Časopis za poslovnu teoriju i praksu
Rad primljen: 05.05.2025.
Rad odobren: 16.06.2025.

UDK 342.738:]341.211:355.40
DOI 10.7251/POS2534143N
COBISS.RS-ID 142876673
Pregledni rad

Novković Đorđe, MUP Republike Srpske, PU Banja Luka, Bosna i Hercegovina,
djordje.novkovich@livecom

DRŽAVNA TAJNA – KONSPIRATIVNOST

Rezime: *U naučnom radu se detaljno razmatraju mjere zaštite povjerljivosti unutar komandnog lanca u sigurnosnim organima. Ključna je interpretacija poštovanja organizacijske strukture i zapovjednog niza, koji je oslonac na tehničku podršku u komandovanju unutar Centara veze i komandnih punktova (KZ), kao i u svim sigurnosno-obrambenim institucijama.*
Iz do sada prikupljenih iskustava vidljivo je da je sigurnosni rad često narušavan posljedičnim ulaskom nižih organizacionih jedinica ili pojedinaca u ulogu viših, što im omogućuje neautorizovano zapovijedanje i zahtjevnost. Takva praksa direktno krši dodijeljene nadležnosti i narušava jasnu liniju odgovornosti utvrđenu važećim procedurama i propisima.
Naučni rad jasno ukazuje na nužnost dosljednog poštovanja zapovjednog lanca i tehničkih procedura, kako bi se očuvao integritet i efikasnost sistema sigurnosnih mjera.

Ključne riječi: *tajnost, povjerljivost, linija komandovanja, odavanje, kazne i kontra mjere*

JEL klasifikacija: *K29*

UVOD

Tajnost i povjerljivost dolazi do izražaja u svim ozbiljnim državama kao i u tehničkoj podršci rukovodnom (komandnom) kadru gdje Centri veze i KZ ne mogu postupati po naredbama nižih organizacionih jedinica, kako radi organizacije, tako i radi odavanja službenih tajni do stepena tajno (državna tajna).
Uzimajući sve rasprostranjenije informaciono-komunikacione tehnologije u korespodenciji između organizacionih jedinica, prestalo se paziti na povjerljivost, kako u svakodnevnom razgovoru rukovodilaca, do planiranja operativnih akcija.
To se ogleda u tome što se u same prostorije za sastanke, kabinete i Centre veze i KZ unose uređaji za slikanje i snimanje, što je strogo zabranjeno, kao i razgovor o određenim stvarima preko mobilnih uređaja na javnim mrežama i korespodencije preko elektronske pošte (interneta), zaobilazeći službu za zaštitu informacija, koja je ustrojena u vidu Centra veze i KZ.
Takođe, u apstrakt ovog rada, osim narušene linije rada u tajnosti, uzeće se u obradu oznake tajnosti i sankcije koje se podrazumijevaju, kao i narušene mjere odavanja kripto kadra i njeno publikovanje na mreži, što sve dovodi u opasnost bezbjednosnu politiku u svim ozbiljnim bezbjednosno - obavještanim i vojnim organizacijama.

1. DRŽAVNA TAJNA - KONSPIRATIVNOST

1.1. Državna tajna - Opšte informacije

U kraćoj verziji, tajni su svi podaci kojima raspolažu organi javne vlasti, a koji su iz opravdanih razloga i na propisani način proglašeni tajnim i označeni kao tajni (Horn 2012, 13).
U dužoj verziji, to mogu biti podaci koji se odnose na teritorijalni integritet i suverenost države, zaštitu ustavnog poretka, ljudskih i manjinskih prava i sloboda, nacionalnu i javnu bezbjednost, unutrašnje i spoljne poslove, kao i strani tajni podaci (oni koje su našoj državi povjerile strane države ili međunarodne organizacije ili oni koji su nastali u saradnji države sa međunarodnim subjektima). Među svim ovim podacima, opravdanom se smatra zaštita podataka čijim bi otkrivanjem bila naneta šteta radu nekog javnog organa ili interesima države, pod uslovom da zaštita interesa države preteže nad interesom za pristup informacijama od slobodan javnog značaja.
Takođe, po zakonu o tajnosti podataka, podaci koji su označeni kao tajni da bi se prikrilo neko krivično djelo, prekoračenje ovlašćenja, zloupotreba službenog položaja ili neko drugo nezakonito djelo, ne smatraju se tajnim. To, nažalost, ne znači da neće neki organ vlasti, svejedno, pokušati da ih uskrati. Ako se takva informacija, ipak, uspije dobaviti ili ako postoji saznanje da postoji takav dokument, treba se obratiti povjereniku za informacije od javnog značaja, koji će tražiti da se s takvog dokumenta skine oznaka tajnosti. Ako se bez toga objavi takav dokument, pred sudom treba dokazivati da nije zadovoljavao uslove i da se smatra tajnim.

1.2. Stepeni povjerljivosti danas

Iako izraz „državna tajna“ u slengu obično obuhvata sve što država želi da sakrije od „neželjenih očiju”, to se, zapravo, odnosi na samo jednu kategoriju tajni, do onih najpoverljivijih (Skolnick 1982, 45). Redom, kategorije tajnosti određene su ovako:
1. INTERNO: ovim stepenom tajnosti označavaju se dokumenti čija zloupotreba mogla da ugrozi rad, odnosno obavljanje poslova organa javne vlasti, koji je odredio stepen poverljivosti;
2. POVJERLJIVO: Ovaj stepen tajnosti određuje se za dokumente čija zloupotreba može izazvati štetu interesima države;
3. STROGO POVJERLJIVO: Može izazvati tešku zloupotrebu i štetu po interese države;
4. DRŽAVNA TAJNA: Ovaj stepen tajnosti određuje se radi sprečavanja nastanka neotklonjive, teške štete po interese države.
Osim što sa sobom nosi različitu dozu uzbudljivosti, neovlašćeni pristup različitim kategorijama tajnih dokumenata može donijeti i različite zakonske posljedice. O tome se može pročitati u segmentu: „Zakonske posljedice objavljivanja poverljivih dokumenata”.

Ko određuje šta je tajna?

Ovlašćenje da proglase tajnim neki podatak imaju samo sljedeće osobe:
Predsjednik Narodne skupštine,
Predsjednik države,
Predsjednik Vlade,
Rukovodilac organa javne vlasti,
Funkcioner organa vlasti koji je za to ovlašćen zakonom ili podzakonskim aktom, ili pismenim ovlašćenjem rukovodioca.

Koliko dugo nešto ostaje tajna?

Tajnost podatka nekog dokumenta može biti vremenski ograničena na različite načine. U zavisnosti od slučaja, nekada će to biti određeni podatak (na primjer, 23. april 2025. godine) ili

određeni događaj poslije koga prestaje dokument da bude tajna (recimo, podatak o mjerama obezbeđenja na nekoj utakmici i on prestaje da bude relevantan nakon što je održana utakmica). Ako nije predviđen prestanak tajnosti nastupanjem određenog datuma ili događaja, primjenjuju se rokovi zavisno od stepene tajnosti, tako da svaki stepen nosi određen broj godina važenja. Pored nabrojanih načina, tajna prestaje da bude tajna i kada, iz bilo kakvog razloga, podatak postane poznat javnosti.

1.3. Obilježavanje dokumenta

Svaki dokument koji sadrži tajne podatke mora biti vidno obilježen. Obilježje obavezno sadrži oznaku stepena tajnosti („interno", „povjerljivo", itd). Pored oznake stepena tajnosti, najčešće će biti naveden I način prestanka tajnosti (podatak, događaj koji je u vezi s prestankom tajnosti, itd), podaci o ovlašćenom licu i podaci o organu javne vlasti, koji je podatak proglasio.

2. OSNOVNE ODREDBE O TAJNOSTI

Osnovnim odredbama uređuje se jedinstven sistem određivanja i zaštite tajnih podataka koji su od interesa za nacionalnu i javnu bezbjednost, odbranu, unutrašnje i spoljne poslove države, zaštite stranih tajnih podataka (Aistrope and Bleiker 2018, 169), pristup tajnim podacima i prestanak njihove tajnosti, nadležnost organa i nadzor nad sprovođenjem ovog zakona (Humayun 2013, 107), kao i odgovornost za neizvršavanje obaveza iz ovog zakona i druga pitanja od značaja za zaštitu tajnosti podataka i pojmova.

