ВОДИЧ ЗА ИМПЛЕМЕНТАЦИЈУ ЗАКОНА О ТАЈНОСТИ ПОДАТАКА

веб: www.nsa.gov.rs

Проф.др Горан Д. Матић

Београд, 2025. година

САДРЖАЈ

Подизање безбедносне свести и културе са примарним и тежишним задатком заштите интереса Републике Србије који се односе на националну и јавну безбедност,унутрашње и спољне послове Републике Србије, одбрану, заштиту уставног поретка, као и људских и мањинских права!

НЕОПХОДНИ КОРАЦИ

Имплементација Закона о тајности података у органу јавне власти (организациона безбедност)

1. Процена стања и безбедности
2. Доношење нормативе за рад са тајним подацима
3. Одређивање руковаоца тајних података
4. Успостављање и спровођење унутрашње контроле
5. Креирање листе «потребно да зна» за запослене
6. Процес сертификације физичких и правних лица (поверљиве набавке)
7. Успостављање општих и посебних мера заштите тајних података
8. Формирање регистра за рад са тајним подацима (страним тајним подацима)
9. Успостављање система интерних едукације за рад са тајним подацима у органу јавне власти
10. Успостављање ИКТ система за рад са тајним подацима
11. Надзор (стручни) од стране Канцеларије Савета за националну безбедност и заштиту тајних података
12. Инспекцијски надзор Министарства правде

ПРИРУЧНИЦИ И СКРИПТЕ:

1. Основе обраде и заштите података (https://nsa.gov.rs/extfile/sr/4326/Osnove_obrade_i_zast_TP_.pdf)
2. Систем заштите тајних података (https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf)
3. Поступак издавања безбедносног сертификата (https://nsa.gov.rs/extfile/sr/1464/Postupak_izdavanja__BS-skripta.pdf)
4. Унутрашња контрола над радом са тајним подацима (https://nsa.gov.rs/extfile/sr/1761/Unutrasnja_kontrola_nad_radom_sa_tp1 .pdf)
5. Умањивање инсајдерске претње (https://nsa.gov.rs/extfile/sr/1485/Umanjivanje_insajderske_pretnjeskripta_.pdf)

СИСТЕМ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА

Систем заштите тајних података осмишљен је првенствено са циљем да се обезбеди усаглашеност са законским и институционалним захтевима, да се реализује концепт „заштите националне безбедности“ и успостави међународна сарадња, као и високи стандарди квалитета корпоративног управљања и адекватног понашања, те да се осигура стварна одговорност и добри системи заштите тајних података.

СИСТЕМ ЗАШТИТЕ ТАЈНИХ ПОДАТАКА ОБУХВАТА:

1. РЕГИСТАРСКИ СИСТЕМ;
2. ПЕРСОНАЛНУ БЕЗБЕДНОСТ;
3. АДМИНИСТРАТИВНУ БЕЗБЕДНОСТ;
4. ФИЗИЧКУ БЕЗБЕДНОСТ;
5. ИНФОРМАЦИОНУ БЕЗБЕДНОСТ;
6. ИНДУСТРИЈСКУ БЕЗБЕДНОСТ;
7. КОНТРОЛУ И НАДЗОР.

РЕГИСТАРСКИ СИСТЕМ предвиђа руковање тајним подацима само у уређеном систему који мора бити успостављен у складу са прописима и стандардима из области заштите тајних података.

ПЕРСОНАЛНА БЕЗБЕДНОСТ обухвата низ процедура чији је основни циљ да се утврди да ли неко лице може бити овлашћено да добије приступ тајним подацима, а да при томе не представља неприхватљив ризик за националну безбедност.

АДМИНИСТРАТИВНА БЕЗБЕДНОСТ је адекватна и ефикасна класификација и заштита званичних информација које захтевају заштиту у интересу националне безбедности као и њихова декласификација када више не захтевају заштиту.

ФИЗИЧКА БЕЗБЕДНОСТ представља примену физичких и техничких мера заштите ради спречавања неовлашћеног приступа тајним подацима и у суштини представља комбинацију безбедносних процедура и техничких стандарда који се заснивају на препорукама, процени и пракси.

ИНФОРМАЦИОНА БЕЗБЕДНОСТ представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ(ИКТ- информационо комуникационе

технологије) система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица.

ИНДУСТРИЈСКА БЕЗБЕДНОСТ представља примену мера ради обезбеђења заштите тајних података од стране извођача или подизвођача у преговорима који претходе закључивању уговора и током целог века трајања тајних/поверљивих уговора. Извршење поверљивог уговора подразумева све радње предузете након његовог закључења до извршења уговорних обавеза, односно до престанка његовог важења.

КОНТРОЛА И НАДЗОР – подразумева посебне мере надзора над поступањем са тајним подацима у органу јавне власти. Посебне мере надзора обухватају непосредан увид, одговарајуће провере и разматрање поднетих извештаја у вези са спровођењем свих мера заштите тајних података или једне, односно одређених мера заштите тајних података и спроводе се у оквиру унутрашње контроле органа јавне власти.

- **УНУТРАШЊА КОНТРОЛА** – руководилац органа јавне власти а у случају потребе систематизује се посебно радно место или се задужује посебна организациона јединица у саставу органа јавне власти
- **КОНТРОЛА И СТРУЧНИ НАДЗОР** – Канцеларија Савета за националну безбедност и заштиту тајних података
- **КОНТРОЛА И ИНСПЕКЦИЈСКИ НАДЗОР** - Министарство надлежно за послове правосуђа

Обавезе које произилазе из Закона о тајности података - Закон о тајности података који је ступио на снагу 2010. године, унео је у правни систем Републике Србије један нов системски приступ утемељен на безбедносним, правним и техничким стандардима који се примењују у Европској унији, НАТО, Руској Федерацији, САД, Народној Републици Кини, али и земљама у окружењу које су га имплементирале у своје правне системе.

Сам Закон о тајности података је наметнуо одређене обавезе органима јавне власти које се огледају у следећем:

1) примена подзаконске регулативе о одређивању критеријума за степен тајности Интерно (И) и Поверљиво (П), као и Строго поверљиво (СП) и Државна тајна (ДТ);
2) примена подзаконске регулативе која се односи на поједине посебне мере заштите;
3) усаглашавање системских и ресорних прописа са Законом о тајности података који се односе на рад са тајним подацима (информациона безбедност, одбрана, унутрашњи послови, кривично законодавство, управни поступци, правосуђе, локална самопурава, јавна предузећа, канцеларијско пословање и слично);
4) измене закључених међународних споразума који подразумевају размену тајних података и формирање посебних регистара за рад са страним тајним подацима, а за те намене;
5) измене аката о унутрашњој организацији и систематизацији или формацији, увођењем степена тајности коме лице има приступ у обављању својих послова, као и обавезе поседовања одговарајућег сертификата за приступ тајним подацима (безбедносни критеријуми);
6) израда интерних аката о преносу тајних података (курирском службом или дигитално), примени општих и посебних мера и слично (формирање регистарског система, безбедносних зона, устројавање посебних евиденција и слично);
7) одређивању руковаоца тајних података и унутрашње контроле у органу јавне власти и формирање регистарског система за рад са тајним подацима Републике Србије (по потреби и регистара за рад са страним тајним подацима);
8) организовању система перманентне едукације из области заштите тајних података у: Канцеларији Савета за националну безбедност и заштиту тајних података, Националној академији за јавну управу, органима јавне власти и на високошколским установама кроз одговарајуће програме;
9) вођењу посебних службених евиденција у складу са Законом о тајности података (које не спадају у опште канцеларијско пословање); 10)

успостављање непосредне сарадње и комуникације са Канцеларијом Савета за националну безбедност и заштиту тајних података око имплементације прописа о заштити тајних података;

11) доношењем унутрашње регулативе о информатичкој сигурности/безбедности у раду са тајним подацима (акт о информационој безбедности за рад са тајним подацима) и умрежавање са другим органима јавне власти уз одговарајуће технолошке и безбедносне акредитације опреме, система и слично;
12) омогућавању спровођења унутрашње контроле, надзора од стране Канцеларије Савета за националну безбедност и заштиту тајних података, инспекцијског надзора од стране Министарства правде, као и организација и држава са којима постоје међународни споразуми о размени тајних података.

Ко може бити руковалац тајним подацима - руковалац тајним податком (чл. 2. тачка 10. ЗТП) је физичко лице или организациона јединица органа јавне власти, који предузима мере заштите тајних података у складу са одредбама чл. 34. Закона о тајности података Модел Одлуке о одређивању руковаоца и Руковалац тајним подацима – инфолист.

Лице које је овлашћено као руковалац тајним подацима, не може истовремено бити и лице које је овлашћено да обавља и послове унутрашње контроле.
Препорука за одређивање руковаоца тајним подацима:

- У министарствима одређују се секретаријати (евентуално кабинети министра).
- У јединицама локалне самоуправе одређују се организационе јединице које су задужене на пословима планирања одбране (евентуално секретаријати организационих јединица).
- У судовима одређују се секретари судова.
- У тужилаштвима одређују се лица на основу одлуке главног тужиоца.
- У јавним предузећима одређују се организационе јединице које су задужене на пословима планирања одбране.

Одлука о одређивању руковаоца тајним подацима не подразумева истовремено и овлашћење за креирање тајних података.

Руководилац органа јавне власти на основу функције коју обавља има обавезу вршења дужности руковаоца тајним подацима до ступања на снагу Одлуке о одређивању руковаоца тајним подацима.

У органима јавне власти чија организациона структура подразумева мањи број запослних лица руководилац органа јавне власти истовремено обавља и функцију руковаоца тајним подацима.

* Детаљније погледати скрипту Систем заштите тајних података (*https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf*)

ПЛАН ЗАШТИТЕ ТАЈНИХ ПОДАТАКА У ОРГАНУ ЈАВНЕ ВЛАСТИ

План заштите тајних података у органу јавне власти је кључни документ организационе безбедности који дефинише све мере и поступке заштите тајних података које орган поседује или обрађује. Као такав, он је пресудан за очување интегритета информација и националне безбедности. План има за циљ да осигура да се тајни подаци обрађују, чувају, преносе и уништавају у складу са највишим стандардима безбедности. Он је основни стуб организационе безбедности у сваком органу јавне власти. Омогућава правилно управљање тајним подацима и осигурава њихову заштиту, што је од кључног значаја за очување националне безбедности.

Основни елементи плана укључују:

1. **Одређивање одговорних лица:** У плану се дефинишу особе које су одговорне за одређивање тајних података, руковалац тајних података, као и лице одговорно за вршење унутрашње контроле. Такође, ова лица су одговорна и за надзор над поступцима заштите тајних података и примењивање мера у складу са изменама у законодавству и технологији.
2. **Процедуре:** План укључује процедуре за правилно одређивање степена тајности података у складу са законом (интерно, поверљиво, строго поверљиво, државна тајна), као и одређивање начина обраде, чувања и уништавања тајних података, и безбедносне мере које се предузимају при сваком кораку.
3. **Процена ризика за рад са тајним подацима**: У оквиру израде и редовног ажурирања плана заштите тајних података, орган јавне власти мора редовно вршити процену ризика који угрожавају

безбедност тајних података. Процена ризика укључује све потенцијалне претње, као што су напади на информационе системе, злоупотреба приступа или лоша примена мера заштите, као и процену њиховог утицаја на безбедност и интегритет података.

