HEURISTIKA I ZAKONSKA REGULATIVA U OBLASTI ZAŠTITE TAJNIH PODATAKA U FUNKCIJI EDUKACIJE SUBJEKATA SISTEMA ODBRANE

Paun J. Bereš
Ministarstvo odbrane Republike Srbije, Uprava za obaveze odbrane, Centar MO za lokalnu samoupravu Zrenjanin

DOI: 10.5937/vojtehg62-4696

OBLAST: bezbednost i zaštita
VRSTA ČLANKA: stručni članak

Sažetak:

Edukacija o zaštiti tajnih podataka trebalo bi da bude u vrhu prioriteta kada je reč o obezbeđenju zaštite vitalnih interesa države. Neki podaci ne treba da budu dostupni javnosti, jer se uglavnom odnose na nacionalnu bezbednost, te niko ne bi trebalo da dovodi u pitanje potrebu zaštite ove vrste podataka. Ovaj rad namenjen je edukatorima koji se bave zaštitom tajnih podataka i posebno onima koji rade ili dolaze u kontakt sa poverljivim podacima, sa ciljem da ih informiše o nacionalnom sistemu zaštite tajnih podataka u Srbiji i osposobi za primenu važeće zakonske regulative primenom heurističkog modela edukacije. U radu su navedeni pravni propisi koji regulišu zaštitu podataka, kao i propisani standardi i mere zaštite tajnih podataka.

Ključne reči: *heuristika, korišćenje informacija, klasifikacija, zaštita.*

Uvod

Heuristika je „nauka o načinima iznalaženja novih naučnih spoznaja“ (Hotomski, 1995), a reč koja označava taj pojam potiče od reči heureka – „našao sam, pronašao sam“ (Bereš, 2005).

Heuristički prilaz problemu je empirijska pretraga ili optimizacioni metod koji obično rešava probleme, ali nema nikakav dokaz koji bi matematičari i fizičari prihvatili. Niko ne zna da li će uvek dati najbolji odgovor (rešenje problema). Dok je metaheuristika shematski metod za pronalaženje dobre heuristike za pojedinačne probleme, to je pojam koji se često javlja u evolutivnim (razvojnim) algoritmima ili fazi-logičkim aplikacijama:

• „Kakve parametre podešavanja da koristim da bih dobio dobre rezultate kada primenjujem heurističku metodu X na problemu Y ? “.

• „Kako da prilagodim parametre heuristike X da bih dobio bolje rezultate problema Y ? ”.

e-mail: paunberes@gmail.com

• „Koje je bolje, heuristika X ili heuristika Y ? ” (Amaldi, Capone, Malucelli, 2003).

Pod heurističkim modelovanjem (Kvaščev, 1978) podrazumeva se stvaranje takvog modela koji ima heurističko značenje i predstavlja originalna rešenja u jednom te istom modelu, tj. taj model omogućava pronalaženje novih znanja i razvija stvaralaštvo zahtevajući od subjekata ovu ili onu samostalnost uz uvažavanje nivoa predznanja svakog subjekta u svom domenu ponaosob (na primer: u našem slučaju oblast bezbednosti i zaštite vitalnih interesa naše države).

Savremenom svetu (postindustrijskom, tehnološkom, informatičkom, globalnom) potrebni su ljudi, obučeni, spremni i sposobni da koriste nova kompleksna oruđa, brzo i efikasno usvajaju, izgrađuju i primenjuju raznovrsna znanja, aktivno i odgovorno učestvuju u složenim društvenim i ekonomskim odnosima i procesima u svakodnevnom životu i donose adekvatne, racionalne i najbolje odluke, a pogotovo u oblasti bezbednosti i zaštite vitalnih interesa države kada je neophodno čuvanje i zaštita istih pod određenim stepenom tajnosti.

U svetu, koji se brzo menja i u kojem se znanja svakodnevno usložavaju i proširuju, a izvori informacija iz svih oblasti, pogotovo interesantnih za *bezbednost i zaštitu vitalnih interesa za državu*, neslućeno umnožavaju, podatak, informacija i činjenica mogu postati bespredmetni i prevaziđeni i pre nego što su upotrebljeni, jer nisu zaštićeni, što može imati negativne posledice, ako neko do njih dolazi nelegalno. Heurističkim pristupom rešavanju problema i projektovanjem budućih sistema u funkciji bezbednosti i zaštite vitalnih interesa za državu teži se prevazilaženju pomenutih problema.

Postoje razne vrste podataka. Oni mogu biti javni ili „otvoreni” podaci, podaci sa ograničenim pristupom (tajni podaci, podaci o ličnosti, poslovne i profesionalne tajne), a mogu biti u državnoj svojini ili u drugim oblicima svojine. Ne mogu svi podaci da budu označeni kao tajni. Klasifikacija određenog podatka nameće se prevashodno iz njegove sadržine. Sadržina ovog tipa podataka opredeljuje potrebu zaštite podatka, u odnosu na interes građana da ostvari uvid u neku informaciju od javnog značaja, jer se u praksi ovi podaci odnose na nacionalnu bezbednost.

Uređenje sistema zaštite podataka u Republici Srbiji je u toku. Zakonska regulativa koja se bavi ovom materijom zaokružena je usvajanjem:

• Zakona o slobodnom pristupu informacijama od javnog značaja;
• Zakona o zaštiti podataka o ličnosti;
• Zakona o tajnosti podataka.

Zakon o tajnosti podataka predstavlja jedinstven sistem određivanja i zaštite tajnih podataka od interesa za nacionalnu i javnu bezbednost, odbranu, unutrašnje i spoljne poslove, kao i zaštitu stranih tajnih podataka. Ovim zakonom uređen je način pristupa tajnim podacima i prestanak njihove tajnosti, nadležnost organa i nadzor nad sprovođenjem ovog zakona, kao i odgovornost za neizvršavanje obaveza i druga pitanja.