1) Podatak od interesa za državu je svaki podatak ili dokument kojim raspolaže organ javne vlasti, koji se odnosi na teritorijalni integritet i suverenost, zaštitu ustavnog poretka, ljudskih i manjinskih prava i sloboda, nacionalnu i javnu bezbjednost, odbranu, unutrašnje poslove i spoljne poslove.
2) Tajni podatak je podatak od interesa za državu koji je zakonom, drugim propisom ili odlukom nadležnog organa donesenom u skladu sa zakonom, određen i označen određenim stepenom tajnosti.
3) Strani tajni podatak je podatak koji državi povjeri strana država ili međunarodna organizacija uz obavezu da ga čuva kao tajni, kao i tajni podatak koji nastane u saradnji države sa drugim državama, međunarodnim organizacijama i drugim međunarodnim subjektima, u skladu sa zaključenim međunarodnim sporazumom, koji je sa stranom državom, međunarodnom organizacijom ili drugim međunarodnim subjektom zaključila država.
4) Dokument je svaki nosač podatka (papir, magnetni ili optički medij, disketa, USB memorija, smart kartica, kompakt disk, mikrofilm, video i audio zapis i dr), na kome je zapisan ili memorisan tajni podatak.
5) Određivanje tajnih podataka je postupak kojim se podatak, u skladu sa ovim zakonom, određuje kao tajni i za koji se utvrđuje stepen i rok tajnosti.
6) Označavanje stepena tajnosti je označavanje tajnog podatka oznakama: „državna tajna", „strogo povjerljivo", „povjerljivo" ili „interno".
7) Organ javne vlasti je državni organ, organ teritorijalne autonomije, organ jedinice lokalne samouprave, organizacija kojoj je povjereno vršenje javnih ovlašćenja, kao i pravno lice koje osniva državni organ ili se finansira u cjelini, odnosno u pretežnom dijelu iz budžeta, a koji postupa sa tajnim podacima, odnosno koji ih stvara, pribavlja, čuva, koristi, razmjenjuje ili na drugi način obrađuje.
8) Bezbjednosna provera je postupak koji prije izdavanja sertifikata za pristup tajnim podacima sprovodi nadležni organ, u cilju prikupljanja podataka o mogućim bezbjednosnim rizicima i smetnjama u pogledu pouzdanosti za pristup tajnim podacima.

9) Šteta je narušavanje interesa države nastala kao posljedica neovlašćenog pristupa, otkrivanja, uništavanja i zloupotrebe tajnih podataka ili kao posljedica druge radnje obrade tajnih podataka i stranih tajnih podataka.
10) Rukovalac tajnim podatkom je fizičko lice ili organizaciona jedinica organa javne vlasti, koji preduzima mjere zaštite tajnih podataka u skladu sa odredbama ovog zakona (u daljem tekstu: rukovalac).
11) Korisnik tajnog podatka je državljanin ili pravno lice sa sjedištem u datoj državi, kome je izdato rješenje od strane nadležnog organa, odnosno strano fizičko ili pravno lice kome je na osnovu zaključenog međunarodnog sporazuma izdata bezbjednosna dozvola za pristup tajnim podacima (u daljem tekstu: dozvola), kao i funkcioner organa javne vlasti koji na osnovu ovog zakona ima pravo pristupa i korišćenja tajnih podataka bez izdavanja sertifikata.
12) Bezbjednosni rizik je stvarna mogućnost narušavanja bezbjednosti tajnih podataka.
13) Mjere zaštite su opšte i posebne mjere koje se preduzimaju radi sprečavanja nastanka štete, odnosno mjere koje se odnose na ostvarivanje administrativne, informatičko - telekomunikacione, personalne i fizičke bezbjednosti tajnih podataka i stranih tajnih podataka.

2.1. Podaci koji se ne smatraju tajnim podacima

Tajnim podatkom ne smatra se podatak koji je označen kao tajna radi prikrivanja krivičnog djela, prekoračenja ovlašćenja ili zloupotrebe službenog položaja ili drugog nezakonitog akta ili postupanja organa javne vlasti.

2.2. Pravo pristupa

Pristup tajnim podacima moguć je na način i pod uslovima utvrđenim ovim zakonom, propisima donesenim na osnovu ovog zakona i međunarodnim sporazumima.

2.3. Svrha prikupljanja

Tajni podaci se mogu koristiti samo u svrhu zbog koje su prikupljeni, u skladu sa zakonom.

2.4. Čuvanje i korišćenje

Tajni podaci se čuvaju i koriste u skladu sa mjerama zaštite koje su propisane ovim zakonom, propisom donesenim na osnovu ovog zakona i međunarodnim sporazumom.
Lice koje koristi tajni podatak ili lice koje se upoznalo sa njegovom sadržinom dužno je da taj podatak čuva, bez obzira na način na koji je za takav podatak saznalo.
Obaveza ostaje i poslije prestanka funkcije ili radnog odnosa, odnosno prestanka obavljanja dužnosti ili članstva u organu javne vlasti ili odgovarajućem tijelu.

3. ODREĐIVANJE TAJNIH PODATAKA

Kao tajni podatak može se odrediti podatak od interesa za državu čijim bi otkrivanjem neovlašćenom licu nastala šteta. Ako je potreba zaštite interesa države, prestaje važenje zakona od interesa za slobodan pristup informacijama od javnog značaja.
Podatak koji se može odrediti kao tajni je onaj koji može uticati na:
1) Nacionalnu bezbjednost države, javnu bezbjednost, odnosno na odbrambene, spoljno-političke, bezbjednosne i obavještajne poslove organa javne vlasti;
2) Odnose države sa drugim državama, međunarodnim organizacijama i drugim međunarodnim subjektima;

3) Sisteme, uređaje, projekte, planove i strukture koji su u vezi sa podacima;
4) Naučne, istraživačke, tehnološke, ekonomske i finansijske poslove.

3.1. Ovlašćeno lice za određivanje tajnosti podatka

Tajnost podatka, pod uslovima i na način utvrđen, određuje ovlašćeno lice.
Ovlašćena lica su:
1) Predsjednik države;
2) Predsjednik Skupštine;
3) Predsjednik Vlade;
4) Rukovodilac organa javne vlasti;
5) Izabrani, postavljeni ili imenovani funkcioner organa javne vlasti koji je za određivanje tajnih podataka ovlašćen zakonom, odnosno propisom donesenim na osnovu zakona ili ga je za to pismeno ovlastio rukovodilac organa javne vlasti;
6) Lice zaposleno u organu javne vlasti koje je za to pismeno ovlastio rukovodilac tog organa.

3.2. Postupak određivanja tajnosti podatka

Ovlašćeno lice određuje tajnost podatka prilikom njegovog nastanka, odnosno kada organ javne vlasti započne obavljanje posla čiji je rezultat nastanak tajnog podatka.
Ovlašćeno lice može odrediti tajnost podatka i naknadno kad se ispune kriterijumi određeni ovim zakonom.
Pri određivanju tajnosti podatka ovlašćeno lice procenjuje moguću štetu po interes države.
Lice koje je zaposleno, odnosno koje obavlja određene poslove u organu javne vlasti, dužno je da, u okviru svojih radnih zadataka, odnosno ovlašćenja, obavijesti ovlašćeno lice o podacima koji bi mogli da budu određeni kao tajni.

3.3. Odluka o određivanju stepena tajnosti

Odluka o određivanju stepena tajnosti podatka donosi se na osnovu procjene i u skladu sa tim, vrši se obilježavanje dokumenta oznakom tajnosti (u daljem tekstu: oznaka tajnosti).
Pri određivanju stepena tajnosti podatka ovlašćeno lice određuje najniži stepen tajnosti koji sprečava nastanak štete po interese države.
Ako dokument sadrži podatke koji se mogu označiti različitim stepenima tajnosti, ovlašćeno lice u odnosu na te stepene tajnosti obilježava dokument višim stepenom tajnosti.

3.4. Posebni slučajevi određivanja i označavanja tajnih podataka

Ovlašćeno lice određuje kao tajni onaj podatak koji je nastao objedinjavanjem ili povezivanjem podataka koji sami po sebi nisu tajni, ali tako objedinjeni ili povezani predstavljaju podatak koji treba zaštititi iz razloga utvrđenih ovim zakonom.
Dokument koji sadrži podatke koji su već određeni kao tajni, u različitim stepenima i rokovima čuvanja tajnosti, označava se u odnosu na te podatke višim stepenom tajnosti i dužim rokom čuvanja tajnosti sadržanog podatka.
Ako manji dio dokumenta sadrži tajne podatke, izdvaja se i prilaže uz dokument kao poseban prilog obilježen oznakom tajnosti.

3.4.1. Oznake tajnosti

Dokument koji sadrži tajne podatke označava se:
1) Oznakom stepena tajnosti;
2) Načinom prestanka tajnosti;

3) Podacima o ovlašćenom licu;
4) Podacima o organu javne vlasti.

Posebno se smatra tajnim ako je dokument u kome je sadržan podatak označen stepenom tajnosti, ako Vlada propisuje način i postupak označavanja tajnosti podataka, odnosno dokumenata.

3.4.2. Stepeni tajnosti i sadržina podatka

1) „DRŽAVNA TAJNA“, određuje se radi sprečavanja nastanka neotklonjive teške štete po interese države;
2) „STROGO POVJERLJIVO“,određuje se radi sprečavanja nastanka teške štete po interese države;
3) „POVJERLJIVO“, određuje se radi sprečavanja nastanka štete po interese države;
4) „INTERNO“,određuje se radi sprečavanja nastanka štete za rad, odnosno obavljanje zadataka i poslova organa javne vlasti koji ih je odredio.

Bliže kriterijume za određivanje stepena tajnosti „DRŽAVNA TAJNA“ i „STROGO POVJERLJIVO“ određuje Vlada, uz prethodno pribavljeno mišljenje nadležnog ministarstva ili agencije. Bliže kriterijume za određivanje stepena tajnosti „POVJERLJIVO“ i „INTERNO“ određuje Vlada, na prijedlog nadležnog ministra, odnosno rukovodioca organa javne vlasti.