4. **Мере физичке, техничке и организационе заштите:** Описују се методе које се примењују за безбедност простора у којима се чувају тајни подаци, као и заштита ИКТ система који обрађују тајне податке. Ово укључује физичке баријере, као што су ограде и приступне контроле, као и технолошке мере, као што су криптовање података, двострука аутентификација и безбедносни протоколи за комуникацију.
5. **Акредитација ИКТ система:** ИКТ системи који обрађују тајне податке морају бити акредитовани од стране Министарства одбране у вези са технолошким аспектима и крипто опремом. Канцеларија Савета за националну безбедност и заштиту тајних података врши безбедносну акредитацију тих ИКТ система како би се осигурало да су у складу са највишим безбедносним стандардима.
6. **Обука и свест:** План предвиђа обуку свих запослених који имају приступ тајним подацима, како би били упознати са својим обавезама у вези са заштитом тајних података, као и са најновијим претњама и методама одбране. Обука се редовно ажурира како би одражавала нове изазове у области безбедности информација.
7. **Санкције за кршење заштите:** Планирање санкција у случају неовлашћеног приступа или откривања тајних података. Санкције се односе на кршења правила рада са тајним подацима, било да се ради о физичким просторима или ИТ системима.
8. **План поступања у вандредним ситуацијама:** Обухвата процедуре и мере које треба предузети у случају напада, злоупотребе или другиј вандредних ситуација које угрожавају безбедност података.
9. **Праћење стања сертификата:** Обухвата праћење издатих сертификата за физичка и правна лица, укључујући проверу ваљаности сертификата у контексту њиховог приступа тајним подацима.
10. **Рад са правним лицима:** Управа и сарадња са правним лицима код поверљивих набавки, посебно у области индустријске безбедности, који укључују безбедност информација и технологија у производним и сервисним процесима.
11. **Евиденције:** Орган јавне власти мора водити евиденције о одређеним степенима тајности, приступу тајним подацима, обуци запослених, инцидентима везаним за безбедност, ревизијама безбедносних мера и уништавању тајних података.
12. **Ажурирање плана**: Напомена је да се донети план заштите тајних података мора редовно ажурирати у складу са изменама и допунама прописа, технолошких стандарда, научених лекција у раду са тајним подацима и новонасталим претњама и ризицима за рад са тајним подацима.

Обавезе које произилазе из Плана:

1. **Усаглашеност са стандардима безбедности :** Обавеза органа да се усагласи са националним и међународним стандардима у области информационе безбедности, посебно у области безбедности ИТ система који обрађује тајне податке.
2. **Хоризонтална и вертикална координација** : Планирање и примена мера заштите тајних података подразумева сарадњу између различитих нивоа руковођења и сектора унутар органа јавне власти. Хоризонтална координација обухвата размену информација и униформну примену мера безбедности међу различитим секторима, док вертикална координација осигурава јасну подршку и надзор руковођења.
3. **Обавезна обука :** Редовна обука запослених који имају приступ тајним подацима, како би се осигурало да су сви усклађени са најновијим мерама и процедурама. Континуирана комуникација између органа јавне власти и свих учесника у процесу заштите тајних података је од изузетног значаја. Обука свих запослених треба укључивати не само прављење и примену плана, већ и разумевање свих аспеката ризика и координације у оквиру органа јавне власти.
4. **Систем мониторинга и ревизије :** Систем за праћење и ревизију који осигурава да се све мере заштите примењују на адекватан начин. Ревизија и ажурирање плана у складу са новим претњама, технолошким напредцима и променама у законодавству.

План заштите тајних података није директно прописан Законом о тајности података, али се он се сматра имплицитно обавезним као део комплетног система заштите тајних података, који обједињује све мере и процедуре заштите тајних података у органу јавне власти и који мора бити у складу са важећим законима и прописима, како о тајности података, тако и о информационој безбедности и канцеларијским пословањем, као и одговарајућим секторским (ресорним) прописима у складу са надлежнсотима и пословима које обавља орган јавне власти.

НАПОМЕНА : СВЕ МОДЕЛЕ ОБРАЗАЦА, ОДЛУКА И ЕВИДЕНЦИЈА КОЈЕ СУ САСТАВНИ ДЕО ПЛАНА ЗАШТИТЕ ТАЈНИХ ПОДАТАКА МОЖЕТЕ ПРОНАЋИ НА САЈТУ КАНЦЕЛАРИЈЕ САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

https://nsa.gov.rs/tekst/577/obrasci.php

РЕГИСТАРСКИ СИСТЕМ

Руковање тајним подацима је предвиђено само у уређеном систему, који мора бити успостављен у складу са прописима и стандардима из области заштите тајних података. Тако уређен и акредитован систем представља регистарски систем.

Основне функције регистарског система су пријем, евидентирање, руковање, дистрибуција и уништавање тајних података. Наведене функције се успостављају унутар јединственог система регистра, при чему се одржава компартментализација тајних података, или се успоставља систем одвојених подрегистара и приступних тачака.

Регистри, подрегистри и приступне тачке делују као одговорне унутрашње целине органа јавне власти за пријем и отпрему тајних података, вођење евиденција о свим тајним подацима из њихове надлежности, правилно руковање и чување тајних података из њихове надлежности и дистрибуцију тајних података унутар система органа јавне власти.

Сваки орган јавне власти, према потреби, треба да успостави регистар, подрегистар или приступну тачку за класификоване податке. Они се могу успоставити на нивоу министарства, управа, канцеларија, агенција и осталих органа јавне власти. Регистарски систем се може успоставити за тајне податке који су у папирној форми, као и за податке у електронском облику, који су записани на било ком медију.

Успостављање регистарског система има за циљ да осигура потпуну контролу над тајним податком и за његово успостављање неопходно је обезбедити минималне услове:

- адекватан простор који испуњава све захтеве за рестриктивни приступ тајним подацима;
- успостављање функција овлашћених лица и одређивање лица одговорних за руковање и заштиту тајних података – руковаоца тајним подацима и руковаоца регистра тајних података;
- прописивање политике заштите тајних података и процедура за поступање са тајним подацима;
- успостављање система едукација запослених за рад са тјним подацима у регистарском систему;
- организовање система надзора и контроле рада регистарског система;
- извршен стручни надзор од Канцеларије Савета;

Начелна организација регистарског система треба да омогући заштиту тајних података, у складу са минималним условима и стандардима који морају бити

испуњени, у односу на степен тајности који је одређен ради заштите тајног податка у свим магистралама система. Такође, систем треба да омогући неометан приступ тајним подацима, корисницима који су овлашћени да приступе и остваре увид у тајни податак, на основу принципа „ПОТРЕБНО ДА ЗНА“.

Успостављањем основних функција и прописивањем политике заштите тајних података и процедура за поступање са тајним подацим, органи који успостављају регистарски систем треба да регулишу:

- одређивање највишег степена тајности тајних података који настају у раду органа јавне власти, односно које органа јавне власти размењује са осталим органима у држави;
- израду анализе ризика, односно процену угрожености тајних података у органу јавне власти;
- доношење одлука о одређивању посебних административних и безбедносних зона, за рад са тајним подацима, у оквиру зоне размештаја органа јавне власти;
- доношење одлуке о овлашћеним лицима за рад у наведеним зонама;
- прописивање мера обезбеђења административне и безбедносне зоне;
- успостављање и акредитација система физичко-техничке заштите тајних података у регистарском систему, у складу са израђеном анализом ризика и прописаним мерама обезбеђења;
- план заштите тајних података у регистарском систему;
- план заштите тајних података у регистарском систему у ванредним и хитним случајевима, односно случајевима нрушавања безбедности и компромитовања тајних података;
- успостављање система криптозаштите за заштиту тајних података који се размењују електронским путем;
- систем евидентирања поступака и извршених процедура за рад и коришћење регистарског система;
- систем остваривања приступа и увида у тајне податке који се чувају у регистарском систему, за овлашћене кориснике;
- систем контроле и надзора над организационим и успостављеним мерама заштите тајних података;
- програм обуке овлашћених лица и запослених у органу јавне власти за рад у регистрима.

Правилно успостављање регистарског система омогућава смањење ризика од неовлашћеног приступа тајним подацима и компромитовање тајних података,

као и обезбеђивање спречавања и откривања неовлашћених радњи које имају циљ нарушавање безбедности тајних података.

ЕВИДЕНЦИЈЕ ЗА РАД СА ТАЈНИМ ПОДАЦИМА

- Евиденција решења и сертификата степена тајности "ПОВЕРЉИВО", "СТРОГО ПОВЕРЉИВО" и "ДРЖАВНА ТАЈНА", за лица која у органу јавне власти обављају функцију или су запослена, односно за лица која обављају послове, у складу са законом којим се уређује тајност података.
- Листа овлашћених лица за приступ тајним подацима у органу јавне власти
- Евиденција тајних података у органу јавне власти (по степену тајности)
- Евиденција копирања и умножавања тајних података
- Евиденција носача тајних података
- Евиденција остваривања увида у тајне податке
- Евиденција уништених тајних података
- Евиденција печата и помоћних штамбиља
- Евиденција издатих безбедносних пропусница за улазак у безбедносну и административну зону, односно регистар тајних података
- Евиденција кључева за приступ тајним подацима у органу јавне власти
- Евиденција замене шифара за приступ тајним подацима у органу јавне власти
- Евиденција улазака у регистар тајних података
- Евиденција увежбавања поступања у случају нарушавања безбедности тајних података, ванредним и хитним случајевима
- Евиденција нарушавања безбедности или компромитовања тајних података
- Евиденција контроле физичко-техничких мера заштите тајних података
- Евиденција инспекција

* Детаљније погледати скрипту Систем заштите тајних података (*https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf*)

ПЕРСОНАЛНА БЕЗБЕДНОСТ

Мере и активности које се спроводе у домену персоналне безбедности имају веома важну улогу у процесу заштите тајних података.

Оне обухватају низ процедура чији је основни циљ да се утврди да ли неко лице може бити овлашћено да добије приступ тајним подацима, а да при томе не представља неприхватљив ризик за националну безбедност.

Лица чије дужности предвиђају приступ тајним подацима претходно морају бити подвргнута одговарајућој безбедносној провери пре него што им се изда одређени безбедносни сретификат/дозвола који ће важити током одобреног трајања тог приступа.

Поседовање безбедносног сертификата је први корак и нужан услов за приступ тајним подацима. Услови за издавање сертификата утврђују се кроз безбедносну проверу коју врше надлежне службе, на захтев органа јавне власти, а преко Канцеларије Савета за националну безбедност и заштиту тајних података.