Tajni podatak po definiciji „predstavlja podatak od interesa za Republiku Srbiju koji je zakonom, drugim propisom ili odlukom nadležnog organa donesenog u skladu sa zakonom, određen i označen određenim stepenom tajnosti, *sa napomenom da se tajnim podatkom ne smatra podatak koji je označen kao tajni radi prikrivanja krivičnog dela, prekoračenja ovlašćenja, zloupotrebe službenog položaja i drugog nezakonitog akta ili postupanja"„*. Nacionalni organ za zaštitu tajnih podataka u našoj državi je *Kancelarija Saveta za nacionalnu bezbednost i zaštitu tajnih podataka* (u daljem tekstu *Kancelarija Saveta*), koja predstavlja stručnu službu Vlade Republike Srbije i nadležna je za zaštitu stranih tajnih podataka (Evropske unije, NATO, EUROPOL, ...), usaglašavanje bilateralnih sporazuma u oblasti razmene i zaštite tajnih podataka, izdavanje bezbednosnih sertifikata za pristup nacionalnim i stranim tajnim podacima, kontrolu i stručni nadzor nad primenom Zakona o tajnosti podataka i potpisanih međunarodnih sporazuma, kao i edukaciju kadrova organa javne vlasti po pitanju zaštite tajnih podataka.

Ministarstvo odgovorno za pravosuđe odgovorno je i za „vođenje politike" zaštite tajnih podataka i inspekcijski nadzor nad primenom zakona (Kovačević, 2013).

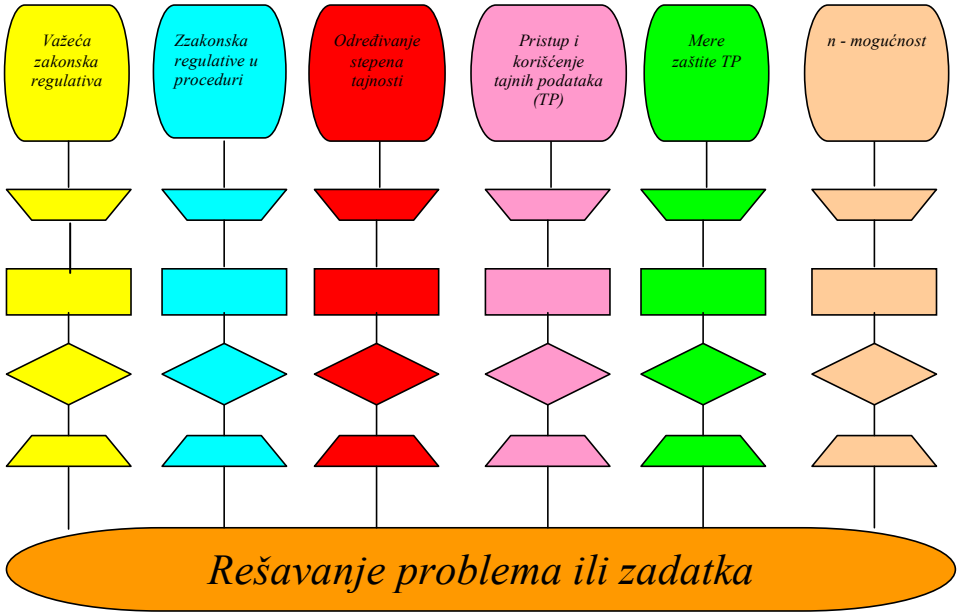
Heuristika, edukacija i bezbednost i zaštita podataka od značaja za vitalne interese države

Heuristički model edukacije u funkciji rešavanja problema i donošenje adekvatnih odluka u oblasti zaštite tajnih podataka opisan je u svim svojim modalitetima primene u skladu sa važećom zakonskom regulativom (Bereš, 2013).

Heuristički model veoma malo determiniše radnje u toku rešavanja problema, tako da ostavlja subjektu – članu tima mogućnost pronalaženja jednog ili svih mogućih rešenja zavisno od predznanja, stepena samostalnosti i njegovih stvaralačkih sposobnosti. Ovakav pristup rešavanju problema omogućuje svakom subjektu – članu tima da postigne svoj maksimum, kako slabijim, prosečnim, tako i natprosečnim, tj. talentovanim članovima tima koji rade ili dolaze u kontakt sa podacima od značaja za bezbednost i zaštite vitalnih interesa države. Postavljanje problema heurističkom strategijom znači da je član tima stavljen u položaj da otkrije, primenom starog iskustva u novim situacijama, da poznata znanja dovodi u novu situaciju (funkciju), otkriva nove puteve kreativnog rešavanja problema u ovoj oblasti.

Heuristički model edukacije upotrebljen je za rešavanje problema frekventnih bezbednosnih situacija u realnom skupu bezbednosnih situacija koje se javljaju u svakodnevnom radu, kada se radi o značajnim podacima i onima koji imaju i stepen tajnosti.

Slika 1 predstavlja problemsku situaciju u vidu heurističkog algoritma, koji prikazuje lepezu mogućnosti i problema koje treba rešiti i staviti ih u funkciju edukacije onih koji rade i dolaze u kontakt sa podacima sa stepenom tajnosti (Bereš, 2013).