3.4.3. Označavanje stranih tajnih podataka

Dokument koji sadrži strani tajni podatak zadržava oznaku stepena tajnosti kojim je označen u stranoj državi ili međunarodnoj organizaciji.
Pri označavanju stepena tajnosti dokumenata, za dokumenta namijenjena za saradnju sa stranim državama, međunarodnim organizacijama, odnosno drugim subjektima međunarodnog prava, osim izraza mogu se koristiti oznake stepena tajnosti na engleskom jeziku i to:
1) Oznaka stepena tajnosti „TOP SECRET“ odgovara oznaci stepena tajnosti „DRŽAVNA TAJNA“;
2) Oznaka stepena tajnosti „SECRET“ odgovara oznaci stepena tajnosti „STROGO POVERLjIVO“;
3) Oznaka stepena tajnosti „CONFIDENTIAL“ odgovara oznaci stepena tajnosti „POVERLjIVO“;
4) Oznaka stepena tajnosti „RESTRICTED“ odgovara oznaci stepena tajnosti „INTERNO“.

4. PRESTANAK TAJNOSTI

4.1. Vremensko ograničenje tajnosti podataka

Tajnost podataka prestaje:
1) Datumom utvrđenim u dokumentu u kome je sadržan tajni podatak;
2) Nastupanjem određenog događaja utvrđenog u dokumentu u kome je sadržan tajni podatak;
3) Istekom zakonom određenog roka;
4) Opozivom tajnosti;
5) Ako je podatak učinjen dostupnim javnosti.

Ovlašćeno lice može da promjeni način koji je određen za prestanak tajnosti podatka, ako za to postoje osnovani razlozi, u skladu sa zakonom.
O promjeni ovlašćeno lice je dužno, bez odlaganja, u pisanom obliku da obavijesti organe javne vlasti i lica koja su tajni podatak dobila ili imaju pristup tom podatku.

4.2. Prestanak tajnosti utvrđivanjem datuma

Ako ovlašćeno lice u postupku određivanja tajnosti utvrdi da nastupanjem određenog datuma prestaju razlozi zbog kojih je podatak proglašen za tajni, utvrdiće datum prestanka tajnosti i označiti ga u dokumentu koji sadrži takav podatak.

4.3. Prestanak tajnosti nastupanjem određenog događaja

Ako ovlašćeno lice u postupku određivanja tajnosti utvrdi da nastupanjem određenog događaja prestaju razlozi zbog kojih je podatak proglašen za tajni, utvrdiće da tajnost prestaje nastupanjem tog događaja i označiti ga u dokumentu koji sadrži takav podatak.

4.4. Prestanak tajnosti istekom roka

Ako prestanak tajnosti podatka nije određen, tajnost prestaje istekom roka koji je određen zakonom koji reguliše tu oblast.
Zakonski rok prestanka tajnosti podataka određuje se prema stepenu tajnosti i to:
1) Za podatak sa oznakom „DRŽAVNA TAJNA" - 30 godina;
2) Za podatak sa oznakom „STROGO POVJERLJIVO" - 15 godina;
3) Za podatak sa oznakom „POVJERLJIVO" - pet godina;
4) Za podatak sa oznakom „INTERNO" - dvije godine.
Rokovi teku od dana određivanja tajnosti podatka.

5. PRODUŽENJE ROKA TAJNOSTI

5.1. Produženje roka čuvanja tajnosti podataka

Ako poslije isteka roka postoje razlozi da se podatak i dalje čuva kao tajni, ovlašćeno lice može produžiti rok za prestanak tajnosti najduže za vremenski period utvrđen za pojedine stepene tajnosti.
Pored ovlašćenog lica, Vlada može produžiti rok čuvanja tajnosti u slučajevima:
1) Kada bi njihovo otkrivanje imalo nepopravljive teške štetne posljedice po nacionalnu bezbjednost i naročito bitne državne, političke, ekonomske ili vojne interese države;
2) Kada je to predviđeno međunarodnim sporazumom ili drugim međunarodnim obavezama;
3) Kada bi njihovo otkrivanje imalo nepopravljive teške posljedice po osnovna ljudska i građanska prava jednog ili više lica ili bi ugrozilo bezbjednost jednog ili više lica.

6. OPOZIV TAJNOSTI

6.1. Opoziv tajnosti podataka

U postupku opoziva tajnosti podataka utvrđuje se da podatak prestaje da bude tajni prije isteka roka.
Odluka o opozivu tajnosti podatka donosi se ako nastupe činjenice i okolnosti usljed kojih podatak prestaje da bude od interesa za državu.
Periodična procijena tajnosti: ovlašćeno lice vrši periodičnu procjenu tajnosti, na osnovu koje može izvršiti opoziv tajnosti i to:
1) Za podatak označen stepenom „DRŽAVNA TAJNA", najmanje jednom u deset godina;
2) Za podatak označen stepenom „STROGO POVJERLJIVO", najmanje jednom u pet godina;
3) Za podatak označen stepenom „POVJERLJIVO", najmanje jednom u tri godine;
4) Za podatak označen stepenom „INTERNO", najmanje jednom godišnje.

Ukoliko utvrdi da postoje razlozi, ovlašćeno lice bez odlaganja donosi odluku o opozivu tajnosti, koja mora biti obrazložena.

6.2. Prijedlog za opoziv tajnosti

Korisnik tajnog podatka može ovlašćenom licu predložiti opoziv tajnosti podatka.
Ovlašćeno lice dužno je da razmotri predlog iz stava 1. ovog člana i o svojoj odluci obavijesti predlagača.

6.3. Opoziv tajnosti u postupku vršenja kontrole

U postupku vršenja kontrole za nacionalnu bezbjednost i zaštitu tajnih podataka može od ovlašćenog lica zahtijevati vanrednu procjenu tajnosti podatka i na osnovu te procjene sama donijeti odluku o opozivu tajnosti.

6.4. Opoziv tajnosti na osnovu odluke nadležnog organa

Ovlašćeno lice organa javne vlasti opoziva tajnost podatka, odnosno dokumenta koji sadrži tajni podatak i omogućava ostvarivanje prava tražiocu, odnosno podnosiocu zahtjeva na osnovu rješenja povjerenika za informacije od javnog značaja i zaštitu podataka o ličnosti u postupku po žalbi, odnosno na osnovu odluke nadležnog suda u postupku po tužbi, u skladu sa zakonom kojim se uređuje slobodan pristup informacijama od javnog značaja i zakonom koji uređuje zaštitu podataka o ličnosti.

6.5. Opoziv tajnosti u javnom interesu

Narodna skupština, predsjednik Republike i Vlada mogu sa pojedinih dokumenata opozvati oznaku tajnosti, bez obzira na stepen tajnosti, ako je to u javnom interesu ili zbog izvršavanja međunarodnih obaveza.

6.6. Promjena stepena tajnosti i vremenskog trajanja tajnosti

Obavještenje o promjeni stepena tajnosti i opozivu tajnosti, o promjeni stepena tajnosti i vremenskog trajanja tajnosti, kao i opozivu tajnosti podatka, ovlašćeno lice bez odlaganja u pisanom obliku obavještava korisnike tajnih podataka ili lica koja imaju pristup tim podacima.
Strani tajni podatak.
Promjena stepena i roka tajnosti, kao i opoziv tajnosti stranog tajnog podatka vrši se u skladu sa zaključenim međunarodnim sporazumom i utvrđenim međunarodnim obavezama.

7. MJERE ZAŠTITE TAJNIH PODATAKA

Kriterijumi zaštite tajnih podataka

Organ javne vlasti u skladu sa ovim zakonom i propisima, donijetim na osnovu ovog zakona, uspostavlja sistem postupaka i mjera zaštite tajnih podataka prema sljedećim kriterijumima:
1) Stepenu tajnosti;
2) Prirodi dokumenta u kome je sadržan tajni podatak;
3) Procjeni prijetnje za bezbjednost tajnog podatka.

7.1. Vrste mjera zaštite

Organ javne vlasti primjenjuje opšte i posebne mjere zaštite u skladu sa zakonom i propisom donijetim na osnovu zakona, radi zaštite tajnih podataka koji se nalaze u njegovom posjedu.

7.1.1. Opšte mjere zaštite

Opšte mjere zaštite tajnih podataka obuhvataju:
1) Određivanje stepena tajnosti;
2) Procjenu prijetnje za bezbjednost tajnog podatka;
3) Određivanje načina korišćenja i postupanja sa tajnim podatkom;
4) Određivanje odgovornog lica za čuvanje, korišćenje, razmjenu i druge radnje obrade tajnog podatka;
5) Određivanje rukovaoca tajnim podacima, uključujući i njegovu bezbjednosnu provjeru u zavisnosti od stepena tajnosti podatka;
6) Određivanje specijalnih zona, zgrada i prostorija namijenjenih zaštiti tajnih podataka i stranih tajnih podataka;
7) Nadzor nad postupanjem sa tajnim podatkom;
8) Mjere fizičko - tehničke zaštite tajnog podatka, uključujući i ugradnju i postavljanje tehničkih sredstava zaštite, utvrđivanje bezbjednosne zone i zaštitu van bezbjednosne zone;
9) Mjere zaštite informaciono - telekomunikacionih sistema;
10) Mjere kripto - zaštite;
11) Zaštitni režim radnih i formacijskih mjesta, u okviru akta o unutrašnjem uređenju i sistematizaciji radnih mjesta;
12) Utvrđivanje posebnih programa obrazovanja i obuke za potrebe obavljanja poslova zaštite tajnih podataka i stranih tajnih podataka;
13) Druge opšte mjere određene zakonom.