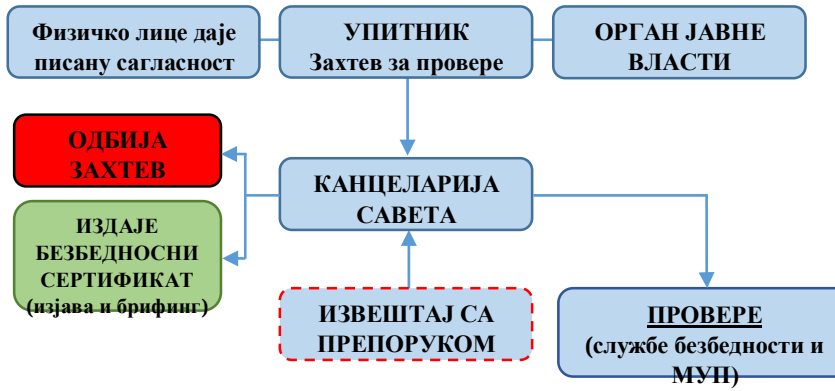
Безбедносном провером врши се процена безбедносног ризика нарочито од приступа и коришћења тајних података. У оквиру безбедносне провере надлежни орган са аспекта безбедности оцењује наводе у попуњеном безбедносном упитнику. Надлежни орган у вези да наводима из безбедносног упитника прикупља личне и друге податке од лица на које се ти подаци односе, од других органа јавне власти, организација и регистара, евиденција, датотека и збирки података које се воде на основу закона.

Безбедносни сертификат је документ који потврђује да лице има право приступа и коришћења тајних података одговарајућег степена тајности, а у складу са принципом „Потребно да зна“.Пре издавања сертификата, односно дозволе, лице коме се издаје сертификат дужно је да потпише изјаву којом потврђује да ће поступати са тајним подацима у складу са законом. Ако лице не потпише изјаву и не преузме сертификат за приступ тајним подацима односно дозволу, поступак издавања се обуставља.

ПОСЕДОВАЊЕ РЕШЕЊА БЕЗ ИЗДАТОГ СЕРТИФИКАТА НЕ ЗНАЧИ МОГУЋНОСТ ПРИСТУПУ ТАЈНОМ ПОДАТКУ. НЕ ПРЕУЗИМАЊЕ СЕРТИФИКАТА ПОДРАЗУМЕВА УГОЖАВАЊЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ РЕПУБЛИКЕ СРБИЈЕ, ШТО УЈЕДНО МОЖЕ ПРЕДСТАВЉАТИ И БЕЗБЕДНОСНУ СМЕТЊУ ПРИЛИКОМ НОВЕ ПРОВЕРЕ.

Подизање безбедносне културе и свести корисника тајних података спроводи се кроз континуирану обуку из области заштите и рада са тајним подацима, која се спроводи на свим нивоима, као и кроз редовне брифинге и дебрифинге о обавезама које произилазе из стицања безбедносног сертификата.

ПРОЦЕС ИЗДАВАЊА СЕРТИФИКАТА



УСЛОВИ ЗА ПРИСТУП ТАЈНОМ ПОДАТКУ

ПОВЕРЉИВО И ВИШЕ

ИНТЕРНО

Безбедносна култура и свест - безбедносна активност која изражава спремност деловања и понашања у складу са стеченим знањима и вештинама, као и у складу са прихваћеним вредносним ставовима. Огледа се у препознавању опасности, реаговању на њих избегавањем опасности, отклањањем опасности или упућивањем на оне субјекте који ће професионално реаговати и сачувати угрожене вредности. Знање и став који

чланови организације имају у погледу заштите одређених вредности – националне безбедности, одбране, унутрашњих и спољних послова, људских слобода и права, као и физичке и интелектуалне имовине, а посебно информација и података којима располаже организација (орган јавне власти, правно лице или комапнија).

Информациона култура и свест - пракса осигурања информација и управљања ризицима везаним за употребу, обраду, складиштење, пренос и архивирање информација. Информациона култура и свест укључује заштиту интегритета, доступности, аутентичности, неповршености и поверљивости корисника. Обухвата и дигиталне заштите и физичке технике. Усвајање адекватног понашања да се пронађу информације, користећи притом било који начин или медијум , који на најбољи могући начин задовољава потребе за информацијама, а које воде мудром и етичком коришћењу информација у друштву (дигитална писменост?).

Информациона безбедносна култура и свест - део у развоју информационе безбедности која се фокусира на прикупљање сазнања и искустава у вези са потенцијалним ризицима и претњама које се брзо развијају, у вези са људским понашањем, како корисника ИКТ система, тако и потенцијалних нападача. 1 ИНФОЛИСТ Манифестије се у оквиру организације кроз аспекте безбедности који се односе на: 1) вредности; 2) понашање; 3) ставове; 4) акције; 5) активности руководства (менџмента); и 6) физичко окружење.

Организациона култура и свест - систем заједничких значења и симбола. • Модел основних претпоставки, вредности и норми, које је дата група развила или открила учећи како да решава проблеме екстерне адаптације и интарне интеграције и који функционишу довољно добро да би били пренети новим члановима организације као исправан начин мишљења и осећања у вези са тим проблемима. • Образац веровања, вредности и научених начина поступања са искуством који су се развили кроз организациону историју и који се манифестују кроз материјалне објекте, као и понашање чланова организације.

Сајбер хигијена - реч је о безбедносној пракси која укључује све кориснике интернета, и са интернетом повезаних ствари, сервиса, апликација, и уређаја са циљем заштите сигурности и интегритета штићених података и спречавања сајбер напада. • Односи се на праксе које имају за циљ спречавање инфекције малициозним софвером (malware), као и сајбер упаде и губљење или корупмирање података и одржавање здравог сајбер окружења.

Међуинституционална сарадња - Канцеларија Савета потписала је више Споразума о сарадњи који обухватају послове унапређења и иновације знања и вештина у обради и заштити тајних података, како података од интереса за Републику Србију, тако и страних тајних података, у циљу стручног усавршавања у државним и другим органима.

Споразуми о међуинституционалној сарадњи потписани су са:

1. Директорат цивилног ваздухопловства Републике Србије, Скадарска 23, 11000 Београд,
2. Министарство финансија - Управа за спречавање прања новца, Ресавска 24, 11167 Београд,
3. Државна ревизорска институција, Макензијева 41, 11111 Београд,
4. Привредна комора Србије, Ресавска 13 - 15, 11000 Београд,
5. Акредитационо тело Србије, Влајковићева 3, 11103, Београд,
6. Универзитет у Београду, Правни факултет, Булевар краља Александра 67, 11120 Београд,
7. Универзитет у Београду, Факултет организационих наука, Јове Илића 154, 11010 Београд,
8. Универзитет у Београду, Факултет безбедности, Господара Вучића 50, 11118 Београд,
9. Криминалистичко-полицијски универзитет, Цара Душана 196, 11080 Београд,
10. БИА - Академија за националну безбедност, Улица краљице Ане бб, 11000 Београд,
11. Министарство спољних послова - Дипломатска академија, Кнеза Милоша 24-26, 11000 Београд,
12. Национална академија за јавну управу Владе Републике Србије, Булевар Михајла Пупина 2, 11000 Нови Београд.

* Детаљније погледати скрипту Систем заштите тајних података
(https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf)

***** Поступак издавања безбедносног сертификата
(https://nsa.gov.rs/extfile/sr/1464/Postupak_izdavanja__BS-skripta.pdf

ФИЗИЧКА БЕЗБЕДНОСТ

Физичка безбедност подразумева примену мера физичке и техничке заштите на појединачним локацијама, у зградама или на отвореним просторима у којима се налазе или чувају тајни подаци који захтевају заштиту од губљења, неовлашћеног приступа, компромитовања или отуђења.

Избор мера које ће се користити за физичку безбедност тајних података зависи од специфичности објекта, броја тајних података, степена тајности. На основу ових параметара ради се општа процена ризика на основу које се примењују мере физичко-техничке заштите. Сврха процене је да се координира и оптимизује коришћење ресурса и надгледају, контролишу и умање претње које могу да угрозе безбедност.

Мере физичког и техничког обезбеђења треба да се заснивају на принципу **„одбрана по дубини“**,Руковање и чување тајних података врши се у **безбедносним и административним зонама**.

Простор или просторије у којима се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА“, „СТРОГО ПОВЕРЉИВО“, и „ПОВЕРЉИВО“ успостављене су као безбедносне зоне првог и/или другог степена.

Простор или просторије у којима се обрађују и чувају тајни подаци степена тајности „ИНТЕРНО“ успостављају се као административне зоне.

Просторије у којима се чувају, користе, обрађују и уништавају тајни подаци обезбеђују се **противпровалним и противпожарним системом**. Једна од мера је и успостављање ефикасне **контроле приступа**.

Простор око просторија у којима се чувају, користе, обрађују или уништавају тајни подаци, као и пут до њих, по правилу, се обезбеђују **видео-надзором**.

Просторије у којима се постављају телефонске централе и друга телекомуникациона опрема за обједињавање целокупног информационотелекомуникационог саобраћаја, као и просторије у којима се постављају централни сервери информационих система, по правилу, су без прозора. Ако просторије имају прозоре, ради предузимања мера одговарајуће техничке заштите, уграђују се **средства за противпровалну заштиту (детектори покрета и лома стакла)**, **сигурносне металне решетке** чији

положај онемогућава отварање прозора, као и **специјална стакла** која онемогућавају поглед у унутрашњост просторије.
Безбедносно техничка опрема, односно одговарајућа средства техничке заштите у којој се чувају тајни подаци су: **противпожарна метална каса са уграђеном бравом** за степен тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО" и/или **канцеларијски или метални ормар** за степен тајности „ИНТЕРНО". Касе или просторије у којој се та каса налази, опремљене су системом јављања и морају испуњавати одговарајуће СРПС/ЕН техничке стандарде.

* Детаљније погледати скрипте Систем заштите тајних података
(https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf)

* Приручник Основе обраде и заштите података
(https://nsa.gov.rs/extfile/sr/4326/Osnove_obrade_i_zast_TP_.pdf)

АДМИНИСТРАТИВНА БЕЗБЕДНОСТ

Административна безбедност представља скуп мера, политика, процедура и пракси које су усмерене на очување безбедности информација, ресурса и операција унутар организације или система. Ова област се односи на управљање ризицима, заштиту података и информација, управљање приступом, обуку запослених и сличне активности које имају за циљ очување поверљивости, интегритета и доступности информација.

Административна безбедност тајних података предузима се у циљу обезбеђивања њихове ефикасне правне и потпуне заштите при руковању истим, као и смањења или отклањања могућих ризика од неовлашћеног приступа и откривања неовлашћеним лицима.

Административна безбедност тајних података успоставља се од тренутка доношења одлуке о одређивању тајности податка и траје до тренутка његовог физичког уништења или скидања ознаке тајности.

Подаци који подлежу означавању степена тајности и који су заштићени једним од законом утврђених степена тајности су из следећих области: заштита територијалног интегритета и суверености Републике Србије, заштита уставног поретка, људских и мањинских права и слобода, национална и јавна безбедност, одбрана, унутрашњи и спољни послови, односно активности

безбедносних и обавештајних служби, економски интереси и међународни положај Републике Србије и сарадња са другим државама и међународним субјектима.