Slika 1 – Problemska situacija – heuristički algoritam
Figure 1 – Problem situation-heuristic algorithm

Na raspolaganje imamo:

I. Pravnu materiju koja je na snazi (Kovačević, 2013):

1. Zakon o tajnosti podataka *(„Službeni glasnik RS“ br. 104/2009)*

2. Uredba o osnivanju Kancelarije Saveta za nacionalnu bezbednost *(„Službeni glasnik RS“ br. 12/2009)*

3. Uredba o obrascima bezbednosnih upitnika *(„Službeni glasnik RS„ broj30/10)*

4. Uredba o sadržini, obliku i načinu dostavljanja sertifikata za pristup tajnim podacima *(„Službeni glasnik RS“ broj 54/10)*

5. Uredba o određivanju poslova bezbednosne zaštite određenih lica i objekata *(„Službeni glasnik RS“ br. 72/2010)*

6. Uredba o uvećanju plate državnih službenika i nameštenika koji obavljaju poslove u vezi sa zaštitom tajnih podataka u Kancelariji Saveta za nacionalnu bezbednost i zaštitu tajnih podataka i Ministarstvu pravde *(„Službeni glasnik RS“ broj 79/10)*

7. Uredba o sadržini, obliku i načinu vođenja evidencija za pristup tajnim podacima *(„Službeni glasnik RS“ broj 89/10)*

8. Uredba o načinu i postupku označavanja tajnosti podataka, odnosno dokumenata *(„Službeni glasnik RS“ broj 8/11)*

9. Uredba o posebnim merama zaštite tajnih podataka u informaciono- telekomunikacionim sistemima *(„Službeni glasnik RS“ broj 53/11)*

10. Uredba o posebnim merama nadzora nad postupanjem sa tajnim podacima *(„Službeni glasnik RS“ broj 090/2011)*

11. Uredba o posebnim merama fizičko-tehničke zaštite tajnih podataka *(„Službeni glasnik RS“ broj 097/2011)*

II. Pravnu materiju koja je u proceduri:

1. Zakon o informacionoj bezbednosti

2. Pravilnik o službenoj legitimaciji i načinu rada lica ovlašćenih za vršenje nadzora nad sprovođenjem zakona

3. Uredba o utvrđivanju kriterijuma za označavanja podataka stepenom tajnosti „DRŽAVNA TAJNA“ i „STROGO POVERLjIVO“

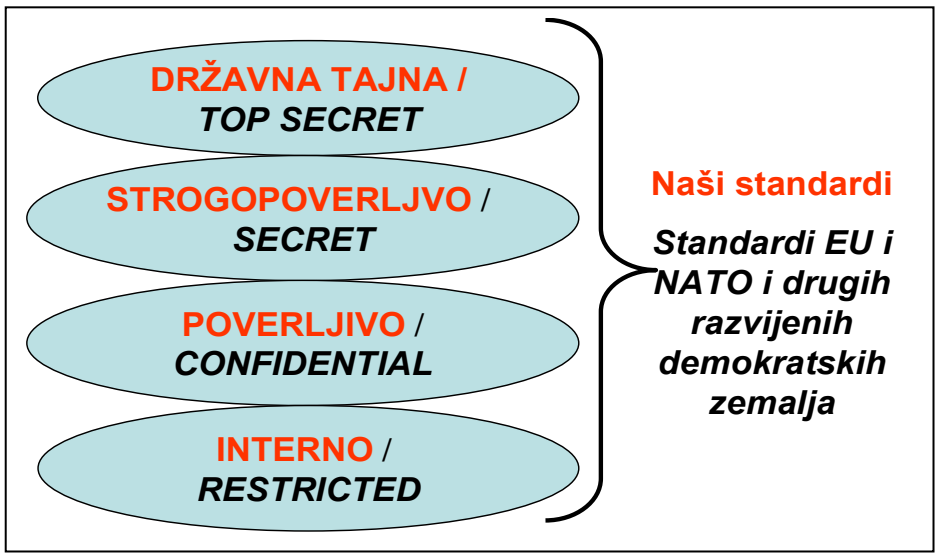
4.Uredba o industrijskoj bezbednosti

III. Moguća rešenja u oblasti zaštite tajnih podataka:

– Određivanje stepena tajnosti:

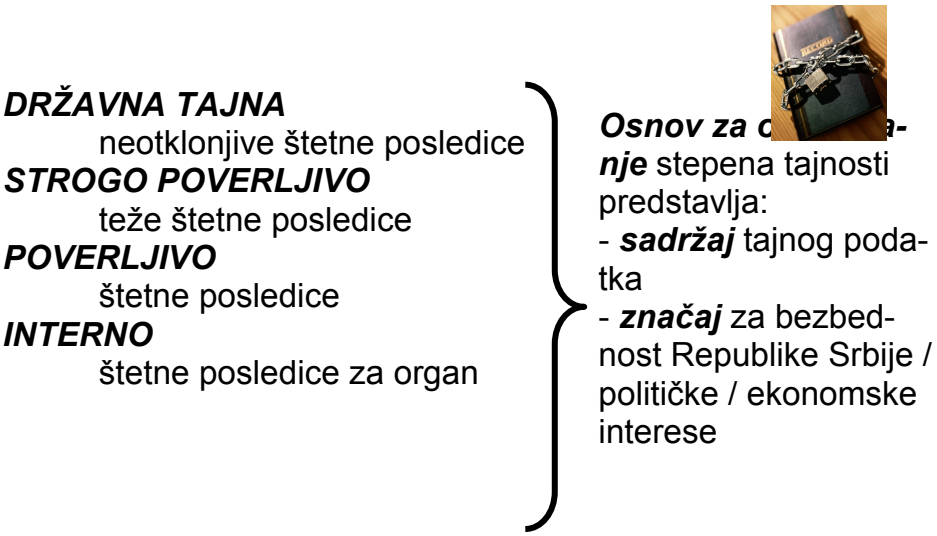
Primena zakona o tajnosti podataka kao jedinstven sistem prikazan je na slici 2, kao i upoređivanje naših standarda sa standardima EU, NATO i drugih (slika 3).

