanju učinkovitega varovanja tajnih podatkov in s tem interesov državnih organov in gospodarskih družb s katerimi sodelujejo.

Hipoteza: Za izboljšanje stanja na področju industrijske varnosti je potrebno razviti model, ki bo s pomočjo numeričnega točkovanja, določil potrebne parametre za vzpostavitev upravnega ali varnostnega območja ter potrebne (vgrajene) sisteme fizičnega in tehničnega varovanja.

Naloga bo zajela naslednje cilje katere mora doseči vsaka država na področju industrijske varnosti:

1. Industrijska varnost kot sestavni del varnostne politike.
2. Ustrezna stopnja zaščite tajnih podatkov na vseh nivojih med organizacijami in gospodarskimi družbami.
3. Potrebno sklepanje bilateralnih varnostnih sporazumov med državami o varovanju tajnosti izmenjanih tajnih podatkov, njihovo hranjenje, distribucija in postopki ob nepooblaščenim seznanitvi ali odtujitvi tajnih podatkov in ustrezen pregon storilcev.
4. Potrebno dopolnjevanje že sprejetih pravnih aktov na področju industrijske varnosti in sprejemanje novih v primeru novih spoznanj in situacij.
5. Potrebno delovanje mednarodnega organa na področju industrijske varnosti.
6. Potrebno zagotavljanje sredstev za vzpostavitev pogojev za zagotavljanje industrijske varnosti.
7. Izdelava priročnika o industrijski varnosti.

Z nalogo bomo predstavili razvojna, organizacijska in druga izhodišča ter določili cilje pri razvoju industrijske varnosti. V nalogi bodo podrobneje predstavljeni razlogi za vključitev gospodarskih družb in drugih organizacij na področju industrijske varnosti in pogoje, ki ji morajo izpolnjevati.

Glede na naše izkušnje s področja zagotavljanja varovanja gospodarskih družb v vseh pogojih, želim vsem, ki se ukvarjajo s tem področjem pokazati, da področje varovanja življenj, materialno tehničnih sredstev in tajnih podatkov zahteva usklajeno delo vseh subjektov, pravočasno načrtovanje in izdelavo modelov varovanja, ki zagotavljajo ustrezno stopnjo zaščite na področju industrijske varnosti.

2.1 Predpostavke in omejitve raziskave

Pri raziskavi industrijske varnosti v nalogi ne bodo vsebovani konkretni podatki o varovanju določenih objektov, zaradi zaščite teh podatkov v smislu šibkih točk in morebitnega vdora v sistem. Prav tako ni namen raziskave razpolagati s konkretnimi podatki, ampak poiskati ustrezne rešitve na celotnem področju, ki ga zajema Slovenska vojska in širše Ministrstvo za obrambo glede na sodelovanje z gospodarskimi družbami.

Omejitev predstavlja tudi širina področja industrijske varnosti, zato v raziskavo ne bomo vključili podrobne tehnične podatke in karakteristike različnih sistemov tehničnega, fizičnega in informacijskega varovanja.

3 INDUSTRIJSKA VARNOST

Industrijska varnost se ukvarja z ukrepi in postopki, ki so potrebni za varovanje tajnih podatkov v odnosih med gospodarskimi družbami in organizacijami, kadar med njimi pride do izmenjave tajnih podatkov.

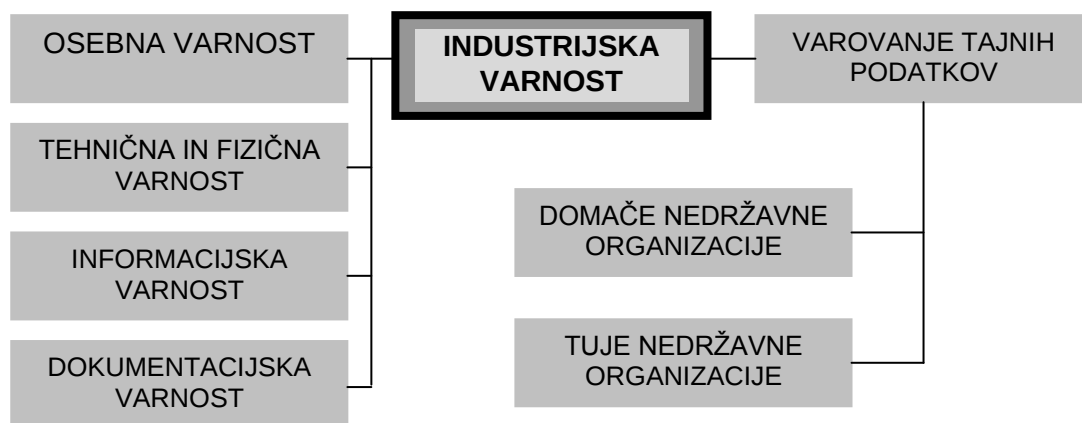
V zadnjem času dobiva industrijska varnost na veljavi, saj prihaja do določenih skupnih nalog in izvajanja projektov, kjer sodelujejo državni organi, druge organizacije in gospodarske družbe in prihaja do izmenjave občutljivih informacij oziroma do prenosa tajnih podatkov na gospodarske družbe.

Uporaba varnostnih ukrepov in postopkov mora preprečevati, odkrivati in povrniti izgubo in ogrožanje tajnih podatkov v kakršnikoli obliki, s katerimi razpolagajo gospodarske družbe in organizacije. Za gospodarske družbe veljajo pravila industrijske varnosti tako za izvajalce kot podizvajalce in sicer pred dodelitvijo posla, med pogajanjem pred dodelitvijo in med izvajanjem tajnega naročila ali podnaročila.

Pogodba s stopnjo tajnosti je vsaka pogodba, ki zahteva ali bo zahtevala, da ima pri izvajanju pogodbe dostop do informacij označenih s stopnjo tajnosti zunanji izvajalec, podizvajalec ali njegovi zaposleni. V to je vključena tudi faza pred sklenitvijo pogodbe, kamor sodijo zbiranje ponudb, cen in predlogov, pogajanja pred sklenitvijo pogodbe ali tudi kakšni drugi projekti državnih organov, ki zahtevajo, da ima pogodbenik dostop do informacij s stopnjo tajnosti.

Pojem industrijske varnosti lahko opredelimo kot del varnostne politike izven državnih organov, ki je sestavljena iz osebne (kadrovske) varnosti, tehnične in fizične varnosti, informacijske varnosti in dokumentacijske varnosti.

Poznavanje sistemov tehničnega varovanja je ključnega pomena za kader, ki načrtuje izvajanje varovanja na področju industrijske varnosti, saj se le na ta način doseže ustrezna stopnja sinergije tehničnega in fizičnega varovanja.



Slika 1: Elementi industrijske varnosti

Glavni problem pri zagotavljanju ustrezne stopnje varovanja gospodarskih družb in organizacij, predstavlja ocenjevanje ustreznosti varnostnih sredstev in izvedenih ukrepov za varovanje.

Po vstopu Republike Slovenije v zvezo NATO in Evropsko unijo je bilo potrebno urediti postopek varovanja tajnih podatkov na področju industrijske proizvodnje in širše na celotnem

prostoru slovenskega gospodarstva v primeru potrebe po posredovanju tajnih podatkov. Tako smo v Republiki Sloveniji uredili postopke in ukrepe za izvajanje industrijske varnosti in predpisali zakonodajo. Pravila v Republiki Sloveniji glede industrijske varnosti so v soglasju s pravili, ki veljajo v NATO in EU. Tako si mora organizacija preden se ji posredujejo tajni podatki, pridobiti ustrezno varnostno dovoljenje ustrezne stopnje. Varnostno dovoljenje je ključni vezni element med državo in gospodarstvom na področju varovanja tajnih podatkov.