Тајни податак се одређује и означава степеном тајности у зависности од процене озбиљности настанка могуће штете по интересе Републике Србије, у случају његовог откривања неовлашћеном лицу, његове злоупотребе или уништавања.

Тајни податак може да креира само орган јавне власти, односно овлашћено лице у органу јавне власти које има одговарајући безбедносни сертификат за приступ тајним подацима и које према својим дужностима и задацима треба да креира тајне податке, тј. да рукује тим подацима.

Тајним податком не сматра се податак који је означен као тајна ради прикривања кривичног дела, прекорачења овлашћења или злоупотребе службеног положаја или другог незаконитог акта или поступања органа јавне власти.

Лица која рукују тајним подацима (креатори и корисници), у складу са Законом о тајности података, предузимају мере и радње за административну безбедност, кад год постоји потреба за руковањем и чувањем тајних података.

Мере и активности за административну безбедност тајних података предузимају органи јавне власти (државни органи, јавне установе и службе, органи јединица локалне самоуправе) и друга правна и физичка лица, у циљу обезбеђења заштите и законитог поступања са тајним подацима као што су: • правилно утврђивање и означавање степена тајности података;

- пријем и евидентирање у књиге евиденције;
- обезбеђивање правилног чувања и руковања;
- правилна дистрибуција, припрема копија, превода и извода из тајног податка и реализација контроле дистрибуције до крајњих корисника по принципу „ПОТРЕБНО ДА ЗНА“;
- спречавање сваког покушаја неовлашћеног приступа и руковања од стране неовлашћених лица;
- правилан одабир архивске грађе, као и правилно издвајање и уништавање одабране непотребне архивске грађе.

Правилном применом административних безбедносних мера и активности у великој мери се омогућава смањење ризика од неовлашћеног приступа тајним подацима, као и лакше откривање нарушавања безбедности тајних података.

* Детаљније погледати скрипту Систем заштите тајних података

(https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf)

ИНФОРМАЦИОНА БЕЗБЕДНОСТ

Информациона безбедност тајних података обухвата интегрисани скуп међузависних мера и активности усмерених на заштиту тајних података које се обрађују у ИКТ системима (ИКТ- информационо комуникационе технологије). Процесом безбедносне акредитације ИКТ система утврђује се да ли је систем постигао адекватан ниво заштите тајних података.

Безбедносна верификација ИКТ система обезбеђује:

- потврду да ли су планиране мере безбедности ИКТ система правилно спроведене;
- потврду да је одговарајућим тестирањем постигнут захтевани ниво безбедности;
- документовање резултата верификације безбедносне имплементације ИКТ система; Ово потврђује да су испоштовани минимални безбедносни стандарди ИКТ система за обраду, чување и размену тајних података.

Проценом могућег нарушавања безбедности тајних података и безбедности ИКТ система, односно проценом безбедносног ризика, утврђује се вероватноћа да ће одређена рањивост тог система бити искоришћена и довести до нарушавања безбедности система.

Процена безбедносног ризика служи за утврђивање безбедносних ризика, тј. претњи и рањивости ИКТ система, утврђивање њихове величине, како би се идентификовале области у којима је потребна заштита тајних података у ИКТ систему.

Применом мера безбедности ради заштите ИКТ система постижу се следећи ефекти:

- идентификација особа које приступају систему;
- контрола и евиденција приступа на основу датог права приступа из дефинисане базе података;
- обезбеђивање поузданог начина да се укаже на степен тајности;
- идентификација корисника и поуздана евиденција одштампаног, копираног, модификованог или избрисаног тајног податка;

- заштита важних техничких и програмских елемената и функционалност система;
- контрола и управљање руковањем и преносом носача података на којима се чувају тајни подаци;
- планирање, конфигурисање, управљање и контрола мрежних уређаја.

Ове мере заједно чине основу за заштиту ИКТ система од различитих претњи, али је важно континуирано пратити нове трендове и технологије како би се осигурало да су системи увек заштићени од најновијих претњи.

Криптографска заштита ИКТ система у којима се обрађују тајни подаци је део информационе безбедности. Применом криптографских средстава и метода обезбеђује се сигуран и заштићен пренос тајних података у ИКТ системима између две тачке кроз неконтролисани простор. Тиме се значајно повећава безбедност тајних података и смањује могућност њиховог компромитовања и наношења штете.

Криптографске методе и средства примењују се са циљем очувања аутентичности, интегритета и доступности тајних података. Приликом преноса тајних података, сваки ИКТ систем који обрађује тајне податке степена тајности „ПОВЕРЉИВО“ и више треба да буде заштићен од компромитујућег електромагнетног зрачења (КЕМЗ).

Према резултатима мерења спроведених уз помоћ одговарајуће опреме за зонирање објеката и мерења електромагнетног зрачења одређују се безбедносне зоне у објектима у којима се обрађују тајни подаци. У ствари, то значи одређивање просторија према степену заштите од електромагнетног зрачења.

На основу резултата који су добијени мерењима, предузимају се одређене безбедносне мере за смањење електромагнетног зрачења ван контролисаног простора установе, чиме се избегава могућност отицања тајних података путем компромитујућег електромагнетног зрачења опреме.

У области емисионе безбедности, мерења електромагнетног зрачења врше се на опреми која ће се користити за обраду тајних података. На основу добијених резултата утврђује се врста опреме која ће се користити у одговарајућим зонама безбедности. Ова врста безбедносних мера је неопходна, јер се суочавамо са великим ризиком од компромитовања тајних података које емитује ИКТ опрема.

АКРЕДИТАЦИЈА ИКТ СИСТЕМА ЗА РАД СА ТАЈНИМ ПОДАЦИМА У РЕПУБЛИЦИ СРБИЈИ

Акредитација ИКТ система за рад са тајним подацима у Републици Србији, иако постоје одређене нејасноће у прописима, обавља се у складу са Законом о тајности података и Законом о информационој безбедности, као и подзаконским актима донетим на основу ова два закона. Процес акредитације обухвата две врсте:

1. **Безбедносна акредитација** - Ово обухвата физичку и административну заштиту података, као што су контрола приступа, обука запослених и примена мера заштите. Спроводи је Канцеларија Савета за националну безбедност и заштиту тајних података и друге институције, у зависности од врсте система.
2. **Технолошка акредитација** - Фокусира се на техничке аспекте као што су заштита од компромитације електромагнетним зрачењем (КЕМЗ) и примена специфичних безбедносних мера, на основу прописа о одбрани, укључујући ЕУ и NATO стандарде.

У Републици Србији, постоје ИКТ системи који се регулишу посебним прописима у областима безбедности и одбране, унутрашњих и спољних послова.

Кључни кораци у процесу акредитације:

- Процена ризика: идентификација претњи и слабости система.
- Пројектовање и имплементација безбедносних мера: успостављање мера заштите као што су криптографија и контрола приступа.
- Документација и подношење захтева: подношење документације надлежним институцијама.
- Инспекција и верификација: провера усклађености са прописаним стандардима.
- Издавање акредитације: уколико је систем усклађен са технолошким и безбедносним захтевима, који се спроводи кроз стручни надзор Канцеларије Савета за националну безбедност и заштиту тајних података.
- Надзор и ревизија: регуларне провере безбедности и могућност опозива акредитације.

Недостатак прописаних услова, процедура и акредитационих тела

Услови за степене тајности

- Услови за степене тајности „ДРЖАВНА ТАЈНА“, „СТРОГО ПОВЕРЉИВО“ и „ПОВЕРЉИВО“ нису детаљно регулисани важећим прописима.
- Стандард SRPS ISO 27001 је довољан само за најнижи степен тајности „ИНТЕРНО“. Виши нивои тајности захтевају додатну регулативу и усклађеност са специфичним безбедносним захтевима и стандардима.

Недостатак процедура за акредитацију

- У важећим прописима не постоји детаљно уређена процедура акредитације ИКТ система за рад са тајним подацима.
- Прописи пружају само општа начела која укључују процену ризика, примену безбедносних мера и основне кораке у акредитацији.

Недостатак акредитационих тела

- У Републици Србији не постоје одговарајућа акредитациона тела која би се бавила сертификацијом опреме и система за рад са тајним подацима.
- Република Србија је у великој мери ослоњена на увоз и усклађивање са стандардизацијом према страним телима, попут NATO SDIP и ЕУ листе.

КЕМЗ и TEMPEST: Шта је КЕМЗ у односу на TEMPEST?

- КЕМЗ (Компромитација електромагнетним зрачењем) представља шири концепт који обухвата техничке и организационе мере за спречавање цурења података путем електромагнетних емисија.
- TEMPEST је стандардизовани скуп техника и тестова за спречавање компромитације. Док КЕМЗ означава све мере заштите, TEMPEST је конкретно оријентисан ка сертификацији и тестирању уређаја (нпр. NATO SDIP-27).

Зонирање

Зонирање представља систематску поделу просторија у зоне различитих нивоа безбедности у складу са Законом о тајности података, Уредбом о посебним мерама заштите тајних података у информационо-телекомуникационим системима и Уредбом о посебним мерама физичко-техничке заштите тајних података:

- **Зоне високе безбедности** – садрже TEMPEST мере, криптографску опрему и физичке баријере (безбедносне зоне 1. и 2. степена).

- **Контролисане зоне** – просторије са ограниченим приступом и додатним мерама заштите (административне зоне).
- **Опште зоне** – просторије са основним мерама безбедности.

Закључак

Процес акредитације у Републици Србији, иако још увек није уређен у потпуности, је важан за безбедност и усаглашавање са међународним стандардима. Иако се ослањамо на спољне стандарде, развој домаћих капацитета за акредитацију и сертификацију је кључан за будућност и већу безбедност и сигурност тајних података.

У складу са тренутним прописима, процес акредитације укључује како безбедносне аспекте у складу са прописима о тајности података, тако и технолошке аспекте у складу са прописима о информационој безбедности. Међутим, потребно је значајно унапређење у делу прописивања детаљнијих процедура и дефинисања компетенција акредитационих тела која би била у стању да сертификују опрему и системе за рад са тајним подацима. Развој домаћих капацитета за акредитацију и сертификацију ИКТ система кључан је за унапређење безбедности тајних података и смањење зависности од страних регулаторних тела и стандарда.

Процес акредитације, иако формално није предвиђен прописима о раду са тајним подацима и информационој безбедности, у Републици Србији спроводи се кроз стручни надзор Канцеларије Савета за националну безбедност и заштиту тајних података, кроз оцену испуњености услова за рад са тајним подацима.