Slika 2 – Zakon o tajnosti podataka – jedinstven sistem
Figure 2 – The Law on Data Confidentiality - A unique system



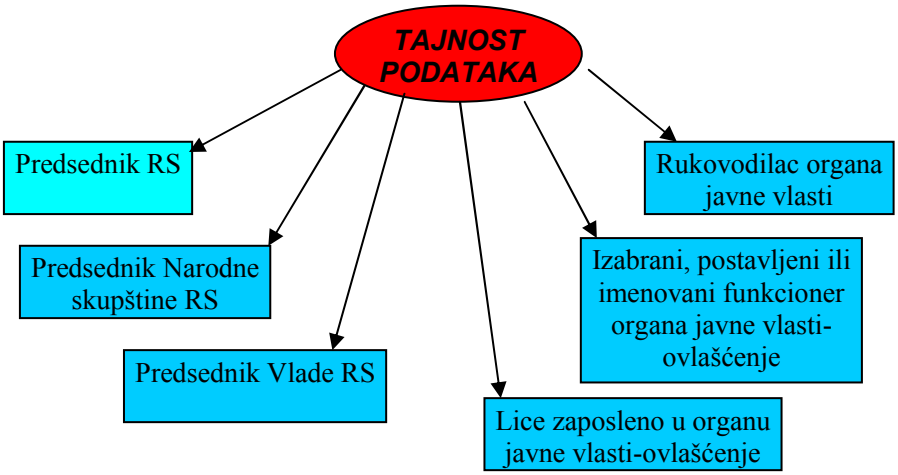
Slika 3 – Standardi u R. Srbiji, EU i u drugim zemljama
Figure 3 – Standards in the Republic of Serbia, the EU and other countries

Osnov za određivanje stepena tajnosti prikazan je na slici 4.



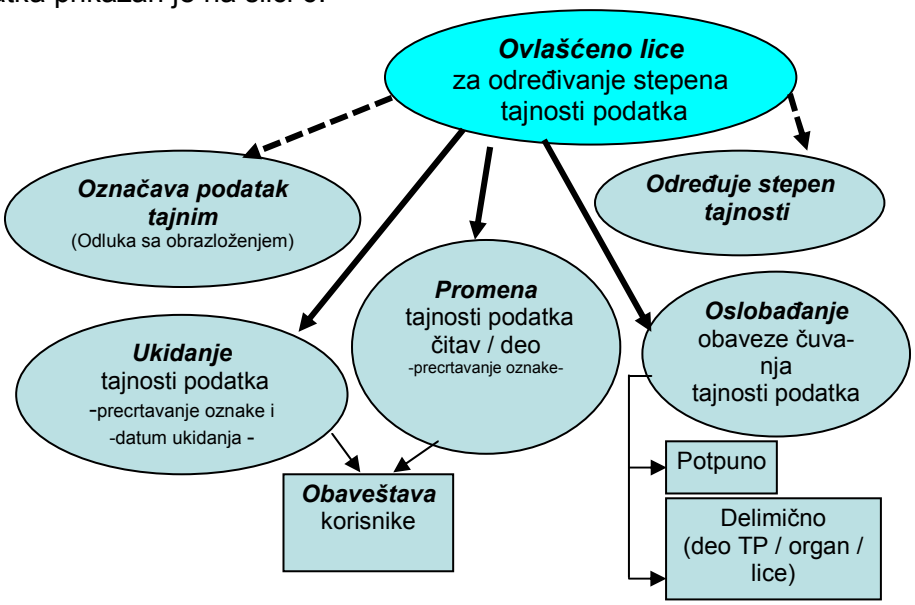
Slika 4 – Određivanje stepena tajnosti podataka
Figure 4 – Determination of data confidentiality

Ovlašćena lica za određivanje stepena tajnosti podataka prikazana su na slici 5.



Slika 5 – Ovlašćena lica za određivanje stepena tajnosti podataka
Figure 5 – Persons authorized to determine the level of data confidentiality

Delokrug poslova ovlašćeng lica za određivanje stepena tajnosti podatka prikazan je na slici 6.



Slika 6 – Ovlašćeno lice za određivanje stepena tajnosti podatka
Figure 6 – A person authorized to determine the degree of confidentiality

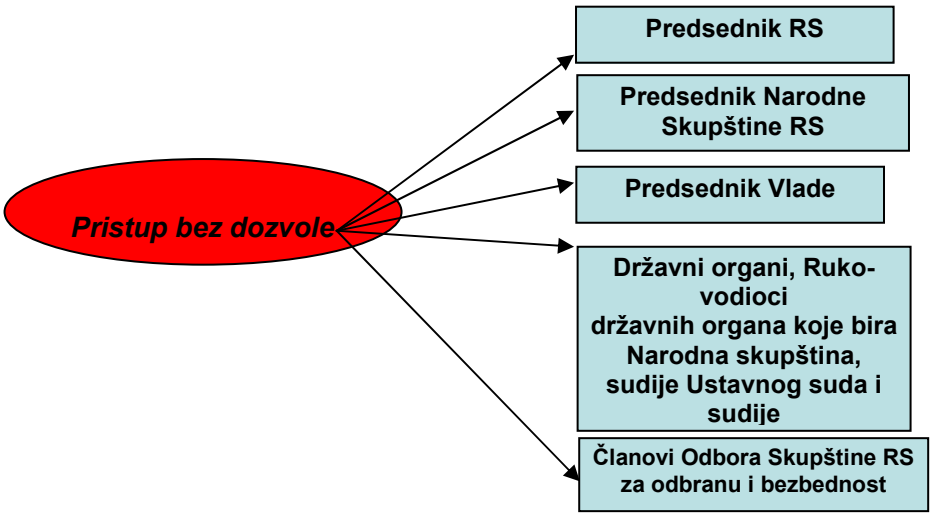
Bereš, P., Heuristika i zakonska regulativa u oblasti zaštite tajnih podataka u funkciji edukacije subjekata sistema odbrane, pp. 121–135

– Pristup i korišćenje tajnih podataka:

- *Princip „potrebno je da zna„ („need to know„)* – opravdana potreba lica za korišćenjem tajnih podataka radi izvršavanja njegovih poslova, na osnovu izdatog sertifikata ili dozvole za pristup tajnim podacima.
- *Sertifikat ili dozvola za pristup tajnim podacima* – stepena tajnosti „DRŽAVNA TAJNA„, „STROGO POVERLJIVO" i „POVERLJIVO"
- „INTERNO" – pristup imaju svi zaposleni u organu i organizaciji, bez dozvole za pristup tajnim podacima.