7.1.2. Posebne mjere zaštite

U cilju efikasne primjene opštih mjera zaštite tajnih podataka utvrđuju se posebne mjere zaštite tajnih podataka.
Pojedine posebne mjere zaštite mogu se bliže urediti aktom nadležnog ministra, odnosno rukovodioca posebne organizacije u skladu sa aktom Vlade.

7.2. Obaveze rukovaoca

Rukovalac tajnim podacima, u skladu sa ovim zakonom i u okviru svojih ovlašćenja, preduzima mjere zaštite tajnih podataka i omogućava korisnicima neposredan pristup tajnim podacima, izdaje kopiju dokumenta koji sadrži tajni podatak, vodi evidenciju korisnika i stara se o razmjeni tajnih podataka.

7.3. Čuvanje, prenošenje i dostavljanje tajnih podataka

Tajni podaci čuvaju se na način tako da je pristup tim podacima dozvoljen samo ovlašćenim korisnicima.
Tajni podaci mogu se prenositi i dostavljati izvan prostorija organa javne vlasti samo uz pridržavanje propisanih mjera bezbjednosti i postupaka kojima se obezbjeđuje da podatke dobije samo lice koje ima sertifikat za pristup tajnim podacima i koje ima pravo da ih dobije.
Prilikom prenošenja i dostavljanja tajnih podataka izvan prostorija organa, postupci i mjere zaštite određuju se prema stepenu tajnosti tih podataka, u skladu sa zakonom i propisom donijetim na osnovu zakona.

Prenošenje i dostavljanje tajnih podataka korišćenjem telekomunikaciono - informatičkih sredstava vrši se uz obaveznu primjenu propisanih mjera kripto - zaštite. Sprovođenje mjera kripto - zaštite, prilikom prenošenja i dostavljanja tajnih podataka, obavlja se u skladu sa zakonom.
Dužnost obavještavanja u slučaju gubitka, krađe, oštećenja, uništenja ili neovlašćenog otkrivanja tajnih podataka i stranih tajnih podataka kada dođe do saznanja da je došlo do gubitka, krađe, oštećenja, uništenja ili neovlašćenog otkrivanja tajnih podataka i stranih tajnih podataka, funkcioner, zaposleno lice, odnosno lice koja obavlja poslove u organu javne vlasti, bez odlaganja obavještava ovlašćeno lice organa javne vlasti (Đorđević 2017, 221).
Lice koje utvrdi da je prilikom prenosa i dostavljanja tajnih podataka izvan prostorija organa javne vlasti došlo do gubitka, krađe, oštećenja, uništenja ili neovlašćenog otkrivanja tajnog podatka i stranog tajnog podatka, bez odlaganja obavještava ovlašćeno lice organa, koji mu je tajne podatke i strane tajne podatke prenio, odnosno dostavio.
Ovlašćeno lice dužno je da bez odlaganja preduzme sve potrebne mjere za utvrđivanje okolnosti zbog kojih je došlo do gubitka, krađe, oštećenja, uništenja ili neovlašćenog otkrivanja tajnog podatka i stranog tajnog podatka, izvrši procjenu prouzrokovane štete, kao i da preduzme potrebne mjere u cilju otklanjanja štete i sprečavanja ponovnog gubitka, krađe, oštećenja, uništenja ili neovlašćenog otkrivanja tajnog podatka i stranog tajnog podatka.

8. PRISTUP TAJNIM PODACIMA

Pristup tajnim podacima bez rješenja

Pristup tajnim podacima i korišćenje podataka i dokumenata, bilo kog stepena tajnosti bez izdavanja sertifikata, na osnovu funkcije i u cilju obavljanja poslova iz njihove nadležnosti imaju predsjednik Narodne skupštine, predsjednik Republike i predsjednik Vlade.
Pristup tajnim podacima bez bezbjednosne provjere i posebna ovlašćenja i dužnosti.
Državni organi, koje bira Narodna skupština, rukovodioci državnih organa, koje bira Narodna skupština, sudije Ustavnog suda i sudije, ovlašćeni su da pristupe podacima svih stepena tajnosti koji su im potrebni za obavljanje poslova iz njihove nadležnosti bez bezbjednosne provjere.
Izuzetno, lica imaju pravo na pristup tajnim podacima koji su označeni stepenom „DRŽAVNA TAJNA“ i „STROGO POVJERLJIVO“, uz prethodnu bezbjednosnu provjeru, ako je to potrebno za obavljanje poslova iz njihove nadležnosti, ako se ti podaci odnose na:
1) Radnje sprečavanja, otkrivanja, istrage i gonjenja za krivična djela, koje sprovode nadležni državni organi, do okončanja istrage, odnosno gonjenja;
2) Način primjene posebnih postupaka i mjera u pribavljanju bezbjednosnih i obaveštajnih podataka u konkretnom slučaju;
3) Pripadnike ministarstva nadležnog za unutrašnje poslove i službi bezbjednosti sa prikrivenim identitetom, dok je to neophodno radi zaštite životnih interesa ovih lica, odnosno članova njihovih porodica (život, zdravlje i fizički integritet);
4) Identitet sadašnjih i bivših saradnika službi bezbjednosti, odnosno trećih lica, dok je to neophodno radi zaštite životnih interesa ovih lica, odnosno članova njihovih porodica (život, zdravlje i fizički integritet).
Lica koja imaju pristup tajnim podacima u skladu sa ovim zakonom, ovlašćena su i dužna da u postupku koji vode i inače, na svaki svrsishodan način i od svakoga zaštite tajnost podataka koje su saznali i da tajnim podacima pristupaju lično.
Pravo pristupa tajnim podacima je dozvoljeno članovima nadležnog odbora Narodne skupštine.
Članovi odbora Narodne skupštine nadležnog za nadzor i kontrolu, u sektoru odbrane i bezbjednosti, imaju pravo na pristup i uvid u tajne podatke u vezi sa vršenjem funkcije nadzora i kontrole, u skladu sa zakonom.

Pravo pristupa tajnim podacima označenim stepenom tajnosti „INTERNO" imaju funkcioneri, zaposlena lica, odnosno lica koja obavljaju poslove u organima javne vlasti i imaju pristup tajnim podacima označenim stepenom tajnosti „INTERNO".

Pristup stranim tajnim podacima

Pristup stranim tajnim podacima vrši se u skladu sa ovim zakonom, propisima donesenim na osnovu ovog zakona, odnosno u skladu sa međunarodnim sporazumom koji je sa stranom državom, međunarodnom organizacijom ili drugim međunarodnim subjektom zaključila država.

8.1. Fizička i pravna lica kao korisnici tajnog podatka

Fizičko i pravno lice - korisnik tajnog podatka, ima pravo pristupa tajnim podacima koji su neophodni za obavljanje poslova iz djelokruga njegovog rada i koji su po stepenu tajnosti određeni u sertifikatu za pristup tajnim podacima (u daljem tekstu: sertifikat), odnosno dozvoli. U slučaju izuzetne hitnosti u postupanju lice kome je izdat sertifikat, odnosno dozvola za pristup tajnim podacima označenim nižim stepenom tajnosti, može biti upoznato sa tajnim podatkom označenim neposredno višim stepenom tajnosti.
Lice je dužno da potpiše izjavu, kojom potvrđuje da će postupati sa tajnim podacima, u skladu sa zakonom i drugim propisom.

8.2. Izjava i rješenje

Pre izdavanja rješenja, odnosno dozvole, lice kome se izdaje rješenje dužno je da potpiše izjavu, kojom potvrđuje da će postupati sa tajnim podacima u skladu sa zakonom i drugim propisom. Ako lice ne potpiše izjavu postupak izdavanja rješenja, odnosno dozvole se obustavlja. Pisana izjava čini sastavni dio dokumentacije na osnovu koje je izdato rješenje, odnosno dozvola.

8.3. Oslobođenje od dužnosti čuvanja tajnosti

Lice kome je izdato rješenje, odnosno dozvola, te podatke ne može da upotrebljava u druge svrhe osim svrhe za koje je rješenje, odnosno dozvola izdata.
Rukovodilac organa javne vlasti može da na zahtjev nadležnog organa oslobodi lice dužnosti čuvanja tajnosti podatka posebnom odlukom kojom će se predvidjeti i mjere zaštite tajnosti podataka, ali samo za namjene i u obimu koji sadrži zahtjev nadležnog organa, u skladu sa zakonom. Na zahtjev nadležnog organa, rukovodioca organa javne vlasti dužnosti čuvanja tajnosti podatka, može osloboditi organ koji ga je imenovao, izabrao, odnosno postavio.