* Детаљније погледати скрипту Систем заштите тајних података ***(https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf)***

* Приручник Основе обраде и заштите података ***(https://nsa.gov.rs/extfile/sr/4326/Osnove_obrade_i_zast_TP_.pdf)***

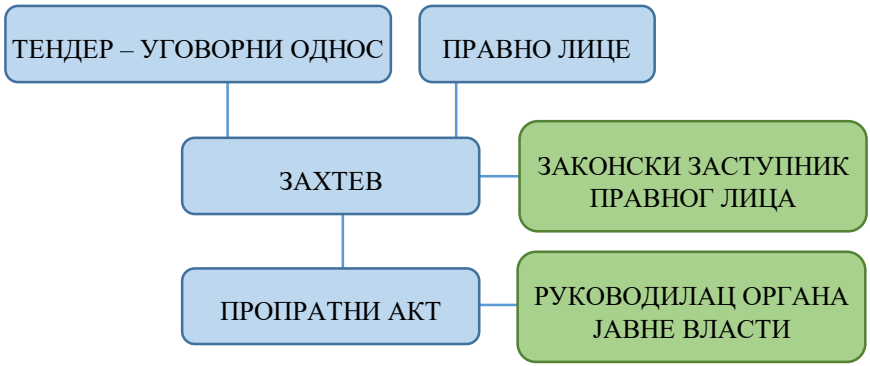
ИНДУСТРИЈСКА БЕЗБЕДНОСТ

Индустријска безбедност представља примену мера ради обезбеђења заштите тајних података од стране извођача или подизвођача у преговорима који претходе закључивању уговора и током целог века трајања тајних/поверљивих уговора. Извршење поверљивог уговора подразумева све радње предузете након његовог закључења до извршења уговорних обавеза, односно до престанка његовог важења.

Мере и активности које треба предузети у раду са тајним подацима из домена индустријске безбедности зависе од степена тајности, процене претње по безбедност тајних података и количине и природе/облика документа у коме је садржан тајни податак. Посебне мере заштите тајних података, прописане одговарајућом уредбом из области индустријске безбедности, односе се на начин и поступак утврђивања испуњености организационих и техничких услова за чување тајних података који су достављени правном или физичком лицу по основу уговорног односа.

Ради заштите тајних података приликом реализације поверљивих уговора, неопходно је да учесници у реализацији уговора претходно обезбеде поседовање одговарајућих безбедносних сертификата за правно лице и за физичка лица. Поседовање решења без издатог сертификата не значи поседовање могућности приступа тајном податку. Неопходне безбедносне сертификате за правна и физичка лица издаје Канцеларија Савета за националну безбедност и заштиту тајних података, по захтеву органа јавне власти, након претходно спроведених безбедносних провера за правна и физичка лица, имајући у виду испуњеност услова за издавање сертификата прописаних чл. 49. Закона о тајности података као и утврђивање одсуства/постојање безбедносног ризика за правно и физичко лице. Сертификовање правних лица омогућава њихов несметан приступ тајним подацима Републике Србије и учешће на расписаним тендерима у државама са којима Република Србија има закључене и ратификоване међународне споразуме о размени и узајамној заштити тајних података.

ПОДНОШЕЊЕ ЗАХТЕВА ЗА СЕРТИФИКАЦИЈУ ПРАВНИХ ЛИЦА



* Детаљније погледати скрипту Систем заштите тајних података *(https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf)*

* Поступак издавања безбедносног сертификата *(https://nsa.gov.rs/extfile/sr/1464/Postupak_izdavanja__BS-skripta.pdf)*

УНУТРАШЊА КОНТРОЛА

Унутрашња контрола осмишљена је са циљем да обезбеди:

- усаглашеност са законским и институционалним захтевима;
- реализацију концепта „заштите националне безбедности“ ;
- постизање високих стандарда квалитета корпоративног управљања;
- адекватно понашање запослених;
- одговорност у раду с тајним подацима; • добре системе заштите тајних података.

Унутрашња контрола представља проверу законитости и правилности поступања унутар органа јавне власти у случајевима када се указује на злоупотребе и прекорачење овлашћења, односно на кршење процедура рада са тајним подацима, а тиме и на угрожавање организационе и националне безбедности.

ЦИЉЕВИ УНУТРАШЊЕ КОНТРОЛЕ

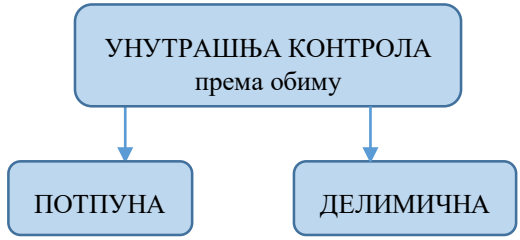
- **ПРАЋЕЊЕ ПОТПУНЕ ИМПЛЕМЕНТАЦИЈЕ ЗАКОНА О ТАЈНОСТИ ПОДАТАКА • ПОУЗДАНО ИЗВЕШТАВАЊЕ РУКОВОДИОЦА ЈАВНЕ ВЛАСТИ**

РАД УНУТРАШЊЕ КОНТРОЛЕ

Унутрашња контрола која се спроводи над радом са тајним подацима не састоји се само у контроли законитости, већ и у контроли целисходности рада, контроли обучености, опремљености и припремљености запослених, руковаоца тајним подацима, поступања са ИКТ системима за рад са тајним подацима, одговорног трошења наменских средстава, благовремености, потпуности и тачности информисања руководства, као и обавеза у области слободног приступа информацијама од јавног значаја.

Унутрашњу контролу у органу јавне власти може обављати и унутрашња организациона јединица у органу јавне власти, која је за те послове одређена актом о унутрашњем уређењу и систематизацији радних места у органу јавне власти, а непосредну контролу може обављати запослени у тој унутрашњој организационој јединици под условом да има одговарајући сертификат за приступ тајним подацима. Канцеларија Савета за националну безбедност и заштиту тајних података врши обуку лица овлашћених за послове унутрашње контроле.

ВРСТЕ УНУТРАШЊЕ КОНТРОЛЕ



Потпуном контролом врши се примена свих прописаних мера за заштиту тајних података, а делимичном контролом једне или више мера.

Најављена унутрашња контрола врши се на основу годишњег плана рада органа јавне власти, а ненајављена на основу одлуке коју доноси руководилац органа јавне власти.

Након извршене унутрашње контроле овлашћено лице сачињава записник и најкасније у року од три дана подноси руководиоцу органа извештај о унутрашњој контроли заједно са записником.

УНУТРАШЊА КОНТРОЛА ЈЕ ВАЖНА ЗБОГ:

- утврђивања усклађености са важећим законима и прописима;
- прописног извршења послова и надлежности органа јавне власти;
- релевантног и поузданог извештавања о раду са тајним подацима у органу јавне власти;
- непристрасних анализа безбедносних инцидената и важећих процедура;
- предлагања мера за унапређење стања безбедности тајних података.

Ко може обављати унутрашњу контролу? – унутрашњу контролу у органу јавне власти може обављати и унутрашња организациона јединица у органу јавне власти, која је за те послове одређена актом о унутрашњем уређењу и систематизацији радних места, а непосредну контролу може обављати запослени у тој унутрашњој организационој јединици под условом да има одговарајући сертификат за приступ тајним подацима.

Сматрамо да у органу јавне власти ако нема успостављен систем унутрашње контроле у смислу члана 84. став 2. (Министарство одбране, Министарство унутрашњих послова, Министарство спољних послова, Безбедносноинформативна агенција и слично) потребно је проширити надлежности интерне ревизије или ФУК-а (Финансијско Управљање Контроле) у сегменту безбедности информација - унутрашње контроле за рад са тајним подацима.

Наравно, да би се успоставила унутрашња контрола потребно је отпочети процес имплементације Закона о тајности података, одредити руковаоца тајних података и донети све потребне одлуке.

Руковалац тајним подацима никако не може бити и унутрашња контрола.

Указујемо да је руководилац органа јавне власти уједно и унутрашња контрола док не успостави систем унутрашње контроле.

Сва лица укључена у процес рада са тајним подацима било да обављају послове руковаоца или унутрашње контроле или да су само корисници тајних података у органу јавне власти морају поседовати одговарајући сертификат и проћи едукације за рад са тајним подацима

* Детаљније погледати скрипту Систем заштите тајних података ***(https://nsa.gov.rs/extfile/sr/1776/Sistem_zastite_tajnih_podataka-skripta).pdf)***

* Приручник унутрашња контрола над радом са тајним подацима (***https://nsa.gov.rs/extfile/sr/1761/Unutrasnja_kontrola_nad_radom_sa_tp1 .pdf)***

СТРУЧНИ НАДЗОР

На основу чл. 86 Закона о тајности података Канцеларија Савета за националну безбедност и заштиту тајних података има у надлежности одређене послове спровођења и контроле примене овог закона и надзор над спровођењем закона.

Стручни надзор се врши на захтев/молбу органа јавне власти који се писаним путем упућује Канцеларији Савета за националну безбедност и заштиту тајних података.

Настао је као резултат потребе органа јавне власти да верификују своје резултате у имплементацији Закона о тајности података.

Он логички и методолошки треба да следи након пуне имплементације Закона о тајности и након извршене унутрашње контроле.

Не представља инспекцијски надзор – инспекцијски надзор је у целини у надлежности Министарства правде.

Стручни надзор Канцеларије Савета има за циљ да утврди да ли је и у којој мери у органу јавне власти имплементиран Закон о тајности података, да ли су у органу јавне власти на адекватан начин примењене опште и посебне мере

заштите тајних података као и да да одговарајуће препоруке за унапређење стања заштите тајних података у органу јавне власти

Приликом вршења стручног надзора цени се функционисање целокупног система заштите тајних података у органу јавне власти са нагласком на:

Статус имплементације закона у органу јавне власти – (подразумева између осталог и доношење Одлуке о одређивању руковаоца, Одлуке о одређивању ТП , Одлуке о одређивању унутрашње контроле и Листе потребно да зна, а на основу годишњег Извештаја), Персонал за руковање подацима,Инфраструктуру за смештај и чување података,Техничке системе за заштиту и обраду података,Регулативу за заштиту података

Након спроведеног надзора, утврђује се чињенично стање и доноси општи закључак о извршеном стручном надзору по сегментима, са којим се упознају лица у органу јавне власти и позивају се да (док траје надзор) дају одговарајуће коментаре уколико их имају. На основу чек листе и коментара саставља се Извештај о извршеном надзору који се доставља органу јавне власти уз позив да се примећени недостаци отклоне.

Напомињемо да орган јавне власти не може самостално утврђивати да ли испуњава законом предвиђене услове за рад са тајним подацима, односно то је тежишни задатак Канцеларије Савета за националну безбедност и заштиту тајних података који се и реализује вршењем стручног надзора и контроле у смислу члана 86 Закона о тајности података.