3.1 Pojem industrijske varnosti

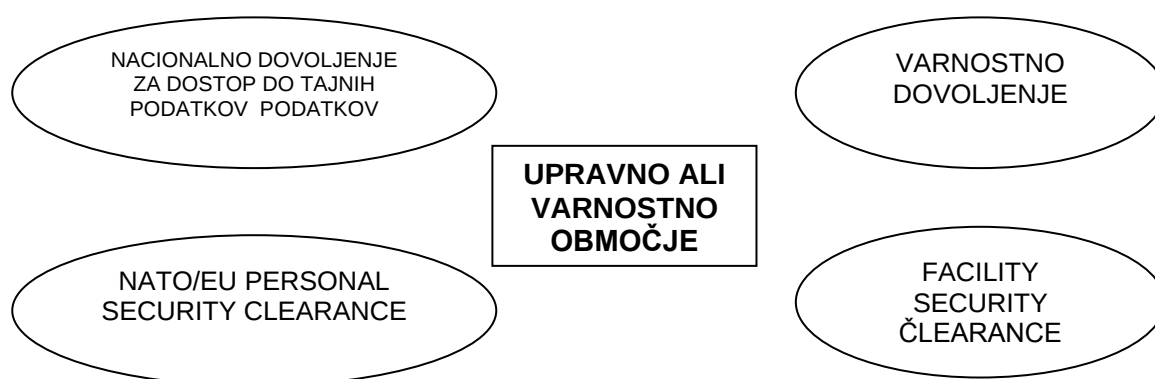
Industrijska varnost v kratjši obliki definicije predstavlja varovanje tajnih podatkov izven državnih organov. Industrijska varnost zagotavlja ukrepe za varovanje tajnih podatkov, kadar naročila in dodelitev naročil med gospodarskimi družbami in organizacijami vsebujejo tajne podatke.

Z industrijsko varnostjo se zagotovijo varnostni postopki za preprečevanje, odkrivanje in povrnitev izgube ali prenehanje ogrožanja nosilcev tajnih podatkov s katerimi razpolagajo izvajalci in podizvajalci v času pogajanj pred sklenitvijo poslov in kasneje med samim izvajanjem tajnih naročil in podnaročil.

Dosedanja praksa kaže, da se je največ tajnih naročil v preteklih letih nanašalo na dobavo in storitve s področja obrambne oz. vojaške industrije, v zadnjem času pa je tudi več tajnih naročil na področju visoko tehnološkega blaga in storitev s področja informatike in komunikacij. V NATO predstavljajo tajna naročila tudi nekatera naročila s področja gradbenih in inženirskih del.

Države v zvezah (NATO, EU) pa so sprejele minimalne standarde varnosti, ki jih je potrebno upoštevati pri zagotavljanju industrijske varnosti. Na nižjih ali podrejenih nivojih morajo te standarde upoštevati in jih ne smejo spreminjati. Tudi na mednarodnem področju predstavlja pojem industrijske varnosti podobno definicijo in sicer so tu zajeti ukrepi varnostne organizacije, fizične, dokumentacijske, kadrovske tehnične in informacijske varnosti. Vse morajo biti usklajene s ciljem zagotavljanja minimalnih standardov varnosti.

Poleg pojma industrijske varnosti je tu potrebno omeniti še soodvisne pojme, ki so pogoj za zagotavljanje varnosti: Dovoljenje za dostop do tajnih podatkov, »Personal Security Clearance«, Varnostno dovoljenje in »Facility Security Clearance«.



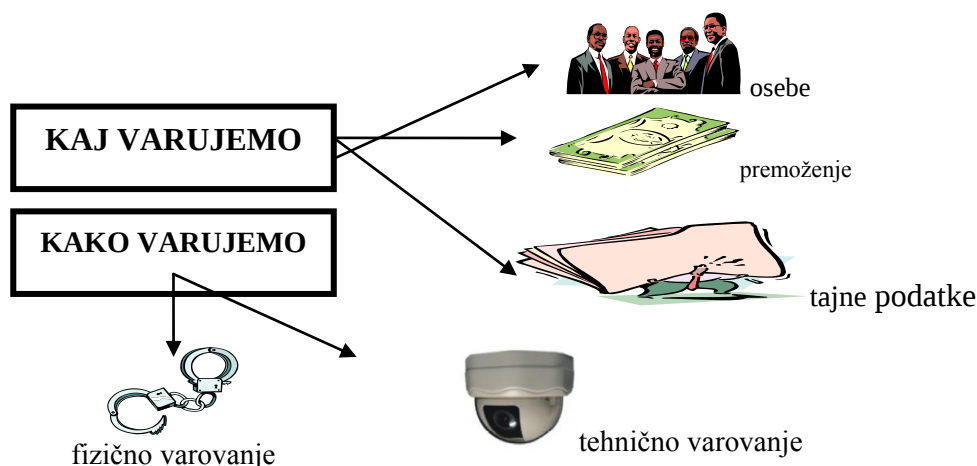
Slika 2: Pridobitev potrebnih dovoljenj za upravno ali varnostno območje

Industrijska varnost predstavlja vse ukrepe in postopke, ki so namenjeni varovanju tajnosti slovenskih in tujih tajnih podatkov v gospodarskih družbah in institucijah. Gospodarska

družba, ki zagotovi izvajanje vseh predpisanih varnostnih postopkov si pridobi varnostno dovoljenje ustrezne stopnje s katerim lahko sodeluje v poslih, ki vsebujejo tajne podatke. Varnostno dovoljenje se izda gospodarski družbi, kjer bodo tajni podatki namenjeni izvajanju pogodb. Izdano varnostno dovoljenje je v tujini poznano kot »Facility Security Clearance. V gospodarski družbi, ki hoče pridobiti varnostno dovoljenje mora imeti vsaj en pooblaščen predstavnik te družbe izdano dovoljenje za dostop do tajnih podatkov oz. tuje »Personal Security Clearance.

3.1.2 Varovanje gospodarskih družb

Vsaka gospodarska družba, ne glede na to ali bo sodelovala v tajnih poslih oziroma naročilih mora za svoje nemoteno delovanje zagotoviti varovanje po različnih kriterijih.



Slika 3: Kriteriji varovanja gospodarskih družb

Najpogostejši vzrok za nepooblaščne vstopne v gospodarske družbe so kraja materialno tehničnih sredstev ali uničenje sredstev, redkeje pa zbiranje informacij in kraja tajnih podatkov.

Vsak gospodarska družba ščiti svoje poslovne tajnosti, ki je predmet zaščite tako pri imetniku teh tajnosti kot tudi pri državi, kadar posreduje gospodarskim družbam svoje tajne podatke. V vsakem primeru gre za interes obeh, saj lahko gre pri gospodarski družbi za zadevo, ki je pomembna za njen obstoj, v primeru države pa za spoštovanje zakonskih določil varovanja tajnih podatkov, v kolikor pride do njihove izmenjave z gospodarskimi družbami.

3.1.3 Značilnosti posredovanja tajnih podatkov gospodarskim družbam

Pri izmenjavi tajnih podatkov med državnimi organi in gospodarskimi družbami gre v primeru, ko so izpolnjeni določeni zakonsko določeni pogoji in kadar so izpolnjeni naslednji pogoji:

- Izmenjava mora biti dejstvo, ne samo namera ali domneva.
- Dana mora biti stopnja tajnosti glede na razmerje do poslovnega dogodka, ki je v interesu države.
- O vsebini poslovnega dogodka, kjer nastopajo tajni podatki ne more biti govora v javnosti. Pri tem gre za bolj ali manj sklenjen krog ljudi, ki to zadevo poznajo.
- Podjetje mora imeti upravičen interes, da se tajni podatki ali materiali ohranijo v tajnosti, poleg spoštovanja zakona tudi zaradi gospodarske koristi, ki jo ima družba.