8.4. Dostavljanje tajnih podataka uz obavezu čuvanja tajnosti

Tajni podaci mogu se dostaviti drugom organu javne vlasti na osnovu pismenog odobrenja ovlašćenog lica organa javne vlasti, koji je podatke označio kao tajne, ako posebnim zakonom nije određeno drugačije. Tajni podatak dobijen od organa javne vlasti ne može se bez saglasnosti organa koji je podatak odredio kao tajni dostaviti drugom korisnik, ako posebnim zakonom nije određeno drugačije. Lica koja obavljaju poslove u organu javne vlasti kome su dostavljeni tajni podaci, dužna su da postupaju u skladu sa odredbama ovog zakona, uz obavezu poštovanja oznake tajnosti i preduzimanja mjera zaštite tajnosti podataka.

8.5. Dostavljanje tajnih podataka na osnovu ugovornog odnosa

Ovlašćeno lice može tajne podatke dostaviti drugim pravnim ili fizičkim licima, koja po osnovu ugovornog odnosa pružaju usluge organu javne vlasti, ako:
1) Pravno ili fizičko lice ispunjava organizacione i tehničke uslove za čuvanje tajnih podataka u skladu sa ovim zakonom i propisom donijetim na osnovu ovog zakona;
2) Su za lica koja obavljaju ugovorene poslove izvršene bezbjednosne provjere i izdati sertifikati;
3) Lica iz tačke 2) pisanom izjavom potvrde da su upoznata sa ovim zakonom i drugim propisima koji uređuju čuvanje tajnih podataka i obavežu se da će sa tajnim podacima postupati u skladu sa tim propisima;
4) Je pristup tajnim podacima potreban radi realizacije poslova predviđenih ugovorom.
Mjere zaštite tajnih podataka koje moraju biti sadržane u ugovoru koji u vezi sa realizacijom poslova zaključe organ javne vlasti i pravno ili fizičko lice.
Vlada bliže propisuje način i postupak utvrđivanja ispunjenosti uslova bezbjednosnih provjera.

Evidencija o tajnim podacima koji su dostavljeni drugim korisnicima

Rukovalac organa javne vlasti uspostavlja i vodi ažurnu evidenciju o tajnim podacima koji su dostavljeni drugim korisnicima izvan organa javne vlasti.

9. POSTUPAK ZA IZDAVANJE RJEŠENJA, ODNOSNO DOZVOLE

9.1. Uslovi za izdavanje rješenja fizičkom licu

Rješenje izdaje nadležni organ utvrđen zakonom, na osnovu pisanog zahtjeva fizičkog lica, ako je podnosilac zahtjeva:
1) Državljanin neke države;
2) Punoljetan;
3) Poslovno sposoban;
4) Neosuđivan na bezuslovnu kaznu zatvora za krivično djelo za koje se goni po službenoj dužnosti, odnosno za prekršaj predviđen ovim zakonom;
5) Prošao odgovarajuću bezbjednosnu provjeru.

9.2. Uslovi za izdavanje rješenja pravnom licu

Sertifikat izdaje nadležni organ, utvrđen zakonom, na osnovu pisanog zahtjeva pravnog lica, koji se podnosi preko zakonskog zastupnika, ako podnosilac zahtjeva:
1) Ima registrovano sjedište na teritoriji države;
2) Obavlja djelatnost u vezi sa interesima utvrđenim u članovima;
3) Prođe odgovarajuću bezbjednosnu provjeru;
4) Nije u postupku likvidacije, odnosno stečaja;
5) Nije kažnjen mjerom zabrane vršenja djelatnosti, odnosno da mu nije izrečena kazna prestanka pravnog lica ili mjera bezbjednosti zabrane obavljanja određenih registrovanih djelatnosti ili poslova;
6) Uredno plaća poreze, odnosno doprinose.

9.3. Izdavanje dozvole stranom licu

Stranom licu nadležni organ izdaje dozvolu ako:
1) Posjeduje odgovarajući sigurnosni sertifikat izdat od strane države, čiji je državljanin, odnosno u kojoj ima sjedište ili od strane međunarodne organizacije čiji je član;

2) Obaveza omogućavanja pristupa tajnim podacima proističe iz zaključenog međunarodnog sporazuma.

9.4. Podnošenje zahtjeva

Zahtjev za izdavanje rješenja, odnosno dozvole podnosi se Ministarstvu bezbjednosti.
Ako dozvolu zahtijeva rukovalac ili drugi zaposleni u organu javne vlasti, zahtjev se dostavlja rukovodiocu organa javne vlasti.
Ako se rješenje traži za pravno lice, zahtjev podnosi zakonski zastupnik pravnog lica.
Zahtjev za izdavanje rješenja licu, koje će u vezi sa izvršavanjem ugovorenih poslova sa organom javne vlasti imati pristup tajnim podacima, podnosi organ javne vlasti na koji se izvršavanje ugovorenih poslova odnosi.

9.5. Sadržina zahtjeva

Zahtjev fizičkog lica za rješenje sadrži: ime i prezime, prebivalište, poslove koje obavlja, razloge zbog kojih se traži sertifikat, kao i stepen tajnosti podataka za koje se traži sertifikat.
Zahtjev pravnog lica sadrži: naziv firme, sjedište i djelatnost pravnog lica, ime i prezime i prebivalište zakonskog zastupnika pravnog lica, razloge zbog kojih se traži rješenje, kao i stepen tajnosti podataka za koje se traži rješenje.

9.6. Bezbjednosna provjera

Za pristup i korišćenje tajnih podataka vrši se bezbjednosna provjera u zavisnosti od stepena tajnosti, i to:
1) Osnovna bezbjednosna provjera, za podatke označene stepenom tajnosti „INTERNO" i „POVJERLJIVO";
2) Potpuna bezbjednosna provjera, za podatke označene stepenom tajnosti „STROGO POVJERLJIVO";
3) Posebna bezbjednosna provjera, za podatke označene stepenom tajnosti „DRŽAVNA TAJNA".

9.7. Organ nadležan za vršenje bezbjednosne provjere

Bezbjednosnu provjeru za pristup tajnim podacima i dokumentima stepena tajnosti „DRŽAVNA TAJNA" i „STROGO POVJERLJIVO" vrši obavještajna služba. Bezbjednosnu provjeru za pristup tajnim podacima i dokumentima stepena tajnosti „POVJERLJIVO" i „INTERNO" vrši ministarstvo nadležno za unutrašnje poslove.
Bezbjednosnu provjeru za pristup tajnim podacima i dokumentima svih stepena tajnosti, za lica kojima je pristup tajnim podacima i dokumentima potreban radi obavljanja funkcija ili radnih dužnosti u ministarstvu nadležnom za poslove odbrane i vojsci, vrši Vojno-bezbjednosne služba.
Izuzetno, bezbjednosnu provjeru za pristup tajnim podacima i dokumentima stepena tajnosti „POVJERLJIVO" i „INTERNO", za lica kojima je pristup tajnim podacima i dokumentima potreban radi obavljanja funkcija ili radnih dužnosti u Bezbjednosno – obavještajnoj agenciji, vrši Bezbjednosno - obavještajna agencija.
Bezbjednosnu provjeru za pristup tajnim podacima i dokumentima stepena tajnosti „STROGO POVJERLJIVO" za lica kojima je pristup tajnim podacima i dokumentima tog stepena tajnosti, potreban radi obavljanja funkcija ili radnih dužnosti u ministarstvu nadležnom za unutrašnje poslove, pored organa, vrši i ministarstvo nadležno za unutrašnje poslove.
Organi nadležni za bezbjednosnu provjeru dužni su da u postupku vršenja bezbjednosne provjere ostvare međusobnu saradnju, a posebno u postupku bezbjednosne provjere za pristup

tajnim podacima označenim stepenom tajnosti „DRŽAVNA TAJNA“ i „STROGO POVJERLJIVO“.

9.8. Saradnja sa stranim državama i međunarodnim organizacijama

Organi nadležni za bezbjednosnu provjeru mogu u postupku bezbjednosne provjere sarađivati sa organima stranih država, međunarodnih organizacija i drugih međunarodnih subjekata nadležnih za bezbjednosnu provjeru, u skladu sa međunarodnim sporazumom koji je sa stranom državom, međunarodnom organizacijom, odnosno drugim međunarodnim subjektom (Dentith i Orr 2018, 166).

9.9. Svrha bezbjednosne provjere

Za bezbjednosnu provjeru podnosioca zahtjeva vrši se procijena bezbjednosnog rizika, naročito kod pristupa i korišćenja tajnih podataka (Olmsted 2011, 98).
U okviru bezbjednosne provjere nadležni organ sa aspekta bezbjednosti ocjenjuje navode u popunjenom bezbjednosnom upitniku.
Nadležni organ, u vezi sa navodima iz bezbjednosnog upitnika, prikuplja lične i druge podatke od lica na koje se ti podaci odnose, od drugih organa javne vlasti, organizacija i lica, iz registara, evidencija, datoteka i zbirki podataka koje se vode na osnovu zakona.