ПРИМЕРИ ЛОШЕ ПРАКСЕ СИСТЕМА РАДА СА ТАЈНИМ ПОДАЦИМА

1. Приступ тајним подацима без институционалног оквира и организационе безбедности -кривично дело из члана 98. Закона о тајности података

2. Третирање тајних података и докумената као отворених и личних података - кривично дело из члана 98. Закона о тајности података

3. Запослени без сертификата приступају тајним подацима - кривично дело из члана 98. Закона о тајности података

4. Лица без овлашћења старешине органа јавне власти креирају тајне податке - прекршај из члана 99. тачка 11. Закона о тајности података

5. Непостојање процедура имплементације Закона о тајности података - прекршај из члана 99. тачка 11. Закона о тајности података

6. Рад са тајним подацима на информационим системима који су прикључени на интернет- прекршај из члана 99. тачка 11. Закона о тајности података

7. Неуспостављање простора (безбедносних зона) за чување тајних података и ненабављање одговарајуће опреме - прекршај из члана 99. тачка 11. Закона о тајности података

8. Спровођење поверљивих набавки без утврђене процедуре рада са тајним подацима и уступање тајних података правним лицима без одговарајућег сертификата (безбедносне акредитације простора и запослених) - кривично дело из члана 98. Закона о тајности података; прекршај из члана 99. тачка 11. Закона о тајности података

9. Објављивање тајних података у медијима без процедуре скидања ознаке тајности- кривично дело из члана 98. Закона о тајности података

10. Непостојање функционалног руковаоца тајних података и система унутрашње контроле рада са тајним подацима у органу јавне власти - прекршај из члана 99. тачка 16. Закона о тајности података; прекршај из члана 99. тачка 11. Закона о тајности података (везује се за члан 32. став 1. тачка 5. Закона о тајности података)

11. Непрописно означавање тајних података, без одговарајуће одлуке и без критеријума за одређивање тајности – прекршај из члана 99. тачка 3. Закона о тајности података

12. Неуспостављање система едукација у раду са тајним подацима на нивоу органа јавне власти - прекршај из члана 100. Закона о тајности података

13. Несистематизовање радних места која имају приступ тајним подацима у органу јавне власти - прекршај из члана 99. тачка 11. Закона о тајности података

14. Прослеђивање тајних података другим органима јавне власти без одговарајуће процедуре „ПОТРЕБНО ПОДЕЛИТИ СА“ и без курирске доставе
- прекршај из члана 99. тачка 11. Закона о тајности података (везује се за члан 32. став 1. тачка 3. Закона о тајности података)

15. Разговор о тајним подацима са лицима која нису сертификована и изван одговарајуће безбедносне зоне (нпр. у ресторану, на улици, у ходнику или тоалету...) - кривично дело из члана 98. Закона о тајности података

16. Увођење страних држављана у административне или безбедносне зоне без одлуке старешине органа јавне власти - кривично дело из члана 98. Закона о тајности података

17. Уступање тајних података непозваним лицима, без одговарајуће процедуре и одлука – кривично дело из члана 98. Закона о тајности података

18. Уношење мобилних телефона, лаптопова, усб-ова и слично у безбедносне зоне без процедуре и одобрења - прекршај из члана 99. тачка 11. Закона о тајности података

ПРИМЕРИ ЛОШЕ ПРАКСЕ ПОРЕД КРИВИЧНОГ ДЕЛА И ПРЕКРШАЈА ПРЕДСТАВЉАЈУ И УГРОЖАВАЊЕ НАЦИОНАЛНЕ БЕЗБЕДНОСТИ РЕПУБЛИКЕ СРБИЈЕ.

ГОДИШЊИ ИЗВЕШТАЈ О РАДУ СА ТАЈНИМ ПОДАЦИМА У РЕПУБЛИЦИ СРБИЈИ

Годишњи извештај о раду са тајним подацима у Републици Србији неопходно је да садржи следеће:

1. Статус имплементације Закона о тајности података у вашој организацији; видети више - ***https://nsa.gov.rs/extfile/sr/1791/Neophodni_koraci-Implementacija_ZTP_u_organu_JV_.pdf***
2. Број креираних тајних података у органу јавне власти у извештајном периоду, по степенима тајности;
3. Активности вашег органа у складу са чланом 94. став 2. и 3. Закона о тајности података - извештај који садржи бројчане показатеље о размени тајних података са страном државом или међународном организацијом.

Органи јавне власти у свом извештају треба да наведу у којој је фази имплементација Закона о тајности података у њиховом органу, односно који су кораци предузети како би се закон имплементирао. То се првенствено односи на достављање података о уређеним интерним нормативним и безбедносним процедурама (између осталог, донете одлуке о одређивању

руковаоца тајним подацима, одлуке о одређивању степена тајности докумената као и сачињене листе „ПОТРЕБНО ДА ЗНА“), сходно позитивном законодавству којим је уређен рад са тајним подацима у Републици Србији.Такође, потребно је навести да ли је формирана унутрашња организациона јединица за вршење унутрашње контроле у органу јавне власти, те да ли су вршене унутрашње контроле.

Уколико у вашем органу није имплементиран закон, није рађено са тајним подацима односно није вршена размена тајних података, потребно је да то наведете у вашем допису. Такође, уколико сматрате да постоји потреба да се у будућности ради са тајним подацима у вашем органу, потребно је да одредите контакт особу како би вам Канцеларија Савета пружила неопходну стручну помоћ у имплементацији закона и подзаконских аката који регулишу област заштите тајних података у Републици Србији.

Због потребе да се адекватно прати рад са тајним подацима у Републици Србији, у складу са законом, потребно је да сваки орган јавне власти достави број тајних података које је креиран у органу, односно да се искаже број докумената на који је стављена ознака тајности, по степенима тајности. Уколико орган јавне власти није креирао тајне податке, довољно је да се то констатује у извештају.
Имплементација Закона и успостављање јединственог система рада са тајним подацима на националном нивоу, предуслов је за рад са страним тајним подацима.

КО ЈЕ У ОБАВЕЗИ ДА ДОСТАВИ ГОДИШЊИ ИЗВЕШТАЈ

Сходно Закону о тајности података Годишњи извештај о раду са тајним подацима су у обавези да доставе сви органи јавне власти, органи територијалне аутономије, органи јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, као и правно лице које оснива државни орган или се финансира у целини, односно у претежном делу из буџета, а која учествују у изради и реализацији Плана одбране Републике Србије.

„Непоштовање и неимплементација Закона о тајности података представља кршење националне безбедности и наношење штете интересима Републике Србије“

ПОЈМОВНИК О РАДУ СА ТАЈНИМ ПОДАЦИМА

1. **Административна безбедност** је адекватна и ефикасна класификација и заштита званичних информација које захтевају заштиту у интересу националне безбедности као и њихова декласификација када више не захтевају заштиту.
2. **Административна зона** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ИНТЕРНО".
3. **Алармни уређаји** су уређаји који служе за обезбеђивање објекта и предмета, тако што звучним или светлосним сигналом упозоравају на недозвољену активност. Могу бити механички, електрични и електронски.
4. **Аутентичност** је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио.
5. **Безбедносна зона I степена** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО". Самим уласком у ову зону сматра се да је остварен приступ тајним подацима.
6. **Безбедносна зона II степена** је простор или просторија у којој се обрађују и чувају тајни подаци степена тајности „ДРЖАВНА ТАЈНА", „СТРОГО ПОВЕРЉИВО" и „ПОВЕРЉИВО".
7. **Безбедносна култура** је безбедносна активност која изражава спремност деловања и понашања у складу са стеченим знањима и вештинама, као и у складу са прихваћеним вредносним ставовима. Огледа се у препознавању опасности, реаговању на њих избегавањем опасности, отклањањем опасности или упућивањем на оне субјекте који ће професионално реаговати и сачувати угрожене вредности.
8. **Безбедносна провера** је поступак који пре издавања сертификата за приступ тајним подацима спроводи надлежни орган, у циљу прикупљања података о могућим безбедносним ризицима и сметњама у погледу поузданости за приступ тајним подацима.
9. **Безбедносна свест** подразумева знање и став који чланови организације имају у погледу заштите одређених вредности – националне безбедности, одбране, унутрашњих и спољних послова, људских слобода и права, као и физичке и интелектуалне имовине, а посебно информација и података којима располаже организација (орган јавне власти, правно лице или компанија).
10. **Безбедносна сметња** представља чињеницу која онемогућава издавање сертификата.

11. **Безбедносне процедуре** су прописана правила за поступање лица у раду са тајним подацима.
12. **Безбедносни брифинг** представља упознавање са прописима којима се уређује тајност података и последицама неовлашћеног приступа и коришћења тајних података.
13. **Безбедносни инцидент** дешава се када постоји стварни или потенцијални ризик за штићене податке и даље категорисан као кривично дело или прекршај.
14. **Безбедносни ризик** је стварна могућност нарушавања безбедности тајних података.
15. **Безбедносни упитник** је саставни део документације у поступку издавања сертификата за приступ тајним подацима.
16. **Безбедност** означава стање неког субјекта (појединца, групе људи, заједнице, институције) које карактерише одсуство невоља, брига, несрећа, опасности и других зла.
17. **Дебрифинг** подразумева упознавање са прописима и обавезама по престанку потребе за приступом тајним подацима по различитим основама.
18. **Data Breach/Компромитација података** је безбедносни инцидент у коме се осетљиви, заштићени или поверљиви подаци копирају, преносе, гледају, краду или користе од стране појединца који је неовлашћен за приступ тим подацима.
19. **Доставница** је потврда о томе да је лично или посредно достављање извршено која садржи лично име и адресу лица и податке којима се идентификује уручено писмено.
20. **Документ** је сваки носач података (папир, магнетни или оптички медиј, дискета, УСБ меморија, смарт картица, компакт диск, микрофилм, видео и аудио запис и др.), на коме је записан или меморисан тајни податак.
21. **Евиденцију корисника тајних података** је евиденција коју води руковалац тајним подацима у органу јавне власти.
22. **Жалба** је правно средство у управном поступку које се може изјавити против управног акта тј. против првостепеног решења.
23. **Заштита података** је скуп различитих технолошких метода којима се дигитални подаци штите током процеса дигиталног преноса података или дигиталне комуникације.
24. **Изјава** чини саставни део документације на основу које је издат сертификат за приступ тајним подацима, односно дозвола.
25. **Индустријска безбедност** представља примену мера ради обезбеђења заштите тајних података, од стране извођача или подизвођача, у

преговорима који претходе закључивању уговора и током целог века трајања тајних/поверљивих уговора.

26. **Инсајдер** (енг. инсидер - "неко унутра") је назив за особу која је припадник неке друштвене групе због чега располаже одређеним сазнањима недоступним широј јавности.
27. **Информанти** су лица која случајно и пригодно сазнају за планирана или извршена кривична дела и њихове учиниоце.
28. **Информатори** (поузданик, вигилант и агент провокатор) су особе спремне да дуже време полицији пружају криминалистички и кривично правне релевантне информације, при чему се њихов идентитет чува у тајности.
29. **Информациона безбедност** представља скуп мера које омогућавају да подаци којима се рукује путем икт система буду заштићени од неовлашћеног приступа, као и да се заштити интегритет, расположивост, аутентичност и непорецивост тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица.
30. **Информациона безбедност тајних података** обухвата интегрисани скуп међузависних мера и активности усмерених на заштиту тајних информација које се обрађују у информационо комуникационим системима (ИКТ).
31. **Информациона гаранција** представља гаранцију од стране органа јавне власти или правног лица да ће адекватно штитит податке од неовлашћеног приступа, коришћења, дељења или злоупотребе уз поштовање прописа и стандарда за заштиту података
32. **Интегритет** значи очуваност изворног садржаја и комплетности података;
33. **Интерна контрола** представља мере пажње усмерене на спречавање грешака, прекомерних трошкова и преваре, проверава и обезбеђује поузданост информација.
34. **ISO/SEC 27001** је међународни стандард за управљање безбедношћу информација. Детаљно описује захтеве за успостављање, имплементацију, одржавање и континуирано побољшање система управљања безбедношћу информација (ИСМС) – чији је циљ да помогне организацијама да учине безбеднијом информациону имовину коју држе.
35. **Компромитација тајног податка** представља умишљајно, нехатно или немарно откривање тајних података непозваним и неовлашћеним лицима.
36. **Компромитујуће електромагнетно зрачење (КЕМЗ)** представља ненамерне електромагнетне емисије приликом преноса, обраде или

чувања података, чијим пријемом и анализом се може открити садржај тих података.