- Volja družbe, da bo zadeva tajna, mora biti jasno izražena. Tej zadevi zadosti podjetje tako, da se določi ozek krog ljudi v podjetju, ki bodo imeli dostop do zadeve in določijo za to ustrezni delovni prostori.
- Družba mora ločiti in razlikovati tajni del posla od tistega dela, ki to ni.

3.1.4 Načini zaščite tajnih podatkov

Vsaka gospodarska družba mora preden pristopi k izvedbi postopkov, ki ji bo omogočala varno obravnavanje tajnih podatkov izvajati splošne ukrepe preprečevalne narave med katere sodijo ukrepi:

- fizične in tehnične narave (preprečitev dostopa nepoklicanim v določene dele družbe s pomočjo fizičnega ali tehničnega varovanja).
- organizacijske narave (seznanjenost delavcev z varnostnim režimom v družbi in zakonodajo, ki ureja področje varovanja tajnih podatkov).
- kadrovskega managementa (zaposlovanje ustreznega in strokovnega kadra, reference kadra).
- pravne oz. zakonodajne narave (podpis pogodb o varovanju, podpis kadrovskih pogodb).

Za gospodarske družbe je pomembno, da se zavedajo, da obstaja možnost za zlorabo ali izdajo tajnih podatkov. Zloraba tajnih podatkov nastopi tedaj, ko določena oseba neupravičeno dostopa do tajnih podatkov in jih zlorabi za svoje namene. Interes pri tej zlorabi ima oseba sama, ne pa kdo drug. Motivov za zlorabo je več in so lahko od želje po uspehu do nezadovoljstva pri delu, finančnih težav in drugo. Tajni podatki državnih organov s katerimi razpolagajo gospodarske družbe so lahko del poslovne tajnosti te družbe in na ta način tudi tarča gospodarskega vohunstva. V takšnem primeru lahko pride do izdaje tajnih podatkov, kar pa je že zahtevnejša pot, saj mora interesent najprej najti osebo, ki mu je pripravljena tajne podatke oz. poslovno tajnost izdati s tem tudi tvegati, da bo razkrinkana.

3.2 Ravnanje s tajnimi podatki in postopek pridobitve varnostnega dovoljenja

Gospodarske družbe, ki prejmejo tajne podatke za realizacijo posameznega posla oz. pogodbe morajo le te varovati v skladu z zakonom ali mednarodno pogodbo. Tajni podatki ostanejo last naše ali tuje države in jih je potrebno varovati v vseh fazah od nastajanja, rabe distribucije, hranjenja do vrnitve ali končnega uničenja (nekateri tajni podatki imajo trajno arhivsko vrednost in jih ni dovoljeno uničiti).

Za pridobitev varnostnega dovoljenja ustrezne stopnje mora gospodarska družba zagotoviti ustrezne prostore in opremo za varovanje tajnih podatkov. Ob izpolnjenem pogoju za izdana osebna dovoljenja za dostop do tajnih podatkov, lahko gospodarska družba enakovredno konkurira na domačih in tujih trgih, kjer se pojavijo razpisi, ki v nadaljevanju zahtevajo ravnanje s tajnimi podatki. Zaradi tega je izdano varnostno dovoljenje dobra referenca za gospodarsko družbo, ki lahko na ta način sodeluje in se vključuje v večje mednarodne projekte in programe.

Gospodarske družbe same ne izdelujejo oz. proizvajajo tajnih podatkov. Tajne podatke pridobijo od državnih organizacij in jih potem v nadaljevanju sami razvijajo na njihovi osnovi. Torej rabijo input – tajni podatek s katerim potem operirajo in vključijo v svoje delo.

3.2.1 Pogoji za varovanje tajnih podatkov v organizacijah

Zakon o varovanju tajnih podatkov določa, da pooblaščen osebe lahko posredujejo tajne podatke dobaviteljem, izvajalcem gradenj ali izvajalcem storitev v naslednjih primerih:

- organizacija izpolnjuje fizične, organizacijske in tehnične pogoje za varovanje tajnih podatkov v skladu s tem zakonom in predpisi, sprejetimi na njegovo podlagi;
- so osebe, ki bodo v organizaciji po službeni dolžnosti imele dostop do tajnih podatkov, varnostno preverjene in imajo dovoljenje za dostop do tajnih podatkov;
- organizacija zagotovi, da bo dostop do tajnih podatkov dovoljen samo tistim osebam, ki morajo imeti vpogled v te podatke po svoji službeni dolžnosti zaradi uresničevanja naročila organa;
- je imenovana oseba, pristojna za nadzor in usmerjanje varnostnih ukrepov v zvezi z izvajanjem naročila, za usposabljanje oseb, ki imajo dostop do tajnih podatkov, poročanje pristojnemu organu o okoliščinah, ki vplivajo na izdajo varnostnega dovoljenja in izvajanje drugih predpisanih ukrepov za varno obravnavanje tajnih podatkov.

Ukrepi za varovanje tajnih podatkov, ki izhajajo iz prejšnjega odstavka, morajo biti vključeni v pogodbo, ki jo v zvezi z naročilom skleneta organ in organizacija. Za osebo, ki bo imela v organizaciji dostop do tajnih podatkov, izdajo dovoljenja od pristojnega organa zahteva organ, za katerega organizacija izvaja naročilo» (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo).

3.2.2 Ugotavljanje pogojev za varovanje tajnih podatkov v organizacijah

Za preverjanje izpolnjevanja pogojev za varovanje tajnih podatkov in posredovanje tajnih podatkov drugi organizaciji so določene pooblaščenice uradne osebe v posameznih resorjih (v MO so to delavci Obveščevalno varnostni službe).

V skladu z Zakonom o splošnem upravnem postopku imajo te osebe pooblastilo za vodenje postopkov ali samo opravljanje posameznih opravil v postopku, ki ga je izdal pristojni minister. Po končanem postopku uradna oseba organa, ki vodi postopek, izdela pisno oceno iz katere je razvidno, da organizacija izpolnjuje vse pogoje za varovanje tajnih podatkov. Pisna ocena je podlaga za izdajo Varnostnega dovoljenja, ki ga izda pristojni minister.

3.2.3. Predlog za začetek postopka varnostnega preverjanja

Predlog za začetek postopka izdaje varnostnega dovoljenja se začne na podlagi pisnega predloga predstojnika:

- organa iz drugega odstavka 1.člena Zakona o tajnih podatkih (UL RS št.50/06 – Uradno prečiščeno besedilo) za organizacije, ki izvajajo naročilo tega organa;
- ministrstva, pristojnega za gospodarstvo, za organizacije, ki potrebujejo varnostno dovoljenje zaradi sodelovanja na javnih razpisih ali izvedbe naročila tuje države ali mednarodne organizacije.

Predlagatelj iz 2.točke prejšnjega odstavka lahko pred vložitvijo predloga pridobi mnenje ministrstva, pristojnega za delovno področje, na katerem deluje organizacija.

Predlagatelj mora predlogu za začetek postopka varnostnega preverjanja predložiti naslednje listine, s katerimi predlagana organizacija dokazuje izpolnjevanje pogojev za priznanje sposobnosti za varno obravnavanje tajnih podatkov

3.2.5 Pregled posredovane dokumentacije gospodarske družbe

Po prejemu dokumentacije (predlog za začetek postopka varnostnega preverjanja in listine) uradna oseba, ki vodi ali le opravlja postopek do pridobitve varnostnega dovoljenja, natančno pregleda spremljajočo dokumentacijo.

Če ima organizacija že vzpostavljeno varnostno območje in izdelan načrt varovanja, ki ga posreduje hkrati z ostalo dokumentacijo, uradna oseba pregleda tudi načrt varovanja. Nosilec načrta varovanja se po potrebi ob izdelavi načrta varovanja nudi ustrezna strokovna pomoč.