.

Pristup tajnim podacima bez bezbednosne provere prikazan je na slici 7.



Slika 7 – Pristup tajnim podacima bez bezbednosne provere
Figure 7 – Access toclassified data without security checks

Organi nadležni za vršenje bezbednosnih provera su (Kovačević, 2013):

- Bezbednosno-informativna agencija (za stepene tajnosti „STROGO POVERLjIVO" i „DRŽAVNA TAJNA"),
- Ministarstvo unutrašnjih poslova (za stepen tajnosti „POVERLjIVO"),
- Vojnobezbednosna agencija (za pripadnike Ministarstva odbrane za sve stepene tajnosti).

Po dobijanju izveštaja o rezultatu bezbednosne provere, od nadležnog organa za vršenje bezbednosnih provera, Kancelarija Saveta izrađuje: *rešenje o odbijanju zahteva za izdavanje sertifikata za pristup tajnim podacima* ili *rešenje o odobrenju izdavanja sertifikata za pristup tajnim podacima.*

Ukoliko lice ne podnese žalbu na doneto rešenje u roku od petnaest dana, Kancelarija Saveta poziva lice i upoznaje ga sa propisanim bezbednosnim pravilima i procedurama za pristup tajnim podacima, kao i sa pravnim i drugim posledicama njihovog neovlašćenog korišćenja. Po potpisivanju izjave, kojom se potvrđuje da je imenovani upoznat sa navedenim bezbednosnim pravilima i procedurama, uručuje mu se bezbednosni sertifikat za pristup tajnim podacima zahtevanog stepena tajnosti.

Period važenja sertifikata je za:

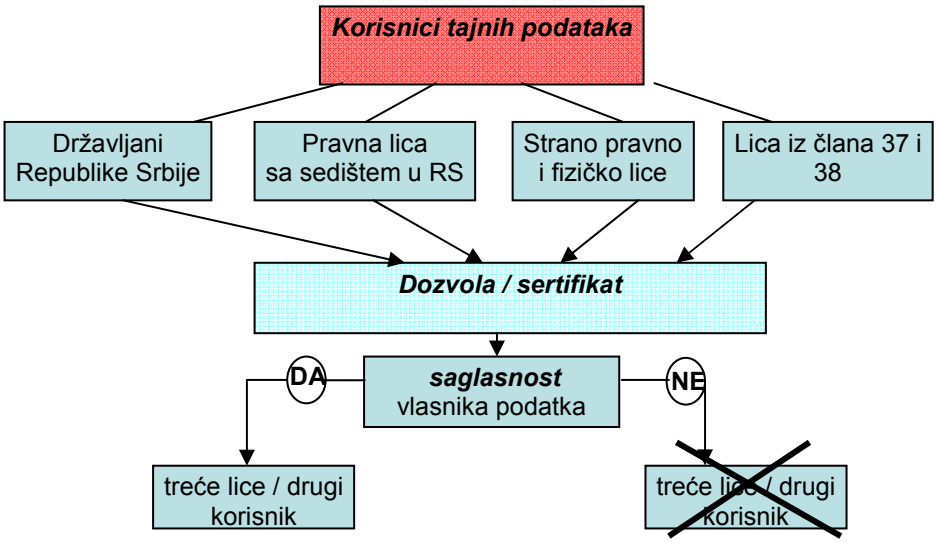
„DRŽAVNU TAJNU“ – 3 godine,

„STROGO POVERLjIVO“ – 5 godina,

„POVERLjIVO“ – 10 godina i

„INTERNO“ – 15 godina –izdaje se pravnim licima, fizička potpisuju izjavu.

Korišćenje tajnih podataka prikazano je na slici 8.



Slika 8 – Korisnici tajnih podataka
Figure 8 – Users of classified information

Mere zaštite tajnih podataka:

1. Fizička zaštita – prostor/prostorija u kojoj se čuvaju, koriste, obrađuju ili uništavaju tajni podaci: bezbednosno-zaštitni mehanizam na ulaznim vratima (deponovanje podataka), oprema za sigurno čuvanje predmeta i dokumenata, energetski priključci (neprekidno i alternativno napajanje), bezbednosni mehanički sistem za zaključavanje (ograničen broj ključeva).
2. Administrativna zaštita.
3. Zaštita lica koja rukuju tajnim podacima.
4. Informatička zaštita.
5. Industrijska zaštita.

Bereš, P., Heuristika i zakonska regulativa u oblasti zaštite tajnih podataka u funkciji edukacije subjekata sistema odbrane, pp. 121–135

Kriterijumi za određivanje mera zaštite tajnog podatka (stepen tajnosti, sadržaj, vrsta i forma).