9.10. Bezbjednosni upitnik

Radi vršenja bezbjednosne provjere, Kancelarija savjeta dostavlja podnosiocu zahtjeva bezbjednosni upitnik.
Podnosilac zahtjeva popunjava osnovni bezbjednosni upitnik, a ako se sertifikat zahtijeva za tajne podatke stepena tajnosti „DRŽAVNA TAJNA“ i „STROGO POVJERLJIVO“, popunjava i poseban bezbjednosni upitnik.
Popunjeni i potpisani upitnik podnosioca zahtjeva istovremeno predstavlja pisanu saglasnost za vršenje bezbjednosne provjere i označava se stepenom tajnosti „INTERNO”.

9.10.1. Osnovni bezbjednosni upitnik za fizička lica

U osnovni bezbjednosni upitnik unose se sljedeći podaci o podnosiocu zahtjeva:
1) Ime i prezime, kao i prethodna imena i prezimena;
2) Jedinstven matični broj građana;
3) Datum i mjesto rođenja;
4) Državljanstvo, prethodna državljanstva i dvojna državljanstva;
5) Prebivalište i boravište, kao i prethodna prebivališta;
6) Bračni status i porodično stanje;
7) Podaci o licima koja žive u zajedničkom domaćinstvu sa licem na koga se odnosi bezbjednosni upitnik (njihova imena i prezimena, zajedno sa prethodnim imenima i prezimenima, njihovi datumi rođenja, kao i odnos sa licem koje je provjeravano);
8) Ime i prezime, datum rođenja i adresa prebivališta srodnika do drugog stepena srodstva u pravoj i prvog stepena srodstva u pobočnoj liniji, usvojioca, staratelja, očuha, maćehe, odnosno hranitelja;
9) Stručna sprema i zanimanje;
10) Podaci o prethodnim zaposlenjima;
11) Podaci u vezi sa izvršenjem vojne obaveze;
12) Podaci o krivičnom i prekršajnom kažnjavanju i krivičnim i prekršajnim postupcima koji su u toku;

13) Medicinski podaci u vezi sa bolestima zavisnosti (alkohol, opojne droge i dr), odnosno duševnim bolestima;
14) Kontakti sa stranim službama bezbjednosti i obavještajnim službama;
15) Disciplinski postupci i izrečene disciplinske mjere;
16) Podaci o članstvu ili učešću u aktivnostima organizacija čije su aktivnosti ili ciljevi zabranjeni;
17) Podaci o odgovornosti za povredu propisa koji se odnose na tajnost podataka;
18) Podaci o pravu svojine ili drugom stvarnom pravu na nepokretnosti, podaci o pravu svojine na drugim stvarima upisanim u javni registar, kao i podatak o godišnjem porezu na ukupan prihod građana za prethodnu godinu;
19) Prethodne bezbjednosne provjere.

9.10.2. Osnovni bezbjednosni upitnik za pravna lica

U osnovni bezbjednosni upitnik za pravna lica unose se sljedeći podaci o podnosiocu zahtjeva:
1) Naziv firme i sjedište, kao i prethodni nazivi firmi i sjedišta;
2) Matični broj pravnog lica i poresko - identifikacioni broj;
3) Ime i prezime zastupnika;
4) Datum i mjesto osnivanja;
5) Podaci o organizacionim jedinicama, ograncima, zavisnim društvima i drugim oblicima povezivanja;
6) Porijeklo osnivačkog kapitala uključujući i promjene u posljednje tri godine;
7) Broj zaposlenih;
8) Broj zaposlenih za koje se traži sertifikat i vrsta poslova koje obavljaju;
9) Podaci o osudama za krivično djelo, privredni prestup i prekršaj pravnog lica i odgovornih lica u pravnom licu, kao i podaci o postupcima za krivično djelo, privredni prestup ili prekršaj protiv pravnog lica koji su u toku;
10) Podaci o kontaktima sa stranim službama bezbjednosti i obavještajnim službama;
11) Podaci o učešću u aktivnostima organizacije čije su aktivnosti i ciljevi zabranjeni;
12) Podaci o odgovornosti za povredu propisa koji se odnose na tajnost podataka;
13) Podaci o prethodnoj bezbjednosnoj provjeri;
14) Podaci o pravu svojine ili drugom stvarnom pravu o nepokretnostima, podaci o pravu svojine na drugim stvarima upisanim u javni registar, kao i podatak o godišnjem finansijskom izvještaju za prethodnu godinu, u skladu sa zakonom kojim se uređuje računovodstvo i revizija.
Uz popunjeni upitnik, zastupnik pravnog lica dostavlja i popunjen osnovni bezbjednosni upitnik za fizičko lice.

9.10.3. Poseban bezbjednosni upitnik

Za bezbjednosnu provjeru utvrđenu zakonom, pored osnovnog, ispunjava se i poseban bezbjednosni upitnik.
U poseban bezbjednosni upitnik, unose se podaci o:
1) Službi u stranim vojskama i paravojnim formacijama;
2) Drugi podaci i činjenice, koje fizičko, odnosno pravno lice čine podložnim uticajima i pritiscima koji predstavljaju bezbjednosni rizik;
3) Dugovima nastalim usljed finansijskih zaduženja ili preuzetih garancija.

9.10.4. Posebna bezbjednosna provjera

Posebna bezbjednosna provjera vrši se kada se izdavanje rješenja, odnosno dozvole traži za podatke stepena tajnosti „DRŽAVNA TAJNA“.

Posebna bezbjednosna provjera obuhvata, pored provjere činjenica u okviru potpune bezbjednosne provjere, i provjeru činjenica, okolnosti i događaja iz privatnog života podnosioca zahtjeva, najmanje u posljednjih deset godina od dana podnošenja zahtjeva za izdavanje rješenja, koje bi, u slučaju postojanja, predstavljale osnov za sumnju u njegovu povjerljivost i pouzdanost, a naročito ako su njegove aktivnosti u suprotnosti sa interesima države ili ako je povezan sa stranim licima koja mogu da ugroze bezbjednost i međunarodne interese države.

9.11. Rok za izvršenje bezbjednosne provjere

Nadležni organ dužan je da, od dana popunjenog upitnika, izvrši bezbjednosnu provjeru u sljedećim rokovima:
1) Do 30 dana za osnovnu bezbjednosnu provjeru;
2) Do 60 dana za potpunu bezbjednosnu provjeru;
3) Do 90 dana za posebnu bezbjednosnu provjeru.
Izuzetno, ako za to postoje opravdani razlozi, mogu produžiti najduže za vremenski period utvrđen u ovim tačkama.
U slučaju da nadležni organ da dozvolu o produženju roka obavijesti rukovodioca organa javne vlasti koji je dostavio zahtjev za bezbjednosnu provjeru.
Ako se bezbjednosna provjera ne izvrši u rokovima, smatra se da ne postoji bezbjednosni rizik pristupa tajnim podacima podnosioca zahtjeva.

9.12. Privremeno rješenje

Radi izvršavanja neodložnih poslova i zadataka organa javne vlasti, u cilju sprečavanja ili otklanjanja štete, direktor bezbjednosne agencije može izuzetno i prije završetka bezbjednosne provjere izdati licu privremeno rješenje za pristup određenim tajnim podacima, ako se na osnovu uvida u podnijeti bezbjednosni upitnik ocjeni da ne postoje sumnje u pogledu bezbjednosti.
Lice je dužno da pisanom izjavom potvrdi da će sa tajnim podatkom koji mu je povjeren postupati u skladu sa ovim zakonom i drugim propisima koji uređuju čuvanje i postupanje sa tajnim podacima.
Privremeno rješenje važi do okončanja postupka za izdavanje sertifikata.

9.13. Dostavljanje izvještaja o rezultatima bezbjednosne provjere

Organi nadležni za vršenje bezbjednosne provjere, u skladu za zakonima, dostavljaju određenom organu izvještaj o rezultatima bezbjednosne provjere, odnosno posebne bezbjednosne provjere, uključujući i popunjeni bezbjednosni upitnik, sa preporukom za izdavanje ili uskraćivanje rješenja.
Izvještaj i preporuka označavaju se stepenom tajnosti „POVJERLJIVO“.

9.14. Rješenje i dopunska provjera

Ako je izvještaj nepotpun ili je dostavljen bez preporuke, donosi se rješenje na osnovu dostavljenog izvještaja.
Izuzetno, ako se iz izvještaja o rezultatima bezbjednosne provjere i preporuke za izdavanje rješenja ne može utvrditi da li su ispunjeni zakonom propisani uslovi za izdavanje rješenja fizičkom ili pravnom licu ili je poslije izvršene bezbjednosne provjere došlo do bitne izmjene proveravanih podataka koja bi mogla biti od uticaja na izdavanje rješenja, Agencija će zahtijevati od nadležnog organa da izvrši dopunsku provjeru, odnosno dopunu izvještaja i izradu nove preporuke, najkasnije u naknadnom roku od 30 dana.

9.15. Izuzeci

Za lica kojima je pristup tajnim podacima potreban radi obavljanja funkcije ili radnih dužnosti u službama bezbjednosti države, ne primjenjuju se opšta pravila o pristupu – odluku o izdavanju rješenja za pristup tim podacima donosi rukovodilac službe bezbjednosti.

9.16. Dostavljanje rješenja

Agencija dostavlja rješenje rukovodiocu organa javne vlasti koji je tražio izdavanje rješenja i licu za koje je tražena dozvola.