Naročnik lahko pozove organizacijo k izvedbi manjkajočih postopkov in ukrepov za varovanje tajnih podatkov ter določi primeren rok za njihovo izvedbo. Pri tem je naročnik dolžan organizaciji zagotoviti potrebno strokovno pomoč.

3.2.6 Ogled varnostnega območja in izdaja varnostnega dovoljenja

Po pregledu dokumentacije organizacije se, v kolikor je dokumentacija popolna, sestavi obvestilo o ogledu, ki se ga posreduje organizaciji, kjer bo ogled opravljen.

Z ogledom uradna oseba preverja izpolnjevanje pogojev varovanja tajnih podatkov v organizaciji. Pri ogledu v organizaciji sta navzoča odgovorna oseba in nosilec načrta varovanja. Ob ogledu uradna oseba izdela zapisnik, ki je kasneje podlaga za izdajo varnostnega dovoljenja ali poziva za odpravo ugotovljenih pomanjkljivosti.

Na podlagi ocene, pristojni minister organizaciji izda varnostno dovoljenje. V primeru, da se z ogledom ugotovi, da organizacija ne izpolnjuje vseh pogojev varovanja, uradna oseba, ki opravlja posamezna dejanja v postopku, izda poziv za odpravo pomanjkljivosti. V pozivu uradna oseba organizaciji določi rok v katerem mora odpraviti ugotovljene pomanjkljivosti.

Na podlagi pisne ocene pristojni minister organizaciji izda varnostno dovoljenje. Varnostno dovoljenje se izda z veljavnostjo petih let ali za dobo, določeno v pogodbi o naročilu, vendar ne več kot za pet let.

4 INDUSTRIJSKA VARNOST V RS

Na področju industrijske varnosti v Republiki Sloveniji so vključeni naslednji državni organi:

- Urad za varovanje tajnih podatkov v vlogi nacionalnega varnostnega organa - NSA¹,
- Ministrstvo za finance in Carinska uprava,
- Ministrstvo za gospodarstvo,
- Ministrstvo za notranje zadeve in Policija,
- Ministrstvo za obrambo,
- Ministrstvo za zunanje zadeve.

Aktivnosti na področju industrijske varnosti koordinira in usklajuje neformalna delovna skupina, katera skuša zagotoviti kar najbolj ugodne pogoje za sodelovanje z gospodarskimi družbami ter zagotoviti doseganje visokih standardov industrijske varnosti.

4.1 Mednarodna industrijska varnost

Mednarodna delovna skupina za industrijsko varnost - MISWG² je bila ustanovljena z namenom ureditve področja industrijske varnosti. Slovenija je članica MISWG že od leta 1996. MISWG je odgovorna za vzpostavljanje postopkov in določanje odgovornosti za uresničevanje posameznih varnostnih zahtev na področju držav članic mednarodne delovne skupine, ki jih na področju posameznih članic uresničujejo nacionalni varnostni organi in pooblašeni

¹ NSA – National Security Authority

² Multinational Industrial Security Working Group

varnostni organi. V mednarodno delovno skupino so vključeni nacionalni varnostni organi in pooblaščen varnostni organi posameznih članic, vodje programov, varnostni uslužbenci vlad in industrijskih delovnih enot. Mednarodna delovna skupina se enkrat letno sestane z namenom:

- obravnavanja aktualnih problemov,
- izdelava dokumentov na področju industrijske varnosti,
- predlaganje rešitev,
- izvajanja izobraževanja
- ustanavljanje začasnih delovnih skupin.

Srečanja mednarodne delovne skupine so pomembne industrijo in državne organe, ki so odgovorni za varovanje tajnih podatkov.

Celotni spekter varovanja tajnih podatkov v mednarodnem prostoru je prepleten z meddržavnimi odnosi ali državo in mednarodno organizacijo. V tem okviru so sprejeti Varnostni sporazumi o varovanju tajnih podatkov ali novejši Sporazum o izmenjavi in varovanju tajnih podatkov³.

Gospodarska družba lahko pridobi informacije o tajnih razpisih na spletnih straneh Ministrstva za gospodarstvo- MG, Evropske obrambne agencije – EDA in NATO agencije za vzdrževanje in podporo – NAMSA. Osnova za izmenjavo tajnih podatkov med Republiko Slovenijo, Evropsko Unijo in NATO je sklenjen mednarodni varnostni sporazum, med Republiko Slovenijo in posameznimi državami pa sklenjen bilateralni varnostni sporazumi, kjer so podrobno urejeni pogoji za ravnanje s tajnimi podatki.

Eden od ključnih elementov pravil ravnanja na področju obrambnih nabav preko Evropske obrambne agencije je tudi sprejet Dokument o ureditvi varovanja podatkov, ki od sodelujočih organizacij in gospodarskih družb zahteva, da ustrezajo merilom, ki jih predpisuje industrijska varnost.

Na področju mednarodne industrijske varnosti morajo vsi subjekti vse tajne podatke, ki se izmenjujejo, uporabljati, prenašati, hraniti, varovati in obravnavati v skladu z veljavnimi zakoni in predpisi v posameznih državah do takšne mere, da zagotovljena stopnja zaščite ne bo nižja od tiste, ki velja za tajne podatke NATO in EU.

5 PRAVNI AKTI S PODROČJA INDUSTRIJSKE VARNOSTI

S sprejeto zakonodajo navedeno v nadaljevanju, se je v Sloveniji dolgoročno uredilo tudi področje industrijske varnosti. Eden zadnjih ključnih dokumentov, ki jih je sprejela vlada RS je Uredba o načinu in postopku ugotavljanja pogojev za izdajo varnostnega dovoljenja organizaciji, ki velja od junija 2007. Z izdajo te uredbe je zaključen postopek pravno-formalne ureditve industrijske varnosti, ki omogoča nove poslovne priložnosti gospodarskim subjektom.

Pravni akti, ki urejajo področje industrijske varnosti so:

- Zakon o tajnih podatkih,
- Zakon o splošnem upravnem postopku,
- Zakon o upravnem sporu,

³ General Security Agreement

- Zakon o policiji,
- Uredba o načinu in postopku ugotavljanja pogojev za izdajo varnostnega dovoljenja organizaciji,
- Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja,
- Uredba o varnostnem preverjanju in izdaji dovoljenj za dostop do tajnih podatkov,
- Uredba o varovanju tajnih podatkov,
- Uredba o obrambnih in zaupnih naročilih

NATO predpisi, ki urejajo področje industrijske varnosti:

- Direktiva o industrijski varnosti AC/35-D/2003, NATO pravila C-M(2002)49 (priloga G), AC/35-D2000-REV3