– *Administrativna zona* je prostor ili prostorija u kojoj je obezbeđen nadzor ulaska, izlaska i kretanja lica i vozila. U ovoj zoni dozvoljeno je rukovanje tajnim podacima stepena tajnosti *„INTERNO“,*

– *Bezbednosna zona* je prostor ili prostorija u kojoj je dozvoljeno rukovanje tajnim podacima svih stepena tajnosti. Bezbednosna zona, pored opštih, mora da ispuni posebne fizičko-tehničke mere zaštite tajnih podataka.

Bezbednosne zone mogu biti I. ili II. stepena:

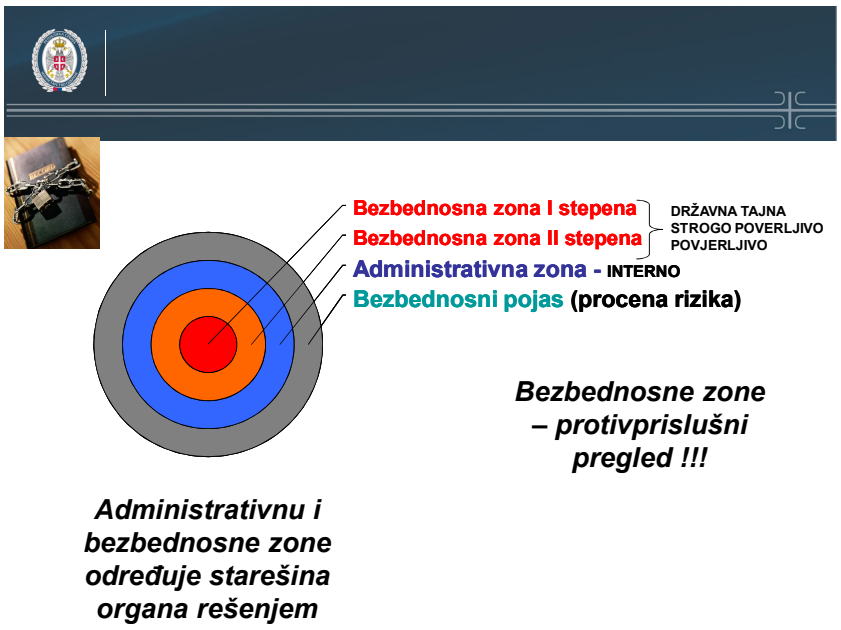
– Bezbednosna zona I. stepena:

- *DRŽAVNA TAJNA, STROGO POVERLJIVO i POVERLJIVO.*
- *Mora biti vidno označena (obaveštenje) osim ako starešina organa odredi drugačije.*
- *Video-nadzor na ulazu i evidencija ulaza/izlaza.*
- *Vođenje evidencija o pristupu TP (korišćenju i uvidu).*
- *Zabrana unošenja sredstava za moguću zloupotrebu.*
- *Neposredno i neprekidno fizičko obezbeđenje/elektronski sistem za protivprovalu (jedinica za intervenciju.)*
- *Neprekidno tehničko obezbeđenje.*
- *Obilaženje prostorija van radnog vremena.*
- *Bezbednosna propusnica/posebna bezbednosna propusnica.*

– Bezbednosna zona II. stepena:

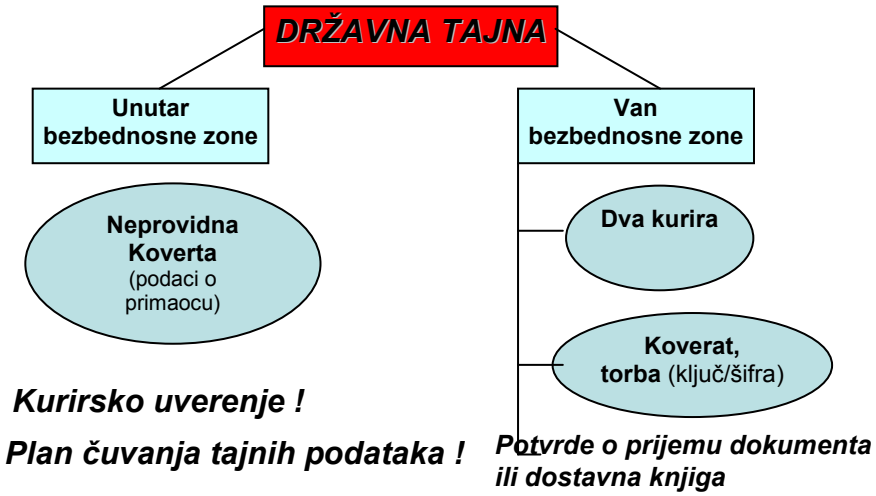
- *DRŽAVNA TAJNA, STROGO POVERLJIVO i POVERLJIVO.*
- *Mora biti vidno označena (obaveštenje) osim ako starešina organa odredi drugačije.*
- *Video nadzor na ulazu i evidencija ulaza/izlaza.*
- *Ulazak drugih lica u pratnji zaposlenog.*
- *Zabrana unošenja sredstava za moguću zloupotrebu.*
- *Fizičko i protivprovalno obezbeđenje kao i povremeno pregledanje van radnog vremena.*
- *Bezbednosna propusnica/posebna bezbednosna propusnica.*

Određivanje bezbednosnih zona prema stepenu tajnosti, kao i ostale aktivnosti starešine prikazane su na slici 9.