9.17. Odbijanje zahtjeva

Agencija rješenjem odbija zahtjev za izdavanje dozvole, ako se na osnovu izvještaja bezbjednosne, odnosno dopunske bezbjednosne provjere utvrdi:
1) Da je podnosilac zahtjeva naveo neistinite i nepotpune podatke u osnovnom, odnosno posebnom bezbjednosnom upitniku;
2) Da podnosilac zahtjeva ne ispunjava uslove za izdavanje dozvole;
3) Da podnosilac zahtjeva nije obezbjedio uslove za preduzimanje propisanih mjera zaštite tajnih podataka;
4) Da postoji bezbjednosni rizik od pristupa i korišćenja tajnih podataka podnosioca zahtjeva.
Obrazloženje rješenja o odbijanju izdavanja dozvole ne sadrži podatke koji se smatraju tajnim u smislu ovog zakona, niti navođenje izvora bezbjednosne provjere.

9.18. Sadržaj, oblik i dostavljanje rješenja

Sadržinu, oblik i način dostavljanja sertifikata propisuje Vlada, dostavlja dozvolu i upoznaje korisnika sa propisanim uslovima za postupanje sa tajnim podacima, kao i pravnim i drugim posljedicama njihovog neovlašćenog korišćenja.
Prilikom prijema sertifikata, korisnik potpisuje sertifikat, kao i izjavu da je upoznat sa odredbama ovog zakona i drugih propisa kojima se uređuje zaštita tajnih podataka i da će koristiti tajne podatke u skladu sa zakonom i drugim propisima.

9.19. Prestanak važenja rješenja

Dozvola prestaje da važi:
1) Istekom vremena za koje je izdata;
2) Prestankom funkcije lica;
3) Prestankom obavljanja dužnosti i poslova iz djelokruga rada lica;
4) Na osnovu rješenja Agencije donijetog u postupku provejre izdatog rješenja;
5) Smrću fizičkog lica ili prestankom pravnog lica kome je izdata dozvola.

9.20. Prestanak važenja sertifikata istekom vremena

Sertifikat izdat za podatak i dokument označen stepenom tajnosti „DRŽAVNA TAJNA" važi tri godine.
Sertifikat izdat za podatak i dokument označen stepenom tajnosti „STROGO POVJERLJIVO" važi pet godina.
Sertifikat izdat za podatak i dokument označen stepenom tajnosti „POVJERLJIVO" važi deset godina.
Rješenje koje se izdaje za podatak i dokument označen stepenom tajnosti „INTERNO" važi 15 godina.

9.21. Produženje važenja rješenja

Agencija u pisanom obliku obavještava imaoca sertifikata da može da podnese zahtjev za produženje važenja sertifikata najkasnije 6 mjeseci prije isteka važenja rješenja.
Uz zahtjev za produženje podnosilac zahtjeva obavještava Agenciju o svim promjenama podataka iz ranije podnetijog bezbjednosnog upitnika sa dokazima i ponovo vrši bezbjednosnu provjeru.

9.22. Privremena zabrana prava pristupa

Ako je protiv lica kome je izdat sertifikat pokrenut disciplinski postupak zbog teže povrede službene dužnosti, teže povrede vojne discipline, odnosno teže povrede radnih obaveza i dužnosti, krivični postupak zbog osnovane sumnje da je počinilo krivično djelo za koje se goni po službenoj dužnosti, odnosno prekršajni postupak za prekršaj predviđen ovim zakonom, rukovodilac organa javne vlasti može rješenjem privremeno zabraniti pristup tajnim podacima tom licu, do pravosnažnog okončanja postupka.

9.23. Provjera rješenja

Ako se utvrdi da lice kome je izdat sertifikat tajne podatke ne koristi ili ne čuva u skladu sa zakonom i drugim propisima, odnosno da više ne ispunjava uslove za izdavanje sertifikata, Kancelarija savjeta donosi rješenje o prestanku važenja sertifikata, odnosno rješenje o ograničenju prava pristupa tajnim podacima označenim određenim stepenom tajnosti.
Obrazloženje rješenja ne sadrži podatke koji se smatraju tajnim u smislu ovog zakona.
Rješenje Kancelarije savjeta je konačno i protiv njega se može pokrenuti upravni spor.

9.24. Izdavanje dozvole stranom licu

Agencija izdaje dozvolu stranom licu, u skladu sa zaključenim međunarodnim sporazumom.
Po prijemu zahtjeva, Agencija putem međunarodne razmjene provjerava da li je podnosiocu zahtjeva izdat sigurnosni sertifikat od strane države čiji je državljanin ili u kojoj ima sjedište, odnosno od strane međunarodne organizacije čiji je član.
Dozvola se izdaje samo za pristup podacima i dokumentima koji su određeni u zaključenom međunarodnom sporazumu koji je sa stranom državom, međunarodnom organizacijom ili drugim međunarodnim subjektom zaključila država.
Na izdavanje dozvole stranom licu shodno se primjenjuju odredbe ovog zakona o izdavanju rješenja.

9.25. Službene evidencije i drugi podaci vezani za rješenje i dozvolu

Agencija vodi jedinstvenu centralnu evidenciju izdatih sertifikata i dozvola, rješenja o izdavanju sertifikata i dozvola, rješenja o odbijanju izdavanja sertifikata i dozvola, rješenja o produženju važenja sertifikata i dozvola i rješenja o ograničenju ili prestanku važenja sertifikata i dozvola, kao i potpisane izjave lica kojima je izdat sertifikat, odnosno dozvola.
Agencija čuva zahtjeve za izdavanje sertifikata, odnosno dozvole, bezbjednosne upitnike i izvještaje o bezbjednosnoj provjeri sa preporukom.

9.26. Evidencija bezbjednosnih provjera

Organ nadležan za vršenje bezbjednosne provjere vodi evidenciju bezbjednosnih provjera i čuva dokumenta o bezbjednosnoj provjeri sa primjerkom izvještaja i preporuke.

Podaci iz bezbjednosne provjere mogu se koristiti samo za namjene za koje su prikupljeni.

9.27. Primjena propisa o zaštiti podataka o ličnosti

Lice ima pravo uvida u podatke iz svoje bezbjednosne provjere, prikupljene u skladu sa ovim zakonom, kao i druga prava koja proizilaze iz tog uvida, u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti, izuzev uvida u podatke koji bi otkrili metode i postupke korišćene prilikom prikupljanja podataka, kao i izvore iz kojih su ti podaci dobijeni.

9.28. Evidencija organa javne vlasti

Organ javne vlasti vodi evidenciju rješenja o sertifikatu za lica koja u organu javne vlasti obavljaju funkciju ili su zaposlena, odnosno obavljaju poslove.
Rješenje o izdatoj dozvoli za lica čuva se u posebnom dijelu kadrovskog dosijea lica, a podaci iz rješenja mogu se koristiti samo u vezi sa sprovođenjem odredaba ovog zakona, odnosno propisa donijetog na osnovu ovog zakona.
Bliži propis o sadržini, obliku i načinu vođenja evidencija vrši Unutrašnja kontrola.
Za unutrašnju kontrolu nad sprovođenjem zakona i propisa donijetog na osnovu ovog zakona odgovoran je rukovodilac organa javne vlasti.
U ministarstvu nadležnom za unutrašnje poslove, ministarstvu nadležnom za poslove odbrane i Bezbjednosno - obavještajnoj agenciji, a po potrebi i u drugim organima javne vlasti, za unutrašnju kontrolu i druge stručne poslove, u vezi sa određivanjem i zaštitom tajnih podataka, sistematizuje se posebno radno mjesto ili se za obavljanje ovih zadataka i poslova posebno zadužuje postojeća organizaciona jedinica u sastavu ministarstva ili agencije.

9.29. Cilj unutrašnje kontrole

Unutrašnjom kontrolom obezbjeđuje se redovno praćenje i ocenjivanje pojedinih djelatnosti, kao i djelatnost organa javne vlasti u cjelini, u vezi sa sprovođenjem ovog zakona i propisa i mjera donijetih na osnovu ovog zakona.
Rukovodilac organa javne vlasti, neposredno ili preko ovlašćenog lica, vrši unutrašnju kontrolu neposrednim uvidom, odgovarajućim provjerama i razmatranjem podnijetih izvještaja.

9.30. Preuzimanje tajnih podataka

Agencija preuzima tajne podatke organa javne vlasti koji su prestali da postoje, a nemaju pravnog sljedbenika, odnosno zadužuje drugi organ javne vlasti za čuvanje i korišćenje tih podataka.

9.31. Centralni registar stranih tajnih podataka

Agencija obrazuje, vodi i obezbjeđuje Centralni registar stranih tajnih podataka i dokumenata.
Organ javne vlasti, koji je primio strani tajni podatak i dokument u skladu sa posebnim zakonom ili zaključenim međunarodnim sporazumom, koji je sa stranom državom, međunarodnom organizacijom ili drugim međunarodnim subjektom zaključila država, obrazuje, vodi i obezbeđuje poseban registar stranih tajnih podataka (Mijalkovski 2002, 128-130).
Izveštaj koji sadrži brojčane pokazatelje o razmjeni tajnih podataka sa stranom državom ili međunarodnom organizacijom, organ javne vlasti dostavlja Agencija najmanje jednom godišnje.