6 IZDELAVA PRIROČNIKA NA PODROČJU INDUSTRIJSKE VARNOSTI

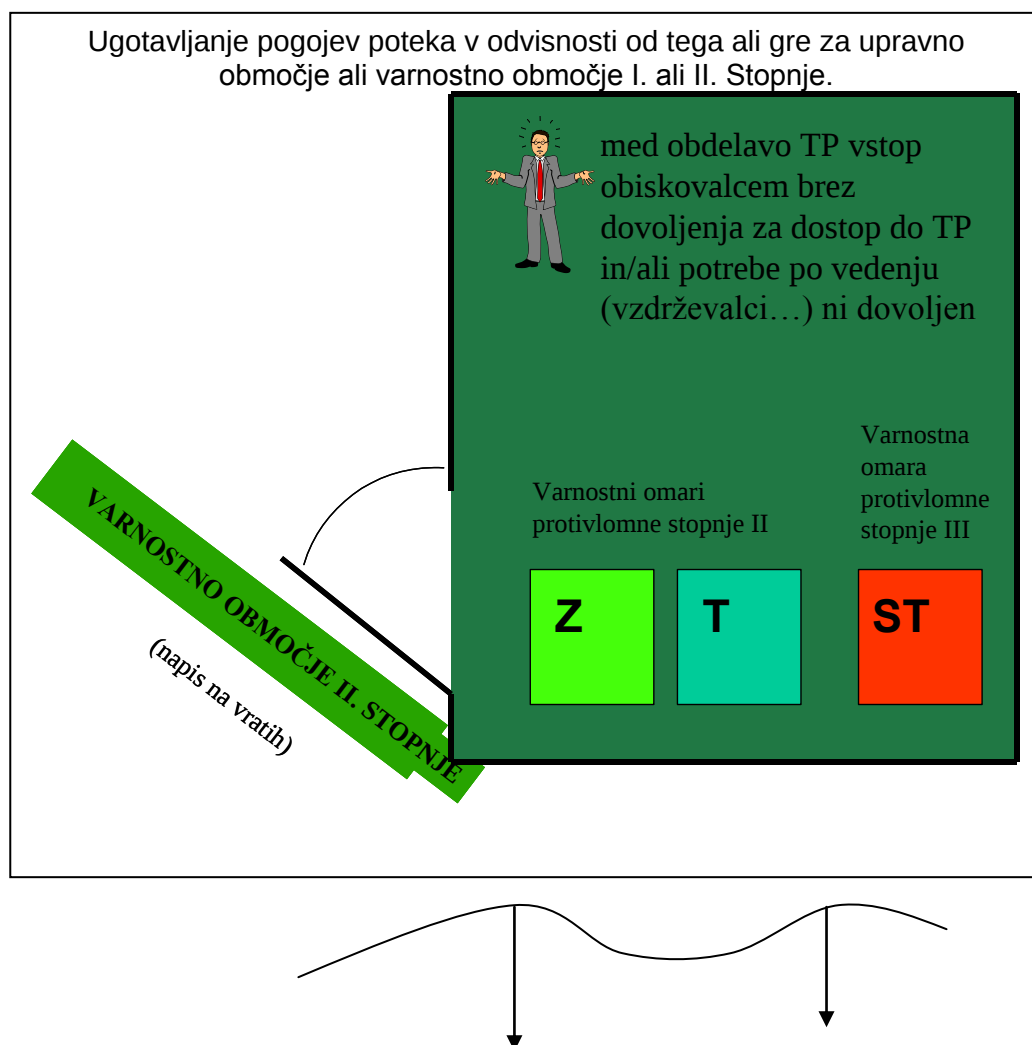
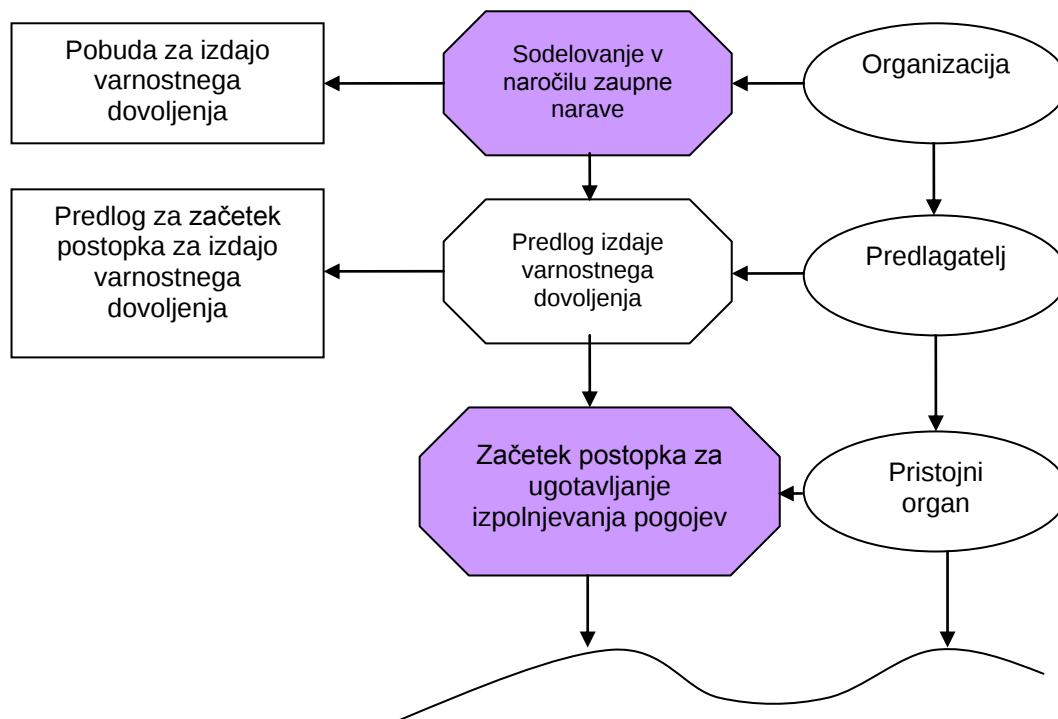
Uspehi na področju industrijske varnosti so v veliki meri odvisni od sodelovanja državnih organov na tem področju in delovanju neformalne delovne skupine.

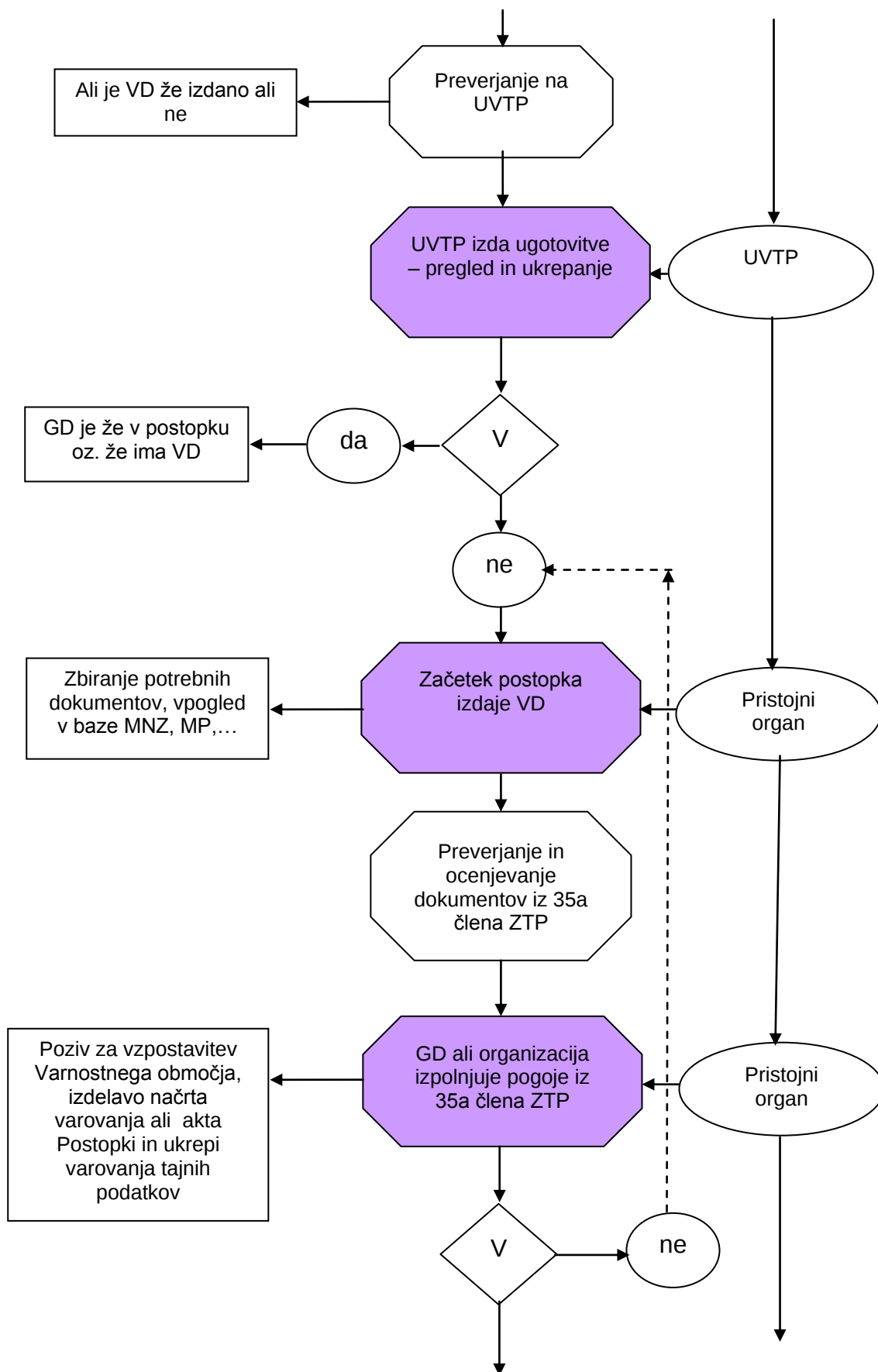
Bistvenega pomena za uveljavitev in doseganje standardov na področju industrijske varnosti je izdelava priročnika, ki bo namenjen gospodarskim družbam. Vsebina priročnika bi morala obravnavala osnovna napotila za organizacije, ki sodelujejo v tajnih projektih na nivoju države in v mednarodnih tajnih projektih. V priročniku bodo opredeljeni napotki in postopki ravnanja gospodarskih družb za ustrezno pripravo organizacije, izgradnjo ustreznih prostorov, preverjanja varovanja tajnih podatkov, transporta in drugo. Razvite države kot sta npr. ZDA in Kanada že imata izdelane priročnike.