37. **Контраобавештајна заштита** је посебан вид обавештајне активности чији је циљ заштита тајних података сопствене државе, заштита виталних државних органа и институција, спречавање деловања противничких обавештајних служби на територији своје земље и друго.
38. **Корисник тајног податка** је држављанин Републике Србије или правно лице са седиштем у Републици Србији, коме је издат сертификат од стране надлежног органа, односно страно физичко или правно лице коме је на основу закљученог међународног споразума издата безбедносна дозвола за приступ тајним подацима, као и функционер органа јавне власти који на основу овог закона има право приступа и коришћења тајних података без издавања сертификата.
39. **Кривично дело** је безбедносни инцидент који би разумно могао да доведе или јесте довео до губитка или компромитовање штићених података и захтева истрагу ради даље анализе и покретања кривичног поступка.
40. **Криптографски производ** је софтвер или уређај путем кога се врши криптозаштита.
41. **Криптозаштита** је примена метода, мера и поступака ради трансформисања података у облик који их за одређено време или трајно чини недоступним неовлашћеним лицима.
42. **Листа "ПОТРЕБНО ДА ЗНА"** представља међународни принцип рада са тајним подацима који подразумева списак лица и радних места који имају приступ тајним подацима у оквиру органа јавне власти/ принцип двоструког кључа приступу тајним подацима.
43. **Листа "ПОТРЕБНО ПОДЕЛИТИ СА"** представља међународни принцип рада са тајним подацима који подразумева списак органа јавне власти који међусобно размењују тајне податке.
44. **Лојалност** је значење изведено преко синонима: оданост, верност, исправност, поданичка верност, честитост, часност, привржености, поверљивост, постојаност, непроменљивост, искреност,поштење.
45. **Мере заштите** су опште и посебне мере које се предузимају ради спречавања настанка штете, односно мере које се односе на остваривање административне, информатичко-телекомуникационе, персоналне и физичке безбедности тајних података и страних тајних података.
46. **Мере заштите ИКТ система** су техничке и организационе мере за управљање безбедносним ризицима ИКТ система.
47. **Непорецивост** представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи.

48. **Надлежност** представља право и дужност доношења одлука које се односе на управљање делегираним ресурсима (људским, буџетским, техником и тајним подацима) да би се остварили циљеви националне и организационе безбедности, односно система зштите тајних података.
49. **Обезбеђење** је планска примена и коришћење оперативно-тактичких метода, мера, радњи, средства и снага ради заштите од угрожавања одређених личности, људи, масовних скупова, имовине, отвореногзатвореног простора, фабричких хала, магацина или других објеката.
50. **Обрада података** је генерално, "прикупљање и употреба података ради стварања смислене информације".
51. **Овлашћено лице за одређивање тајности података (произвођач)** подразумева да креатор тајних података може бити свако лице које има одговарајући безбедносни сертификат и које према својим дужностима и задацима треба да креира, тј. рукује тајним подацима - информацијама.
52. **Одлука о одређивању тајних података у органу јавне власти** је одлука којом се одређују се тајни подаци у органу јавне власти, што укључује и утврђивање степена и рока тајности.
53. **Одређивање тајних података** је поступак којим се податак, у складу са овим законом, одређује као тајни и за који се утврђује степен и рок тајности.
54. **Одлука о одређивању руковаоца тајним подацима у органу јавне власти** је одлука којом се одређује се руковалац тајним подацима у органу јавне власти.
55. **Одговорност** када је у питању систем заштите тајних података и организациона безбедност, представља обавезу да се даваоцу овлашћења одговара за испуњавање тих овлашћења (обавеза поступања). Одговорност обухвата и давање информација и образложења за спровођење одређених поступака, активности или одлука, када је у питању рад са тајним подацима.
56. **Означавање степена тајности** је означавање тајног податка ознакама: "ДРЖАВНА ТАЈНА", "СТРОГО ПОВЕРЉИВО", "ПОВЕРЉИВО" или "ИНТЕРНО".
57. **Орган јавне власти** је државни орган, орган територијалне аутономије, орган јединице локалне самоуправе, организација којој је поверено вршење јавних овлашћења, као и правно лице које оснива државни орган или се финансира у целини, односно у претежном делу из буџета, а који поступа са тајним подацима, односно који их ствара, прибавља, чува, користи, размењује или на други начин обрађује.

58. **Организационе мере заштите** представљају организацију заштите процеса рада и функционисања информационо-комуникационог система у редовним околностима и ванредним ситуацијама.
59. **Организациони услови** односе се нарочито на организацију процеса рада, заштиту приступа тајним подацима, заштиту од неовлашћеног коришћења тајних података, одређивање одговорног лица задуженог за спровођење мера заштите, као и утврђивање поступка у случају ванредних и хитних околности.
60. **Патролирање** је услуга обезбеђења коју врше службеници обезбеђења крећући се у одређено време између више међусобно раздвојених места/објеката.
61. **Периметар је део физичке безбедности** који се мора поставити око објеката у којима се налазе штићени подаци, како би се спречило неовлашћен приступ.
62. **Персонална безбедност** представља низ процедура чији је основни циљ да се утврди да ли неко лице може бити овлашћено да добије приступ тајним подацима, а да при томе не представља неприхватљив ризик за безбедност.
63. **Податак од интереса за Републику Србију** је сваки податак или документ којим располаже орган јавне власти, који се односи на територијални интегритет и суверености, заштиту уставног поретка, људских и мањинских права и слобода, националну и јавну безбедност, одбрану, унутрашње послове и спољне послове.
64. **Податак о личности** је сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета.
65. **Правно лице** има регистровано седиште на територији Републике Србије;обављање делатности у вези са интересима из члана 8. овог закона; постојање одговарајуће безбедносне провере; ако није у поступку ликвидације или стечаја; није кажњавано мером забране вршења делатности, односно да му није изречена казна престанка правног лица или мере безбедности забране обављања одређених регистрованих делатности или послова,уредно измирење пореских обавеза и доприноса;
66. **Прекршај** је безбедносни инцидент који не доводи до губитка, компромитовања или сумње да је дошло до безбедносни инцидент.

67. **Процена ризика** је одређивање квантитативних и квалитативних вредности ризика који се односе на конкретну ситуацију и уочене претње.
68. **Регистарски систем** представља уређен систем који мора да буде реализован у складу са прописима и стандардима из области ЗТП.
69. **Решење** представља управни акт надлежног органа којим је решена управна ствар која је била предмет управног поступка.
70. **Ризик информационо-комуникационог система** подразумева могућност нарушавања информационе безбедности, односно могућност нарушавања тајности, интегритета, расположивости, аутентичности или непорецивости података или нарушавања исправног функционисања ИКТ система;
71. **Руковалац тајним податком** је физичко лице или организациона јединица органа јавне власти, који предузима мере заштите тајних података у складу са одредбама овог закона.
72. **Расположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
73. **Саботажа** описује намерне радње којима се наноси штета физичкој или виртуелној инфраструктури организације, укључујући непоштовање процедура одржавања или ИТ, контаминирање чистих простора, физичко оштећење објеката или брисање кода ради спречавања редовних операција.
74. **Сецуриту бреацхес/кршење безбедности** представља неовлашћени приступ информацијама на мрежама, серверима или уређајима, заобилажење сигурности на тим системима, што на крају резултира отицањем или компромитацијом података.
75. **Сајбер безбедност** представља примену технологије, процеса и контроле ради одбране рачунара, сервера, мобилних уређаја, електронских система, мрежа и података од сајбер напада.
76. **Сајбер претња** укључује крађу, шпијунажу, насиље и саботажу свега што је повезано са технологијом, виртуелном стварношћу, рачунарима, уређајима или интернетом.
77. **Сертификат за приступ тајним подацима** је документ који потврђује да лице има право приступа и коришћења тајних података у одговарајућој мери по принципу „потреба да зна“.
78. **Сертификовање привредних субјеката** омогућава њихово учешће на расписаним тендерима у државама са којима Република Србија има закључене и ратификоване међународне споразуме о размени и узајамној заштити тајних података.
79. **Служба безбедности** је служба безбедности у смислу закона којим се уређују основе безбедносно-обавештајног система Републике Србије.

80. **Страни тајни податак** је податак који Републици Србији повери страна држава или међународна организација уз обавезу да га чува као тајни, као и тајни податак који настане у сарадњи Републике Србије са другим државама, међународним организацијама и другим међународним субјектима, у складу са закљученим међународним споразумом који је са страном државом, међународном организацијом или другим међународним субјектом закључила Република Србија;
81. **Тајност** је својство које значи да податак није доступан неовлашћеним лицима.
82. **Тајни податак** је податак од интереса за Републику Србију који је законом, другим прописом или одлуком надлежног органа донесеном у складу са законом, одређен и означен одређеним степеном тајности. 83. **Техничка заштита** је обезбеђење лица и имовине које се врши техничким средствима и уређајима, њиховим планирањем, пројектовањем, уградњом и одржавањем.
84. **Техничке мере заштите** представљају обезбеђење и заштиту података и информација и других елемената информационокомуникационог система, који се остварују применом посебних техничко-технолошких процеса рада и/или спровођењем физичкоманипулативних мера заштите у било којој процедури у оквиру рада ИКТ система.
85. **Уговор** је документ који подразумева посебне мере заштите тајних података које се примењују на све организационе и техничке услове за чување тајних података у поступку закључења уговора између органа јавне власти и правног или физичког лица на основу којег се тајни подаци достављају овим лицима.
86. **Унутрашња контрола** је процес установљен и спровођен од стране руководиоца органа јавне власти, организационе јединице или овлашћеног појединца.
87. **Управни поступак** је поступак доношења управних аката. Под управним поступком подразумевају се процедурална правна правила која се примењују у вези са доношењем одлука у управним стварима.
88. **Физичка безбедност/сигурност** представља примену мера физичке и техничке заштите на појединачним локацијама, зградама или отвореним просторима на којима се налазе или чувају тајни подаци који захтевају заштиту од губљења, неовлашћеног приступа, компромитовања или отуђења.
89. **Физичка заштита** је услуга обезбеђења која се пружа првенствено личним присуством и непосредном активношћу службеника обезбеђења у одређеном простору и времену у складу са планом обезбеђења, применом мера и овлашћења службеника обезбеђења;