Davanje i primanje obavještenja

Agencija obavještava stranu državu, odnosno međunarodnu organizaciju o bezbjednosti stranih tajnih podataka dobijenih u međunarodnoj razmjeni.
Agencija prima obavještenja od strane države, odnosno međunarodne organizacije o bezbjednosti tajnih podataka koje je država predala u međunarodnoj razmjeni.

9.32. Razmjena podataka bez zaključenog međunarodnog sporazuma

U krajnje nepovoljnim političkim, ekonomskim ili odbrambeno - bezbjednosnim okolnostima za državu i ako je to neophodno radi zaštite interesa, na zahtjev organa javne vlasti, Agencija razmjenjuje tajne podatke sa stranom državom, odnosno međunarodnom organizacijom i bez prethodno zaključenog međunarodnog sporazuma.

9.33. Nadzor

Nadzor nad sprovođenjem zakona i propisa donijetih na osnovu zakona vrši ministarstvo nadležno za pravosuđe (u daljem tekstu: ministarstvo).
U skladu sa ovim zakonom, u vršenju nadzora, ministarstvo:
1) Prati stanje u oblasti zaštite tajnih podataka;
2) Priprema propise neophodne za sprovođenje ovog zakona;
3) Daje mišljenje na prijedloge propisa u oblasti zaštite tajnih podataka;
4) Predlaže Vladi sadržinu, oblik i način vođenja evidencije tajnih podataka, kao i propise kojima se uređuju obrazac bezbjednosnog upitnika, odnosno obrazac preporuke, sertifikata i dozvole;
5) Nalaže mjere za unapređivanje zaštite tajnih podataka;
6) Kontroliše primjenu kriterijuma za označavanje stepena tajnosti i vrši druge poslove kontrole u skladu sa odredbama zakona;
7) Podnosi krivične prijave, zahtjeve za pokretanje prekršajnog postupka i predlaže pokretanje drugog postupka zbog povrede odredaba zakona, a u skladu sa zakonom;
8) Sarađuje sa organima javne vlasti u sprovođenju ovog zakona u okviru svoje nadležnosti;
9) Obavlja i druge poslove koji su predviđeni zakonom i propisima donijetim na osnovu ovog zakona.
Ministar nadležan za pravosuđe podnosi odboru Narodne skupštine nadležnom za nadzor i kontrolu u oblasti odbrane i bezbjednosti godišnji izvještaj o aktivnos tima u sprovođenju i kontroli primjene ovog zakona.
U obavljanju nadzora ministarstvo vrši kontrolu sprovođenja mjera obezbjeđenja, korišćenja, razmjene i drugih radnji obrade tajnih podataka, bez prethodnog obavještavanja organa javne vlasti, ovlašćenog lica, rukovaoca, odnosno korisnika tajnog podatka. Poslove iz st 1, 2. i 4. ministarstvo vrši preko ovlašćenih lica, koja su prethodno prošla posebnu bezbjednosnu provjeru.
Ovlašćena lica vrše nadzor shodnom primjenom propisa o inspekcijskom nadzoru.
Ovlašćena lica imaju pravo na službenu legitimaciju. Zbog posebnih uslova rada, složenosti i prirode posla ovlašćenim licima može se uvećati plata do 20% u odnosu na platu državnog službenika i namještenika u ministarstvu nadležnom za pravosuđe koji obavlja poslove nadzora nad radom pravosudnih organ, u skladu sa aktom Vlade.
Bliži propis o službenoj legitimaciji i načinu rada ovlašćenih lica donosi ministar nadležan za pravosuđe.

10. KAZNENE ODREDBE

10.1. Krivično djelo

Ko neovlašćeno nepozvanom licu saopšti, preda ili učini dostupnim podatke ili dokumenta koji su mu povjereni ili do kojih je na drugi način došao ili pribavlja podatke ili dokumenta, a koji predstavljaju tajne podatke sa oznakom tajnosti „INTERNO" ili „POVJERLJIVO", određene prema ovom zakonu, kazniće se zatvorom od tri mjeseca do tri godine.
Ako je djelo učinjeno u odnosu na podatke označene u skladu sa zakonom, stepenom tajnosti „STROGO POVJERLJIVO",kazniće se zatvorom od šest mjeseci do pet godina.
Ako je djelo učinjeno u odnosu na podatke označene u skladu sa zakonom, stepenom tajnosti „DRŽAVNA TAJNA", učinilac će se kazniti zatvorom 01-10 godina.
Ako je djelo učinjeno iz koristoljublja ili radi objavljivanja ili korišćenja tajnih podataka u inostranstvu ili je izvršeno za vrijeme ratnog ili vanrednog stanja, učinilac će se kazniti za djelo zatvorom od šest mjeseci do pet godina.
Ako je djelo učinjeno iz nehata, učinilac će se kazniti za djelo zatvorom, a u zavisnosti od stepena tajnosti i do više godina zavisno od zakonodavstva.

11. RELEVANTNA PODRUČJA IZVRŠENIH EMPIRIJSKIH ISTRAŽIVANJA – PREPORUKE

Obradom i analizom zadate teme ovog naučnog rada došlo se do zaključka iz kojeg se mogu izvući sljedeće preporuke za organizaciju i rukovođenje u sistemu bezbjednosti:

1. Vratiti, organizovati zasebnu Upravu za vezu i KZ ustrojenu po jasnoj liniji komandnog lanca, kako je i bila organozovana do ukidanja.
2. Zbog opisa poslova i posebnog odabira kadrova vratiti ovlašćenja i činove po opisu posla.
3. Vezati datu službu direktno uz direktora policije ili uz novu Službu predsjednika Republike, Služba za zaštitu ustavnog poretka, bivša RDB.
4. Vratiti u pravnu proceduru oznake tajnosti i povjerljivosti koje jasno definišu stepene i vrste istih.
5. Radi jedinstvenog lanca komandovanja (rukovođenja) uvesti, kao dopunski udžbenik, koji jasno definiše ovu problematiku, koja se pokazala kao nedostatak, kako među studentima, tako i među novopostavljenim rukovodnim radnicima.
6. Posvetiti više pažnje i tumačenju tajnosti rukovodnim radnicima, što znači komandna linija i njena zaštita putem sistema veza u rukovođenju i komandovanju i operativnost službe, kao i tajnost njenih izvršilaca u sistemu bezbjednosti u prenosu naređenja.
7. Lancu komandovanja posvetiti više pažnje u obradi naredbi, koje se za sad rade na otvorenim mrežama, računarima i elektronskim komercijalnim programima.

ZAKLJUČAK

U ovom naučnom radu, koji se odnosi na organizaciju i rukovođenje u sistemu bezbjednosti, prikazani su elementi podjela i opisa poslova, kako po linijama rada, tako i po teritorijalnoj podjeli.
Svaka bezbjednosna organizacija, bila vojna ili civilna, sa aspekta preventivnog djelovanja u formi obavještajnog rada ili represivnog, mora da bude ustrojena po ovom principu nadležnosti i ovlašćenja po opisu poslova koje obavlja.
Kao što se vidi gore iz navedenog rada na zadatu temu, da bi se što bolje sagledala data problematika izvršena je analiza u metodološkom smislu sa aspekta empirijskog istraživanja, kao i sa anketiranjem građana koji su upoznati sa organizacijom policije i uzeto je u obzir njihovo mišljenje o tome.

Dalji zaključak ovog naučnog rada jeste da je sve što se radi, organizuje u formi nekog planiranja i izvršenja jako bitno dobro organizovati, kako poslove, tako je bitno organizovati i ljude koji će prije svega rukovoditi, a onda i sprovesti zadane i planirane ciljeve.

LITERATURA

1. Aistrope Tim, and Roland Bleiker. 2018. "Conspiracy and foreign policy." *Security Dialogue* 49(3): 165-182.
2. Dentith, Matthew, and Martin Orr. 2018. “Secrecy and conspiracy” *Episteme* 15(4): 433 – 450.
3. Đorđević, Dejan. 2017. Mehanizmi prevencije za uspešno funkcionisanje sistema odbrane u vanrednim situacijama."*Vojno delo* 69(2): 219-249. DOI: 10.5937/vojdelo1702219D https://redun.educons.edu.rs/bitstream/handle/123456789/298/295.pdf?sequence=1&isAllowed=y
4. Horn, Eva. 2012. „Logics of Political Secrecy." *Theory, Culture & Society* 28(7-8):1-20. DOI: 10.1177/0263276411424583 https://journals.sagepub.com/doi/abs/10.1177/0263276411424583
5. Humayun, Zafar. 2013. Human resource information systems: Information security concerns for organizations." *Human Resource Management Review* 23(1):105-113.
6. Mijalkovski, Milan. 2002. „Međunarodna baza podataka o teroristima.” *Vojno delo* 54(6): 127-145.
7. Olmsted, Kathryn. 2011. "Government secrecy and conspiracy theories." *Research in Social Problems and Public Policy* 19: 91-100.
8. Skolnick, Jerome. 1982. "Deception by the police." Criminal Justice Ethics 1(2):40-54.