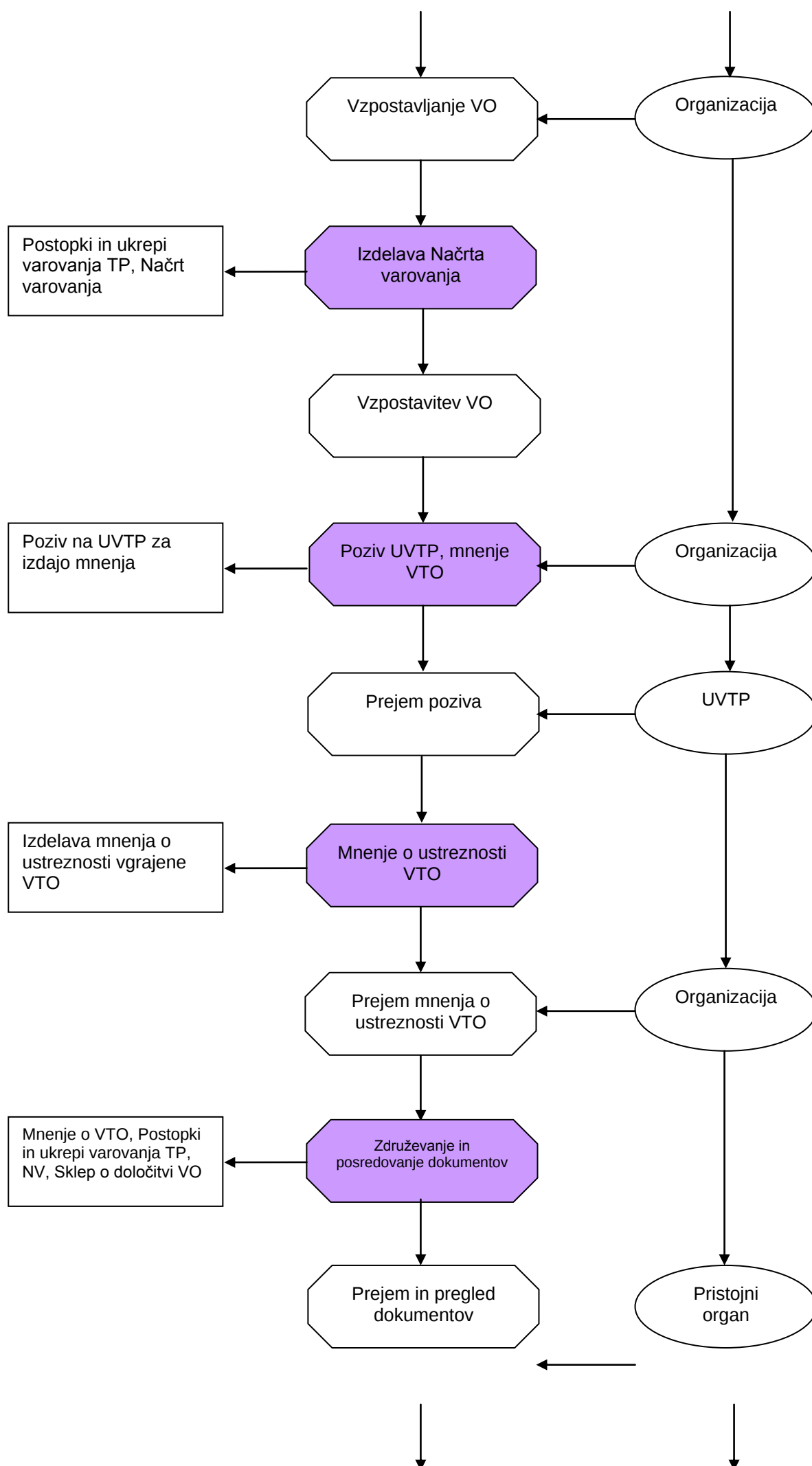
S priročnikom bi se vsem zainteresiranim gospodarskim subjektom podale v kratki in pregledni obliki osnovne informacije o industrijski varnosti in predstavitev ureditve tega področja v gospodarskih organizacijah in drugih institucijah, ki sodelujejo v teh procesih. Skozi obravnavo vseh ključnih elementov bi priročnik predstavil in ponudil vse podlage za urejanje procesa industrijske varnosti vseh subjektov, ki se srečujejo in ravna s tajnimi podatki.