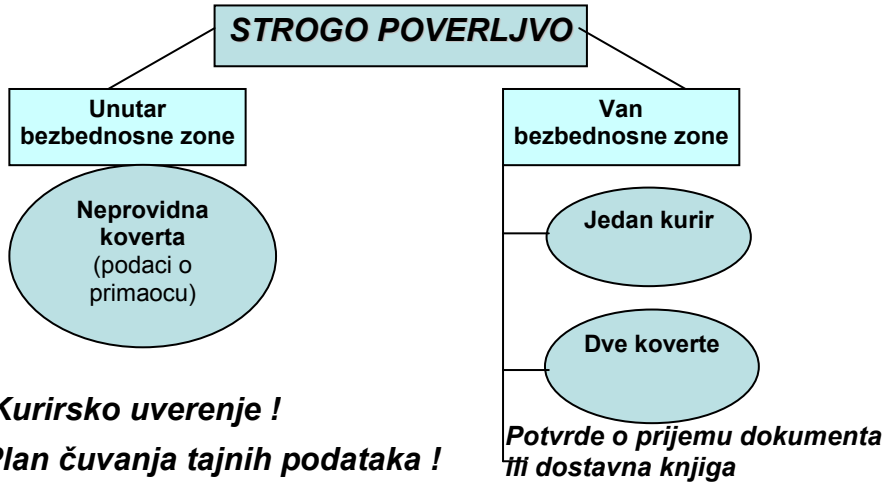
Slika 9 – Određivanje bezbednosnih zona
Figure 9 – Determination of security zones

Dosadašnja praksa u dostavljanju dokumenta sa stepenom tajnosti prikazani su kao: „Državna tajna“ (slika 10) i „Strogo poverljivo“ (slika 11).



Slika 10 – Dostavljanje dokumenta „Državna tajna“
Figure 10 – Submitting a document „Top Secret“

Bereš, P., Heuristika i zakonska regulativa u oblasti zaštite tajnih podataka u funkciji edukacije subjekata sistema odbrane, pp. 121–135



Slika 11 – Dostavljanje dokumenta „Strogo poverljivo“
Figure 11 – Submitting a document „ Secret“

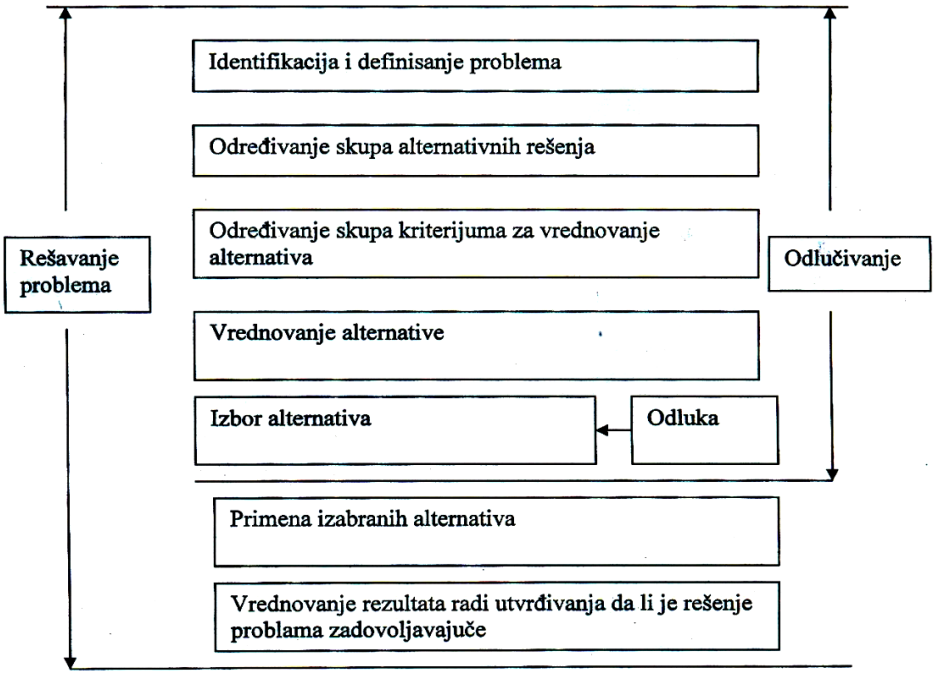
Rešavanje problema i donošenje adekvatnih odluka

Donošenje odluke je problem koji se pojavljuje u svakoj delatnosti. U kontekstu višekriterijske optimizacije, problem odlučivanja se najčešće posmatra kao problem u kojem se donositelj odluke mora opredeliti za jednu od alternativa, uzimajući u obzir sve relevantne faktore, odnosno kriterije. Kako su kriteriji po pravilu konfliktni, izbor donositelja odluke neće biti optimalno rešenje u tradicionalnom smislu, već će biti reči o zadovoljavajućem rešenju od kojeg u datoj situaciji ne postoji bolje, a to su heurističke metode, u našem slučaju primenjene u edukaciju štabova za vanredne situacije i svih onih koji dolaze u kontakt sa podacima sa stepenom tajnosti pri rešavanju problema i donošenja odluka (Bereš, 2013).

Članovi štaba za vanredne situacije suočeni su sa lepezom problema (slika 1 i 2), koje treba rešavati heurističkim metodama i lepezom mogućnosti (slika 3, 4, 5, 6, 7, 8, 9, 10 i 11), koje treba staviti u funkciju rešavanja problema, tj. doneti pravovremenu i adekvatnu odluku (slika 12) po pitanju određivanja stepena tajnosti, čuvanju i određivanju bezbednosnih mera i bezbednosnih zona.

Štab za vanredne situacije čine predstavnici iz:
- lokalnih samouprava (gradova i opština),
- MUP-a/Sektor za vanredne situacije,
- MO/Uprava za obaveze odbrane,
- javnih-komunalnih preduzeća,

• zdravstva/hitne medicinske pomoći,
• Crvenog krsta,
• medija i dr.



Slika 12 – Odnos – rešavanje problema/odlučivanje
Figure 12 – Relation-problem solving /decision making

Zaključak

Prednosti heurističkog modela edukacije jesu: timski rad u rešavanju problema na zaštiti tajnih podataka u vanrednim situacijama; više ljudi donosi različite veštine u tim, što pospešuje efikasnost; više znanja i informacija; heuristička predviđanja problema; veće razumevanje i posvećenost problemima u svim situacijama; fokus, usredsređenost na problem; proces odlučivanja po fazama sa odgovarajućim aktivnostima.