90. **Физичко-техничка заштита** је обезбеђење лица и имовине применом физичке заштите и коришћењем средстава техничке заштите.
91. **Тајни податак означен степеном тајности „ДРЖАВНА ТАЈНА“** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала неотклоњива тешка штета по интересе Републике Србије.
92. **Тајни податак означен степеном тајности „СТРОГО ПОВЕРЉИВО“** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала тешка штета по интересе Републике Србије.
93. **Тајни податак означен степеном тајности „ПОВЕРЉИВО“** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала штета по интересе Републике Србије.
94. **Тајни податак означен степеном тајности „ИНТЕРНО“** представља податак чијим би откривањем неовлашћеном лицу, његовом злоупотребом или уништавањем настала штета по рад, односно обављање задатака и послова органа јавне власти.
95. **Технички услови** односе се нарочито на физичко-техничку заштиту простора, односно просторија у којима се чувају тајни подаци, противпожарну заштиту, заштиту тајних података приликом преношења и достављања изван просторија у којој се чувају, транспорт тајних података, обезбеђивање и заштиту информационотелекомуникационим средстава којима се врши преношење и достављање тајних података и спровођење прописаних мера криптозаштите.
96. **Шифра** је пресликавање (трансформација, правило) којим се тајна порука пресликава у неразумљив низ знакова (слова, бројеве...)
97. **Шпијун** је ухода, доушник, достављач, потказивач, вребач, жбир...
98. **Шпијунажа** је прикривена или недозвољена пракса шпијунирања за потребе стране владе, организације, субјекта или особе ради добијања поверљивих информација ради војне, политичке, стратешке или финансијске користи.
99. **Штета** је нарушавање интереса Републике Србије настала као последица неовлашћеног приступа, откривања, уништавања и злоупотребе тајних података или као последица друге радње обраде тајних података и страних тајних података.
100. **Штићени простор** је објекат или простор на којем се врше услуге обезбеђења.

ОБРАСЦИ, МОДЕЛИ ОДЛУКА И ЗАХТЕВА ЗА ИМПЛЕМЕНТАЦИЈУ ЗАКОНА О ТАЈНОСТИ ПОДАТАКА

Модели одлука које су неопходне за имплементацију Закона о тајности података у органу јавне власти

1. Одлука о одређивању тајних података у органу јавне власти
2. Одлука о одређивању руковаоца тајним подацима
3. Одлука о одређивању унутрашње контроле у органу јавне власти
4. Листа „Потребно да зна“
5. Листа „Потребно поделити са“
6. План заштите података за вандредне и хитне случајеве
7. Упутство за рад са тајним подацима

Обрасци и упутство за попуњавање безбедносног упитника

1. Образац безбедносног упитника за физичка лица 2.
Образац безбедносног упитника за правна лица
3. Упутство за попуњавање безбедносног упитника
4. Изјава

Модели захтева за имплементацију Закона о тајности података у органу јавне власти

1. Модел захтева за издавање сертификата за органе јавне власти
1. Захтев за давање мишљења Министарства правде (статус органа јавне власти)
2. Модел захтева за издавање сертификата за правна лица
3. Модел захтева за организацију састанка на тему имплементације Закона о тајности података

Модели одлука

1. Модел одлуке о овлашћеном лицу за одређивање тајности података
2. Модел одлуке о одређивању Административне зоне
3. Модел одлуке о одређивању Безбедносне зоне
4. Модел одлуке о промени степена тајности

5. Модел одлуке о опозиву тајности – периодична процена
6. Модел одлуке о престанку тајности истеком рока
7. Модел извештаја приликом достављања извештаја о раду са тајним подацима
8. Модел Акта о информационој безбедности
9. Евиденције за рад са тајним подацима **Модели образаца**

1. Образац безбедносне напомене приликом достављања тајног податка другој држави или међународној организацији
2. Образац о копији документа
3. Образац о означавању докумената који садржи тајне податке степена тајности ДТ, СП, П и И
4. Образац потврде о пријему тајног податка

Детаљније погледати на сајту

https://nsa.gov.rs/tekst/577/obrasci.php

КАТАЛОГ ПРОПИСА ЗА РАД СА ТАЈНИМ ПОДАЦИМА

- Закон о тајности података
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ДРЖАВНА ТАЈНА” и „СТРОГО ПОВЕРЉИВО” - "Службени гласник РС", број 46 од 24. маја 2013.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у органима јавне власти - "Службени гласник РС", број 79 од 29. јула 2014.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Министарству одбране - "Службени гласник РС", број 66 од 29. јуна 2014.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Министарству унутрашњих послова "Службени гласник РС", број 105 од 29. новембра 2013.
- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Безбедносно-информативној агенцији "Службени гласник РС", број 70 од 7. августа 2013.

- УРЕДБА о ближим критеријумима за одређивање степена тајности „ПОВЕРЉИВО” и „ИНТЕРНО” у Канцеларији Савета за националну безбедност и заштиту тајних података "Службени гласник РС", број 86 од 30. септембра 2013.
- УРЕДБА о посебним мерама заштите тајних података које се односе на утврђивање испуњености организационих и техничких услова по основу уговорног односа "Службени гласник РС", број 63 од 19. јула 2013.
- УРЕДБА о посебним мерама физичко-техничке заштите тајних података "Службени гласник РС", број 97 од 21. децембра 2011.
- УРЕДБА о посебним мерама надзора над поступањем са тајним подацима „Службени гласник РС“, број 90 од 30. новембра 2011.
- УРЕДБА о посебним мерама заштите тајних података у информационотелекомуникационим системима "Службени гласник РС", број 53 од 20. јула 2011.
- УРЕДБА о начину и поступку означавања тајности података, односно докумената "Службени гласник РС", број 8 од 11. фебруара 2011.
- УРЕДБА о садржини, облику и начину вођења евиденција за приступ тајним подацима "Службени гласник РС", број 89 од 29. новембра 2010.
- УРЕДБА о садржини, облику и начину достављања сертификата за приступ тајним подацима „Службени гласник РС“, број 54 од 4. августа 2010.
- УРЕДБА о увећању плате државних службеника и намештеника који обављају послове у вези са заштитом тајних података у Канцеларији Савета за националну безбедност и заштиту тајних података и Министарству правде "Службени гласник РС", број 79 од 29. октобра 2010.
- УРЕДБА о обрасцима безбедносних упитника "Службени гласник РС", број 30 од 07. маја 2010.
- -ПРАВИЛНИК о службеној легитимацији и начину рада лица овлашћених за вршење надзора "Службени гласник РС", бр. 85 од 27. септембра 2013, 71 од 11. јула 2014.

ОСТАЛИ ПРОПИСИ

- Стратегија националне безбедности
- Стратегија одбране
- Закон о основама уређења служби безбедности
- Закон о одбрани и Закон о Војсци
- Закон о полицији

- Закон о спољним пословима
- Закон о Безбедносно-информативној агенцији
- Закон о Војнобезбедносној агенцији и Војнообавештајној агенцији
- Законик о кривичном поступку и Кривични законик
- Закон о организацији и надлежности државних органа у сузбијању организованог криминала, тероризма и корупције
- Закон о државним службеницима
- Закон о информационој безбедности
- Закон о јавним набавкама и Уредба о јавним набавкама у области одбране и безбедности "Службени гласник РС", број 93 од 1. јула 2020.
- Закон о електронским комуникацијама
- Закон о пореском поступку и пореској администрацији
- Закон о заштити узбуњивача
- Закон о приватном обезбеђењу

КАНЦЕЛАРИЈА САВЕТА ЗА НАЦИОНАЛНУ БЕЗБЕДНОСТ

И ЗАШТИТУ ТАЈНИХ ПОДАТАКА

Адреса електронске поште за заказивање онлине консултација:

online.konsultacije@nsa.gov.rs

Адреса електронске поште за заказивање актуелних обука:

obuke@nsa.gov.rs

Адреса електронске поште за заказивање брифинга:

termini.sertifikati@nsa.gov.rs

Web:

www.nsa.gov.rs

О АУТОРУ

Проф. др Горан Матић

Директор Канцеларије Савета за националну безбедност и заштиту тајних података Републике Србије, ванредни професор за област безбедност Универзитета УНИОН – „НИКОЛА ТЕСЛА'' и стални судски вештак за безбедност информација.

Учествовао је у процесу израде предлога више закона, Стратегије за супротстављање и борбу против тероризма, Стратегије националне безбедности и Стратегије одбране и у раду Радних група Владе Републике Србије за имплементацију акционих планова за поглавља 10, 24 и 31 за приступање Републике Србије ЕУ.

Од 2015. до 2019. године руководио је Сталном мешовитом радном групом за борбу против тероризма (СМРГ) – формиране одлуком Бироа за координацију рада служби безбедности, од 2019/2021. године обављао и дужност заменика националног координатора Националног координационог тела (НКТ) за спречавање и борбу против тероризма Републике Србије.

У оквиру међународне сарадње Републике Србије на плану заштите тајности података учествовао је као шеф делегације у преговорима за потписивање 14 међународних споразума и био потписник више споразума које је Р. Србија потписала са међународним телима и страним државама у области заштите тајних података. Такође, са Мисијом ОЕБС-а у Београду учествовао је у више пројеката око заштите тајних података, сајбер безбедности и обраде и заштите личних података у сектору безбедности и одбране.

Од 2012. године учествује у раду Форума директора националних безбедносних органа за заштиту тајних података земаља Југоисточне Европе (СЕЕНСА), као и у оквиру Иницијативе „6С'' која окупља директоре националних безбедносних органа земаља региона.

Аутор је више објављених научних и стручних радова и учесник више научних конференција, као и научне монографије „Политички деликти – атентат и побуна'' и коаутор књиге „Тактика и методика деловања обавештајно-безбедносних служби'' у издању Медија центра Одбрана у Београду, и „Основи безбедности'' у издању Факултета за пословне студије и право у Београд

Предавач је на основним академским студијама Војне академије Универзитета одбране и на Факултету за пословне студије и право Универзитета Никола Тесла Унион у Београду.

Гостујући је предавач на Факултету безбедности и Факултету организационих наука Универзитета у Београду, као и на Криминалистичко-полицијском универзитету, Академији за националну безбедност и на Високим студијама безбедности и одбране при Универзитету одбране у Београду. Поред тога предавач је на кратким струковним студијама на Факултету безбедности: "Заштита тајних података и пословне тајне" и "Заштита личних података" од 2022. године. Био је гостујући предавач на мастер студијама Универзитета у Београду – Тероризам, организовани криминал и безбедност до 2024. године

Акредитовани је предавач Националне академије за јавну управу. Учествује је у раду посебних стручних тела те институције, и то као члан Сталне програмске комисије за електронску управу и дигитализацију (2022-2023) и Сталне програмске комисије за јавну управу (2023-2024).

Члан је Испитне комисије за државни испит (високо образовање) државних службеника и за комуналне милиционере у оквиру министарства државне управе и локалне самоуправе.

Председник је Савета „САМКБ – Српске асоцијације менаџера корпоративне безбедности'' у Београду; члан удружења „ИТ вештак'' у Београду и „Удружења за међународно кривично право'' у Београду. У Привредној комори Србије и Привредној комори Београда више година изводи едукације на тему корпоративне безбедности и обраде и заштите података.