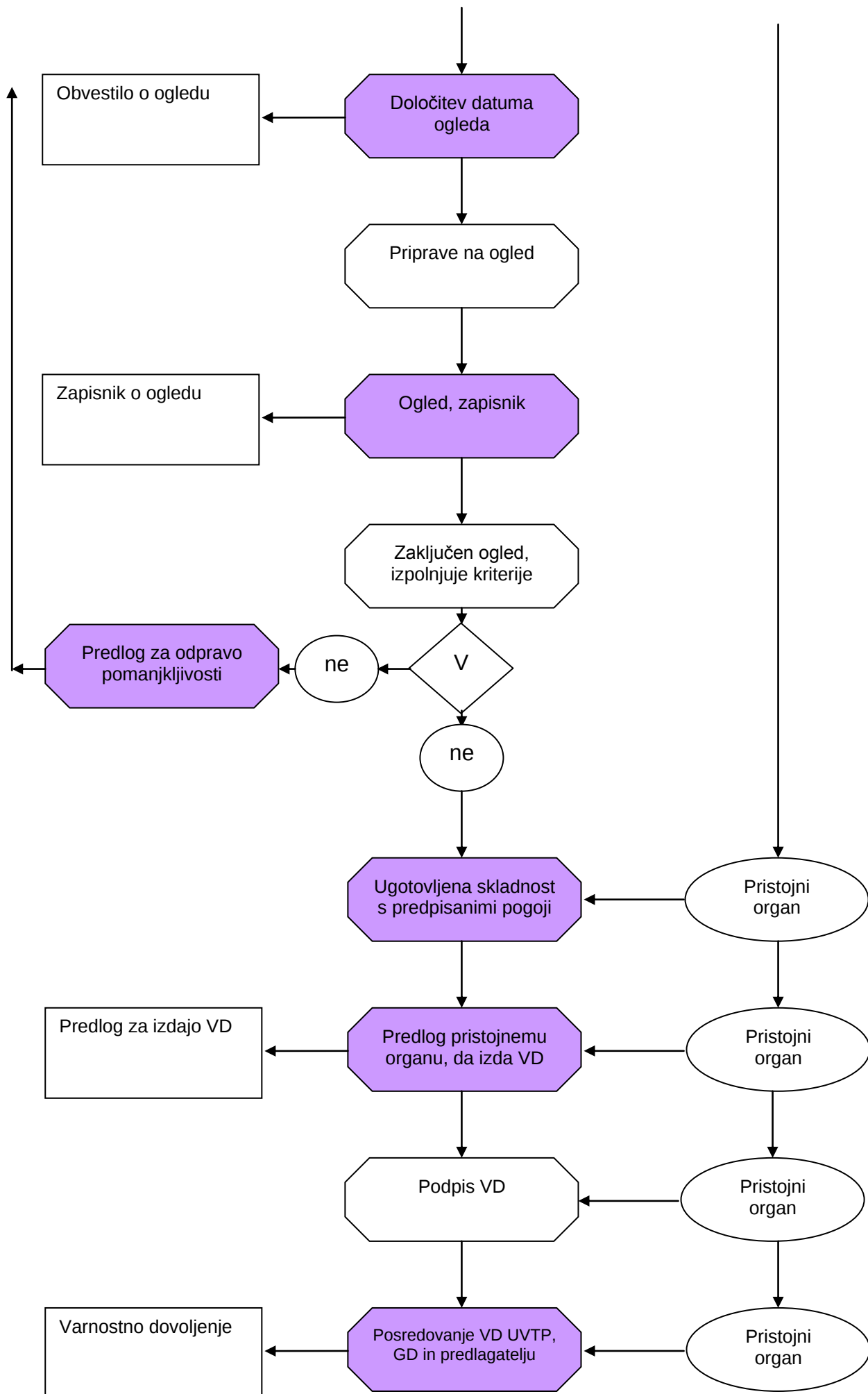
Prav tako je bistvenega pomena dosegljivost informacij na področju industrijske varnosti za slovenske gospodarske družbe na spletnih straneh (UVTP, MG, MO, MNZ, MZZ, MF).

V nadaljevanju je podan predlog v shematski in tekstovni obliki, ki bi bil sestavni del dela vsebine priročnika v katerem so opredeljeni koraki, ki jih morajo storiti gospodarske družbe in organizacije, da si pridobijo varnostno dovoljenje.









Slika 4: Postopek izdaje varnostnega dovoljenja gospodarski družbi

V pobudi za izdajo varnostnega dovoljenja organizaciji je potrebno navesti naročilo, podatke o osebah v organizaciji, ki imajo dostop do tajnih podatkov ali pobudo za uvedbo postopka za izdajo dovoljenja za dostop do tajnih podatkov za te osebe.

V predlogu za izdajo varnostnega dovoljenja je potrebna navedba iz registra organizacij in skupnosti, naslov organizacije, stopnja tajnosti tajnih podatkov, stopnjo varnostnega območja in kratek opis predvidenega posla – zaupne narave.

Listine, ki jih mora imeti gospodarska družba se priložijo dokumentom v postopku in so izpis iz sodnega registra, potrdilo, da niso v postopku zaradi suma storitve kaznivega dejanja, potrdilo o plačanih davkih in prispevkih, potrdilo, da niso v postopku prisilne poravnave, stečaja ali likvidacijskega postopka, registracija pri pristojnem sodišču in dokazilo o lastniški strukturi.

6.1 Razvoj modela za ocenjevanje ustreznosti varnostnih sistemov

Za učinkovito varovanje oseb, materialni sredstev in tajnih podatkov bi bilo potrebno razviti model ocenjevanja ustreznosti varnostnih sistemov in ukrepov za varovanje, s katerim bi lahko ustrezno strokovno usposobljene osebe s pomočjo točkovanja presodile ali določen subjekt zadovoljuje minimalne varnostne kriterije oz. na področju industrijske varnosti, ali določena gospodarska družba izpolnjuje varnostne kriterije za varno ravnanje s tajnimi podatki.

Namen modela za ocenjevanje je v sistemskem poenotenju varovanja vseh subjektov, zagotavljanju enotnega opremljanja s sistemi tehničnega varovanja, kompatibilnosti sistemov. Končni cilj, ki ga skušamo doseči je izgradnja sodobnih sistemov varovanja, ne samo gospodarskih družb, ki bo vključeval:

- Ukrepe tehničnega varovanja.
- Ukrepe in postopke fizičnega varovanja.
- Kombinirane ukrepe.
- Ukrepe za zmanjšanje ogroženosti.

V modelu bi se poleg osnovnih podatkov o subjektu varovanja nahajali še splošni podatki o tem kaj se varuje in stopnja ogroženosti subjekta.

Ocenjevalni del bi vseboval vse vgrajene varnostne elemente:

- Sekcija 1 – varnostni vsebniki in ključavnice na varnostnih vsebnikih.
- Sekcija 2 – prostori (konstrukcija) in varnostne ključavnice za zaklepanje prostorov.
- Sekcija 3 – Zgradba (lega in konstrukcija).
- Sekcija 4 – Nadzor dostopa: do zaposlenih in obiskovalcev.
- Sekcija 5 – Fizično varovanje (stalno, občasno, obhodi) in sistem za zaznavanje vlomov (sistem za zaznavanje vloma, prenos alarmnega signala na intervencijo).
- Sekcija 6 – Perimeter (karakteristika, nadzor dostopa v ograjeno območje, naključni pregledi ob vstopu ali izstopu, perimetralni sistem za zaznavanje in javljanje vdora, varnostna osvetlitev, videonadzorni sistem in drugo).

Model ocenjevanja zahteva sistemski pristop, v katerega bi bilo potrebno vključiti več strokovnjakov s področja tehničnega varovanja.

7 VLOGA URADA ZA VAROVANJE TAJNIH PODATKOV NA PODROČJU INDUSTRIJSKE VARNOSTI

Urad Vlade RS za varovanje tajnih podatkov - UVTP je kot nacionalni varnostni organ, organ državne varnosti in prva avtoriteta, ki ureja tudi področje industrijske varnosti in najvišji organ za zavarovanje tajnih podatkov.

Urad za varovanje tajnih podatkov lahko na področju nacionalnih tajnih podatkov kot nacionalno varnostni organ – NSA del svojih pristojnosti prenese na drug pooblaščen varnostni organ - DSA⁴. Pooblaščen varnostni organ je lahko imenovan za opravljanje določenih funkcij in nalog nacionalnega varnostnega organa - NSA, ki pa je še vedno odgovoren za njihovo izvajanje in ima pristojnost nadzora. Pooblaščen varnostni organ je odgovoren za usklajevanje in izvajanje nacionalnih vidikov industrijske varnosti v okviru programov in projektov.

Pri povečanemu obsegu dela lahko glede na trenutno situacijo pride do zastoja dela UVTP kot NSA, zato bi bilo potrebno zaposliti nov kader (kar ni vedno možno in smotrno) ali pa prenesti del svojih pristojnosti na pooblaščen varnostni organ – DSA.

Urad za varovanje tajnih podatkov izmenjuje tajne podatke z tujimi nacionalno varnostnimi organi. Zaradi tega bo potrebno v prihodnje pripraviti in podpisati sporazume o izmenjavi in varovanju tajnih podatkov prioriteto z vsemi državami NATO in EU ter državami v interesni sferi Slovenije.