Faza odlučivanja predstavlja proces donošenja odluke i obuhvata sledeće aktivnosti: analizu problema i definiciju ciljeva, analizu rizika, razradu strategija, razradu modela i simulacija ponašanja i donošenje odluke i njeno prenošenje na subjekte; primenu heurističkih tehnika na rešavanje kombinatornih problema u svim situacijama; primenu heurističkih metoda koja je usmerena na dva pravca : (a) na rešavanje složenih problema koji se mogu predstaviti u

kvantitativnom obliku, ali su toliko složeni da njihovo rešenje nije moguće naći pomoću strogih analitičkih tehnika i (b) na probleme koji se ne mogu predstaviti matematičkim modelom, jer su promenljive u modelu kvantitativne prirode. Cilj heurističeke metode jeste da omogući nalaženje prihvatljivih rešenja složenih problema koji ne mogu da se reše pomoću klasičnih metoda.

Rešavanje problema može da se ostvari na dva načina: *primenom heurističkih metoda* (rešavanje problema sa aspekta upravljanja podacima) i *primenom analitičkih metoda* (rešavanje problema sa aspekta upravljanja modelima). Pored toga, potrebno je razvijati modele i metode kojima bi se unapredio kvalitet donošenja odluka kvantitavnim sredstvima (softverska podrška), a radi racionalnijeg korišćenja resursa (energije, novca, vremena, radne snage, hrane, itd.) u svim, pa i u vanrednim situacijama.

Važno je predlagati originalna rešenja i biti konkurentan vodećim istraživanjima u oblasti vanrednih situacija uz primenu propisa o određivanju podataka od interesa za Republiku Srbiju. Takođe, potrebno je uključivati mlade istraživače i osposobljavati ih da u budućnosti budu vodeći domaći i svetski eksperti u oblasti vanrednih situacija (Bereš, 2013).

Neuređen sistem zaštite podataka odražava se na nacionalnu bezbednost, ali i sve druge aspekte svakodnevnog života i rada. Svest zaposlenih o značaju poštovanja propisa o zaštiti podataka i dalje nije na zadovoljavajućem nivou.

Neophodno je što hitnije donošenje svih propisa koji uređuju oblast zaštite podataka i praktičnu primena u radu sa tajnim podacima.

Potrebno je obezbediti permanentnu edukaciju zaposlenih u oblastima zaštite tajnih podataka, a posebnu pažnju posvetiti edukaciji lica koja se bave poslovima zaštite u IKT sistemima.

Radi sprečavanja kompromitacije tajnih podataka trebalo bi da svi nadležni organi preduzmu preventivne mere iz svoje nadležnosti:

- redovno praćenje stanja i rada sa tajnim podacima kojima raspolažu;
- u slučaju saznanja o kompromitaciji tajnih podataka pokretanje procedure vanrednog događaja;
- u zavisnosti od vrste tajnosti, obaveštavanje BIA, MUP-a, itd.,
- prikupljanje saznanja o događaju (o kompromitaciji tajnih podataka),
- izrada izveštaja;
- pokretanje disciplinskog postupka i podnošenje krivične prijave;
- preispitivanje mera bezbednosti i personalnih rešenja.

Literatura

Amaldi, E., Capone, A., & Malucelli, F. 2003. *Optimization models with power control and algorithm.* Preuzeto sa https://www.google. rs/?gws_rd=cr&ei=kz-BUvvEAs-WatQbT4YGwBw#q=planning+umts+base+station+location+optimization+models+with+power+control+and+algorithms

Bereš, P. 2005. *Heuristički modeli nastave politehničkog obrazovanja u osposobljavanju kadrova za potrebe civilne odbrane.* Zrenjanin: Univerzitet u Novom Sadu, Tehnički Fakultet.

Bereš, P. 2013. Heuristički model edukacije i prototip sistema za daljinsko aktiviranje sirena u vanrednim situacijama. *Vojnotehnički glasnik,* 61(1), str. 46–57. doi:10.5937/vojtehg61–2400

Kovačević, N. 2013. *Zaštita tajnih podataka.* Preuzeto sa http://www.arhivinfo. org. rs/radovi-2012/radovi/Zastita%20tajnih%20podataka. pdf 2013 Oct 14.

Kvaščev, R. 1978. *Modeliranje procesa učenja.* Beograd: Prosveta.

Hotomski, P. 1995. *Sistemi veštačke inteligencije.* Zrenjanin: Tehnički fakultet 'Mihajlo Pupin'.

HEURISTICS LEGISLATION IN THE FIELD OF CLASSIFIED INFORMATION AS A FUNCTION OF TRAINING SUBJECTS OF DEFENSE

FIELD: Security and Protection
ARTICLE TYPE: Professional Paper

Abstract

Education on the protection of classified information should be the top priority when it comes to ensuring the protection of the vital interests of the state. Some information should not be made available to the public because it is mainly related to national security, and no one should question the need to protect this kind of data. This paper is intended for educators dealing with the protection of classified information, and especially to those who work with or come into contact with confidential information in order to inform them of our national system of protection of classified information and enable the implementation of the existing legislation applying the heuristic model of education. This article describes the legal regulations governing the protection of dataand shows mandatory standards and measures for the protection of classified information.

Keywords: *heuristics; Information use; classification; protection.*

Datum prijema članka/Paper received on: 24. 10. 2013.
Datum dostavljanja ispravki rukopisa/Manuscript corrections submitted on: 15. 11. 2013.
Datum konačnog prihvatanja članka za objavljivanje/ Paper accepted for publishing on: 17. 11. 2013.