Vloga Urada za varovanje tajnih podatkov na področju industrijske varnosti je, pridobivanje podatkov o tujih gospodarskih družbah na področju varovanja tajnih podatkov in dajanje informacij o gospodarskih družbah v Sloveniji tujim nacionalno varnostnim organom na področju varovanja tajnih podatkov. Cilj tega je, da čimveč slovenskih podjetij začne razmišljati o vzpostavitvi pogojev v okviru svoje organizacije za nastop na razpisih, ki zahtevajo dostop do tajnih podatkov v mednarodnem okolju.

Organizacija, ki si pridobi mednarodno varnostno dovoljenje lahko nastopa na razpisih, ki jih izdaja zveza NATO in EU, kjer je že v razpisnih pogojih opredeljeno, da bo pri izvedbi posla potrebno imeti dostop do tajnih podatkov. Prav tako organizacija pridobi prednost pred ostalimi organizacijami v primeru podpisa komercialnih pogodb, katerih izvedba pogojuje dostop do tajnih podatkov, z organizacijami iz držav, s katerimi ima Republika Slovenija podpisan t.i. varnostni sporazum.

8 ZAKLJUČEK

Industrijska varnost v današnjem času predstavlja velik izziv za gospodarske družbe in organizacije, ki sodelujejo na domačem in mednarodnem področju. Zaradi tega je potrebno to področje neprestano izboljševati v smislu večje varnosti poslovanja s tajnimi podatki med gospodarskimi družbami in organizacijami. V prihodnosti lahko večjo podporo industrijski varnosti zagotovimo z:

- Spremembami in dopolnitvami zakonodaje v kolikor se za to izkažejo potrebe.
- Izboljšanjem postopkov na področju industrijske varnosti (priročnik).

⁴ Designated Security Authority

- Izboljšanjem informacijske varnosti, ki predstavlja trenutno še največji izziv sodobni varnosti in s tem tudi problem v industrijski varnosti.
- Spodbujanjem gospodarskih družb, da si pridobijo oz. zagotovijo pogoje za pridobitev varnostnega dovoljenja, kar je lahko s pridobitvijo varnostnega dovoljenja do neke mere prednost na domačem in mednarodnem trgu, odvisno od trenutnega stanja.

Prav tako bi bilo potrebno širši javnosti predstaviti možnosti, ki jih imajo gospodarske družbe doma in na mednarodnem prostoru v kolikor investirajo v (industrijsko) varnost. Pridobljeno varnostno dovoljenje predstavlja navzven resno podjetje, ki je kot partner lahko vredno zaupanja.

Glede na obseg nalog, ki jih ima danes nacionalni varnostni organ se lahko pričakuje vse več nalog na področju industrijske varnosti in potrebo po imenovanju pooblaščenega varnostnega organa.

Na mednarodnem področju industrijske varnosti bo potrebno pripraviti in podpisati sporazume o izmenjavi in varovanju tajnih podatkov v prvi vrsti z državami članicami EU in NATO, katerih državni organi in gospodarske družbe predstavljajo potencialne partnerje našim družbam.

Gospodarske družbe morajo del svojih sredstev investirati v varnost. Predvsem gre tu za investiranje v kader, ki bo skrbel za varnost v podjetju. Gre za osebo – vodjo varnosti⁵, ki bo v podjetju skrbela za vse nivoje varnosti torej tudi industrijsko varnost.

Za boljše informiranje javnosti in gospodarskih družb pa bo v kratkem času potrebno izdelati priročnik, ki bo olajšal pot tistim, ki bodo hoteli sodelovati z državnimi organi pri izvedbi zaupnih naročil. Z izdanim priročnikom na področju industrijske varnosti bo pot za gospodarske družbe občutno lažja.

Za lažje odločanje glede varovanja tajnih podatkov in varovanja v splošnem pomenu, bi bil razvit model točkovanja vseh vgrajenih varnostnih elementov v veliko pomoč vsem sodelujočim pri izbiri ustreznega varovanja v smislu izbire med fizičnim varovanjem, tehničnim varovanjem in kombinacijo varovanja. Na ta način bi dosegli določeno fleksibilnost, saj se varovani subjekti nahajajo v različnih okoljih in so različno ogroženi in enostavno »uniformirano« določanje potrebnih varnostnih sistemov povzroča določene težave v smislu pretirane varovanja ali tudi neustreznega varovanja. Na ta način bi se lahko privarčevala tudi določena finančna sredstva, ki bi bila racionalno uporabljena.

9 LITERATURA

- Arnejčič, B. (2005). Posameznik, varnost, država, Strokovno gradivo za usposabljanje po Zakonu o obrambi.
- Dolinar, D. (2006). Obrambna industrija v Evropski uniji – izzivi in priložnosti za Slovenijo, Gornja Radgona.
- Golob, R. (1997). Sistem zaščite in varovanja oseb in premoženja. Ljubljana.
- Kop, I. (1995). Varovanje in zaščita poslovne skrivnosti. GV.
- Murphy, D. (2007) Security Risk Assessment & Security Risk Management in NATO Civil Bodies, NOS.

⁵ Facility Security Officer

- Pagoria, B. (13. 7. 2004). Implementing Robust Physical Security, SANS Institute.
- Podbregar, I. (2007). Varnostni in varstveni standardi v podjetju, Skripta za usposabljanje za pridobitev pooblaščenega gospodarskega subjekta AEO po standardih TAXUD/2006/1450, Samozaložba, Ljubljana.
- Zelenika, R. (2005) Logistički sustavi, Rijeka.

Internet

- EDA <http://www.eda.europa.eu/> (15.3.2008).
- NAMSA <http://www.namsa.nato.int/> (17.3.2008).
- NISPOM <http://fas.org/sgp/library/nispom.htm> (21.3.2008).
- Physical Security http://en.wikipedia.org/wiki/Physical_security (5.3. 2008).
- Reliability of security systems <http://www.cl.cam.ac.uk/~rja14/#Econ> (5.3.2008).
- UVTP <http://www.uvtpgov.si> (10. 3. 2008).

Zakonodaja

- Zakon o splošnem upravnem postopku (Ur. l. RS, št. 24/06 – ZUP- UPB2).
- Zakon o tajnih podatkih – uradno prečiščeno besedilo (Ur. list RS, št. 50/2006 z dne 16. 5. 2006).
- Uredba o obrambnih in zaupnih naročilih Ur. l. RS, št. 80/07 z dne 4. 9. 2007).
- Uredba o varovanju tajnih podatkov (Ur. list RS, št. 74/2005 z dne 5. 8. 2005).
- Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Ur. list RS, št. 48/2007 z dne 1. 6. 2007).
- Uredba o načinu in postopku ugotavljanja pogojev za izdajo varnostnega dovoljenja organizaciji (Ur. list RS, št. 70/2007 z dne 3. 8. 2007).
- Sklep o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja (Ur. list RS, št. 94/2006 z dne 8. 9. 2006).
- Pravilnik o načinu in postopku določanja tajnih podatkov s področja obrambe v gospodarskih družbah, zavodih in organizacijah (Ur. list RS, št. 108/2002 z dne 12. 12. 2002).
- Pravilnik o varovanju tajnih podatkov na Ministrstvu za obrambo (MORS, šifra 0070-5/2006-4 z dne 21. 2. 2006 in šifra 0070-5/2006-30 z dne 31. 8. 2006).
- Directive on industrial security, AC/35-D/2003.
- NATO Security Policy, C-M (2002)49, Physical Security.

Intervju:

- MOHAR Boris, Urad za varovanje tajnih podatkov.
- STEKLASA Bogo, Goran VIDRIH, Ministrstvo za obrambo.

O avtorju:

Aleš Kotnik, univerzitetni diplomirani ekonomist, višji svetovalec za področje industrijske varnosti na Ministrstvu za obrambo, elektronski naslov: ales.kotnik@mors.si.